Netrust Pte Ltd

Certification Authority Compliance Audit Report
Netrust Certification Authority

Audit Completed: 15th Mar 2024
Report Generated: 29th Mar 2024

1. Executive Summary

BDO Advisory Pte Ltd, hereafter known as BDO, was contracted by Netrust Pte Ltd, hereafter known as Netrust, to conduct an independent third-party CA Audit on Netrust CA Systems – CA2. The scope of this audit included an assessment of policies, procedures, processes, systems, and controls included in Compliance Audit Checklist for Certification Authority issued by IMDA.

The assessment conducted by BDO commenced from 24th Feb 2024 – 15rd Mar 2024. The auditor team undertook a process of collecting evidence and evaluating evidence to determine the level of compliance. As part of the CA audit, we conducted a Post Implementation Review (PIR) of Netrust management follow-up on the audit findings and recommendations outlined in the CA Audit performed in 2023.

Except for five (5) low risk findings, Netrust was in all material respects, in compliance with the Audit Checklist for Certification Authority issued by IMDA. We have provided recommendations provided in to address any issues, findings and areas for improvements identified by our audit team.

Our opinion is that Netrust has implemented critical security controls and we acknowledged that Netrust is taking active corrective actions to implement control measures to mitigate the potential risks that could result from the control deficiencies highlighted in our review. Netrust CA2-1, Netrust CA2-2 systems, for the period since the last CA Audit on 20th February 2023 to 19th February 2024, have been fairly executed in all material aspects, in accordance with the Compliance Audit Checklist for Certification Authority issued by Infocomm Media Development Authority Singapore IMDA.

The information contained in this report represents the view of BDO on the issues as of the date of assessment, BDO shall not be held liable for any damage due to the negligence of the vulnerabilities.

2. Background

As the first Certification Authority (CA) in Southeast Asia, Netrust provides individuals, businesses and government organizations with a complete online identification and security infrastructure to enable secure electronic transactions via the Internet and other wireless media.

In its capacity as a CA, Netrust acts as a trusted third party that issues and manages digital certificates. Netrust maintains a Public Key Infrastructure (PKI) certification service and its CA role creates and signs X.509 digital certificates which bind individuals, organizations, and application servers with the particular public key of each subscriber.

The key information processing resources are located at:

- CA Production site
- CA Disaster Recovery site

3. Scope of Work

BDO has examined **NETRUST MANGAEMENT ASSERTION**, that for its Certification Authority ("CA") operations in Singapore, throughout the period 20th February 2023 to 19th February 2024, for its CAs outlined below,

Root CA:

CA Name	Subject DN	SHA2 Thumbprint	Certificate Serial Number	Valid From	Valid To
Netrust Root CA 2	CN=Netrust Root CA 2, OU=Netrust Certificate Authority, O=Netrust Pte Ltd, C=SG	65353833CF234C79562164F90849C0D104DBABF8EE41064D83E8CBE03BA1C5A5	57c7ecf4	01/09/2016	01/09/2041

Intermediate CA:

CA Name	Subject DN	SHA2 Thumbprint	Certificate Serial Number	Valid From	Valid To
Netrust CA 2-1	CN=Netrust CA 2-1, OU=Netrust Certificate Authority, O=Netrust Pte Ltd, C=SG	863B2D43886B1B807B07D7DFDA5986F1D78A54C437EEF554C23E4547A3A1F3E7	57c7ed31	02/09/2016	02/09/2036
Netrust CA 2-2	CN=Netrust CA 2-2, OU=Netrust Certificate	A478AD193683DD4138E3D1533D71800C1B1147643C885D3CB3DF283FFC05FB88	57c7ed32	02/09/2016	02/09/2036

	Authority, O=Netrust Pte Ltd, C=SG				

We have also reviewed that Netrust:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Netrust Certification Practices Statement ("CPS") and Netrust Certificate policy ("CP") as published at https://www.netrust.net/ourpractices/.
- maintained effective controls to provide reasonable assurance that:
  - the CPS is consistent with its CP; and
  - Netrust provides its services in accordance with it's CP and CPS
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated; and
  - subordinate CA certificate requests are accurate, authenticated, and approved.
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals.
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

Our review of the Netrust's controls and procedures with the IMDA's Security Guidelines for Certification Authorities as provided in the Compliance Audit Checklist, (URL: (**https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Acts-Regulations/CA_AuditChecklist.pdf?la=en**), also covered the following areas.

