SIX Generic AFME Questionnaire 2025

TABLE OF CONTENTS

1 Credentials

1.1 Respondent Information

1.1.1 Respondent information

Name of legal entity responding	SIX Digital Exchange AG
Market	Switzerland
Designated responding manager (name/title)	Federica Tulino / Specialist Sales Support
Contact details (email/phone)	federica.tulino@sdx.com / +41 585083515
Date submitted	
Signature (if not responding via electronic platform)	

1.1.2 Which services are in scope of your response?

- [x] Custody Services
- [ ] Client money services
- [ ] Both

1.2.1 Please advise the name of the contracting party providing custody and/or client money services in your jurisdiction and responding to this questionnaire. If applicable, please also advise the name of the local delegate if different from the contracting entity.

SIX Digital Exchange AG

1.3 Your regulatory environment

1.3.1 Which official body regulates your business (including banking, custody and client money)? If they license or provide a formal approval of your business, how frequently does this need to be renewed?

	Licensed/regulated by	Frequency
(a) Banking	N/A	N/A
(b) Custody	FINMA	Ongoing Supervision
(c) Client money	FINMA	Ongoing Supervision

Please provide a copy of each current licence or approval notification.

(No file attached)

(No file attached)

(No file attached)

1.3.2 Has your regulator(s) raised any material issues in respect of your banking, custody and client money activities within the last 12 months?

☐ Yes

☑ No

If yes, provide details.

N/A

1.3.3 Are you a branch of an entity incorporated in another country?

☐ Yes

☑ No

If yes, please explain the division of regulatory responsibility between your host and home state regulators.

N/A

1.3.4 Please confirm that you comply with local regulatory requirements in relation to the provision of custody or client money services in your jurisdiction.

Custody

☑ Yes

☐ No

☐ N/A

Client Money

☑ Yes

☐ No

☐ N/A

Comments:

N/A

1.3.5 Have you been subject to any fines, enforcement actions or other admonishments by authorities during the last 12 months?

☐ Yes

☑ No

If yes, provide details.

N/A

1.3.6 Please confirm which of the following criteria you meet in order to serve as an eligible custodian under Rule 17(f)5 of the US Investment Company Act 1940.

☐ A U.S. bank as specified in Section 17(f) or a member of a U.S. national securities exchange as specified in Section 17(f).

☐ Eligible Foreign Custodian - an entity incorporated or organised under the laws of a country, other than the US and that is a Qualified Foreign Bank or a majority owned direct or indirect subsidiary of a U.S. bank or bank holding company.

☐ A Qualified Foreign Bank - a banking institution or trust company, incorporated or organised under the laws of a country, other than the US, that is regulated by its national regulator.

1.3.7 Please confirm which of the following criteria you meet to be an "approved bank" under the UK Financial Conduct Authority (FCA) guidelines:

☐ A Central Bank of a member state of the OECD (including the Bank of England).

☐ A bank which is supervised by the Bank of England, or a central bank or other banking regulator of a member state of the OECD.

☐ A credit institution established in an EEA State other than the United Kingdom and duly authorised by the relevant Home State regulator, or a bank which is regulated in the Isle of Man or the Channel Islands.

☐ Supervised by the South African Reserve Bank.

☐ Regulated by a local banking regulator, required to provide audited accounts; have minimum net assets of £5 million (or equivalent) and have had a surplus revenue over expenditure for the last two financial years.

Comments:

N/A

1.3.8 Please confirm which of the following criteria you meet to comply with the current European Union (EU) directives and regulations applicable to Alternative Investment Fund (AIF) and Undertakings for Collective Investment in Transferable Securities (UCITS).

☐ A Central Bank of a member state of the EU

☐ A credit institution authorised in accordance with Directive 2013/36/EU on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms

☐ A third country credit institution subject to prudential regulation and supervision which have the same effect as EU law and are effectively enforced and in accordance with the principles laid down in Article 16 of Directive 2006/73/EC. (Such prudential regulation and supervision would include aspects of the following: (a) custody services being governed by law; (b) your assets being clearly segregated from those of your clients; (c) there being a deposit guarantee schemes in place for cash in the event of your failure; (d) your regulator being a member of the International Organisation of Securities Commissions (IOSCO).)

Comments:

N/A

1.3.9 Please confirm that you are subject to prudential regulation, including minimum capital requirements?

☑ Yes

☐ No

Comments:

SDX is obliged to comply with the capital adequacy requirements set ou in the Siwss Financial Market Infrastructure Act, the Financial Market Infrastructure Ordinance and the Capital Adequacy Ordinance.

1.3.10 Have regulators required your organisation to undertake any stress testing to ensure your risk management and capital planning decisions can sufficiently withstand adverse market events?

☐ Yes

☑ No

If yes, did you pass the test?

N/A

If no, provide details.

N/A

1.4 Your group

1.4.1 Have there been any changes to your group's ownership structure in the last 12 months?

☐ Yes

☑ No

If yes, provide details.

The owners of SIX Group AG comprise around 120 national and international financial institutes.

The major shareholders of SIX Group AG include:

Big Banks: 34.5%

Commercial and Investment Banks: 17.6%

Foreign Banks: 15.1%

Cantonal Banks: 14.3%

Regional and Raiffeisen Banks: 8.5%

Others. 4.1%

Own Shares. 3.1%

Private Banks: 2.8%

1.4.2 What is your relationship to your group?

☐ Parent entity

☐ Full branch (if proposed sub-custodian is a bank)

If a branch, please confirm where your parent entity is incorporated.

N/A

☑ Subsidiary - wholly owned

☐ Subsidiary - not wholly owned

If not wholly owned, what percentage of share capital does your group own?

N/A

☐ Other

If other, provide details.

N/A

1.4.3 Please provide an organisational chart which clearly indicates in which strategic business area your custody business fits, and highlight if there have been any changes in the last 12 months.

Please attach file here:

ORG CHART SDX.png (61.6 Kb)

Comments:

The attached chart represent SDX organisation as per December 2024.

SIX Group, and thus SDX as its part, operates with four business units (Exchanges, Securities Services, Banking Services and Financial Information) as well as IT, Finance & Services, Risk, Security & Compliance, Legal & Regulatory, Marketing & Communications and Human Resources as support functions.

1.4.4 Does your organisation have measures in place to identify and prevent conflicts of interest between custody and other businesses (e.g. prime brokerage, execution, asset management services)?

☑ Yes

☐ No

If no, please outline why not and provide details of alternative controls that exist.

N/A

1.4.5 Please state the latest available Basel III ratios. If your local regulators specify more stringent requirements than the Basel Agreement, please indicate the requirements and whether you comply.

Please specify if Basel III is in transition or fully implemented.

☑ In transition

☐ Fully implemented

Capital adequacy ratio (%)

227.7%

Basel III (estimated %)

Meets local requirements

☑ Yes

☐ No

Meets regulatory requirements

☑ Yes

☐ No

Comments:

Capital fulfillment ratio as end of December 2024 at 215.5% vs. 110% required by FINMA. Capital adequacy ratio is indicated as end of December 2024.

Please specify the basis of calculation for your Risk Weighted Assets (i.e. standardised or advanced).

☑ Standardised

☐ Advanced

1.4.6 Please state the credit ratings of the contracting party in the table below.

Contracting party:	SIX Group AG			
	Credit rating (year end)	S&P	Moody	Fitch
Long-term rating	Current	A	- Select answer -	- Select answer -
	Preceding year	A	- Select answer -	- Select answer -

Comments:

Rating of the parent company (SIX Group AG)

1.4.7 Please provide a copy (in English) of or link to the latest annual report for the contracting party and, if applicable, the local delegate. If not available, please provide this for the parent organisation.

Please attach file here:

SIX Digital Exchange Ltd_financial statements_2024.pdf (322.6 Kb)

Comments:

N/A

1.4.8 Please confirm if your organisation is considered a systematically important financial institution as defined by the Financial Stability Board/Basel Committee on Banking Supervision or as defined in the jurisdiction where it is registered.

☐ Yes

☑ No

Comments:

1.5 Insurance

1.5.1 Please confirm that you maintain adequate insurance policies to cover (select all that apply):

☑ Any liabilities and indemnities that you may incur in connection with services you provide.

☑ Professional Liability

☑ Crime Insurance that covers dishonest acts

☐ Enterprise privacy liability (cyber)

Please attach copies of all relevant insurance certificates.

Insurance Certificates_2025.zip (457.2 Kb)

Comments:

SIX has a Public and Office Liability Insurance policy from Liberty Mutual Insurance Europe, a Directors' & Officers' Liability insurance policy under Zurich Insurance Company and a Cyber Risk, Fraud and Indemnity insurance through XL Group. Further details of coverage can be seen in our Insurance Certificates attached. Unfortunately, we cannot state the level of insurance coverage due to confidentiality reasons.

1.5.2 Please confirm that a qualified team within your organisation, independent of your custody business, reviews your insurance cover on at least an annual basis.

☑ Yes

☐ No

Comments:

SIX Digital Exchange is a subsidiary of SIX and is as such covered by the group insurance policies. Please note that the answers contained in the Questionnaire are provided for information purposes only. Information in this document is subject to change and does not represent a commitment on the part of SIX Digital Exchange, or any other entity in the SIX Group of companies. SIX Digital Exchange, its subsidiaries and affiliates expressly disclaim liability for errors or omissions in the information contained in this document.

1.6 Your strategy

1.6.1 In the last 12 months have there been any changes to your business activities which are relevant to the services that you provide to your custody or client money clients?

Custody

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

Client money

☑ Yes

☐ No

☐ N/A

If yes, provide details.

SDX is participating in a pilot project to implement the usage of CBDCs as a cash option to settle in the CSD

1.6.2 Do you undertake other business activities which could compromise your ability to provide custody or client money services?

Custody

☐ Yes

☑ No

If yes, provide details.

N/A

Client money

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

1.6.3 Are there any regulatory changes being implemented that will directly impact your custody or client money business strategy over the next 24 months?

☑ Yes

☐ No

Comments:

The EU Digital Operational Resilience Act (DORA) as well as the FINMA Circular 2023/1 ”Operational Risks and Resilience – Banks” impose on providers to restore critical functions in case of a disruption within the tolerance for disruption. SIX operates the infrastructure for the

financial centre in Switzerland, thus ensuring the flow of information and money between financial market players. This business is being replicated and continuously improved on by SIX Digital Exchange AG and SIX Trading AG (collectively: "SDX") by leveraging the Distributed Ledger Technology ("DLT") for its own bespoke financial market infrastructures. These services of SIX Group as a whole are critical not only in the corporate context, but also for the national economy in Switzerland. Resilience and emergency preparedness are general security topics embedded into the companywide integrated security activities. SIX and SDX address operational resilience in a targeted and tailored fashion to the different audiences within the company (staff/management) and beyond (stakeholders). Operational resilience is the ability of financial institutes, Financial Market Infrastructures (FMIs) and the financial sector as a whole to identify and protect against threats and potential failures, to respond and adapt to disruptive events, and to recover and learn from them to minimize their impact on the delivery of critical functions. Central aspects for increasing operational resilience are the greater involvement and strategic guidance from top management and the fostering of an optimal interplay between the different disciplines. In addition to the above-mentioned regulatory provisions applicable to SIX Group as a whole, ongoing regulatory developments specifically targeting crypto asset- and DLT-based service providers are being closely monitored by SDX (e.g., monitoring of and compliance with the EU Regulation "Markets in Crypto Assets"), where applicable to SDX.

1.6.4 Are there any IT developments that will directly impact your custody and/or client money provisions over the next 24 months?

☑ Yes

☐ No

Comments:

We have several initiatives and IT projects that will impact our business in the coming 24 month. Asset creation process enhancements, fractionalization of securities, depository receipts

segment, technical platform enhancements, CBPR+ messaging and SWIFT releases. On top of those we are continuously enhancing our portal, CSD and exchange via smaller initiatives and bug fixing.

1.7 Your organisation

1.7.1 Is your custody or client money operations department (e.g. including the systems used) a segregated unit from any trading/investment banking activity?

- [x] Yes
- [ ] No
- [ ] N/A

Comments:

Please note that SDX does not run any trading/investment banking activity.

1.7.2 Where your organisation has centralised, offshored or outsourced activities to a third party (i.e. not the legal entity that has been contracted with for the provision of services), what is the relationship of that third party to your organisation?

Relationship	Yes/No	Location (country/city)	Legal name	Activities
Branch	☐ Yes ☐ No			
Subsidiary	☐ Yes ☐ No			
Joint venture	☐ Yes ☐ No			
Affiliate	☐ Yes ☐ No			
External party	☐ Yes ☐ No			
Other	☐ Yes ☐ No			
N/A	☐ Yes ☐ No			

Comments:

N/A

1.7.3 In the past 12 months, have there been any changes to custody and/or client money activities which you centralise, offshore or outsource? (e.g. instruction capture, matching, settlements, reconciliations, corporate actions).

Centralised/Offshored

☐ Yes

☑ No

☐ N/A

Comments:

N/A

Outsourced

☐ Yes

☑ No

☐ N/A

Comments:

N/A

1.7.4 In the next 12 months, does your organisation plan to centralise, offshore or outsource any additional custody and/or client money activities to another part of your group or to a third party?

Centralised/Offshored

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

Outsourced

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

1.7.5 Are there any legal or regulatory changes planned for your market which will affect your centralised, offshored or outsourced activities?

Centralised/Offshored

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

Outsourced

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

1.7.6 Where you have centralised, offshored or outsourced activities, how are they monitored by management in the home jurisdiction? Please select all that apply.

Centralised/Offshored

☐ DDQ (please specify frequency)

☐ SLAs

☐ KPIs

☐ Service Review meeting/call

☐ Other (please provide details)

☐ None

☐ N/A

Comments:

N/A

Outsourced

☐ DDQ (please specify frequency)

☐ SLAs

☐ KPIs

☐ Service Review meeting/call

☐ Other (please provide details)

☐ None

☐ N/A

Comments:

N/A

1.7.7 Where you have centralised, offshored or outsourced activities, has the accountability for service standards and operational functions been diverted from the contracting party?

Centralised/Offshored

☐ Yes

☐ No

☐ N/A

If yes, provide details.

N/A

Outsourced

☐ Yes

☐ No

☐ N/A

If yes, provide details.

1.7.8 Do you have all necessary regulatory approvals in place, for centralised, offshored or outsourced activities?

Centralised/Offshored

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

Outsourced

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

1.7.9 Do you receive and review a copy of the internal and external audit reports for centralised, offshored and outsourced services?

Centralised/Offshored

☐ Yes

☐ No

☑ N/A

If no, provide details.

N/A

Outsourced

☐ Yes

☐ No

☑ N/A

If no, provide details.

N/A

1.7.10 Do you conduct a risk assessment of activities that are centralised, offshored or outsourced?

Centralised/Offshored

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

Outsourced

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

1.7.11 Do you have plans in place to substitute centralised, offshored or outsourced services if a provider is unable to continue?

Centralised/Offshored

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

Outsourced

☐ Yes

☐ No

☐ N/A

If no, provide details.

N/A

1.7.12 Do you have an exit strategy (e.g. policies and procedures to ensure data protection, retention and retrieval) when terminating a contract or business relationship with a third-party supplier?

- [x] Yes
- [ ] No
- [ ] N/A

If no, provide details.

N/A

1.7.13 Please confirm that you assess the following criteria for entities providing centralised, offshored or outsourced services.

