DSB Information Security

Frequently Asked Questions

Author: Derivatives Service Bureau

Date: 25th April 2025

Version: 3

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
25th April 2024	Addition	2.2	Balwinder Singh Ajrah	Historic entries being updated
25th April 2025	Re-write	3	Balwinder Singh Ajrah, DSB-CISO	Removed references to Rackspace. Updated sections and links according to 2025 policies.

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.
DSB Security Policy v8_2025_Clean- DSB (anna-dsb.com)

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 receives more requests for information. This document is located on the DSB Website, accessible to all stakeholders.
DSB Information Security FAQ - DSB (anna-dsb.com)

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)?

The active list of subcontractors is maintained on the DSB's website which can be viewed here:

https://www.anna-dsb.com/subcontractors/

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
Etrading Software Limited	UK & Philippines	181

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 (Ireland) and the secondary US-EAST-1 (North Viginia). The service is managed out of London and the Philippines.

2.5 Who do the DSB partners sub-contract to?

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

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. The latest pentest was performed in April 2024.

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?

The DSB has used different companies, however, FSP conducted the latest pentest.

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 1.3 (and TLS 1.2 for backwards-compatibility), ECDHE_RSA with P-256 (a strong key exchange), and AES_256_GCM (a strong cipher).

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

DSB enforces connectivity exclusively from the user's network by implementing robust network security controls and strong user authentication measures.

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

All support staff are required to use a FIDO U2F-compliant device when accessing critical systems (e.g., Production or UAT). Multi-factor authentication (MFA) is mandatory for all support staff.

2.12 How are private keys stored?

Private and encryption keys used by the system (e.g., for S3 or volume encryption) are securely stored in AWS Key Management Service (KMS). AWS KMS is 140-3 compliant.

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?

AWS is assessed for security and other risks, however vendor risk assessments are considered sensitive and proprietary in nature and are not provided to clients.
AWS SOC 2: SOC Compliance - Amazon Web Services (AWS)
AWS SOC Reports | AWS Security Blog (amazon.com)

2.15 What is the breakdown of security related responsibilities between DSB & Amazon.

The breakdown of security responsibilities aligns with the AWS Shared Responsibility Model. AWS is responsible for the security of cloud infrastructure, including, but not limited to, physical data centers, networking, and managed service components. DSB is responsible for the security of the application stack including, but not limited to, application code, data encryption, access controls, and secure configuration of AWS services.

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 DR and Business Continuity Policy and the DSB Business Continuity FAQ (See section 1.3).

2.17 AWS maintains ISO 27001, AICPA SOC, and other security compliance and certifications. Where can clients obtain copies of such compliance and certification documents?

AWS makes these documents available for the public on their "AWS Compliance Programs" website (https://aws.amazon.com/compliance/programs/). 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, usernames, email address and client support contact information

2.19 How is Data leakage going to be managed?

DSB implements Data Leakage Prevention as described in the DSB Security Policy (DSB Security Policy v8_2025_Clean- DSB (anna-dsb.com)

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?

DSB implements backup systems and processes aligned with ISO 27001 security standards and described in the DSB Security Policy (DSB Security Policy v8_2025_Clean- DSB (anna-dsb.com)

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.

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

Yes. The DSB has undergone independent audits as part of its governance framework. For the OTC ISIN Service, the DSB completes an annual ISAE 3402 Type II audit, covering the full calendar year. The most recent report covers the period from 1 January to 31 December 2024 and was conducted by an Independent Service Auditor. This audit assesses the design and operational effectiveness of the DSB's controls, including those relating to Disaster Recovery and Business Continuity.

For the UPI Service, the DSB completed an ISAE 3402 Type I audit as of 31 December 2024, also carried out by an Independent Service Auditor, evaluating the design of relevant controls at a point in time.

More information can be found on the DSB Website[1]. Copies of the ISAE 3402 reports are available upon request to both existing and potential users. All reports are for internal use only and cannot be redistributed. To request a copy, please email: Client-Admin@ANNA-DSB.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 (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?

The DSB mitigates potential impacts from cyber intrusion events through robust incident detection using continuous monitoring and threat intelligence, rapid response, and swift recovery through tested backup, restoration, and resilience procedures. These practices minimize downtime, data loss, and operational disruption.

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

Please see the DSB Website for details.

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 1.3 and 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.

[1] https://www.anna-dsb.com/third-party-assurance-audit/

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 National Cyber Security Centre (NCSC) and 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.