- Certification Authority Overall Guidance
  - Obligations to Subscribers, Relying Party and User Community
  - Certificate Practice Statement (CPS) and Certificate Policies (CP)
  - Security Management
  - Risk Management
  - Personnel Controls
  - Subscriber's data
  - Incident Management
  - Business Continuity Planning

- Certificate Management Controls
  - Registration Process
  - Generation Process
  - Issuance Process
  - Publication Process
  - Renewal Process
  - Certificate Suspension Process
  - Revocation Process
  - Archival Process

    - Audit Trails

- Key Management Controls
    - Generation
    - Distribution
    - Storage
    - Usage
    - Backups
    - Key Change
    - Destruction
    - Key Compromise
    - Key Archival
    - Cryptographic Engineering

- System and Operational Controls
    - Physical Security
    - General Security Controls
    - General Operational Controls
    - Change and Configuration Management
    - Network Security
    - Monitoring and Audit Trails

- Application Integration Controls

- Compliance with ETA and ETR
    - Compliance with ETA
    - Compliance with ETR

3.1 Limitation of Scope

Our Services were performed in accordance with CoBiT, COSO and ISO 27001 standards and guidelines. The work performed did not constitute an examination or a review in accordance with generally accepted auditing standards or attestation standards.

Our work was limited to the specific procedures and analysis described herein and was based only on the information made available up to the date of this Report. Accordingly, changes in circumstances after this date could affect the findings outlined in this Report and we reserve the right to amend findings, conclusions, or recommendations, if necessary, based on factual information that comes to our attention after that date.

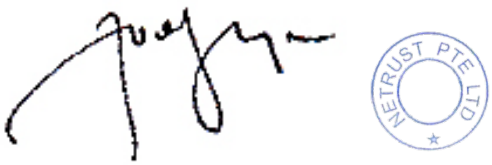
Our Services are not designed to and are not likely to reveal fraud or misrepresentation by the Management. Accordingly, we cannot accept responsibility for detecting fraud (whether by Management or by external parties) or misrepresentation by the Management or any other person.

4. Sign-off & Acknowledgement

BDO would like to take this opportunity to thank management and staff of Netrust for all their assistance and time during the course of this audit.

The report is intended solely for use by Management of Netrust and BDO accept no responsibility for any reliance on the report by any third parties, unless our permission is sought for the provision of this particular report to specified third parties and such request is conveyed to BDO in writing prior to provision of this report.

This acknowledgement represents the agreement between BDO and Netrust with respect to the objectives, obligations and responsibilities performed in the CA audit that had been completed.

Netrust Contact:	BDO Auditor:
Accepted by:	Prepared by:
Foo Jong Ai	Cecil Su
Chief Executive officer	Director, Cybersecurity Division
	
Date: 11th Apr 2024	Date: 11th Apr 2024

5. Assessment Framework

The following table outlines the five audit report assessment categories, together with descriptions and an indication of the implied level of concern for senior management and the audit committee. This framework is applied to provide an overall assessment of the audit based on the audit issues identified.

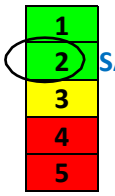
Assessment Rating	Description	Level of Concern
1	On an overall basis, an appropriate control environment was in place given the inherent business risks. Some improvements to routine control activities were noted.	No to limited scope for improvement
2	Although a number of issues were noted, no major concerns were noted.	No major concerns were noted
3	Needs Strengthening - Significant number of issues were noted although our work did not identify any major issues. However collectively, they indicate a weak control	Cause for concern
4	Inadequate - Significant weaknesses were noted that could expose the auditable unit to unacceptable levels of risk if left uncorrected.	Cause for considerable concern
5	Unacceptable - Significant weaknesses were noted which could expose the Corporation to significant financial or other loss, or otherwise significantly impair its reputation.	Immediate attention of CEO & Board of Directors required

Our audit issues are rated based on the following risk table.