Centralised/Offshored

- [ ] Financial
- [ ] Audit
- [ ] Physical
- [ ] Service continuity
- [ ] Cybersecurity
- [ ] N/A

Comments:

N/A

Outsourced

- [ ] Financial
- [ ] Audit
- [ ] Physical
- [ ] Service continuity
- [ ] Cybersecurity

Comments:

N/A

1.8 Your performance

1.8.1 Please briefly describe your market advocacy activities and achievements in the last 12 months, both locally and globally, in making improvements to local and worldwide custody.

N/A

1.8.2 Please indicate your membership and participation in local industry bodies and initiatives.

☐ CSD working group

☐ Central Bank working group

☐ National trade association

☐ Other

If yes to any of the above, provide details.

N/A

1.8.3 Please complete the following table indicating the domestic and foreign clients you currently serve, plus current client assets under custody in each case.

Currency	CHF, EUR			
	Number of domestic clients	Assets under custody	Number of foreign clients	Assets under custody
Banks/global custodians	14		2	
Asset managers/institutions				
Brokers/dealers				
Private clients				
Mutual funds				
Public sector				
Other (please specify)				

Comments:

We cannot provide more detailed figures. Main clients are financial institutions.

1.8.4 Please complete the following table, showing the total number of custody employees located domestically plus a breakdown by key activities.

	Number of custody employees
Total	110
Management	6
Operations	14
Client services	
Relationship managers	3
Account officers	0
Other	85

Comments:

The above figures apply to the "Entire SDX Organisation" across all locations as per December 2024.

1.8.5 What is the staff turnover in your custody and/or client money services businesses in the past 12 months?

Custody

☐ 0-5%

☐ 5-10%

☐ 10-15%

☑ > 15%

☐ N/A

Client Money

☐ 0-5%

☐ 5-10%

☐ 10-15%

☑ > 15%

☐ N/A

1.8.6 Has your organisation been named in a lawsuit in the last 12 months relating to your custody and/or client money businesses?

☐ Yes

☑ No

If yes, explain the circumstances of each lawsuit and the outcome(s) to the extent legally permissible.

N/A

1.8.7 Does your organisation provide ongoing training to all relevant staff to ensure that knowledge is maintained at the requisite levels for the performance of their respective duties?

☑ Yes

☐ No

2 Asset Safety and Custody

2.1 Regulations, laws and market practices

2.1.1 Do you have processes in place to manage, capture and communicate regulatory rule changes within your organisation and, where applicable, to clients?

☑ Yes

☐ No

Comments:

We monitor the regulatory trends and rule changes that may affect SDX.

2.1.2 Are you subject to local regulatory disclosure reporting requirements? If yes, please provide details.

☑ Yes

☐ No

Comments:

Persons subject to a notification obligation must provide all information and surrender any documents to FINMA which the latter requires to perform its duties. FINMA has the power to transmit information and documentation that are not in the public domain to the other Swiss financial market supervisory authorities and to the Swiss National Bank where required by these institutions to fulfil their remit.

2.1.3 Do you obtain an external Legal Opinion?

☑ Yes

☐ No

If yes, provide a copy.

(No file attached)

If no, please explain why.

We obtain legal opinions on a case by case basis that we do not share with external parties.

2.1.4 In the last 12 months have there been any changes that affect either legal requirements or market practices related to the holding of client assets?

Legal requirements

☐ Yes

☑ No

If yes, provide details.

N/A

Market practices

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.5 In the last 12 months have there been any changes to local law in your jurisdiction which require us to grant you a security interest, lien or right of set-off over our clients' assets to recover debts that are not related to our clients?

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.6 **Concerning laws which a) affect the assurance that your organisation's clients have rights to have securities and cash held by you returned in the event of your insolvency, and b) that would protect your clients from having their assets taken by an insolvency authority to satisfy claims against you by any other person including creditors, please confirm the following:**

Do the laws assuring the above currently exist?

☑ Yes

☐ No

If yes, have there been any changes in the last 12 months and if so, provide details.

☐ Yes

☑ No

Comments:

N/A

Are new insolvency/bankruptcy laws or amendments to those that exist pending implementation?

☐ Yes

☑ No

If yes, provide details of relevant legislation.

N/A

That you will, within a reasonable time, inform us should there be any changes in the insolvency/bankruptcy laws.

☑ Yes

☐ No

If no, provide details.

N/A

2.1.7 Would your clients be protected from having their assets taken by an insolvency authority to satisfy claims against you by any other person including creditors?

☑ Yes

☐ No

If no, provide details.

N/A

2.1.8 In the last 12 months have there been any changes to the current legal framework regarding the required account structure (e.g. omnibus or segregated accounts)?

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.9 Are there any planned changes to the current legal framework regarding the required account structure (e.g. omnibus or segregated accounts)?

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.10 Please specify or confirm under which names it is legally possible to record or register legal title to securities in your jurisdiction. (Please answer "confirmed" next to each possible name listed below). (Please note that "legal title holder" in this case is the person that the issuer of the securities would recognise as having direct ownership of the securities).

	Our client's/ investor/ beneficial owner name:	Our name:	Our nominee name:	Your name below:	Your nominee name below:	A Third party nominee name:
Equities	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed
Exchange traded funds	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed
Funds	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed
Corporate, municipal, sovereign bonds, and Eurobonds* (* only held at ICSDs)	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed
Government instruments	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed
Physical securities	☑ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed	☐ Confirmed

2.1.11 Please confirm that you verify your client's assets are registered or that legal title to them is recorded as above.

☑ Yes

☐ No

If no, provide details.

N/A

2.1.12 Please confirm that you record assets to reflect the legal requirements in your jurisdiction?

☑ Yes

☐ No

If no, provide details.

N/A

2.1.13 Please confirm that you record assets to reflect the market practice in your jurisdiction?

☑ Yes

☐ No

If no, provide details as to how they are recorded at the CSD.

N/A

2.1.14 Please confirm that all assets held by you on behalf of your clients are recorded or held by you on your books and records in accordance with local law, rules, regulations and market practice.

☑ Yes

☐ No

If no, provide details.

N/A

2.1.15 Is the level of account segregation and record-keeping applicable and implemented by you sufficient to ensure that such assets are protected from your insolvency under the law of your jurisdiction?

☑ Yes

☐ No

If no, describe what additional arrangements you have implemented to minimise the risk of loss and ensure that such assets held for your clients are protected on your insolvency.

N/A

2.1.16 In the last 12 months, have there been any errors which have resulted in securities (proprietary or client assets) not being adequately safeguarded?

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.17 Within which entity or entities is legal ownership recorded? Please select all that apply:

☐ CSD

☐ Custodian

☑ Registrar

Comments:

N/A

2.1.18 In your market, is the nominee concept fully recognised and accepted?

☑ Yes

☐ No

Comments:

There is no specific law in Switzerland. Registration of ownership is relevant in connection with registered shares (cf. Art. 686 of the Swiss Code of Obligations).

2.1.19 If the answer to the previous question is yes, does the definition of a nominee company under your local market laws/regulations comply with the following definition: 'a body corporate whose business consists solely of acting as a nominee holder of investments or other property'?

☐ Yes

☐ No

☑ N/A

Comments:

N/A

2.1.20 If you adopt the use of a nominee concept, is it used to hold only client assets?

☐ Yes

☐ No

☑ N/A

Comments:

N/A

2.1.21 If you adopt the use of a nominee concept, is it required by law or general market practice?

☐ Required by law

☑ Market Practice

☐ N/A

Comments:

N/A

2.1.22 Is there a difference between a legal owner and a beneficial owner of securities according to local rules and regulations?

☑ Yes

☐ No

If yes, provide detials.

The legal owner is holding the securities but has no right to the entitlements. The beneficial owner is the real owner of the securities is being entitled to all corporate actions, voting rights, etc.

2.1.23 In the last 12 months have there been any changes to the registration practices for client securities in your jurisdiction?

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

2.1.24 Are there any legal requirements or market practices related to the holding of our assets or our clients' assets that could adversely affect our rights or our clients' rights?

☐ Yes

☑ No

If yes, provide details.

N/A

2.1.25 Can securities that you hold in an omnibus account, or an omnibus account itself, be restricted for any reason other than a valid court order?

☐ Yes

☑ No

Comments:

N/A

2.1.26 In the last 12 months have there been any changes to the protection or compensation available to our organisation if you are unable to meet your obligations?

☐ Yes

☑ No

Comments:

N/A

2.1.27 In the last 12 months have there been any changes to the action we need to take to recover our assets/monies in the event of your bankruptcy?

☐ Yes

☑ No

Comments:

N/A

2.2 Your accounts

2.2.1 Are you able to identify assets / securities held in your omnibus accounts as client assets?

☑ Yes

☐ No

Comments:

In SDX's records, the participant will be considered as the legal owner of the intermediated securities. It is the participant's responsibility to ensure client custody assets and proprietary assets are identifiable in the books and records of the participant and SDX is instructed properly as to the crediting of any particular intermediated security.

2.2.2 Acting as custodian, do you provide segregation between your proprietary holdings and clients' holdings?

☑ Yes

☐ No

Acting as custodian, do you provide segregation between clients' proprietary holdings and your clients' clients' holdings?

☑ Yes

☐ No

Acting as custodian, do you provide segregation throughout the custody chain including at CSD level?

☑ Yes

☐ No

Comments:

N/A

2.2.3 Are assets settled directly into a segregated client account or are they settled into a commingled firm / client account and subsequently segregated?

a) Settlement at sub-custodian

Fully segregated

☐ Yes

☐ No

Commingled, then segregated

☐ Yes

☐ No

Comments:

N/A

b) Settlement at CSD

Fully segregated

☑ Yes

☐ No

Commingled, then segregated

☐ Yes

☑ No

Comments:

Securities held with SDX are stored using our innovative distributed ledger technology (DLT). Assets are stored in a segregated manner directly in our members' nodes.

2.2.4 At the request of your client, do you segregate the following on your books and records?

Clients' UCITS securities from other clients' non-UCITS securities

☐ Yes

☐ No

If yes, describe how.

N/A

Clients' UCITS cash holdings from other clients' non-UCITS cash holdings

☐ Yes

☐ No

If yes, describe how.

N/A

Clients' AIF securities from other clients' non-AIF securities

☐ Yes

☐ No

If yes, describe how.

N/A

Clients' AIF cash holdings from other clients' non-AIF cash holdings

☐ Yes

☐ No

If yes, describe how.

N/A

2.3 Central Securities Depository (CSD)

2.3.1 In the last 12 months have there been any changes that affect the securities account structure and/or account naming conventions at either the CSD or local custodian?

CSD

☐ Yes

☑ No

If yes, provide details.

N/A

Local custodian

☐ Yes

☐ No

If yes, provide details.

N/A

2.3.2 Please advise on the following:

Are your clients' assets held in an account at the CSD entitled "Clients" or in the name of the client?

☑ Yes

☐ No

☐ N/A

Are your clients' assets segregated at the CSD from your proprietary holdings?

☑ Yes

☐ No

☐ N/A

Are your clients' assets held at the CSD in a different nominee name to your proprietary assets (including those of affiliates)?

☑ Yes

☐ No

☐ N/A

If no to any of the above, provide details.

N/A

2.3.3 For functions performed by a CSD(s) in the market, can you confirm that in the event of any errors by the CSD, you will pursue a claim on our behalf?

☐ Yes

☐ No

Comments:

N/A

2.3.4 Does the CSD have any right of lien, retention or sale over client assets that you hold in safe custody?

☐ Yes

☑ No

If yes, specify under which circumstances.

N/A

2.3.5 Please confirm that you would notify us of any changes in respect of the CSD and its right of lien, retention or sale over our assets that you hold in safe custody?

☑ Yes

☐ No

Comments:

We confirm.

2.3.6 In the last 12 months have there been any changes to your relationship with any delegate or sub-custodian that would change their rights to offset balances or which affect their lien over our cash and securities accounts?

☐ Yes

☑ No

If yes, please provide details.

N/A

2.3.7 In the last 12 months have you identified any changes to the CSD's terms and conditions and/or rulebook that increased the risks for you as a member and/or your clients?

☐ Yes

☑ No

If yes, provide details.

N/A

2.3.8 Do you perform a risk assessment and/or an operational due diligence review of the CSD (or equivalent infrastructure) to identify risks for you as a member and your clients on an annual basis?

☑ Yes

☐ No

If no, please advise why not.

N/A

Were there any areas of material concern noted as part of your most recent review?

☐ Yes

☑ No

If yes, provide details.

N/A

2.3.9 In the last 12 months, have there been any regulatory actions/adverse findings against the CSD?

- [ ] Yes
- [x] No

If yes, provide details.

N/A

2.3.10 How do you ensure sufficient liquidity for your obligations at the CSD?

- [ ] Cash Funding
- [ ] Collateral
- [ ] Self-Collateralisation
- [x] Other (please advise)

Comments:

N/A we are the CSD

2.3.11 In the last 12 months have there been any changes to the settlement methodology used by the CSD?

- [ ] Yes
- [x] No

If yes, provide details.

N/A

2.4 Control and reconciliation

2.4.1 Please confirm that neither you nor your affiliates will transfer securities in the absence of an instruction from us.

☑ Yes

☐ No

Comments:

N/A

2.4.2 Please confirm that you would notify us prior to making any changes that were not initiated by our instruction to the numbers or titles of our accounts in your books or at the CSD.

☑ Yes

☐ No

Comments:

SDX does not make any changes that were not initiated by an instruction sent by yourselves. Please consider that our of a corporate action the numbers or titles could change but this would always be notified.

2.4.3 Please confirm your organisation has adequate procedures and controls to prevent brokers/third parties accessing clients' CSD holdings directly.

☑ Yes

☐ No

Comments:

We only maintain a contractual relationship with our direct clients (Business Partners). Therefore, the account set up and access rights are only related to these direct clients. Hence, third parties/indirect clients have no access.

2.4.4 Where assets are being held in any of your nominee companies, please provide evidence that these and any new nominee companies are owned and controlled by you. Suitable evidence is in the form of extracts from financial statements, directors' reports or other forms of official company documentation.

Please attach file here:

(No file attached)

Comments:

Please note that SDX does not maintain a nominee company.

2.4.5 In the last 12 months, have there been any changes to your measures to minimise the risk of loss or diminution of financial instruments or of rights in connection with those instruments in case of abuse, fraud, inadequate administration, improper record keeping or negligence?

☐ Yes

☑ No

Comments:

N/A

2.4.6 Please confirm that you would advise us as soon as you became aware of any loss of securities.

☑ Yes

☐ No

If no, please explain.

N/A

2.4.7 Please confirm the frequency and automation of reconciliation of securities and cash balances to the following entities.

	Securities		Cash	
	(Frequency of reconciliation)	Automation	(Frequency of reconciliation)	Automation
CSD (Balance)	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A
CSD (Transaction)	Intraday	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A	Intraday	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A
Central Bank (Balance)	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A
Central Bank (Transactions)	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A	Daily	☑ Fully automated ☐ Semi automated ☐ Manual ☐ N/A
Registrar (Balance)	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A
Registrar (Transactions)	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A	N/A	
Delegated Sub-Custodians (Balance)	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A	N/A	

Delegated Sub-Custodians (Transactions)	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A
Transfer Agents	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A	N/A	☐ Fully automated ☐ Semi automated ☐ Manual ☑ N/A

Where manual intervention is required, describe the entity and process.

N/A; in the Swiss market, reconciliation is performed by the participants themselves since SDX is the CSD in Switzerland. In foreign markets, nostro reconciliation for cash and securities is performed daily and is highly automated, based on the receipt of SWIFT MT940/50 (cash) and MT535/536 (securities) from custodians.

