MAKING ANY CHANGE TO YOUR BUSINESS?

Ensuring Business Continuity During Digital Transformation

dcs.tech

Digital Transformation
What does it mean for your business continuity?

Making a change to your business?

Make sure your business continuity solution is still appropriate and will help support you during a period of change.

When making any changes to the way you work, it is vital to understand how your risk profile changes and how it affects your ability to recover your data and continue running the business, in the event of a breach or outage. It is important to protect your business during and after any changes.

For example, moving to cloud environments or utilising shared or public cloud services to run elements of your business can deliver significant performance, cost and resilience benefits. But, it does not remove the risk or responsibility you have around data legislation, compliance and business continuity. The same applies to changes in the way you utilise third-party or in-house solutions, and the way your staff access data, where from, and how.

This guide provides some general information about planning for and accommodating changes to your organisation. It also provides specific information around the critical areas of cloud, cyber threats and workplace location.

CONTENTS

Understanding your risk profile

Public cloud

- Risk considerations for moving to public cloud
- Questions to ask your cloud provider
- How Daisy helps with cloud

Cyber breach

- Business continuity considerations for beating a cyber breach
- Cyber breach invocations
- Cyber breach considerations
- How Daisy helps with a cyber breach

Work area recovery

- In-house solution vs industry work area recovery (WAR)
- Working from home strategy vs industry work area recovery
- Serviced office strategy vs industry work area recovery

Why Daisy for business continuity?

About Daisy

CLICK ON THE TAB YOU'D LIKE TO VISIT

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Understanding your risk profile

There are fundamental questions to answer when accommodating any changes to your business, into your business continuity planning.

- What has changed?
- Will my existing security practices and architectures be as effective after the changes?
- How have the changes altered my business continuity planning?
- What do I need to address to maintain the right level of protection for the business?
- What new risks do I need to plan for as a result of the changes?
- What actions do I need to take?

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Public cloud considerations

While every organisation is different, here are some of the more common elements to consider and facilitate further reflection on decision-making and solutions for risk mitigation:

On-premise risk	Cloud risk
Flood/fire/environmental at your site	Flood/fire/environmental where your data is stored
Data held and accessed via a LAN	Maintaining connectivity to data in the cloud and ensuring its resilience in the cloud Loss of control of the location and sovereignty of your data
Email data stored in Microsoft Exchange	Email data in O365 (still needs to be backed up)
Over-reliance on IT resilience, leading to a lack of planning for recovery from serious incidents requiring data and IT system recovery from backups	Lack of visibility of supplier's level of reliance on IT resilience (and level of recovery arrangements) Careful project planning required in preparation to failback/recover from backups, in the event of a major incident during the migration to the cloud
Not having up to date and tested plans to recover from IT disasters and major business incidents	Not having up-to-date and tested plans to recover from IT disasters and major business incidents
Make sure SLAs are appropriate and applicable in the event of downtime	Public cloud platform SLAs can be difficult to interpret in the event of downtime How will I maintain control of my IT spend when I move to the cloud? Can services be impacted if this gets out of control?
Understanding how to make changes to the service provision and the implications to the business	Understanding how to get your data out of the public cloud and how much it will cost. Egress charges can be difficult to interpret

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Questions to ask your cloud provider

Questions to ask your cloud provider:

What happens to my data if there is an interruption to service?

How long will it take you to recover my data if you suffer damage, loss, corruption or a breach?

Where and how is my data stored?

Where are my data backups held?

Where will my data be restored to?

Do you have an IT resilience or IT service continuity policy (and can you share a desensitised version)?

Do you have an IT recovery plan to restore technical elements of the service provided (and can you share a desensitised version)?

Do you have a business continuity plan setting out how you will recover from a major business incident, e.g. if a data centre has a fire (and can you share a desensitised version)?

Do you test your IT recovery plans and business continuity plan (and can you share a desensitised version of test reports)?

Did you know?

The financial conduct authority (FCA) recommends that regulated businesses do not store their backup in the public cloud with the same provider as their production cloud services.

Did you know?