Risk Rating	Des
High	The item mentioned is a requirement to be followed as it has significant impact on controls, finance, or operations. We advise that these items be addressed immediately.
Medium	The item mentioned may have a moderate impact on controls, finance or operations and should be addressed within a short
Low	The item mentioned may have a low impact to controls, finance or operations if left uncorrected.

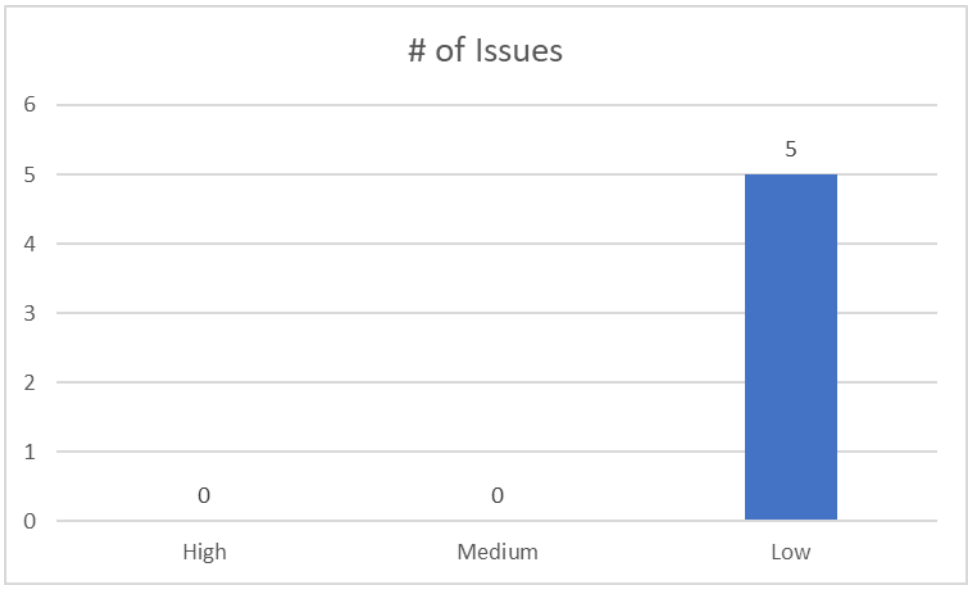
5.1 Overall assessment

A total of five (5) issues were identified during our audit and all the five (5) issues were identified as Low risk. Collectively, they indicate a satisfactory and adequate environment.



SATISFACTORY **SUFFICIENTLY ADEQUATE**

The table below highlights the resultant number of issues raised from our audit of Netrust Production and Disaster Recoery sites.



6. Contacts

6.1 Netrust Pte Ltd Contacts

Role	First Name	Last Name	email	Phone
Service Delivery Manager	Yu Jie	Tay	Yujie.tay@netrust.net	+65 8750 5770
Technical Manager	Eng Jing	Wee	engjing.wee@netrust.net	+65 9662 5936

6.2 BDO Cybersecurity Advisory Auditors Contact

First Name	Last Name	email	Phone
Gerald	Tang	geraldtang@bdo.com.sg	+65 6990 2847
Sandeep	Singh	sandeepsingh@bdo.com.sg	+65 6828 9118
Cecil	Su	cecilsu@bdo.com.sg	+65 6990 2846

7. Version Control

Version	Date	Author	Remarks
1.0	27 Mar 2024	Gerald Tang	Draft.
1.1	29 Mar 2024	Gerald Tang	Peer review by Cecil Su.
1.2	4th Apr 2024	Gerald Tang	Included feedbacks and comments from Netrust.
1.3	9th Apr 2024	Gerald Tang	Included feedbacks and comments from Netrust.