2.4.8 In the last 12 months, have there been any changes to your reconciliation processes or procedures used when a discrepancy is identified?

☐ Yes

☑ No

If yes, provide details.

N/A

2.4.9 Do you have a tracking process for aged discrepancies (e.g. standardised thresholds, Key Performance Indicators (KPIs))?

☑ Yes

☐ No

Comments:

Positions that are not confirmed are pro-actively followed up with the respective Operations teams. Differences in positions are investigated through to resolution. A stringent control system is in place to ensure that aged differences are given appropriate management attention.

2.4.10 In the last 12 months, have there been any changes to the way your system records if securities are held in custody but are unavailable for delivery? (e.g. due to being out for transfer or splitting, being used for collateral or lending, stopped for any other reasons).

Transfer

☐ Yes

☑ No

If yes, provide details.

N/A

Splitting

☐ Yes

☐ No

If yes, provide details.

N/A

Collateral

☐ Yes

☐ No

If yes, provide details.

N/A

Lending

☐ Yes

☐ No

If yes, provide details.

N/A

Other

☐ Yes

☑ No

If yes, provide details.

N/A

2.4.11 In the last 12 months has the number of unreconciled items increased by more than 10% for any of the following:

Securities balances

☐ Yes

☑ No

If yes, provide details.

N/A

Cash balances

☐ Yes

☑ No

If yes, provide details.

N/A

Securities transactions

☐ Yes

☑ No

If yes, provide details.

N/A

Cash transactions

☐ Yes

☑ No

If yes, provide details.

N/A

2.4.12 In the last 12 months have there been any changes or enhancements regarding the process for reconciliation of breaks or outstanding items?

☐ Yes

☑ No

If yes, provide details.

N/A

2.5 Physical holdings (answer if applicable)

2.5.1 If physical securities exist in the market, please complete this section (2.5). If not, please tick the 'Not applicable' box below and move to section 2.6.

☑ N/A

2.5.2 Please confirm that your vault security features include the following:

☐ Security guards

☐ 24-hour closed-circuit camera surveillance

☐ Dual control over all activities

☐ Monitoring of access via a log book

☐ Alarms

☐ Panic buttons

☐ Movement detectors

☐ Timed locks

☐ Fire suppression systems

☐ Flood control systems

Please list any additional features:

N/A

2.5.3 Please state the location of the vault (e.g. is it in the same building as your securities services operations, which floor is it located on)?

N/A

2.5.4 Do you have procedures and controls for the physical transportation of securities?

☐ Yes

☐ No

If no, please explain why.

N/A

2.5.5 Has there been any changes to these procedures in the past 12 months?

☐ Yes

☐ No

If yes, provide details.

N/A

2.5.6 Has there been an internal audit in the last 12 months?

☐ Yes

☐ No

Comments:

N/A

2.5.7 Were there any exceptions noted?

☐ Yes

☐ No

If yes, provide details.

N/A

2.5.8 Has there been an external audit in the last 12 months?

☐ Yes

☐ No

Comments:

N/A

2.5.9 Were there any exceptions noted?

☐ Yes

☐ No

If yes, provide details.

N/A

2.5.10 Do you outsource the safekeeping of physical assets?

☐ Yes

☐ No

If yes, provide details.

N/A

2.5.11 Please confirm that there are dual controls in place for all physical security management (e.g. delivery of physical securities).

☐ Yes

☐ No

If no, please explain why.

2.5.12 Please confirm that there is a segregation of duties between the maintenance of physical custody records and their reconciliation.

☐ Yes

☐ No

If no, please explain why.

2.5.13 Please outline how client assets are segregated within the vault from your organisation's and other clients' assets.

N/A

2.5.14 Please advise in which entity's name physical securities are registered, where applicable.

N/A

2.5.15 Please outline how you record bearer instruments in your books and records so that you know who the beneficial owner is.

N/A

2.5.16 At what capacity is your vault currently operating?

N/A

2.5.17 How do you monitor vault capacity levels?

N/A

2.5.18 Please outline your Business Continuity Plan (BCP) should the operation of your vault become impaired.

N/A

2.5.19 How frequently are physical securities counted and reconciled to your records?

☐ Quarterly

☐ Semi annually

☐ Annually

☐ Other (please specify)

2.5.20 Do your procedures include how exceptions are investigated, reported and escalated and corrected?

☐ Yes

☐ No

If not, please explain why.

N/A

2.5.21 Do you reconcile registered physical securities to registrar's records at least once every six months?

☐ Yes

☐ No

If not, please advise the scope and frequency of vault counts.

N/A

2.5.22 Do local rules and regulations stipulate how frequently you are required to perform vault reconciliations?

☐ Yes

☐ No

If yes, please advise the frequency.

☐ Quarterly

☐ Semi annually

☐ Annually

☐ Other

If other, please specify.

N/A

2.5.23 Do local rules and regulations stipulate how frequently you are required to perform reconciliations against registrar records?

☐ Yes

☐ No

If yes, please advise how often.

☐ Quarterly

☐ Semi annually

☐ Annually

☐ Other

If other, please specify.

N/A

2.6 Building Security

2.6.1 Please confirm which of these applies to the security on your premises.

☑ 24-hour security coverage

☑ External security personnel

☑ Internal security personnel

☑ Armed security personnel

☑ Building entry security clearance and ID if required

☑ Physical entry barriers

☑ Restricted access ID cards for all staff and visitors

☑ Security cameras

☑ Alarms to detect unauthorised entry

☑ Alarms to detect smoke

☑ Alarms to detect heat and fire

☑ Alarms to detect flooding

If security is not provided on a 24-hour basis, provide details of arrangements in place.

N/A

2.6.2 Are all staff, visitors and vendors properly identified, required to sign in, and wear badges?

☑ Yes

☐ No

Comments:

The management of physical access is an essential part of integral security across SIX. In regular audits, compliance with the guidelines, which are coordinated with the Physical Security Officer, are checked. Videotaping and recording of access data are archived under consideration of the data privacy act. Access is restricted to authorized personnel. A personal security code in addition to the ID badge is needed to enter or leave a building before 7am and after 6pm as well as on weekends. Moreover, SIX has secured areas and these zones are subject to the strictest security measures.

2.6.3 Are all visitors and vendors supervised whilst on the premises?

☑ Yes

☐ No

Comments:

N/A

2.6.4 Is data centre access limited to employees with appropriate job responsibilities?

☑ Yes

☐ No

Comments:

N/A

3 Risk mitigation

In scope services: custody services (with or without a sub-custodian) and, if applicable, client money services.

3.1 Operational controls

3.1.1 Do you maintain written operational controls and procedures for all custody operations and banking functions?

☑ Yes

☐ No

Comments:

SIX Digital Exchange (CSD) and SDX Web3 Ltd has a internal control system in place covering the same high quality standards as SIX Group.

SDX Risk Management follows SIX standardized risk management process (identify, assess, manage, monitor and report) to help analyze and appropriately aggregate risks and report to target audience.

3.1.2 How frequently are the operational controls and procedures reviewed/updated and by whom?

Review

Annually

Reviewed by:

Operational controls and procedures are reviewed/updated annually by authors and owners representing the 1st line of defense (LoD) business or when underlying controls/processes changes.

In the last 12 months have there been material changes to your operational controls and procedures?

☐ Yes

☑ No

If yes, provide details.

N/A

3.1.3 In the last 12 months has your local regulator raised any concerns in relation to your operational controls and procedures?

☐ Yes

☑ No

If yes, provide details.

N/A

3.1.4 Are unique user names and passwords used for internal and external systems?

☑ Yes

☐ No

If yes, please state the frequency of change of passwords.

All privileged interactive accounts are personal and so can be traced. Associated access privileges are defined with user IDs and redundant user IDs are not re-issued for use. Access rights are reported and must be reviewed four times a year.

3.2 Risk management

3.2.1 Do you have an independent risk management function in your organisation?

☐ Yes

☑ No

If yes, please provide an organisation chart showing (or explain) where risk management resides within your organisation including reporting lines, roles and responsibility for the management of risk, oversight breaches and remediation in relation to securities services or client money.

(No file attached)

N/A

3.2.2 Do you use Risk and Control Self-Assessment (RCSA)?

☑ Yes

☐ No

If you use RCSA, please confirm a risk assessment is carried out for custody and specify the frequency.

Custody

☑ Yes

☐ No

☐ N/A

Frequency

☐ Monthly

☐ Quarterly

☐ Biannually

☑ Annually

☐ Ad-hoc

If no, please explain why.

N/A

If you use RCSA, please confirm a risk assessment is carried out for client money and specify the frequency.

Client Money

☑ Yes

☐ No

☐ N/A

Frequency

☐ Monthly

☐ Quarterly

☐ Biannually

☑ Annually

☐ Ad-hoc

If no, please explain why.

N/A

3.3 Audit

3.3.1 Who are your external auditors responsible for operational audit?

Ernst & Young

3.3.2 Please confirm if you have within your internal audit function staff dedicated to your custody and/or client money operations.

Custody

☑ Yes

☐ No

☐ N/A

If yes, provide details.

The Internal Audit function of SIX conducts audits according to IIA standards. It conducts operational and financial audits in all focus areas in accordance with the yearly risk assessment. The annual plan is coordinated with Ernst & Young and submitted to the Audit Committee of the Board of Directors for approval. The independence of the Audit function is assured by the functional reporting line directly to the Audit Committee and the administrative reporting line to the Chairman of the Board of Directors. Internal Audit reports are also distributed to Ernst & Young on behalf of the Swiss authorities.

Client money

☑ Yes

☐ No

☐ N/A

If yes, provide details.

The Internal Audit function of SIX conducts audits according to IIA standards. It conducts operational and financial audits in all focus areas in accordance with the yearly risk assessment. The annual plan is coordinated with Ernst & Young and submitted to the Audit Committee of the Board of Directors for approval. The independence of the Audit function is assured by the functional reporting line directly to the Audit Committee and the administrative reporting line to the Chairman of the Board of Directors. Internal Audit reports are also distributed to Ernst & Young on behalf of the Swiss authorities.

3.3.3 Please provide an overview or (as an attachment) a diagram showing where your internal audit function resides and who it reports to.

Attachment:

Internal Audit.pdf (93.6 Kb)

Comments:

N/A

3.3.4 Do any supervisory regulations apply to the design of your internal audit function?

☑ Yes

☐ No

If yes, provide details.

The internal audit function is in accordance with the requirements of the Financial Market Infrastructure Act (FMIA) and was confirmed by the supervisory authority (FINMA) as part of the licensing procedure. The internal audit function complies with the requirements of FINMA Circular 2017/01 and is assessed annually as part of the supervisory audit. Internal Audit follows the IPPF Standards as required by FINMA including defined process controls, self-assessments, and independent reviews of the audit function.

3.3.5 Do your regulators review your internal procedures?

☑ Yes

☐ No

If yes, how frequently?

SDX is subject to annual reviews, mandated by FINMA and conducted by Ernst & Young.

3.3.6 How frequently are your custody operations audited by your internal auditors? Please provide the date of the last internal audits.

Frequency	Date	Type
☐ 6 months ☐ 12 months ☐ 18 months ☐ 24 months ☑ Other (specify):	Ongoing; this is meant to be a permanent process where our Internal Audit, according to its audit plan, which was agreed on in the Audit Committee, assesses all departments on a frequent basis.	Business audit: organizational structure is appropriately designed, the processes are carried out properly and the internal control system is adequately designed and operating effectively.

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

Comments:

Internal audits are being done frequently over the year according to the yearly audit plan. The Internal Audit team performs those regular audits and quality controls on custody operations, reviews operational processes and supervises reconciliations. This includes in-depth checks on certain business areas on an ad-hoc basis while critical business areas are audited on an regular basis. The findings of such checks are reported to the Executive Committee and to the Audit Committee of the Board of Directors of SIX Group but are not made available to third parties. Internal Audit is auditing custody businesses throughout the year according to the IIA standards. The audits generally cover the last twelve months on a sample basis.

3.3.7 How frequently are your custody operations audited by your external auditors? Please provide the date of the last external audits.

Frequency	Date	Type
☐ 6 months ☑ 12 months ☐ 18 months ☐ 24 months ☐ Other (specify):	29th April 2025	Regulatory Audit

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

Please attach a copy of the last audit report from your external auditors.

(No file attached)

Comments:

SDX treats audit reports confidential and does not share any details.

3.3.8 How frequently are your custody operations audited by your market regulators? Please provide the date of the last market regulators audits.

Frequency	Date	Type
☐ 6 months ☑ 12 months ☐ 18 months ☐ 24 months ☐ Other (specify):	1st January 2024 to 31st December 2024	Regulatory Audit

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

Comments:

SDX treats audit reports confidential and does not share any details.

3.3.9 How frequently are your custody operations audited by your Central Bank? Please provide the date of the last Central Bank audits.

Frequency	Date	Type
☐ 6 months ☐ 12 months ☐ 18 months ☐ 24 months ☐ Other (specify):		

Has this frequency changed in the last 12 months?

☐ Yes

☐ No

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

Comments:

3.3.10 How frequently are your client money operations audited by your internal auditors? Please provide the date of the last internal audits.

Frequency	Date	Type
☐ 6 months ☐ 12 months ☐ 18 months ☐ 24 months ☑ Other (specify):	Ongoing; this is meant to be a permanent process where our Internal Audit, according to its audit plan, which was agreed on in the Audit Committee, assesses all departments on a frequent basis.	Internal audits are being done frequently over the year according to the yearly audit plan. The Internal Audit team performs those regular audits and quality controls on custody operations, reviews operational processes and supervises reconciliations.

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

☐ N/A

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

N/A

Comments:

SDX treats audit reports confidential and does not share any details.

3.3.11 How frequently are your client money operations audited by your external auditors? Please provide the date of the last external audits

Frequency	Date	Type
☐ 6 months ☑ 12 months ☐ 18 months ☐ 24 months ☐ Other (specify):	29th April 2025	Regulatory Audit

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

☐ N/A

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

N/A

Please attach a copy of the last audit report from your external auditors.

(No file attached)

Comments:

SDX treats audit reports confidential and does not share any details.

3.3.12 How frequently are your client money operations audited by your market regulators?

Please provide the date of the last market regulators audits.

Frequency	Date	Type
☐ 6 months ☑ 12 months ☐ 18 months ☐ 24 months ☐ Other (specify):	1st January 2024 to 31st December 2024.	Regulatory Audit

Has this frequency changed in the last 12 months?

☐ Yes

☑ No

☐ N/A

If yes, please provide details.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

N/A

If frequency is greater than 24 months, please advise next anticipated audit date below.

N/A

Comments:

SDX treats audit reports confidential and does not share any details.

3.3.13 How frequently are your client money operations audited by your Central Bank? Please provide the date of the last Central Bank audits.

Frequency	Date	Type
☐ 6 months ☐ 12 months ☐ 18 months ☐ 24 months ☑ N/A		

Has this frequency changed in the last 12 months?

☐ Yes

☐ No

☑ N/A

If yes, please provide details.

If frequency is greater than 24 months, please advise next anticipated audit date below.

Comments:

3.3.14 Do you prepare assurance reports to prove internal control operations and procedures are efficient, effective, robust and satisfy their control objectives?

☐ Yes

☑ No

If yes, provide a copy of the report.