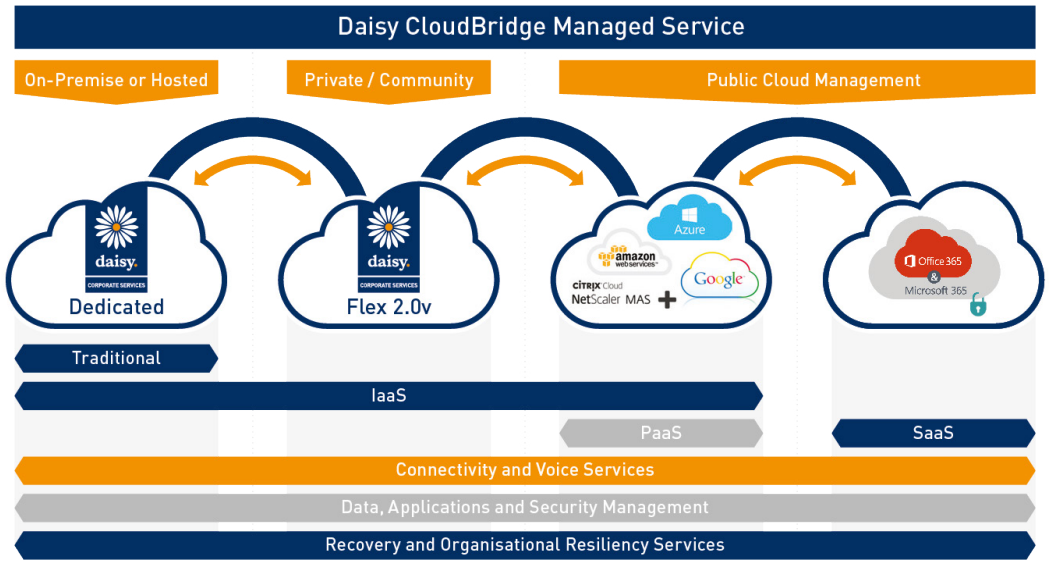
The guidelines for outsourcing cloud services, issued by the European Banking Authority (EBA) recommends a business continuity plan to ensure access to data that is moved to the cloud.

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

How Daisy helps with Cloud

How do Daisy services help?

Daisy has an established solution for getting you into the cloud safely and managing your cloud environment in a way that is cost-effective and compliant. Our CloudBridge solution manages your journey to the cloud and keeps you in control of data sovereignty, compliance and spend. More importantly, Daisy has an established data protection and recovery portfolio that can integrate with CloudBridge to deliver recovery assurance that matches your expectations for all your business data depending on urgency and importance.



Workload placement and management

Hybrid platform deployment

Optimised and resilient

eBackup and Safe Haven integration

Technology-agnostic tiered services

CloudBridge integration

Safe Haven data recovery

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Business Continuity considerations for beating a cyber breach

Preparing to continue business operations in the event of a cyber breach

There are many things that you need to consider in the event of a cyber breach, but there are even more that you need to have already undertaken or planned for, so that you are ready to act effectively to minimise the disruption when a breach occurs. Here are seven questions to help you evaluate your readiness to continue business operations following a cyber breach. To get into the best possible shape to minimise disruption, we recommend having each of these steps in place and reviewing them whenever any changes are made to your business environment.

1. A separate and protected network

In the event of a cyber breach, does your business have a second network to fall back to, which is safe, secure and unaffected from the cyber breach, which you can use to resume IT services?

2. A separate and protected recovery environment

Does your fall-back secure data network:

- Have an IT recovery environment which is ready to use to recover IT services within the safe environment?
- Have workspace (desks, computers and telephones) ready to use to get staff working within the safe environment?

Remember that working from home or at another office location won't be an option if staff are connecting to the breached network or one that you do not know is clean.

3. Effective data backup generations

Do your data backups stretch back far enough to recover from a cyber breach that has been sitting on your system for some time, corrupting data unnoticed?

4. A comprehensive technical recovery plan

Do you have technical recovery plans setting out the detailed recovery of IT services (including screenshots and commands)? Time may be lost and mistakes made during a serious IT failure without these.

5. A management-level IT recovery plan

Do you have a management-level IT recovery plan to help plan the recovery of IT services in the event of multiple IT failures, including cyber breach? At a time when all eyes in the business will be on you, it's important to be able to respond effectively.

6. A business recovery plan

Do you have a robust and tested business recovery plan that has identified all the critical areas of your business and how quickly they need to be recovered?

7. A business resilience steering group

Do you have a business resilience steering group within your organisation to coordinate and manage your overall approach to threats, which incorporates the functions of business continuity, information security, and IT continuity?