8. About BDO Cyber Security

BDO Cybersecurity ® is the advanced security team at BDO Cyber Security focused on incident response, network penetration testing, physical security, application security, and security research. BDO Cyber Security provides thought leadership to the local and national community and our clients. BDO Cyber Security has responded to security incidents, performed penetration tests, and tested the security of a large number of business applications for organizations ranging from the largest companies in the world to nimble start-ups. Members of the BDO Cyber Security teams are frequently asked to speak at security conferences such as OWASP, ISC2, ACFE, ISACA and SICW Government Ware.

NETRUST
YOU CAN BE SURE

NETRUST MANAGEMENT ASSERTION

Netrust Pte Ltd. ("Netrust") operates the Certification Authority ("CA") services for the CAs outlined below.

Root CA:

CA Name	Subject DN	SHA2 Thumbprint	Certificate Serial Number	Valid From	Valid To
Netrust Root CA 2	CN=Netrust Root CA 2, OU=Netrust Certificate Authority, O=Netrust Pte Ltd, C=SG	65353833CF234C79562164F90849C0D104DBABF8EE41064D83E8CBE03BA1C5A5	57c7ecf4	01/09/2016	01/09/2041

Intermediate CA:

CA Name	Subject DN	SHA2 Thumbprint	Certificate Serial Number	Valid From	Valid To
Netrust CA 2-1	CN=Netrust CA 2-1, OU=Netrust Certificate Authority, O=Netrust Pte Ltd, C=SG	863B2D43886B1B807B07D7DFDA5986F1D78A54C437EEF554C23E4547A3A1F3E7	57c7ed31	02/09/2016	02/09/2036
Netrust CA 2-2	CN=Netrust CA 2-2, OU=Netrust	A478AD193683DD4138E3D1533D71800C1B1147643C885D3CB3DF283FFC05FB88	57c7ed32	02/09/2016	02/09/2036

	Certificate Authority, O=Netrust Pte Ltd, C=SG				

In addition, Netrust provides the following CA services as outlined below:

- Subscriber registration
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate renewal
- Certificate recovery
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of Netrust is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its repository, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Netrust's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Netrust management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in Netrust management's opinion, in providing its CA services throughout the period from 20th February 2023 to 19th February 2024, Netrust has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Netrust Certification Practices Statement ("CPS") and Netrust Certificate policy ("CP") as published at https://www.netrust.net/ourpractices/.
- maintained effective controls to provide reasonable assurance that:
    - the CPS is consistent with its CP; and
    - Netrust provides its services in accordance with its CP and CPS.
- maintained effective controls to provide reasonable assurance that:
    - The integrity of keys and certificates it manages is established and protected throughout their lifecycles.
    - The integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles.
    - subscriber information is properly authenticated; and
    - subordinate CA certificate requests are accurate, authenticated, and approved.
- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals.
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity.

Based on IMDA's Security Guidelines for Certification Authorities, Netrust has also complied with:

CA Business Practices Disclosure
- Certificate Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management
- Certificate Policy (CP) Management
- Certification Practice Statement (CPS) Management
- CP and CPS Consistency

CA Environmental Controls
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance Audit Logging

CA Lifecycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation
- CA Key Migration

Subscriber Key Lifecycle Management Controls
- CA-provided Subscriber Key Generation Services
- CA-provided Subscriber Key Storage and Recovery Services
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls
- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate and Cross Certificate Lifecycle Management Controls
- Subordinate CA Certificate and Cross Certificate Lifecycle Management

Netrust does not escrow its CA keys and as such, our assertion does not extend to controls that would address this criterion.

The list of in-scope Netrust assets audited are outlined below:
- Certificate Practice Statement
- Certificate Policies
- List of CAs:
    - Netrust Root CA 2
    - Netrust Intermediate CA : CA 2-1, 2-2