(No file attached)

Comments:

N/A

3.3.15 Please highlight any concerns raised in any of the above audits together with actions to remediate these points.

Comments:

EY did not report any significant audit issues in 2024. They confirmed appropriate business conduct, adequacy of risk management and effectiveness of internal control system.

Please attach file here:

(No file attached)

3.3.16 Please confirm that follow-up procedures exist to ensure that internal/external audit or regulatory audit recommendations are implemented.

☑ Yes

☐ No

Comments:

Mitigating measures are captured and tracked in the internal control system.

3.3.17 Are there any recommendations that have not been implemented?

☐ Yes

☑ No

If yes, provide details.

N/A

3.3.18 Are all key operating procedures and escalation procedures clearly documented and shared with relevant staff?

☑ Yes

☐ No

Comments:

SIX Digital Exchange maintains a comprehensive operational risk management system (ERM Tool) to manage operational risks as well as to ensure compliance with internal processes, controls, and regulatory requirements.

3.3.19 Do your external auditors verify that assets held by you are in your custody and control?

☑ Yes

☐ No

If no, provide details.

N/A

3.3.20 In the past 12 months, please confirm that such external audits have taken place in respect of assets recorded in your books and are reconciled with the Central Securities Depository / Registrar or any other sub-custodian?

☑ Yes

☐ No

Comments:

N/A

3.4 IT Disaster recovery (systems and data)

3.4.1 Please confirm that you have disaster recovery plans (DRP).

☑ Yes

☐ No

Comments:

Datacenter failover, backup and restore recovery plans exist on all productive platforms which are tested annually.

3.4.2 In the last 12 months have there been any material changes to these plans?

☐ Yes

☑ No

If yes, provide details.

N/A

3.4.3 Are these plans reviewed by your regulator?

☐ Yes

☑ No

Comments:

N/A

3.4.4 Who within your organisation has oversight over your DRP?

SDX BCM Manager

3.4.5 Who has authority to activate your DRP?

Head of IT Operations

3.4.6 How often is your DRP tested? What was the date of the last test?

☐ 6 months

☑ 12 months

☐ 18 months

☐ 24 months

☐ Other (Specify:)

Date of last test (DD/MM/YYYY)

23/09/2023

3.4.7 Was the last DRP test successful?

☑ Yes

☐ No

If not, please describe items that require remediation and confirm that a remediation plan is in place.

3.4.8 Is your DRP testing live and/or simulated?

☑ Live

☐ Simulated

☐ Both

Comments:

For DR tests we replicate scenarios that would arise that would require DRP plans to be executed in full. We must be certain that these plans work in full thus the need for live testing on productive systems outside of business hours.

3.4.9 Does the DRP testing include financial market infrastructures?

☑ Yes

☐ No

Comments:

We test the DR capabilities of the full production systems necessary for all business services.

3.4.10 Does the DRP testing include other third parties?

☑ Yes

☐ No

Comments:

All SDX clients are informed about DRP tests and can participate in respective validations steps.

3.4.11 Please confirm that testing replicates a full business day.

☑ Yes

☐ No

Comments:

The end to end DR testing executed in conjunction with SIX requires a full business day to execute, validate and reset back to pretest status. Thus its always executed on a Saturday.

3.4.12 Are the results of the DRP test audited by internal or external auditors?

☐ Yes, internal

☐ Yes, external

☑ Yes, both (internal and external)

☐ No

If yes, provide a copy of the reports.

(No file attached)

Comments:

The documentation of the Business Continuity Tests are classified as Confidential and cannot be shared with externals.

3.4.13 How do you monitor gaps from these findings and ensure action is taken to remediate these issues?

The normal Software Development Lifecycle in leveraged. We record gaps found during a test in JIRA tickets which gets sent to SDX Engineering for full resolution and testing before being deployed into production to resolve the gap.

3.4.14 How and when would clients be advised in the event of a disaster?

Email or phone

3.4.15 In a disaster event, how soon do you commit to reconstituting your system/parallel system?

- ☐ Within 1 hour
- ☑ Within 4 hours
- ☐ Within 12 hours
- ☐ Within 24 hours
- ☐ More than 24 hours

Comments:

Client side SLA's commit to 4 hours.

3.4.16 In a disaster event, how soon are you able to revert to normal business operations?

- ☐ Within 1 hour
- ☑ Within 4 hours
- ☐ Within 12 hours

☐ Within 24 hours

☐ More than 24 hours

Comments:

Due to system enhancements recent testing in lower environment has demonstrated RTA of 55 minutes for a full system recovery. These system improvements will be officially tested in production on 24/05/2024.

3.4.17 Have you tested your capability to meet your Recovery Time Objective within the last 12 months?

☐ Yes

☐ No

If yes, what was the outcome?

3.4.18 Are there any limitations to your system capabilities whilst in DR mode?

☐ Yes

☑ No

If yes, provide details.

N/A

3.4.19 Do you back up your data in real time?

☐ Yes

☑ No

If no, how often is data backed up?

☐ Mirrored with delay

☑ Daily

☐ Weekly

☐ Other

Comments:

All productive system are backed up outside of business hours daily.

3.4.20 In the last 12 months have you invoked your DRP?

☐ Yes

☑ No

If yes, provide details.

N/A

3.4.21 Did the results comply with your plan?

☐ Yes

☐ No

☑ N/A

Comments:

N/A

3.4.22 How far apart are your primary and secondary processing hardware located?

Distance ( )km

27.3km

3.4.23 Are your primary and secondary processing hardware located in the same power grid?

☐ Yes

☑ No

Comments:

This was one of the key criteria for the choice of SIX's new secondary Datacenter location which was decided together with SNB in 2015.

3.4.24 If your primary and secondary processing hardware are located in the same power grid, how do you mitigate this risk?

N/A

3.4.25 Do you operate a "hot" disaster recovery site?

☑ Yes

☐ No

Comments:

N/A

3.4.26 Are backup systems available at the primary data centre?

☑ Yes

☐ No

Comments:

SDX leverage SIX tooling and services (Velero and Nettapp) for all our productive backup and restore capabilities.

3.4.27 If the primary lines of communication between your primary data centre and the back-up site fail, what contingency measures are in place?

There are two independent connectivity lines operating and in place between both data centers.

3.5 Cybersecurity

3.5.1 Does your organisation have a documented cybersecurity policy in place?

☑ Yes

☐ No

If yes, provide a copy or overview.

six-brochure-corp-security-en.pdf (4 Mb)

Comments:

SIX Group (including SDX) has a Security Policy framework in place including cyber security. The security policies cover all relevant areas like security governance, risk assessment, access control, data classification and protection, system hardening and vulnerability management, incident response, awareness, and training. We run our cyber resilience framework based on the standards published by the Information Security Forum (ISF) and use as basis the Standard of Good Practice for Information Security. For reasons of confidentiality, please note that our policies are for internal use only and cannot be shared. Please take a look at our attachment SIX Group (including SDX) "six-corporate-security-brochure-en" likewise.

SIX Group (including SDX) established a Security Operations Center (SOC) that provides cyber-security services by elaborating cybersecurity insights derived from a library of over one million known threats. The SOC has access to the latest security tools and is a leading defender against cybercrime. Hence, the SOC is a specialized cyber security competence centre which works 24/7, monitors infrastructures, applications, suspicious behaviours, and data centrally and searches for indicators of cyber-attacks. It arms security analysts with the collective knowledge and instinct needed to respond to threats with greater confidence, with speed and scale. Additionally, our Cyber Security Hub provides banks and insurance companies with reliable and relevant information on current risks and dangerous developments in the cyber security area. SIX Group (including SDX) has set up a closed community for financial institutions in Swit-

zerland around cyber security matters. Community members regularly exchange information and receive insights from their peers and our experts.

3.5.2 Please confirm that your staff receive relevant training about this policy.

☑ Yes

☐ No

Comments:

Our staff receives ongoing training and instructions about cyber security and the respective threats. Annual mandatory training sessions on security awareness, phishing, data privacy and other topics are held for all employees, including the top management.

3.5.3 Please provide an overview of your policy for continuity of business in the event of a large data breach or cyber-attack against your organisation.

The cyber security incident response process follows the standard IT security incident process. SIX protects against zero-day attacks using defence in depth, security monitoring and analysis strategies as well as specific prevention measures for critical assets. A SIRT (Security Incident Response Team) organization is in place in order to ensure that cyber threats are detected in a timely manner and patches are implemented accordingly. The defence in depth strategy consists of various policies, methods and technologies implemented to protect sensitive information at-rest, in-transit, and in-use. The following measures support the prevention and detection of such information: data classification policies, access management according to the “need-to-know” principle, endpoint security including the encryption of mobile devices and blocking of removable media, blocking of access to web-based cloud services as well as e-mail content filtering and encryption.

3.5.4 In the last 12 months have there been any changes to the policy?

☐ Yes

☑ No

If yes, provide details.

N/A

3.5.5 How often do you review the policy?

☐ Semi-annually

☑ Annually

☐ Other (please specify):

Comments:

Our Security Policy is reviewed periodically but at least on a yearly basis.

3.5.6 Please provide (as an attachment) a diagram showing where your cybersecurity function resides and who it reports to.

Please attach file here:

six-corporate-security-brochure-en.pdf (5 Mb)

Comments:

Our Cyber Defense group resides in the Infrastructure & Operations department which is part of the IT organization. The Head of Infrastructure & Operations is responsible for Cyber Security and reports directly to the Chief Information Officer.

3.5.7 How does your organisation identify which business functions carry a cyber risk?

SIX has worked out Business Impact Analyses (BIA) for business units and corporate functions. Criticality is determined for every business process and relevant interdependencies are identified. The security structure is based on the ISF (Information Security Forum) Standard of Good

Practice for Information Security and is aligned with the NIST (National Institute of Standards and Technology) Cyber Security Framework. SIX conducts regular cyber risk and control assessments. In addition, SIX established an automated vulnerability scanning system, which alerts detected vulnerabilities in the Security Information and Event Management (SIEM) system of the 7x24h Security Operations Center (SOC). Several monitoring tools are in place like Intrusion Detection System (IDS), log monitoring, web applications firewalls, antivirus on the client and server side as well as vulnerability scans and a Data Leakage Prevention (DLP) program.

3.5.8 Do you conduct ongoing testing and monitoring processes to ensure that all internal and external connectivity and system configurations are not at risk of cybersecurity breaches?

☑ Yes

☐ No

If yes, provide details and indicate frequency.

Please refer to the following types of cyber-risk testing and their frequency:

- Penetration testing is conducted on a yearly basis for web facing applications
- Vulnerability scans are applied on a monthly basis
- Malware scans exist for all files leaving and entering the SIX network as well as on access for critical data and on servers
- Intrusion detection occurs between zones

3.5.9 What technological controls and protections are in place for your systems and networks?

Please also refer to our response to question 3.5.8. There are several protective controls in place such as:

- Controls as part of our Internal Controls System (ICS)
- Network architecture based on different zones, protected against each other, DMZ etc.
- Web Entry Server at the entrance points

- Encryption of critical data
- Digital signatures for massages exchanged with our clients
- Filtering of incoming traffic

Our security posture is based on the ISF control framework and is aligned with the NIST Cyber Security Framework. We conduct regular cyber risk and control assessments resulting in the need of additional mitigation measures and a continuous improvement.

Additional technological controls such as IDS/IPS, SIEM, DLP, DDoS Protection are in place.

3.5.10 Does your organisation use multi-factor authentication?

☑ Yes

☐ No

Comments:

We use a 2-factor authentication using biometric and MFA Authenticator App.

3.5.11 Where your organisation has outsourced activities or functions to a third-party provider, is your cyber risk exposure documented?

☑ Yes

☐ No

Comments:

Please note that SIX has not outsourced any activities or functions to a third-party provider. In contrast, we maintain our own Security Operations Center (SOC) to protect ourselves against cyber-attacks. Our practices are aligned with the National Institute of Standards and Technology (NIST) Cyber Security Framework. For cyber threats including malware or DDoS attacks, SIX has implemented protection and detection measures and is maintaining and developing solutions to respond and recover. Continuous improvements are implemented along the SIX Information Security Strategy.

3.5.12 What measures does your organisation have to ensure early detection of a cyber-attack?

SIX protects against zero-day attacks using defence in depth, security monitoring and analysis strategies as well as specific prevention measures for critical assets. A SIRT (Security Incident Response Team) organization is in place in order to ensure that cyber threats are detected in a timely manner and patches are implemented accordingly. A Security Board supervises IT security with a cyber-security monitoring team working around the clock. The Security Operations Center (SOC) is a specialized cyber security competence centre which works 24/7, monitors infrastructures, applications, suspicious behaviours, and data centrally and searches for indicators of cyber-attacks.

There are several measures in place:

- Network architecture; intrusion detection with monitoring at the zone boundaries including neuralgic points insides the zones protecting against each other, DMZ etc.
- Web Entry Server at the entrance points
- Encryption of critical data
- Digital signatures for massages exchanged with our clients
- Filtering of incoming traffic
- Log Monitoring
- Web Application Firewall
- Antivirus on client and server side
- Vulnerability scanning
- Firewalls

3.5.13 What is the agreed resumption time for critical operations following a cyber-attack?

Our business functions and processes are subject to ongoing risk assessments in terms of criticality and availabilty requiurements.

The different services offered by SIX Group (including SDX) are classified in terms of business-critical criteria (i.e., availability requirement, service level agreements). This classification serves as the basis for the respective RPO and RTO.

3.5.14 How would you advise clients of a successful cyber-attack against your organisation?

We would urgently advice our clients according to our crisis management plans and policies. Please note that we have not had any system security breaches recently.

3.5.15 In the last 12 months has your organisation been subject to a cyber-attack that impacted the service you provide to us?

☐ Yes

☑ No

If yes, provide details.

Standard attacks on our infrastructure occur daily. These are detected and handled by our security systems. From time to time we encounter broader (D)DOS attacks which have not a had big impact in the past, also due to different communication services providers and their measures. All incidents are handled by the 24x7 incident response organization and processes. The cyber security incident response process follows the standard IT Security incident process established at SIX. Processes for the identification, treatment and escalation of IT Security incidents are implemented.

3.5.16 Are the following elements of your cybersecurity framework tested pre and post deployment of changes?

☑ Vulnerability assessment

☑ Scenario based penetration tests

☑ Testing of incident response process and technical/business/operations (e.g. table-top exercise)

☑ Other (please describe in comments):

Comments:

Our security structure is based on the ISF Standard of Good Practice and is aligned with the NIST Cyber Security Framework. SIX conducts regular cyber risk and control assessments. All monitoring tools like IDS, log monitoring, penetration tests, web applications firewalls, antivirus on the client and server side as well as vulnerability scans are in place and tested prior to and after being employed.

3.5.17 Does your organisation use a cloud service provider(s)?

☑ Yes

☐ No

If no, please advise if you are planning to move to a cloud service provider.

☐ Yes

☐ No

3.5.18 When utilising cloud technology, do you have appropriate controls in place, including those to protect our information from cybersecurity risks, such as mishandling and theft?

☑ Yes

☐ No

☐ N/A

If yes, do these procedures and controls adhere to your record retention policy?

☑ Yes

☐ No

☐ N/A

If no, provide further information.

N/A

3.5.19 Does your organisation conduct dark web searches for signs of a breach (e.g., internet protocol or customer/client personally identified information for sale)?

