DSB Business Continuity

Frequently Asked Questions

Author: Derivatives Service Bureau
Date: 08/09/2020
Version: **1.0**

Contents

Preface 3

Change History 3

1 Introduction 4

1.1 Document Purpose 4

1.2 Background 4

1.3 Alternate FAQs 4

2 Frequently Asked Questions 4

2.1 Does the DSB have a BC plan, can we see it?? 4

2.2 Can you tell us what topics are in your BC plan? 4

2.3 Which continuity scenarios have been considered and planned for? 5

2.4 Do you perform a Business Impact Analysis/ Risk assessment? Can we see it? How often is it reviewed? 5

2.5 Is there a designated individual or group responsible to stakeholders for business continuity? 5

2.6 Is there formal BCP training for all staff? How often is this performed?? 5

2.7 Do you involve third parties or subcontractors in your continuity tests?? 5

2.8 Has a business continuity / disaster recovery plan been completed and tested, and what is the frequency of recurring tests going to be?? 6

2.9 Did your SOC1 audit specifically cover Business Continuity? 6

2.10 How often do you perform tests of these Plans? What evidence do you collect to confirm testing results in improvements? 6

2.11 Are the results of your testing activities available for us to review? 6

2.12 Have you made arrangement for alternate location or remote working practices? What proportion of you staff can utilise this concurrently?? 6

2.13 Are all DSB datacentres located at a suitable physical distance apart and do not operate with shared physical dependencies 7

2.14 Do you utilise redundant data stores, systems and datacentres?? 7

2.15 Are your recovery services dedicated solely to your use or only on a first come – first served basis? 7

2.16 Do you have a publicly Recovery Time Objective and Recovery Point Objective for your service? 7

2.17 Are your internal continuity documentation sets available to staff 24x7x365? 7

2.18 In case of critical cyber-attack do you have plans to enable you to report to the relevant Data Protection authorities. 7

2.19 Can you sustain your continuity objectives for 6 weeks or longer? 7

Preface

Change History

Date	Change	Version	Author	Revision Details
08/09/2020	Creation	1.0	Will Braithwaite	First release.

1 Introduction

1.1 Document Purpose

The purpose of this document is to detail the frequently asked questions posed by the industry related to Business Continuity (BC), and the corresponding answers provided by the DSB. It is intended to enhance the already published DSB Disaster Recovery and Business Continuity Policy.

https://www.anna-dsb.com/download/dsb-business-continuity-policy_v4_2021_final/

1.2 Background

The DSB provides a Disaster Recovery and Business Continuity Policy on its website to provide useful information to its clients. However, this document is maintained on an annual basis and in the interim the DSB continues to receive further questions around business continuity. The DSB Business Continuity FAQ document aims to answer those questions and will be a "living" document, updated as the DSB receive more requests for information. This document is located on the DSB website, accessible to all stakeholders -

https://www.anna-dsb.com/download/dsb-business-continuity-faq/

1.3 Alternate FAQs

The DSB provides additional Information Security information by way of an equivalent FAQ, which is located on the DSB website here:

https://www.anna-dsb.com/download/dsb-information-security-faq/

2 Frequently Asked Questions

2.1 Does the DSB have a BC plan, can we see it??

The full DSB BC plan is not publicly available at this time. However, the DSB has issued notifications to industry regarding testing and invocation of its strategy (https://www.anna-dsb.com/coronavirus-covid-19/). The DSB expects to consult with the Technology Advisory Committee (TAC) to determine what materials should be made publicly available in future.

2.2 Can you tell us what topics are in your BC plan?

The DSB BC plan contains the following topics:

- Crises management protocol/incident response
- Staff relocation planning
- Recovery team definitions
- Third party dependencies
- Client notification procedures
- Staff communications

2.3 Which continuity scenarios have been considered and planned for?

The DSB BC plans and procedures consider a wide range of scenarios, including but not limited to:

- Natural Disasters
- Pandemic flu
- Cyber Attack
- Critical Service provider failure
- Building Disruptions

The scenarios are reviewed at least annually to ensure they are applicable to the operations of the DSB.

