DSB Information Security

Frequently Asked Questions

Author: Derivatives Service Bureau
Date: 25th February 2022
Version: **2.1**

Contents

Preface

Change History

Date	Change	Version	Author	Revision Details
21 Sept 2017	Creation	1.0	Inder Rana	
14 Oct 2017	Addition	1.1	Inder Rana	Additional questions added
9th Feb 2018	Addition	1.1	Inder Rana	Additional questions added
4th May 2018	Addition	1.3	Will Braithwaite	Additional questions added
8th May 2019	Addition	1.4	Will Braithwaite	Additional questions added
16th March 2020	Addition	1.5	Will Braithwaite	Additional question added
20th August 2020	Major Re-write	1.6	Will Braithwaite	Historic entries updated, content amended.
16th December 2020	Addition	1.6.2	Will Braithwaite	Additional question added
11th February 2021	Addition	1.7	Will Braithwaite	Additional question added
6th July 2021	Addition	1.8	Kurt Aquino	Additional question added
17th December 2021	Addition	1.9	Kurt Aquino	Additional question added
20th December 2021	Content Amendment	1.9.1	Kurt Aquino	Section 2.32 updated
19th January 2022	Addition	2.0	Kurt Aquino	Additional question added
25th February 2022	Addition	2.1	Marc Tabujara	Additional question added

1 Introduction

1.1 Document Purpose

The purpose of this document is to detail the frequently asked questions posed by the industry, related to information security matters, and the corresponding answers provided by the DSB. It is intended to enhance the already published DSB Security policy.

https://www.anna-dsb.com/download/dsb-security-policy-2020/

1.2 Background

The DSB provides a Security 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 Information Security . The DSB InfoSec 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-information-security-faq/

1.3 Alternate FAQs

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

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

2 Frequently Asked Questions

2.1 Will/Does the Vendor utilise any Subcontractor(s) to provide the product(s) or service(s)?

There are two sub-contractors contracted to the Derivative Service Bureau. These being;

Contractor Name	Address	Service Provided
etradingsoftware Ltd	Cannon Place, 78 Cannon Street, London, EC4N 6HL, United Kingdom	The Management Services Partner (MSP) to the DSB. Reporting to the DBS Board and liaising with the SPP for infrastructure operations functions.
Rackspace Technology	8 Millington Road, Hyde Park Hayes, Middlesex UB3 4AZ	The Service Provision Partner (SPP) provides Infrastructure procurement and management for the DSB.

2.2 How many Vendor employees are involved in providing the product(s) or service(s) dedicated to a Single Client?

There are no staff dedicated to servicing individual customers.

2.3 How many staff will be providing the service and where are they located.

Contractor Name	Location	Staff Number
etradingsoftware Ltd	UK & Philippines	105
Rackspace Technology	UK, NA, Asia	6500 worldwide

2.4 Where are the services hosted?

The infrastructure is designed as high availability and hosted in AWS cloud with the primary service located in EU-WEST-1 and the secondary US-EAST-1. The service is managed out of London and the Philippines.

2.5 Who do the DSB partners sub-contract to?

Rackspace (SPP) subcontracts infrastructure provisioning to Amazon Web Services (AWS).

2.6 Can the DSB be classified as a software service?

Yes, the DSB can be classified as a software service.

2.7 Does the-DSB perform an ethical hack on the web interfaces?

Yes – Penetration testing is performed on an annual basis and any remediation is tracked to completion.

2.7.1 Can we see a copy of the report?

Yes, however a formal request sent to DSB-CISO@anna-dsb.com to see the summarised report is required by the client.

2.7.2 Which company performs the assessment?

JumpSec - http://www.jumpsec.com

2.8 How are passwords protected at rest?

Database stored with Hash values - PBKDF2 (Password-Based Key Derivation Function 2) is used

2.9 Which TLS cipher suites are used?

The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).

2.10 How is the DSB going to ensure connectivity is only from the user's network?

Security groups and dedicated port assignments for each user

2.11 What two-factor authentication method is being used and when?

A FIDO U2F compliant device is mandatory all support staff when accessing critical (i.e. Production or UAT) systems.

2.12 How are private keys stored?

Private keys are only available to the services that need them, or are stored in the Keepass database (for administrator access). Private keys/encryption keys used by the system itself (e.g. S3, volume encryption, etc.) are stored in Amazon Web Services' Key Management Service (KMS). As per documentation from AWS, the FIPS certification level is being evaluated for FIPS 140-2..

2.13 Is data encrypted in motion internally?

For frontend services, we encrypt data in motion via the use of HTTPS. For backend services, the principle is data is only decrypted on the device itself. For this we heavily use file encryption.

2.14 Has DSB done a security assessment of Amazon, can they share their findings?

Both Rackspace and AWS are assessed for security and other risks, however vendor risk assessments are considered sensitive and proprietary in nature and are not provided to clients.

2.15 What is the breakdown of security related responsibilities between DSB, Amazon and Rackspace.

Infrastructure -> Rackspace over AWS (intrusion detection, virus checking, etc.) Application stack -> DSB over the Rackspace managed service.

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

Latest details regarding the DSBs Business Continuity practices can be found in the DSB Business Continuity policy and the DSB Business Continuity FAQ (See section 1.3).