☑ Yes

☐ No

Comments:

Our Cyber Security team conducts active dark web searches and looks for signs of a breaches. We search for key words, SIX assets, threat actors who plan any campaigns again the Swiss financial center and we do also receive threat intelligence reports in order to counter any threats. We have rapid, safe, extensive access to illicit communities including closed, invite-only, and password-protected sources, as well as paste sites, technical data, stolen credentials, and social media sites exploited by threat actors. We are also able to engage directly with threat-actors on behalf of CTI (Cyber Threat Intelligence) teams when necessary.

Subject matter experts (SMEs) produce Finished Intelligence daily on the latest threats, trends, events, and research findings relevant to CTI teams. Reporting includes expert context and analysis to help teams reduce alert fatigue and more effectively identify and mitigate imminent or existing cyber threats to their organizations.

Our community serves as an extension of customers' teams. FPCollab, an information-sharing group for SMEs and customers, includes leading CTI experts who frequently collaborate, share critical insights, and give and receive support within this community.

3.5.20 Does your organisation comply with SWIFT's Customer Security Program controls?

☑ Yes

☐ No

Comments:

We comply with the SWIFT CSP controls and have the controls assessed by an independent external assessor.

3.5.21 Does your organisation respond to requests for your attestations?

☑ Yes

☐ No

Comments:

We have established a corresponding process to respond to these requests. We provide our attestation to a third party only when it maintains a business relationship with SDX.

3.5.22 Does your organisation request the attestations of your counterparties and incorporate the responses into ongoing relationship and risk management programs?

☑ Yes

☐ No

Comments:

Whenever SDX receives a request for attestation as outlined in response to question 3.5.18, we therefore ask for the attestation details of our counterparty too.

3.6 Business Continuity Programme (BCP) (Operations and Premises)

3.6.1 Please confirm that you have a BCP, including alternate offices, power, communications and all necessary facilities.

☑ Yes

☐ No

Comments:

N/A

3.6.2 In the last 12 months have there been any material changes to the BCP?

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

3.6.3 Is your organisation compliant with all current regulatory requirements for BCP in each of the countries where you provide securities services and/or client money services?

☑ Yes

☐ No

Comments:

N/A

3.6.4 Who within your organisation has oversight and control over the BCP?

Head Crisis, BCM & Physical Security

3.6.5 Who has authority to activate your BCP?

Every BCM Responsible of the Business Unit and Legal Entity

3.6.6 How often is your BCP tested? What was the date of the last test?

☐ 6 months

☑ 12 months

☐ 18 months

☐ 24 months

☐ Other (Specify below)

Date of last test (DD/MM/YYYY):

Usually every 12 months, at least once in a calendar year.

24.05.2024 (IT Disaster Recovery Test SIX Digital Exchange AG)

13.12.2024 (Emergency Board Exercise Swiss Value Chain)

3.6.7 Is testing completed during business hours?

☐ Yes

☑ No

Comments:

IT Service Continuity Testing is performed outside business hours

Emergency Board Exercises without touching IT Infrastructure is tested during business hours

3.6.8 Was your last BCP test successful?

☑ Yes

☐ No

If no, describe items that required remediation and confirm that a remediation plan is in place.

N/A

3.6.9 Is your BCP testing conducted in a live and/or simulated environment?

☑ Live

☐ Simulated

☐ Both

Comments:

N/A

3.6.10 Does your BCP testing include Financial Market Infrastructures?

☑ Yes

☐ No

If yes, please provide details.

SIX Digital Exchange AG obtained a license as a Financial Market Infrastructure by FINMA.

3.6.11 Does your BCP testing include any other third parties?

☐ Yes

☑ No

If yes, please provide the names of the third parties.

N/A

3.6.12 Are the results of your BCP test audited by internal or external auditors?

☐ Yes, internal

☐ Yes, external

☑ Yes, both (internal and external)

☐ No

If yes, provide a copy of the report.

(No file attached)

Comments:

The documentation of the Business Continuity Tests are classified as Confidential and cannot be shared with externals.

3.6.13 How do you monitor gaps from these findings and ensure action is taken to remediate these issues?

SIX has established a yearly BCP lifecycle in which potential gaps are documented and the remediation is tracked by the Crisis, BCM and Physical Security Team.

3.6.14 How and when would clients be advised in the event of the BCP being activated in a live environment?

SDX Client Communication by E-Mail in case Service Disruption or Service degradation for customers is expected.

3.6.15 Following a BCP event, how soon are you able to revert to business as usual (BAU)?

- ☐ Within 1 hour
- ☑ Within 4 hours
- ☐ Within 12 hours
- ☐ Within 24 hours
- ☐ More than 24 hours

Comments:

Recovery Time Objective for Emergency Operation is 4 hours

3.6.16 Are there any limitations to your business capabilities whilst in BCP mode?

- ☐ Yes
- ☐ No

If yes, provide details.

Depends on the BCP Scenario

3.6.17 In the last 12 months have you invoked your BCP?

☐ Yes

☑ No

If yes, provide details.

3.6.18 If invoked, did the results comply with your plan?

☐ Yes

☐ No

☐ N/A

Comments:

N/A

3.6.19 For custody and/or client money, state the distance of the contingency site(s) from your primary location.

Custody

Distance ( )km

The primary and secondary locations are situated in different hazard zones according to the Swiss hazard.

Client money

Distance ( )km

The primary and secondary locations are situated in different hazard zones according to the Swiss hazard.

Comments:

N/A

3.6.20 Is the business contingency site a hot site?

☑ Yes

☐ No

Comments:

N/A

3.6.21 Is the business contingency site shared?

☑ Yes

☐ No

If yes, provide details.

SIX Group AG and its subsidiaries including SDX uses the same site.

3.6.22 Please specify the percentage of staff defined as critical to your business continuity arrangements.

☐ 100%

☐ 75-100%

☐ 50-75%

☑ 25-50%

☐ <25%

Comments:

N/A

3.6.23 Do critical staff have access to all necessary systems?

☑ Yes

☐ No

Comments:

N/A

3.6.24 Please confirm that your contingency site has all the necessary communications, linkages, infrastructure interfaces, work stations, hardware and systems applications to resume business operations.

☑ Yes

☐ No

Comments:

N/A

3.6.25 Please state how long you can continue to operate from the BCP site.

For an undefined period of time.

3.6.26 Is it possible for employees to access systems remotely (e.g. from home or other branches/ offices)?

☑ Yes

☐ No

Comments:

A few employees need physical access to the datacenters to operate the business.

3.6.27 Please confirm if an alternative means of communication is in place with the following.

Stock exchange

☐ Yes

☑ No

☐ N/A

If yes, which method is used?

N/A

Clients

☐ Yes

☑ No

☐ N/A

If yes, which method is used?

N/A

CSD

☐ Yes

☑ No

☐ N/A

If yes, which method is used?

N/A

Central Bank

☑ Yes

☐ No

☐ N/A

If yes, which method is used?

Satellite phone

Central Counterparty (CCP)

☐ Yes

☐ No

☐ N/A

If yes, which method is used?

N/A

Comments:

The following answers are targeting to the scenario Power Disruption where no traditional e-Mail / Phone and Websites are working.

3.6.28 What percentage of staff can work from home?

- ☐ 100%
- ☑ 75-100%
- ☐ 50-75%
- ☐ 25-50%
- ☐ <25%

Comments:

N/A

3.6.29 Are there any restrictions or exceptions to working from home within your organisation?

- ☑ Yes
- ☐ No

Comments:

Restrictions are applied for people who need physical access to on-premise infrastructure which is inaccessible from working from home.

3.6.30 Does your organisation have a dedicated pandemic plan?

- ☑ Yes
- ☐ No

If no, explain why.

N/A

3.6.31 Does your pandemic plan address any of the following?

☑ Track and monitor staff availability

☑ Reduce transmission amongst staff

☑ Return to work

☑ Mass absenteeism

Comments:

Measures in regards to the mass absenteeism are defined in the loss of staff scenario.

3.6.32 In the past 12 months has your pandemic plan been tested?

☐ Yes

☑ No

If yes, were there any areas of concern noted?

☐ Yes

☐ No

Comments:

N/A

3.6.33 During a pandemic, please confirm that your organisation can accept digital/electronic signing/scanning of legally binding and related documents?

☑ Yes

☐ No

☐ Other: Please specify

Comments:

N/A

3.6.34 During a pandemic, please advise if there are any known restrictions within the local market in accepting digital/electronic signing/scanning of legally binding and related documents?

☐ Legal

☐ Regulatory

☐ Taxation

☐ Financial Market Infrastructure

☐ Other

Comments:

N/A

3.6.35 What options are available if documents cannot be represented in electronic format?

N/A

3.6.36 What options are available if AGM/EGM related meetings cannot be represented remotely or electronically?

N/A

3.6.37 Where you have centralised, offshored, or outsourced arrangements in place, please confirm that adequate plans are in place to minimise any impact from a pandemic.

Centralised / Offshored

☑ Yes

☐ No

☐ N/A

Comments:

N/A

Outsourced

☑ Yes

☐ No

☐ N/A

Comments:

N/A

3.6.38 Please confirm that steps have been taken to address any potential impacts with market infrastructures or your regulator resulting from a pandemic?

CSD(s)

☑ Yes

☐ No

☐ N/A

Central Bank(s)

☑ Yes

☐ No

☐ N/A

CCP(s)

☐ Yes

☐ No

☐ N/A

Registrar(s)

☐ Yes

☐ No

☐ N/A

Payment Systems

☑ Yes

☐ No

☐ N/A

Regulator(s)

☑ Yes

☐ No

☐ N/A

Other (please specify):

N/A

Comments:

- NO CCP's due to atomic trading and settlement
- No equities on SDX available (Registrars)

3.6.39 Who is responsible for your pandemic plan?

Corporate Crisis, BCM & Physical Security Team

3.7 Financial Crime Prevention, Compliance, KYC and Enhanced Governance

3.7.1 Please confirm that your group has policies in place covering the below: Please specify how frequently you and your regulator review these policies and the name of the regulator undertaking the review.

	Policy	Frequency of internal review	Other (please specify the frequency)	Last date of internal review	Frequency of review by regulatory body	Other (please specify the frequency)	Last date of regulatory review and name of the regulator
AML	☑ Yes ☐ No	Annually	Please see our comments below.		Other	Please see our comments below.	
CTF	☑ Yes ☐ No	Annually			Other		
ABC	☑ Yes ☐ No	Annually			Other		
KYC	☑ Yes ☐ No	Annually			Other		
PEP	☑ Yes ☐ No	Annually			Other		
Sanctions	☑ Yes ☐ No	Annually			Other		

Comments:

SIX Digital Exchange AG is licensed as an FMI by the FINMA under the laws of Switzerland and is therefore required to implement state-of-the-art AML/CTF/ABC/KYC/PEP policies and procedures. It has written directives both as to the due diligence duties and the establishment of a proper 'Know-your-Customer' (KYC) process. This is all in line with the Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector of 10 October 1997 and the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA) of 8 December 2010. The relevant policies and procedures are updated on an annual basis. Please note that SIX Digital Exchange AG only accepts clients (e.g. banks, securities firms) that are subject to AML procedures themselves and are subject to AML oversight by an authority accepted by FINMA. SIX Digital Exchange AG does not have any non-supervised participants. SIX has internal rules in place to comply with local laws and regulations. Anti-corruption and anti-bribery are also regu-

lated in an internal Group Directive. SIX and its subsidiary companies do not tolerate any form of corruption whatsoever. SIX engages in fair competition, based on the quality and efficiency of its services. The internal audit department monitors compliance with the internal policies and procedures. Policies are not directly reviewed by FINMA but annually by our external auditor Ernst & Young. EY is also mandated by FINMA for the regulatory audits.

3.7.2 Please confirm that the policies in the above question have been implemented in your jurisdiction and that you have a process in place to monitor and action changes in applicable laws and regulation?

	Implemented	Process in place
AML	☑ Yes ☐ No	☑ Yes ☐ No
CTF	☑ Yes ☐ No	☑ Yes ☐ No
ABC	☑ Yes ☐ No	☑ Yes ☐ No
KYC	☑ Yes ☐ No	☑ Yes ☐ No
PEP	☑ Yes ☐ No	☑ Yes ☐ No
Sanctions	☑ Yes ☐ No	☑ Yes ☐ No

Comments:

We cannot provide a copy of the mentioned policies due to confidentiality reasons.

Please provide a copy of the policies as an attachment below.

AML (No file attached)

CTF (No file attached)

ABC (No file attached)

PEP (No file attached)

KYC (No file attached)

Sanctions (No file attached)

3.7.3 Do you have a whistle-blower policy in place?

☑ Yes

☐ No

If yes, provide details.

There is a Group Directive “Reporting Misconduct or Malpractice” including whistle-blower procedures. Any form of whistleblowing can be addressed to the supervisor or to the Compliance team. Compliance has the primary responsibility for investigating the incidents reported and for documenting the results of its investigation. Employees may also use a SIX external reporting tool to send anonymous reports.

3.7.4 Do you have a conflicts of interest policy in place?

☑ Yes

☐ No

If yes, provide a copy of this policy.

(No file attached)

According to the articles of association, the management of the business of SIX Digital Exchange AG and the execution of resolutions taken by the BoD are incumbent on the senior management (see art. 716a (2), 716b (1) Swiss Code of Obligations). The members of the BoD and third parties engaged in managing the company’s business, e.g., the senior management, must perform their duties with all due diligence and safeguard the interests of the company in good faith (art. 717 (1) Swiss Code of Obligations). Conflicts of interest are to be avoided and can lead to liability claims against the corresponding member of the BoD or senior management (see art. 754 Swiss Code of Obligations). The Compliance department must intervene in cases of (potential) conflicts of interest.

SIX Digital Exchange AG has established guidelines for its corporate governance and administration.

In general, SIX has established high standards of professional conduct which shall direct the ongoing activities of its units. These standards are formalized in the Code of Conduct (six-code-of-conduct-en.pdf) and in various policies and procedures applicable to directors, senior management, and employees across the Group. The BoD of SIX Digital Exchange AG has its performance regularly assessed by external audit (see art. 8 (3) FMIO).

3.7.5 Do you have a dedicated AML compliance team at both group and local level who is responsible for the implementation, monitoring, escalation, reporting and management of all policies related to combating financial crime?

Group Level

☑ Yes

☐ No

Local Level

☑ Yes

☐ No

Comments:

Our Compliance Financial Crime team has specific tasks within its remit such as the AML policies and directives. It is also responsible for AML at an operational level such as the detection of conspicuous transaction patterns and the operation of the sanction filtering system for SIX Digital Exchange AG.

3.7.6 In the last 12 months have there been any material changes to your policies to combat financial crime?

☑ Yes

☐ No

If yes, provide details.

N/A

3.7.7 How does your organisation identify, report (including to whom) and monitor suspicious securities and cash transactions?

We enforce sanctions and embargoes in connection with payments and transactions subsequent to trades. We operate a sanction filtering system that screens customer master data, cash, and securities transactions for designated sanctioned persons, entities and countries as defined in the sanctions lists, for example OFAC, UN and EU.

The sanctions screening process consists of the following features:

- Screening of all cash payments and settlement transactions
- Customer master data screening incl. PEP screening

We operate an automated AML transaction monitoring system which monitors customer activities for suspicious securities and cash transactions.

Please note that as the participants are acting for their clients, they are responsible in fulfilling their requirements regarding transaction monitoring. For the avoidance of doubt, it should be noted that we provide settlement and custody services to our participants, but we do not know the underlying clients or ultimate beneficial owners.

3.7.8 Do you have a systematic and technological capability to ensure that any suspicious securities and cash transactions are identified, monitored and reported?