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Cyber breach invocation examples 1

Our snapshot of recent cyber breach invocations shows the variety and longevity of recovery scenarios and points to a growing trend in cyber-related disruption. It also shows the length of time it takes an organisation to recover following a breach:

SAFE HAVEN INVOCATION

- **SECTOR:** FINANCIAL
- **SIZE:** ENTERPRISE, GLOBAL
- **TYPE OF BREACH:** RANSOMWARE
- **EXTENT OF DISRUPTION:** 50 SERVERS, 30 PEOPLE
- **DURATION OF RECOVERY:** 3 WEEKS
- **RECOVERY TYPE:** PHYSICAL SERVER RECOVERY AND REPLICATION TO THE CLOUD, WORK AREA RECOVERY FOR STAFF
- **OUTCOME:** ACHIEVED BUSINESS CONTINUITY WITH DAISY

SAFE HAVEN INVOCATION

- **SECTOR:** CONSTRUCTION
- **SIZE:** ENTERPRISE
- **TYPE OF BREACH:** RANSOMWARE
- **EXTENT OF DISRUPTION:** 15 SERVERS, TAPE DRIVES & STORAGE
- **DURATION OF RECOVERY:** 48 HOURS
- **RECOVERY TYPE:** PHYSICAL SERVER RECOVERY SHIPPED TO SITE WITH ON-SITE TECHNICAL SUPPORT
- **OUTCOME:** ACHIEVED BUSINESS CONTINUITY WITH DAISY

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Cyber breach invocation examples 2

SAFE HAVEN INVOCATION

- **SECTOR:** PUBLISHING
- **SIZE:** MID-MARKET
- **TYPE OF BREACH:** DDoS
- **EXTENT OF DISRUPTION:** COMPANY-WIDE NETWORK DISRUPTION
- **DURATION OF RECOVERY:** 6 DAYS
- **RECOVERY TYPE:** CLEAN, SEPARATED WIFI "IN A BOX" SOLUTION
- **OUTCOME:** ACHIEVED BUSINESS CONTINUITY WITH DAISY

SAFE HAVEN INVOCATION

- **SECTOR:** FINANCIAL
- **SIZE:** ENTERPRISE, GLOBAL
- **TYPE OF BREACH:** VIRUS
- **EXTENT OF DISRUPTION:** UK BUSINESS
- **DURATION OF RECOVERY:** 3 WEEKS
- **RECOVERY TYPE:** WORK AREA RECOVERY FOR 60 CRITICAL STAFF AND TECHNOLOGY ENVIRONMENT
- **OUTCOME:** ACHIEVED BUSINESS CONTINUITY WITH DAISY

SAFE HAVEN INVOCATION

- **SECTOR:** MANUFACTURING
- **SIZE:** MID-MARKET, GLOBAL
- **TYPE OF BREACH:** RANSOMWARE
- **EXTENT OF DISRUPTION:** BUSINESS-CRITICAL SERVER
- **DURATION OF RECOVERY:** 11 DAYS
- **RECOVERY TYPE:** PHYSICAL SERVER SHIPPED TO SITE WITH ON-SITE TECHNICAL SUPPORT
- **OUTCOME:** ACHIEVED BUSINESS CONTINUITY WITH DAISY

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Cyber breach considerations

Did you know?

88% of UK businesses reported breached in the **last 12 months**

...of those **more than 1/4** have been breached **5 or more times**

89% reported that the threats they are experiencing are growing in complexity

93% of UK organisations plan to increase cyberdefence spending

BUT what about the budget to continue the business effectively when breaches occur?

Business Continuity Invocations: What's the Cyber Difference?

Invocations due to a cyber breach are becoming more prevalent and on top of this, they have a longer-lasting impact compared to invocations for other common reasons, such as power, utilities, hardware or communications failure.

High profile - a cyber breach tends to be more damaging to an organisation's reputation (tip - this can be well-managed with a planned communications strategy as part of your business continuity planning)

Residual problems - a cyber breach tends to "drag on" with customers battling non-critical issues, long after the business is back up and running (customers often need to keep recovery systems on site for longer than six months after discovering a breach)