2.17 Rackspace maintains SOC 1, SOC 2, ISO 27001, FedRAMP, FISMA, PCI, and HITRUST compliance and security standards." Will the reports be made available to DSB's clients?

Yes, with an NDA with Rackspace in place, these documents can be made available to clients: SOC 1 & SOC 2 reports, ISO 27001 certificate, PCI ROC/AOC, and HITRUST myCSF report. For further information contact DSB-CISO@anna-dsb.com

2.18 When DSB refers to PII (personally identifiable information), what are they referring to?

Contact information, user names, email address and client support contact information

2.19 How is Data leakage going to be managed?

Security alerts, monitoring, client communication. 2-factor authentication, can correlate logs to user access. Logs are monitored.

2.20 How will the destruction of devices be managed? How will our data be destroyed?

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800 - 88 ("Guidelines for Media Sanitization") as part of the decommissioning process.

Ref AWS Security White Paper:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

Keep data forever, unless not required. i.e. no maximum retention policy, only a minimum retention policy.

2.21 How and where will backups be managed?

For backups, encrypted EBS Volumes are snapshotted and storage in S3. Amazon EBS encryption handles key management. Each newly created volume is encrypted with a unique 256-bit key. Any snapshots of this volume and any subsequent volumes created from those snapshots also share that key. These keys are protected by AWS key management infrastructure, which implements strong logical and physical security controls to prevent unauthorized access. Data and associated keys are encrypted using the industry standard AES-256 algorithm.

2.22 Does Amazon have remote access to the applications and data (including encryption keys)?

No

2.23 How are logs protected from privileged users?

Segregation of duties, and 2-factor authentication.

2.24 Meltdown and Spectre Vulnerabilities

AWS in conjunction with our third-party vendor, Rackspace, have proactively scanned and patched all DSB virtual instances against these vulnerabilities on both the hardware and operating system level where applicable.. AWS and Rackspace have assured the DSB that after further scans across the platform no vulnerabilities currently exist with the platform.

2.25 Has an independent internal or external auditor evaluated your Disaster Recover and Business Continuity policies?

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 report can assist users and their auditors with information on the policies, procedures and controls in place, as well as understand the design and implementation of controls. Copies of the ISAE 3402 and AAF 01/06 Type I Report can be made available upon request to both existing and potential users of the

DSB. Further information is available here. To obtain a copy please email client-admin@ANNADSB.com.

2.26 Have you or your managed service providers, managed security services or cloud provider been notified by any government authority or organization that your systems or data in your possession or control, or data held by your service providers, has been or may have been compromised?

The DSB has not been contacted by any Government Agency in relation to the attempted or successful penetration of its systems. The DSB has been advised by each of its cloud service suppliers (Rackspace and Amazon Web Services) that DSB systems are not within scope of any external investigation nor have DSB systems or data been compromised by a cyber intrusion.

2.27 How does the DSB mitigate potential impacts from cyber intrusion events?

Please see the existing DSB Security policy - section “Monitoring Info Sec Events, first paragraph”.

2.28 What is the latest information from the DSB regarding the COVID-19 pandemic planning?

Please see the DSB Website for details.

2.29 Has the DSB been affected by the Solarwinds hack of December 2020?

Neither the DSB, nor it’s subcontractor Rackspace Technology, has ever operated a Solarwinds product for, or in conjunction with, any part of the DSB platform. The DSB consequently has assessed its risk on this topic as negligible.

2.30 Does the DSB manage user security differently whilst remote working?

The DSB adopts a Zero Trust approach to maximise the security of endpoint user services whether in office or remote. SaaS Services for users are protected through suitable encryption in transit (TLS 1.2), Multi Factor Authentication and the principle of least privilege. All user services are subject to annual security reviews, including penetration tests (unless explicitly disallowed by vendor).

2.31 Has the DSB been affected by the “zero-day “exploit which is a known vulnerability of the “Pulse Secure” systems for VPN remote access?

The DSB is not affected by the “Pulse Secure” vulnerability as we are running the version of Fortinet VPN solution that is not affected by the Fortinet (CVE-2018-13379, CVE-2020-12812, and CVE-20195591) or Pulse Secure (CVE-2021-22893, CVE-2019-11510, and CVE-2020-8243) vulnerabilities.

2.32 Is the DSB aware of its use of Apache Log4J and is the vulnerability CVE-2021-44228 remediated?

Yes, the components using Log4J have been identified. Those components at risk of being exploited have been shut down or have been patched. Monitoring is in place to identify anomalies.

2.33 Is the DSB aware of its use of Apache Log4J and is the vulnerability CVE-2021-45105 remediated?

Yes, the components using Log4J have been identified. Those components at risk of being exploited through CVE-2021-45105 have been shut down or have been patched. Monitoring is in place to identify anomalies.

2.34 Is the DSB aware of the potential increase in Cybersecurity activity due to the current geopolitical situation?

This notification informs you that we have received and acknowledge the latest communication from the Cybersecurity & Infrastructure Agency (CISA) regarding the potential increase in Cybersecurity activity due to the current geopolitical situation.

Where relevant, we are following the guidelines laid out in the notification.

The DSB currently has no staff or infrastructure in the areas affected by this geopolitical situation.