☑ Yes

☐ No

If no, how do you ensure that suspicious transactions are identified, monitored and reported?

N/A

3.7.9 In the last 12 months have there been any breaches of your AML, CTF, ABC, KYC, PEP or sanctions policies reported to your regulator? If yes, please elaborate and state what remedial actions were taken.

AML

☐ Yes

☑ No

Actions taken:

N/A

CTF

☐ Yes

☑ No

Actions taken:

N/A

ABC

☐ Yes

☑ No

Actions taken:

N/A

KYC

☐ Yes

☑ No

Actions taken:

N/A

PEP

☐ Yes

☑ No

Actions taken:

N/A

Sanctions

☐ Yes

☑ No

Actions taken:

N/A

3.7.10 In the last 5 years, has a regulator or other independent body applied any publicly disclosed warnings, sanctions, fines or penalties on your bank/group related to your AML, CTF, ABC, KYC, PEP or sanctions procedures?

☐ Yes

☑ No

If yes, briefly describe the circumstances and include details of the amount of any fines or sanctions and regulatory body concerned.

N/A

3.7.11 In the last 12 months have there been any regulatory investigations into bribery against your organisation, its parent, employees or affiliates?

☐ Yes

☑ No

If yes, provide details.

N/A

3.7.12 Please confirm that your staff servicing our activities receive regular training on AML, CTF, ABC, KYC, PEP and sanctions issues. Describe the frequency and scope of the training provided. Advise if it is mandatory and if attendance is monitored.

Frequency	Mandatory training	Employee attendance monitored
AML		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		
CTF		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		
ABC		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		
KYC		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		
PEP		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		
Sanctions		
Annually	☑ Yes ☐ No	☑ Yes ☐ No
Scope:		
N/A		

Comments:

SIX Digital Exchange AG has a designated Compliance Officer who provides ongoing mandatory training to all relevant employees as well as advice to the management. The employee attendance is monitored.

3.7.13 Is your organisation a member of the Wolfsberg Group and has your organisation completed the Wolfsberg Group Questionnaire on AML?

Member

☑ Yes

☐ No

Completed questionnaire

☑ Yes

☐ No

If yes, please provide a copy as an attachment.

20250212 SIX Digital Exchange AG Wolfsberg Questionnaire.pdf (1.1 Mb)

Comments:

Please refer to the attached file.

3.7.14 How frequently do you perform your AML/KYC screening checks on your clients?

☐ Semi-annually

☐ Annually

☑ Other (please state the frequency)

Comments:

The KYC process at SIX Digital Exchange AG requires comprehensive information about the client. This includes identification and checks of client's management, regulatory status, ownership and control, PEP status, business activity (e.g., brokerage, asset management etc.) and reasoning, sanction/blacklist screenings, and other information in order to ensure that SIX Digital Exchange AG knows its clients. Changes of relevant client data are screened against sanctions/PEP lists on a daily basis. Depending on the client risk classification, clients are obliged to answer the KYC questionnaire every 6, 12 or 18 months, depending on the risk classification of the participant. SIX Digital Exchange AG conducts a KYC due diligence process in order to ad-

equately identify the business-specific risks and thus meet the requirements of the supervisory authority FINMA. Please note that as part of the participant onboarding and review process, SIX Digital Exchange AG must comply with the due diligence obligations pursuant to the Swiss Anti-Money Laundering Act (AMLA).

3.7.15 Does your organisation adhere to a record retention period imposed by your regulators? If yes, please provide us with the record retention period. If no, please provide us with the record retention period applied by your organisation.

Regulatory requirement

☑ Yes

☐ No

Retention period

The retention period in Switzerland is 10 years.

Internal requirement

☑ Yes

☐ No

Retention period

The retention period in Switzerland is 10 years.

3.7.16 Have you adopted a risk-based approach for the assessment of KYC and AML checks or do you treat all client relationships in the same way?

☑ Risk-based

☐ Same treatment

Please outline your approach to each.

Business relationships with increased risk are subject to authorization by Compliance and SDX Management. SIX Digital Exchange AG also undertakes to promptly notify the Swiss authorities

and report respective observations and concerns. For the avoidance of doubt, it shall be clarified that we provide settlement and custody services to our participants, but we do not know their clients and ultimate beneficial owners of the asset.

3.7.17 Do you have an enhanced KYC process when reviewing and assessing PEPs.

☑ Yes

☐ No

Comments:

Please refer to our response to question 3.7.14.

3.7.18 Please confirm that your organisation has procedures to ensure that no accounts are set up for, and no type of transaction (cash, securities or otherwise) is made, to the following:

Embargoed jurisdictions

☑ Yes

☐ No

Individuals or entities that are the target of US, UK, UN or EU sanctions programs

☑ Yes

☐ No

Anonymous account holders

☑ Yes

☐ No

Shell banks

☑ Yes

☐ No

Comments:

N/A

3.7.19 Do you have an automated systematic technological capability to ensure the above policies are implemented? If no, please describe how this is achieved and how the system is kept up-to-date.

Embargoed jurisdictions

☑ Yes

☐ No

Individuals or entities that are the target of US, UK, UN or EU sanctions programs

☑ Yes

☐ No

Anonymous account holders

☑ Yes

☐ No

Shell Banks

☑ Yes

☐ No

Comments:

N/A

3.7.20 Does your institution perform sanction screening against the OFAC, UN, EU and UK sanctions lists at the time of onboarding and for each transaction?

☑ Yes

☐ No

Comments:

During the on-boarding process of a new participant, the relevant client data, e.g., management, ownership, etc. are checked against the sanctions lists. Please also refer to our response to question 3.7.14. With regard to sanctions screening of transactions, please refer to our response to question 3.7.7.

3.7.21 Please provide a copy of your US Patriot Act Compliance certificate.

Please attach file here:

(No file attached)

Comments:

N/A

3.7.22 Please give a detailed overview of your compliance monitoring procedures including your sanctions monitoring process.

SIX Digital Exchange AG only accepts clients (e.g. banks) that are subject to an adequate degree of regulation and supervision as well as adequate money laundering regulation and supervision at their time of their admission as participants and during their period of participation. The compliance monitoring procedures require comprehensive information about the client. AML transaction monitoring and sanctions screening of transaction and customer data is carried out by the Compliance department. In the event of suspicious or prohibited activity, Compliance reports, based on the decision of the SDX Management, to the respective Swiss authority.

3.7.23 Which department in your organisation is responsible for implementing, monitoring, escalating, reporting and managing sanctions?

The Compliance department is responsible for implementing, monitoring, escalating, reporting, and managing sanctions. It is also responsible for the reporting to the respective authority.

3.7.24 Do you have a list of countries for which your institution has sanctions related controls and procedures.

☑ Yes

☐ No

If yes, please specify.

Compliance List of Sanctioned Countries. Specific inquiries regarding sanctions or SDX's anti-money laundering measures will be reviewed and answered on a case-by-case basis. We cannot provide a copy of the mentioned annex due to confidentiality reasons.

Please attach file here:

(No file attached)

3.7.25 Does your organisation operate a formal Code of Conduct for procurement?

☑ Yes

☐ No

If yes, provide details of anti-corruption and conflicts of interest. Requirements.

Please refer to our Code for Suppliers

3.8 Data Protection

3.8.1 In the last 12 months have there been any changes to data protection and privacy legislation in your jurisdiction or in the jurisdiction of your group?

Local jurisdiction

☑ Yes

☐ No

If yes, provide details.

Switzerland has adopted ist Federal Act on Data Protection as per 1 September 2023. The new version adapts the law to the requirements of the GDPR.

The Federal Act on Data Protection and the Ordinance to the Swiss Data Protection Act can be found under the following link:

https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadp.html

Group jurisdiction

☐ Yes

☑ No

If yes, provide details.

SIX Digital Exchange has its local jurisdiction in Switzerland. SIX Group applies the GDPR standards to all its entities, including those in Switzerland and the EU.

3.8.2 Are you required to report data breaches to your regulators?

☑ Yes

☐ No

Comments:

Data breaches must be reported to the data protection regulator(s) of the affected countrie(s).

3.8.3 In the last 12 months have you reported any data breaches to your regulators?

☐ Yes

☑ No

If yes, provide details.

N/A. There have been no breaches recorded for SDX.

3.8.4 Where you are in possession of personal data, of our employees or clients, do you have policies and procedures to ensure compliance with applicable data protection legislation including data processing and storage?

☑ Yes

☐ No

3.8.5 If you are based in the European Economic Area (EEA), do you send personal data outside the EEA?

☐ Yes

☑ No

☐ N/A - Not based in the EEA

Comments:

Switzerland has not become part of the EEA.

3.8.6 Is personal data used to sell additional products beyond our relationship?

☐ Yes

☑ No

Comments:

According to our General Terms & Conditions, we are not allowed to sell additional products beyond our relationship with regards to personal data.

3.8.7 Do you have a data breach policy?

☑ Yes

☐ No

If yes, please briefly describe and explain how and when you would notify us of a data breach.

In case of a data breach, our Data Protection Officer would notify clients within 24 hours at latest.

Comments:

N/A

3.8.8 Do you have a data protection policy?

☐ Yes

☐ No

Comments:

3.8.9 In the last 12 months have there been any changes in your formal data protection policy, including in relation to sharing of data with other business units and/or third parties/ affiliates?

☐ Yes

☑ No

If yes, please attach a copy of the revised policy.

(No file attached)

Comments:

Please consider that we cannot share a copy of our Compliance Directive 1: Data Protection due to confidentiality reasons. The policy and its annexes reflect the standards of the EU General Data Protection Regulation (GDPR) and is applicable to all SIX entities, including SDX.

3.8.10 Are there any exemptions from your data protection policy?

☐ Yes

☑ No

If yes, provide details.

N/A

3.9 ESG

Please base answers on group-level policies and data.

3.9.1 ESG Action Plan

3.9.1.1 Please provide a copy of your CSR and ESG reports (if available).

Please attach your files here

six-sustainability-report-2023-en.pdf (2.2 Mb)

Comments:

Find further information in the Sustainability Statements at the following link: https://www.six-group.com/dam/download/company/report/annual/2024/six-annual-report-2024-en.pdf

3.9.1.2 Are your organisation's ESG policies reviewed and approved by both the executive management and the Board of Directors on at least an annual basis?

☐ Yes

☐ No

Comments:

3.9.1.3 Has your organisation conducted a materiality assessment on ESG issues?

☐ Yes

☐ No

If yes, what were the key issues identified and how are you managing them?

3.9.1.4 Is the remuneration of your organisation's Board of Directors linked to the achievement of ESG objectives?

☐ Yes

☐ No

Comments:

3.9.1.5 In which of the following initiatives does your organisation participate?

☑ United Nations Global Compact

☑ Principles for Responsible Banking

☑ Net Zero Banking Alliance

☑ Other (please specify)

Please provide the link to the page and document source for each option selected.

(No file attached)

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX.

Please find link to SIX Memberships and Partner Organizations:

https://www.six-group.com/en/company/sustainability.html#network

SIX participates in the dialog between business and politics, in Switzerland, Spain and the EU. In Switzerland, SIX is in constant dialog with political parties, associations, the administration, and other stakeholders regarding the current development of the Swiss financial market infrastructure and relevant location factors. Each year, SIX draws up responses to consultations that are significant to the Swiss financial center.

SIX supported the following sustainable charters, principles, and initiatives:

- Advance – Gender Equality in Business, Zurich, Switzerland
- Zurich Energy Model, Switzerland

- Global Reporting Initiative (GRI), Amsterdam, Netherlands (GRI Community Member, use of reporting standard)
- Sustainable Stock Exchanges (SSE) Initiative, United Nations Initiative, New York, USA

3.9.1.6 Have environmental, social and governance considerations been introduced to:

☐ Client onboarding processes

☐ KYC assessments

☐ Client portfolio monitoring

☐ Client portfolio reporting

☐ Selection of third-party providers and/or vendors

☑ Other (please specify)

Please provide the link to the page and document source for each option selected.

Please note that we do not conduct any client portfolio monitoring nor reporting. Environmental, social and governance considerations have not been especially introduced to the client onboarding nor KYC assessments.

We are reporting on climate issues in accordance with the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD). By 2024 at the latest, SDX aims to start making disclosures in compliance with the TCFD and the EU CSRD, including the risk disclosures required under these standards.

3.9.1.7 Does your organisation have enhanced due diligence or exclusion policies when accepting business from the following sectors?

☐ Coal power generation

☐ Oil and gas

☐ Mining

☐ Agriculture

☐ Palm oil

☐ Tobacco

☐ Woodpulp

☐ Defence

☐ Nuclear energy

☑ Other

Please provide the link to the page and document source for each option selected.

Please consider that SDX has no working relationship with the mentioned sectors.

3.9.2 Environment

3.9.2.1 Do you have an environmental policy?

☐ Yes

☑ No

3.9.2.2 Which of these issues are covered by your environmental policy? Please provide links to these policies where applicable.

☐ Energy efficiency

☐ Waste management

☐ Paper consumption

☐ Business travel minimisation

☐ Investment and lending policies

☐ Biodiversity impact assessment and management

☑ Other (please specify)

Please provide the link to the page and document source for each option selected.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX.

SIX has clearly communicated its objective: "SIX Reduces Its Emissions to Net Zero by 2050". SIX is committed to improving its energy efficiency by a further 1.5% per year in the period from 2021 to 2030 and has been making efforts to reduce its consumption of non-renewable resources as well as its CO2 emissions. SIX has signed the commitment Letter of the Science Based Targets initiative (SBTi) and will work on further professionalizing the framework for the collection and calculation of environmental data. It is reporting on climate issues in accordance with the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD). By 2024 at the latest, SIX aims to start making disclosures in compliance with the TCFD and the EU CSRD, including the risk disclosures required under these standards.

3.9.2.3 Which of the following initiatives are undertaken by your organisation?

☐ Inclusion of environmental risks in business continuity plans

☐ Inclusion of climate risks in capital adequacy model

☐ Stress test development to cover environmental risk

☐ Environmental and social suppliers assessment

☐ Externally certified Environmental Management System

☑ Other

Please provide the link to the page and document source for each option selected.

We have no such initiatives ongoing.

3.9.2.4 Which of the following issues are covered by your internal environmental awareness training?

☑ Organisation's strategy and initiatives

☑ Skills and understanding development

☑ Local and global engagement campaigns

☐ No dedicated training available

☐ Other

Please provide the link to the page and document source for each option selected.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. Education and training are key elements for enabling all employees to give their best and offering them a working environment with prospects. Employee expertise and the transfer of knowledge to the next generations are essential in order to ensure both the stability of the infrastructure and continuous innovation. The SIX Academy provides employees with training offerings that are geared toward business requirements as well as strategic issues. Through the SIX Digital Academy, SDX employees also have access to extensive digital learning offerings that can also be used on mobile devices.

3.9.2.5 Does your organisation plan to achieve net zero carbon emissions?

☑ Yes

☐ No

If yes, please provide a copy of the plan or the link to the page and document source.