2.4 Do you perform a Business Impact Analysis/ Risk assessment? Can we see it? How often is it reviewed?

The DSB annually performs an internal Business Impact Assessment to determine operational capabilities, mapping internal functional dependencies and risk categories. This document is not publicly released however, identified risk is tracked at DSB Board level.

2.5 Is there a designated individual or group responsible to stakeholders for business continuity?

The DSB has Continuity Stakeholders across the organisation who constitute the Response Team. Action plans for the Response Team are reviewed at least annually in conjunction with the entire team.

2.6 Is there formal BCP training for all staff? How often is this performed??

The DSB approach is for training activities to be conducted under the responsibility of the relevant Primary Response Team member. Every DSB staffer has a designated Primary and Secondary Response Team stakeholder and updates to training and material occurs at least annually.

2.7 Do you involve third parties or subcontractors in your continuity tests??

The DSB considers the services provided by its Third Parties as part of its Business Impact Assessment and engages with account / vendor managers to facilitate internal Continuity testing.

2.8 Has a business continuity / disaster recovery plan been completed and tested, and what is the frequency of recurring tests going to be??

The DSB DR infrastructure is built and running in its secondary region. The DSB periodically runs a range of internal tests to validate this environment. In addition, the DSB is currently running a program (in conjunction with the TAC) to facilitate a public Industry DR test in a non-production environment for users to validate their own Disaster Recovery plans. More information is available here.

2.9 Did your SOC1 audit specifically cover Business Continuity?

The DSB has undergone the International Standard on Assurance Engagements 3000 (revised) and 3402 ("ISAE 3000 and 3402") and the Institute of Chartered Accountants in England and Wales Technical Release AAF 01/06 ("AAF 01/06") Type I audit, dated 31 December 2019. The audit covered specific Organisation Controls, some of which fall under the umbrella of Business Continuity. Typically, Third Party Assurance (TPA) audits are unsuited to assessing Business Continuity in its entirety however, the DSB continues to add appropriate controls as part of its ongoing SOC I&II assessments for client transparency. To obtain a copy of the audit report please email client-admin@ANNA-DSB.com .

2.10 How often do you perform tests of these Plans? What evidence do you collect to confirm testing results in improvements?

DSB policy is to ensure a period of no longer than 12 months between testing activities. The DSB collates all testing results to produce a Continuity Report which identifies a delta against previous testing. These Reports will be reviewed by the DSB board.

2.11 Are the results of your testing activities available for us to review?

Currently they are not but a summarised set of results may be made available in future, subject to guidance from the DSB TAC.

2.12 Have you made arrangement for alternate location or remote working practices? What proportion of you staff can utilise this concurrently??

The DSB makes full use of remote working practices and has successfully worked 100% using this methodology.

2.13 Are all DSB datacentres located at a suitable physical distance apart and do not operate with shared physical dependencies

The DSB operates across two continents utilising AWS datacentres in Europe (Ireland) and in the US (North Virginia). Additional detail regarding the DSB architecture can be found in the DSB Disaster Recovery and Business Continuity Policy.

2.14 Do you utilise redundant data stores, systems and datacentres??

By design, the DSB ensures single point of failure is ruled out of all elements of its technology stack. For more information please see the DSB Disaster Recovery and Business Continuity Policy.

2.15 Are your recovery services dedicated solely to your use or only on a first come – first served basis?

At a technology level, the DSB's public Cloud infrastructure is reserved solely (warm standby) for its use with its supplier AWS.

2.16 Do you have a publicly Recovery Time Objective and Recovery Point Objective for your service?

Please see the DSB Disaster Recovery and Business Continuity Policy for current specific RTO and RPO.

2.17 Are your internal continuity documentation sets available to staff 24x7x365?

The DSB provides its internal documentation on two separated and independent documentation systems to ensure continuous availability.

2.18 In case of critical cyber-attack do you have plans to enable you to report to the relevant Data Protection authorities.

The DSB has plans in place to engage directly with the European and UK Data Protection agency's as a minimum.

2.19 Can you sustain your continuity objectives for 6 weeks or longer?

Yes. The DSB has announced BCP invocation activities to industry previously (here) and has effectively run in this mode for over 5 months.