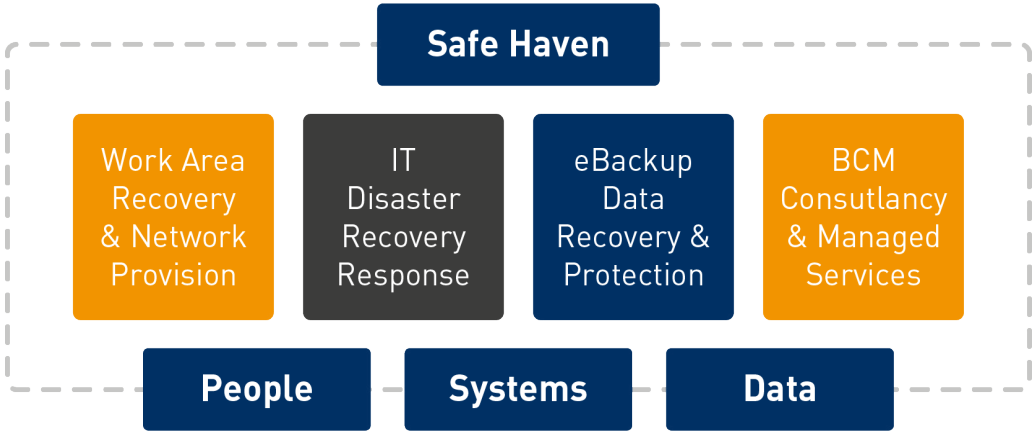
WARNING!
If you or your public cloud provider has a cyber incident, do you have the ability to create a clean environment to continue business operations?

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

How Daisy helps with a cyber breach

Daisy's Safe Haven service:

- Provides an uninfected environment for users to work from, clean network, devices and systems and data rollback to pre-infection, tested independently
- Changes the attack vector, keeping you safe from a repeat attack
- Enables you to continue your core business activities even while you have an active breach in your live working environment
- Identifies and recovers your clean data from the most recent uninfected point in time



Have you thought about..?

Security – We can help to improve your security posture with our mature and comprehensive portfolio of Security services for discovery, prevention and response across your cloud, network and users.

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

In-house solution vs industry work area recovery (WAR)

In-house solution	Daisy WAR facility
No dedicated on-site support, IT staff would be split between sites	Our services come with a support community of experienced recovery engineers
May not meet customer/market expectations	Meets customer/market expectations - we deliver a credible solution that will satisfy any scrutiny or audit
Is there a recovery system available to log into?	Recovery system set up and separate from any infected or non-operational environment
No regular testing programme or capability inherent in the solution	Regular testing available as part of the contract
Is connectivity back to the live or recovery site available?	Connectivity to the live or recovery site is available
Is there a remote desktop service to allow remote workers to connect to the live or recovery site?	Remote desktop available to allow remote workers to connect to the same network as the work area and recovery or live environment
Substantial investment in additional infrastructure (generator, air conditioning, access controls, fire detection, reception, meeting rooms, security etc.) Regular injections of capital are required to refresh technology as it becomes out of date	Pay only a part of this cost even if the resources provided are dedicated rather than syndicated Services are provided on an annual subscription basis avoiding the need for capital investment Services are provided on short-term contracts where an in-house solution may necessitate a longer-term lease The technology is refreshed on a regular basis with no cost to the customer
Your 'ring-fenced' set of resources are liable to production creep for short-term production solutions, which compromise the ability to recover should a disaster occur. It is not uncommon for in-house solutions to fail because components have been 'borrowed' for production purposes and never returned	Secure, dedicated facilities used solely for business continuity customer requirements
In-house solutions are inflexible and usually very costly to change in line with business changes	Our flexible solutions are designed to meet the needs of dynamically changing businesses whether they are of a geographical or technical nature
In-house solutions are limited and usually very costly to expand in line with business growth	Our UK-wide infrastructure and industry relationships enable us to deliver growth paths that are both timely and cost-effective

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Working from home strategy vs industry work area recovery

Working from home	Daisy WAR facility
Inconsistent or unknown access to technology Capital outlay for laptops/mobile devices	Expected technology provided
No dedicated on-site support	Experienced recovery engineers assigned to support
You will not be able to link your communications into the building	You can link into our secure sites (MPLS, point to point etc.)
Loss of security controls and compliance	Security and compliance maintained
Less collaborative working	Maintain usual collaborative working
May not meet customer/market expectations	Meets customer/market expectations - we deliver a credible solution that will satisfy any audit or scrutiny
Is there a recovery system available to log into?	Recovery system set up and separate from any infected or non-operational environment
Difficult to test scenarios	Can regularly test scenarios
Unable to use business telephony DDIs or hunt groups	Full telephony functionality including hunt groups, call trees, DDIs, voice recording, call statistic displays etc.
Is connectivity back to the live or recovery site available?	Connectivity to the live or recovery site is available
Is there a remote desktop service to allow remote workers to connect to the live or recovery site?	Remote desktop available to allow remote workers to connect to the same network as the work area and recovery or live environment

Please **click here** for more useful information in our practical guide: Working from home or work area recovery?