(No file attached)

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. SIX has clearly communicated our objective: "SIX Reduces Its Emissions to Net Zero by 2050". SIX knows from discussions with its clients that a climate strategy and a corresponding net zero target are becoming a prerequisite for existing and new

business partnerships. SIX is committed to improving its energy efficiency by a further 1.5% per year in the period from 2021 to 2030. SIX has been making efforts to reduce its consumption of non-renewable resources as well as its CO2 emissions. Please find link to our Sustainability Report 2023: https://www.six-group.com/dam/download/company/report/annual/2023/six-sustainability-report-2023-en.pdf

3.9.2.6 If yes, please specify the year which you target to reach net zero emissions.

Year (YYYY)

2050

3.9.2.7 Please specify the baseline year for your carbon neutrality target.

Year (YYYY)

2022

3.9.2.8 Please specify which policies are used for emissions reduction.

- [x] Energy efficiency
- [ ] Offsets
- [ ] Investment and lending policies
- [ ] Biodiversity impact reduction
- [ ] Other

Please provide copies of or links to these policies where applicable.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. Please find link to our Sustainability Report 2023: https://www.six-group.com/dam/download/company/report/annual/2023/six-sustainability-report-2023-en.pdf

3.9.2.9 By which organisations has your net zero target been validated?

- ☐ Science Based Targets Initiative (SBTI)
- ☑ Net Zero Banking Alliance (NZBA)
- ☐ RACE to ZERO
- ☐ The target has not been validated
- ☐ N/A

Other, please specify

Please provide the link to the page and document source for each option selected.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. SIX wants to be net zero by 2050. This goal was signed off by the SIX Board of Directors in April 2022. In order to move on a credible path toward net zero, e.g., in line with the 1.5-degree target of the Paris Climate Agreement, SIX is seeking a commitment to the Science Based Targets Initiative (SBTI). Hence, our net-zero interim target will be set in 2024 and validated by SBTI in 2024. For the time being, we only have the overall target to reach net-zero emissions by 2050.

3.9.2.10 Please select which activities are covered by the target:

- ☐ Stock investments
- ☐ Corporate bonds
- ☐ Sovereign bonds
- ☐ Private equity shares
- ☐ Corporate loans
- ☑ Electricity project finance
- ☐ Real estate investment trusts
- ☐ Private debt and equity

Other, please specify

Please provide the link to the page and document source for each option selected.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. Please find link to our Sustainability Report 2023: https://www.six-group.com/dam/download/company/report/annual/2023/six-sustainability-report-2023-en.pdf

3.9.2.11 Please indicate the percentage of total assets (investment and lending activities) covered by your target:

Please provide the link to the page and document source.

N/A; SDX is a Swiss central securities depository (CSD) and does not provide any investment and lending activities.

3.9.2.12 Please state your total emissions in tCO2e for each of the below categories

Category:	Total emissions (tCO2e):
Total scope 1 emissions	514
Total scope 2 location-based emissions	2,550
Total scope 2 market-based emissions	805
Total scope 3 emissions	114,822
Total revenue (state currency)	N/A

Please provide the link to the page and document source for each item.

SDX being a SIX Group company, SIX's ESG policies, initiatives and guidelines are fully implemented and followed by SDX. Please note the numbers provided above represent the total consolidated numbers for SIX Group (incl. BME).

Please find the details in our Sustainability Report 2023 on page 30:

https://www.six-group.com/dam/download/company/report/annual/2023/six-sustainability-report-2023-en.pdf

3.9.2.13 Do you have an external agency that is validating and auditing your carbon emissions disclosures?

☐ Yes

☑ No

If yes, please provide the link to the page and document source.

The SIX Sustainability Report 2023 has not been subjected to an external audit. Under the CSRD, the external audit for the Sustainability Report will become a regulatory requirement.

3.9.3 Social

3.9.3.1 Do you have an equal opportunity policy?

☑ Yes

☐ No

3.9.3.2 What areas of employment does your equal opportunities and fair treatment policy cover? Please provide links to these policies where applicable.

☑ Migrant labour

☑ Hiring

☑ Compensation / remuneration

☑ Promotion

☑ Termination

☑ Retirement

Other, please specify

N/A

Please provide the link to the page and document source for each option selected.

SDX being a SIX Group company, SIX's Social policies, initiatives and guidelines are fully implemented and followed by SDX.

Please find the link to our Code of Conduct:

https://www.six-group.com/dam/download/company/publications/six-code-of-conduct-en.pdf

3.9.3.3 Does your organisation ensure that individuals are treated equally irrespective of the following characteristics?

☑ Age

☑ Disability

☑ Gender reassignment

☑ Marriage and civil partnership

☑ Medical conditions

☑ Pregnancy and maternity

☑ Race (including colour, nationality, ethnic or national origin)

☑ Religion or belief

☑ Gender

☑ Sexual orientation

Please provide the link to the page and document source for each option selected.

SIX (and SDX) fosters diversity, equity, and inclusion. In this respect, SIX (and SDX) has set itself the goal increasing the percentage of women in middle and top management to a minimum of 25% by the end of 2023. SIX (and SDX) also promoted community building among employees, for example with the peer coaching program parents@work, gender diversity and LGBT+ communities or sport and leisure clubs. In collaboration with the Advance network for "Gender

Equality in Business," SIX (and SDX) offers ongoing mentoring and education opportunities specifically for women.

Please find the link to our Code of Conduct: https://www.six-group.com/dam/download/company/publications/six-code-of-conduct-en.pdf

3.9.3.4 Do you have a health and safety policy?

- [x] Yes
- [ ] No

3.9.3.5 Which of the following topics are covered by your health and safety policy?

- [x] Assessment of health and safety risk
- [ ] Employees being required to attend or complete health and safety training
- [ ] Employees being required to report any defects in their work area, equipment or any other hazards
- [ ] Employees being required to report any health and safety incidents (including hazards / near misses)

Please provide the link to the page and document source for each option selected.

Employees safety and well-being is of utmost importance for SIX (and SDX). Protecting measures were consistently adapted to the current situation. Fostering an open and inclusive workplace culture continues to remain a priority for SIX (and SDX) as well. It is a prerequisite to successfully executing the strategy.

To ensure business continuity and the stability of critical financial market infrastructure, the health and wellbeing of employees is of utmost importance for SIX (and SDX). Topics like work-life balance – and related issues such as the compatibility of work and family, gender equality, and (mental) health – came even more into focus. SIX (and SDX) therefore offered free external assistance and confidential counselling to employees for both work-related and personal

problems. In specific leadership training, SIX (and SDX) focused on employee care, including awareness and prevention of mental health issues, the promotion of a good working atmosphere, and collaboration.

Please find the link to our Code of Conduct: https://www.six-group.com/dam/download/company/publications/six-code-of-conduct-en.pdf

3.9.3.6 Do you have a statement on modern slavery for your business and your suppliers? If yes, please provide a copy or a link to where this can be found on your website.

☑ Yes

☐ No

Please attach file here:

(No file attached)

Comments:

https://www.six-group.com/dam/download/procurement/other/supplier-code-en.pdf

3.9.3.7 If not covered in a separate statement, please provide details of:

(a) Your policies in relation to slavery and human trafficking (please include links to these policies where relevant).

N/A; please refer to our response to question 3.9.3.6.

(b) Your due diligence processes in relation to slavery and human trafficking in your business and supply chains.

N/A; please refer to our response to question 3.9.3.6.

(c) The parts of your business and supply chains where there is a risk of slavery and human trafficking taking place, and the steps that you have taken to assess and manage that risk.

N/A; please refer to our response to question 3.9.3.6.

(d) Your effectiveness in ensuring that slavery and human trafficking are not taking place in your business or supply chains measured against performance indicators that you consider appropriate.

N/A; please refer to our response to question 3.9.3.6.

(e) The training about slavery and human trafficking available to your staff.

N/A; please refer to our response to question 3.9.3.6.

Please provide the link to the page and document source for each of the above items.

N/A; please refer to our response to question 3.9.3.6.

3.9.3.8 Do you support and respect globally recognised principles and standards (e.g., principles of UN Global Compact, International Labour Organisation standards) promoting humane and safe work environments and respecting employee rights?

☑ Yes

☐ No

If yes, please provide the link to the page and document source.

SDX being a SIX Group company, SIX's Social policies, initiatives and guidelines are fully implemented and followed by SDX.

3.9.3.9 Please confirm that you have a firm commitment to enable and enforce adequate procedures and policies to ensure the workplace is free from discrimination, harassment, victimisation or any other form of inappropriate behaviour or abuse on any grounds.

☑ Yes

☐ No

If yes, please provide the link to the page and document source.

SDX being a SIX Group company, SIX's Social policies, initiatives and guidelines are fully implemented and followed by SDX.

3.9.3.10 Does your organisation's procurement policy include corporate social responsibility requirements?

☑ Yes

☐ No

If yes, please provide a brief overview and the link to the page and document source.

SDX being a SIX Group company, SIX's Social policies, initiatives and guidelines are fully implemented and followed by SDX.

3.9.4 Governance

3.9.4.1 What percentage of your organisation's Board are independent non-executive directors?

☐ 75 - 100%

☐ 50 - 75%

☑ 25 - 50%

☐ 0 - 25%

☐ 0%

3.9.4.2 What is the frequency of board meetings?

☐ Monthly

☑ Quarterly

☐ Semi annually

☐ Annually

☐ Other (please specify)

If other, please specify the frequency.

N/A

3.9.4.3 Does your organisation have a process in place for managing conflicts of interest (at the board level)?

☐ Yes

☐ No

If yes, please specify how these conflicts of interest are managed:

☑ Directors have the duty to identify and disclose any conflicts of interest to the board

☐ Conflicts authorised by the board are recorded in a conflicts register

☐ Conflicts register is reviewed by the board at least annually

☐ None

Comments:

SIX Group has effective organizational and policy tools in place that aim to comprehensively identify and mitigate potential conflict of interests ("CoI") throughout the organization. Notably, SIX Group has enrolled a CoI directive that applies to all wholly owned companies of SIX, including the various SDX legal entities. This directive equally covers potential, apparent as well as actual CoI according to the respectively applicable legal provisions (per legal entity) and based on SIX Group's overall code of conduct (applicable to every legal entity). Furthermore, SIX Group has also rolled out a specific disclosure tool in instances where CoI cannot be avoided that allows for the tracking and assessment of CoI by the 2nd Line Of Defense. It should be noted that 2nd Line Of Defense owns the process/controls (not the BoD).

3.9.4.4 Is there an evaluation of board effectiveness?

☐ External evaluation

☐ Internal evaluation

☐ No evaluation

☑ Not disclosed

4 Your Systems

In scope services: custody services (with or without a sub-custodian) and, if applicable, client money services.

4.1 Reporting

4.1.1 Please outline any enhancements to your operational reporting capability planned for the next 12 months.

There are several initiatives under way to enhance our operational reporting in order to implement market practices, to achieve greater harmonization and automation of business processes, which thus lead to achieve non-pecuniary and financial benefits for customers.

4.1.2 Please outline any enhancements to your market infrastructures' (e.g. CCP, CSD) operational reporting capabilities planned for the next 12 months.

Please refer to our response to question 4.1.1.

4.2 Protecting your systems

4.2.1 Do you have a data security policy?

☑ Yes

☐ No

If yes, attach or provide details.

Please attach file here:

six-brochure-corp-security-en.pdf (4 Mb)

Comments:

The Compliance Directive 1: Data Protection based on the level of confidentiality aims to adequately protecting information from unauthorized access, misuse, or theft. Our security policies are for internal use only and for confidentiality reasons cannot be shared.

4.2.2 Please outline your spyware protection procedures.

SDX has spyware protection product installed on all servers and workstations including integrated virus scanning, intrusion detection and proxy filtering.

4.2.3 Does your organisation have spyware protection installed on all servers and workstations?

☑ Yes

☐ No

Comments:

Exception are partially appliances

4.2.4 Is your spyware protection software updated whenever a new version is released?

☑ Yes

☐ No

Comments:

Please refer to our response to question 4.2.3. Anti-malware products are updated regularly on automated basis.

4.2.5 Please outline your antivirus checking procedures.

We use two methods that comprise the use of off the shelf products like virus scanners, device control, NAC, etc., and for higher level threats (i.e., web-based applications), then we employ a regular penetration testing. There is always the latest virus protection in place.

4.2.6 Does your organisation have antivirus protection installed on all servers and workstations?

Comments:

All workstations and servers are being updated daily with the latest anti-virus/malware patterns.

4.2.7 Is your antivirus protection software updated whenever a new version is released?

☑ Yes

☐ No

Comments:

N/A

4.2.8 In the last 12 months have there been any external security breaches of your system?

☐ Yes

☑ No

If yes, please provide details including actions to minimise the likely recurrence of such a breach.

N/A

4.2.9 In the last 12 months has your company been mentioned in the media regarding an information security event?

☐ Yes

☑ No

Comments:

N/A

4.2.10 How is internet access policed to prevent misuse by your staff?

We use content filtering.

4.2.11 How are your systems protected from unauthorised use?

Due to confidentiality reasons, we are unable to share detailed information. We want to emphasize, however, that SIX SIS is of systemic importance for the financial market in Switzerland, and therefore, our procedures and safety measures comply with the highest standards and are approved by both FINMA and the Swiss National Bank (SNB).

Please consider that SIX fulfils the SWIFT Customer Security Programme (CSP), a dedicated initiative to reinforce and evolve the security of global banking, consolidating, and building upon existing SWIFT and industry efforts. The Customer Security Programme addresses three key aspects such as the security and protection of customers' local environments, preventing and detecting fraud in their counterparty relationships, and working together as a community to prevent future cyber-attacks. It focuses on five mutually reinforcing strategic initiatives such as:

- Improving information sharing amongst the global community
- Enhancing SWIFT related tools for customers
- Enhancing guidelines and providing assurance frameworks
- Supporting increased transaction pattern detection
- Enhancing support by third party providers

SIX is a key member of the CSP Expert Group and hence at the forefront in the area of cyber security. Furthermore, SIX has set up Switzerland's first Security Operations Center (SOC) tasked with protecting the critical infrastructure of the Swiss financial centre. The SOC of SIX works around the clock (24x7x365) and uses a unique combination of sector-specific threat intelligence and technology.

4.2.12 Do your procedures allow individual employees to have different levels of access to programs and data?

☑ Yes

☐ No

If yes, provide details.

The Identity and logical Access Management (IAM) outlines the baseline requirements for SIX's internal identity and logical access management including privileged access management. Access to information is restricted to authorized personnel, access rights are given only on a need-to-know principle. As the access is granted on a per user basis, rather than on a terminal or site trust, every unauthorized access will be recognized and accordingly blocked. SIX does not perform any terminal or site authentication. Furthermore, "Localization as a Service" is a central service offered to SIX applications to enhance the level of security by providing transparency on the geolocation of application users. Application representatives decide on the use of the service and underlying user groups, considering regulatory requirements (e.g., access to CID data), contractual obligations as well as risk considerations.

4.2.13 Please outline your process for incorporating system changes and releases into the live environment.

Structured change and project management processes ensure the efficient and prompt handling of all changes, in order to minimise the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the organization. System changes are tested and reviewed in a test environment and an integration environment, where clients can test their interfaces before they are promoted into production. All changes are scheduled on a limited number of releases to ensure structured testing (user, technical, performance, parallel, regression and client testing) and a coordinated implementation of the changes.

There is a documented change management process where changes are tested prior to being applied to the live environment. All changes are reviewed to ensure they do not compromise security. Emergency changes are handled on an ad-hoc basis by pre-defined incident management teams, with planned escalation procedures which depend on the type of emergency. If required, decisions will be made at Management Committee level. Post-mortem reviews follow as a matter of course.

4.2.14 In what circumstances do you notify clients before making changes to your systems?

We do pre-notify clients of all the changes via our CloseUp Update and communicate when the SECOM releases will enter into effect. Participants are requested to read the documents carefully and ensure that they are prepared to implement the mandatory changes. Please find all announced changes on our Private Site:

https://sws.six-group.com/private/en/home/secom/updates-release-info.html

4.2.15 Is each employee given a unique ID so that access to any part of the system is limited to authorised personnel and can be traced back to an individual?

☑ Yes

☐ No

Comments:

Access to any part of the system can be traced back to an individual.

4.3 Plans for your systems

4.3.1 In the last 12 months have there been any major developments or enhancements to your systems that support your custody and/or client money business?

Custody

☑ Yes

☐ No

☐ N/A

If yes, provide details.

SDX has recurring enhancements to his CSD service that they are regularly applied thanks to the several annual releases. Where appropriate, specific customization can also be done to meet particular client needs.

Client money

☑ Yes

☐ No

☐ N/A

If yes, provide details.

SDX has recurring enhancements to his CSD service that they are regularly applied thanks to the several annual releases. Where appropriate, specific customization can also be done to meet particular client needs.

4.3.2 Briefly outline any major systems developments or enhancements to your custody and/or client money businesses that are planned for the next three years. Indicate the planned timescales.

Custody

N/A

Client money

N/A

4.3.3 In the past 12 months, have there been any changes to your change control policy/process relating to major IT implementations?

☐ Yes

☑ No

If yes, describe the changes.

N/A

4.3.4 Are there any plans to outsource your systems during the next 12 months?

☐ Yes

☑ No

If yes, provide details.

4.4 System Performance

4.4.1 In the last 12 months have you had system outages or slowdowns that have impacted your ability to service your clients?

☑ Yes

☐ No

If yes, how many?

2

4.4.2 In the last 12 months what has been your average core processing system uptime (expressed as a percentage)?

99.83%

4.4.3 What percentage of your system capacity do you use on a daily basis?

0.2%

4.4.4 In the last 12 months have there been any changes to your end-to-end system infrastructure?

☑ Yes

☐ No

If yes, provide details.

Backup tooling enhancements. Openshift container platform upgrades.

4.5 System Development

4.5.1 What time period do you allow between vendors releasing high priority security patches (to operating systems/network devices/applications) and your implementation of them to production environments?

30 days

4.5.2 Are security requirements included in the software development lifecycle documentation?

☑ Yes

☐ No

Comments:

All productive systems have approved Security Documentation inline with SIX compliance and requirements.

4.5.3 Is client data ever used in the test or development environments?

☐ Yes

☑ No

If yes, confirm if it is anonymised.

☐ Yes

☐ No

Comments:

N/A

4.6 Operational Resilience

4.6.1 Is operational resilience part of your Board or Executive Management agenda, discussion and decision-making process?

☑ Yes

☐ No

Comments:

SIX operates the infrastructure for the financial centre in Switzerland, thus ensuring the flow of information and money between financial market players. SIX offers exchange services, securities services, financial information, and banking services with the aim of increasing efficiency, quality, and innovative capacity along the entire value chain. These services are critical not only in the corporate context, but also for the national economy in Switzerland. Resilience and emergency preparedness are general security topics embedded into the companywide integrated security activities. SIX addresses operational resilience in a targeted and tailored fashion to the different audiences within the company (staff/management) and beyond (stakeholders). Operational resilience is the ability of financial institutes, Financial Market Infrastructures (FMIs) and the financial sector to identify and protect against threats and potential failures, to respond

and adapt to disruptive events, and to recover and learn from them to minimize their impact on the delivery of critical functions. Central aspects for increasing operational resilience are the greater involvement and strategic guidance from top management and the fostering of an optimal interplay between the different disciplines. SIX strives to learn from disruptions to minimize their impact and to continuously improve its operational resilience, especially with regard to severe but plausible scenarios.

4.6.2 Have you undertaken a criticality assessment of the products and services offered supporting your core custody/client money activities?

☑ Yes

☐ No

Comments:

SIX Digital Exchange prepares and updates annually a Business Impact Analysis (BIA) in the recovery plan which sets out the recovery objectives for the business processes that are necessary for operations. The goal of the recovery plan is to ensure the continued service of critical operations. The recovery strategy shall therefore contribute towards maintaining the operations of critical services. It comprises several recovery options, which allow SIX Digital Exchange to recover from potential severe crisis scenarios. The recovery plan is reviewed and submitted to the competent authorities while the criticality is determined for every business process and relevant interdependencies are identified. Along with the BIA a continuity requirements analysis is carried out.

4.6.3 Does your criticality assessment/ resilience planning include critical technology services?

☑ Yes

☐ No

Comments:

The criticality assessments contain all processes which do depend on the respected technology services. These technology services are assessed as well.

4.6.4 How frequently does executive management review your operational resilience plan?

- ☐ Quarterly
- ☐ Semi Annually
- ☑ Annually
- ☐ Other (please specify)

Comments:

SIX conducts Business Impact Analyses (BIA) in all business units and corporate functions. To allow a comparison across the company, the BIA process is conducted in a dedicated tool with a common methodology. BC managers maintain and update their BIA annually and let them approve by their business unit head or corporate function head.

4.6.5 Is the resilience planning of your organisation (including mapping of critical products and services) a regulatory requirement?

- ☑ Yes
- ☐ No

Comments:

The resilience planning and the mapping of critical services is required by FINMA Circular Letter 2023/1 for all FMIs, what includes SIX Digital Exchange.

4.6.6 How are organisational service deficiencies identified?

☑ Proactively (e.g. from testing/exercising)

☑ Reactively (because of incidents)

☐ Other: Please specify

Comments:

We proactively identify deficiencies and conduct lessons learned after each incident also considering alternative methods of providing the required level of resilience.

4.6.7 In the last 12 months have all identified resilience related deficiencies been remediated, evaluated, and addressed?

☑ Yes

☐ No

☐ N/A

Comments:

N/A

4.6.8 Please confirm you have a framework for staff succession planning?

☑ Yes

☐ No

Comments:

Succession planning is a key topic on the management board.

5 Core Services

In scope services: custody services (with or without a sub-custodian).

5.1 Settlements

5.1.1 In the last 12 months have there been any material changes to your settlement processes?

☐ Yes

☑ No

If yes, provide details.

N/A

5.1.2 Please confirm which of the following controls are in place to ensure that an individual client's securities are used only to settle that client's trades (i.e. not used to settle trades belonging to either yourself or your other clients).

	Automated Manual	Process in place
Transactions are only settled upon receipt of instruction from the client	☑ Yes ☐ No	☐ Yes ☑ No
Internal position checks occur	☑ Yes ☐ No	☐ Yes ☑ No
All transactions are matched prior to settlement	☑ Yes ☐ No	☐ Yes ☑ No
No third party has power of attorney over the depository accounts containing client securities	☑ Yes ☐ No	☐ Yes ☑ No
Other (please provide details in comments below)	☑ Yes ☐ No	☐ Yes ☑ No

Comments:

SDX settles transactions on a true delivery versus payment basis. Trades will only settle if both

securities and cash are available. Cash and securities will be booked simultaneously and irrevocably. Real-time online processing is a matter of course by providing real-time notifications on trade status to participants. These status intimations provide participants with information reflecting the most current status of the transactions.

5.1.3 In the last 12 months have there been any changes that have led to a reduction or increase in manual processing for the items below?

Client instruction to the custodian

☐ Yes

☑ No

If yes, provide details.

N/A

Custodian instruction to the CSD

☐ Yes

☑ No

If yes, provide details.

N/A

5.2 Asset Servicing

5.2.1 In the last 12 months have there been any changes or enhancements to your corporate events information sources?

Corporate events information sources

☐ Yes

☑ No

If yes, provide details.

N/A

Market information sources

☐ Yes

☑ No

If yes, provide details.

N/A

5.2.2 In the last 12 months have there been any changes or enhancements to your proxy voting service?

☐ Yes

☑ No

If yes, provide details

N/A

5.2.3 Have any of the changes to your proxy voting service increased the levels of manual intervention in these processes?

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

5.3 Taxation

5.3.1 If you provide taxation services (e.g. reclaim, relief at source, tax vouchers), please complete this section (5.3). If not, please tick the 'Not Applicable' box below and move to section 5.4.

N/A

5.3.2 In the last 12 months have there been any changes or enhancements to your taxation reclaim, relief at source or tax voucher processes?

Tax reclaim

☐ Yes

☑ No

If yes, provide details.

N/A

Relief at source

☐ Yes

☑ No

If yes, provide details.

N/A

Tax voucher

☐ Yes

☑ No

If yes, provide details.

N/A

5.3.3 Have any of the changes above increased the levels of manual intervention in these processes?

☐ Yes

☑ No

☐ N/A

If yes, provide details.

N/A

5.3.4 Is your organisation FATCA compliant?

☑ Yes

☐ No

If no, please state your plans to become compliant.

N/A

5.4 Cash

5.4.1 If you provide cash management services, please complete this section (5.4). If not, please tick the 'Not Applicable' box below and move to section 5.5.

N/A

5.4.2 In the last 12 months have there been any changes to your treasury, FX and cash management products and services?

Treasury

☐ Yes

☑ No

If yes, provide details.

N/A

FX

☐ Yes

☑ No

If yes, provide details.

N/A

Cash management

☐ Yes

☑ No

If yes, provide details.

N/A

5.4.3 In the last 12 months have there been any changes regarding FX policies or currency restrictions?

☐ Yes

☑ No

If yes, provide details.

N/A

5.4.4 In the last 12 months have there been any changes to the structure, options or naming conventions used for cash accounts in your records?

☐ Yes

☑ No

If yes, provide details.

N/A

5.4.5 Is the account holder the legal owner of cash balances held with your organisation?

☑ Yes

☐ No

If no, please confirm who is:

N/A

5.5 Client service management

5.5.1 In the last 12 months have there been any changes to your client service model and/or management structure?

☐ Yes

☑ No

If yes, provide details.

N/A

5.5.2 In the next 12 months, do you plan to make changes to your client service model and/or management structure?

☐ Yes

☑ No

If yes, provide details.

N/A

6 Client money

In scope services: client money services.

6.1 Segregation of client money

6.1.1 If you hold client money, please complete this section (7). If not, please tick the 'Not Applicable' box below.

N/A

6.1.2 Please confirm that, based on the laws in the jurisdiction where your organisation is incorporated, the level of account segregation implemented by yourselves and applicable to the client money held with you would ensure that, upon our insolvency, such cash will be deemed to belong to our underlying clients and will be protected from you, our creditors or any other third parties.

☑ Yes

☐ No

Comments:

Upon your insolvency, such cash will belong to you as participant of SDX. If this was client money coming originally from your clients, they would have a claim against you. However, under Swiss insolvency law, if applicable, cash deposits by a client of yours with you as participant of SDX, up to the amount of CHF 100,000 for each client are treated preferentially under the Banking Act (Art. 37a para. 1bis Banking Act in conjunction with Art. 219 para. 4 Federal Act on Debt Collection and Bankruptcy of 11 April 1989).

6.1.3 Please confirm that client money held by you is segregated and properly identified in your books and records by means of differently titled accounts or equivalent measures as follows:

(a) Segregated and identified separately as belonging to your client or your clients' clients in accordance with instructions (as applicable).

☐ Yes

☑ No

(b) Segregated and identified separately from your proprietary money.

☑ Yes

☐ No

(c) Segregated and identified separately from money belonging to other clients of yours.

☑ Yes

☐ No

(d) Segregated and identified separately from the money of any subsidiary or affiliate of yours.

☑ Yes

☐ No

Comments:

SDX does not distinguish in its records between money booked in a money account with reference to the participant's clients and such money booked in a money account with reference to the participant itself. Under Swiss law, book money is treated as a claim of the account holder towards the custodian the accounts are held with. The owner of the money claim against SDX is the participant and not the participant's client.

6.1.4 In the last 12 months have there been any changes in your ability to make newly opened client money accounts "inactive" until a client acknowledgement letter has been executed?

☐ Yes

☑ No

If yes, provide details.

N/A

6.1.5 Does your jurisdiction support a deposit protection scheme in the event of your bank's insolvency?

☐ Yes

☐ No

If no, please describe what additional arrangements you have implemented to minimise the risk of loss and ensure that such cash held for your clients is protected in the event of your insolvency.

Please note that SDX is licensed as an FMI (Financial Market Infrastructure) by the Swiss Financial Market Supervisory Authority (FINMA) under the Federal Market Infrastructure Act (FMIA) and not as a bank. Under Swiss law, participants of SDX will have an unsecured claim against SDX (irrespective of whether the account description contains a reference to the participant's clients or the participant itself).

If yes and if a scheme exists, please provide a link to the details.

N/A

6.2 Credentials

6.2.1 Do you undertake other business activities which could compromise your ability to provide services as a client money bank?

☐ Yes

☐ No

If yes, provide details.

6.3 Operations and service provision

6.3.1 Are there controls in place to prohibit debit balances on client money accounts?

☑ Yes

☐ No

Comments:

N/A

6.3.2 Please confirm that you will ensure that only authorised instructions sent specifically to/for the account are actioned.

☑ Yes

☐ No

Comments:

N/A

6.3.3 Please confirm that payment instructions formatted to allow straight through processing and received by the cut-off time will be applied to the account on the same day.

☑ Yes

☐ No

If no, provide details of the process to remediate.

N/A

6.3.4 Are there any circumstances in which the account title could change without our request?

☐ Yes

☑ No

If yes, provide details.

N/A

6.3.5 Please confirm that there are controls in place to prevent charges and interest being applied to client money accounts?

☑ Yes

☐ No

Comments:

N/A

6.4 Regulatory requirements

6.4.1 Please confirm that the balances remain in the currency that they are credited (i.e. there is no conversion).

☑ Yes

☐ No

Comments:

N/A

6.4.2 Please confirm that any monies held by us for our clients will not be set-off against other monies held by you for us on our insolvency.

☑ Yes

☐ No

Comments:

N/A

6.4.3 Please confirm that on your insolvency our claim to the deposit held with you will rank pari passu with all other unsecured claims.

☑ Yes

☐ No

Comments:

N/A

6.4.4 In the last 12 months have there been any changes to the legal status of creditors granted seniority of claims against your assets?

☐ Yes

☑ No

If yes, provide details.

N/A

6.4.5 For 15c3-3 accounts only: If the entity holding the account is a US branch of a foreign bank, please confirm that the branch is eligible to hold 15c3-3 deposits of broker dealers.

☐ Yes

☐ No

☑ N/A

Comments:

N/A

6.4.6 In the last 12 months have there been any changes that affect either legal requirements, local regulations or market practices related to the holding of client monies?

Legal requirements

☐ Yes

☑ No

If yes, provide details.

N/A

Local regulations

☐ Yes

☑ No

If yes, provide details.

N/A

Market practices

☐ Yes

☑ No

If yes, provide details.

N/A

6.5 Correspondent banks

6.5.1 Provide a list of all correspondent banks that your organisation uses, as an attachment or link to your website.

(No file attached)

Comments:

CHF - Swiss National Bank

EUR - SECB Swiss Euro Clearing Bank GmbH

6.5.2 Do you have a team dedicated to managing your network of correspondent banks?

- [x] Yes
- [ ] No

6.5.3 Do you maintain contingency correspondent bank relationships where you do not self-clear?

- [ ] Yes
- [ ] No
- [x] N/A

6.5.4 Can you realign to the contingency correspondent banks within 48 hours?

- [ ] Yes
- [ ] No
- [x] N/A

6.5.5 Please confirm that, within 48 hours above, you would make us aware of any standing settlement instructions (SSI) changes required by our organisation.

- [ ] Yes
- [ ] No
- [x] N/A