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Serviced office strategy vs industry work area recovery

Serviced offices	Daisy WAR facility
No technology provided	Expected technology provided
No dedicated on-site support	Experienced recovery engineers assigned to support
Choice of locations available but availability not guaranteed, the location to be used is likely to be unknown at the time of need	Availability is assured (dedicated) or first-come, first-served (syndicated) with known secondary and tertiary options available to roll back to
Loss of security controls and compliance	Security and compliance maintained
May not be physically secure rooms once through main reception	Physically secure areas for your access only
You will not be able to link your communications into the building	You can link into our secure sites (MPLS, point to point etc.)
May not meet customer/market expectations	Meets customer/market expectations - we deliver a credible solution that will satisfy any audit or scrutiny
Is there a recovery system available to log into?	Recovery system set up and separate from any infected or non-operational environment
Do they have a BCM strategy for the continuance of services?	ISO 22301 certification (certificate number BCMS 563370)
Difficult to test scenarios	Can regularly test scenarios
Subscription rates of office locations unknown (difficult to evaluate risks)	Exact number of subscribed customers known so risks can be assessed (Our Voluntary Supplier Risk Declaration)
Do they offer full telephony functionality?	Full telephony functionality, including hunt groups, call trees, DDIs, voice recording, call statistic displays etc.
Is secure, dedicated Internet connectivity available?	Secure and dedicated Internet connectivity available
Is connectivity back to the live or recovery site available?	Connectivity to the live or recovery site available
Is there a remote desktop service to allow remote workers to connect to the same work area?	Remote desktop available to allow remote workers to connect to the same network as the work area and recovery environment

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

Why Daisy for business continuity?

- The largest UK provider of continuity, resilience and availability services
- More than 30 years' experience delivering continuity, resilience and availability services
- Recovering more than 240 customer instances on average, year on year
- Multiple service and innovation awards from recognised business continuity bodies throughout this time
- More than 100 UK business continuity, resilience and availability engineers and support staff
- Protecting more than 6PB of customer data and more than 100,000 backups every month

bsi. ISO 22301 Business Continuity Management
BCMS 563370

bci Founding Partner

Have you thought about..?

FlexConsult – Our flexible Business Continuity Management (BCM) consulting services can deliver business impact analyses and risk assessments that help you through any business changes. For example, moving to the cloud and mitigating disruption from a cyber breach or any other business interruption.

Shadow-Planner – Our multi award-winning business continuity management planning software can make your BCM planning run smoothly and in the event of an incident, puts the right information into the right hands at the right time.

Understanding your risk profile
Risk considerations for moving to public cloud
Questions to ask your cloud provider
How Daisy helps with cloud
Business Continuity considerations for beating a cyber breach
Cyber breach invocation examples 1 2
Cyber breach considerations
How Daisy helps with a cyber breach
In-house solution vs industry work area recovery (WAR)
Working from home strategy vs industry work area recovery
Serviced office strategy vs industry work area recovery
Why Daisy for business continuity?
About Daisy

About Daisy: your best partner for digital transformation

Daisy Corporate Services is the leading UK organisation for business continuity, resilience and availability services. We are also the UK's #1 independent provider of secure IT, communications and cloud. With a thousand employees across 30 UK locations, we provide these solutions to more than 2,000 UK organisations:

Mobile	LAN & WiFi
Unified Communcations	Cloud & Hosting
Lines & Calls	Business Continuity
Security	Workplace Computing
Connectivity	Servers, Storage & Virtualisation

Our portfolio is underpinned by a strong managed services heritage, professional services and supply chain services. This breadth of expertise and depth of experience enables us to create intelligent IT and communications solutions to help our customers in all industries to be more productive and successful, and we play an integral role in keeping the UK's commercial and public sectors operational.

With long-standing relationships with the biggest industry-leading vendors, we are committed to providing the highest levels of service possible for our customers.

To find out more about addressing your current and future continuity and resilience challenges, speak to one of our sales specialists today:

T 0344 863 3000

dcs.tech