Information Security Framework Agreement
Version 4.0

DBG Emergency Contact

Mail: CERT@deutsche-boerse.com
Phone: +352 243 33555

Initials:_____/_____

Confidential

Content

Initials:_____/_____

Initials:_____/_____

Initials:_____/_____

Confidential

Initials:_____/_____

Confidential

Information Security Framework Agreement

Version 4.0

between

Deutsche Börse AG, 60485 Frankfurt am Main, Germany

– hereafter referred to as **DBAG** –

and

[Vendor Name], [location and full headquarters address]

– hereafter referred to as **Third-party** –

PREAMBLE

DBAG and its **affiliate**s (within the meaning of § 15 Aktiengesetz) (DBAG and each of its **affiliate**s may individually or collectively be referred to herein as "Deutsche Börse Group" or "**DBG**") is a highly reputable international exchange organisation and innovative market infrastructure provider. **DBG** ensures capital markets that are transparent, reliable and stable. With its wide range of products, services and technologies. **DBG** organises safe and efficient markets for sustainable economies. **DBG** strongly relies on the **availability**, **integrity, authenticity,** and **confidentiality** of data and services. To that end, **DBG must** ensure that these protection requirements are met and maintained throughout its organisation and are equally met where services are provided to **DBG**. **DBG** is also obliged under law and regulation to ascertain that **third-parties** providing services to **DBG** are accountable for establishing and maintaining **Information Security** across all service deliveries.

Thus, the **Parties** agree to implement an **Information Security** framework as further set out in this **Information Security** Framework Agreement ("**ISFA**") which **shall** safeguard **Information Security** throughout the entire business relationship of the **Parties**.

1. INTERPRETATION / GOVERNING LAW / MISCELLANEOUS

(a) This **ISFA** defines **DBG**'s **Information Security** requirements and the corresponding obligations of the **Third-party**. It constitutes a **third-party** beneficiary agreement to the benefit of, and enforceable by, DBAG's **affiliate**s (§ 15 AktG), including its **affiliate**s listed in Appendix 1 "**Affiliate**s" ("echter Vertrag zugunsten Dritter").

(b) This **ISFA shall** be effective as of the date of last signature below and **shall** be valid for an initial term of 3 years upon the effective date and **shall** renew thereafter for renewal terms

Initials:_____/_____

of further 2 years if on the last date of the initial term or a renewal term of this **ISFA** the **Third-party** has an active contractual relationship with **DBG** besides this **ISFA**.

Notwithstanding anything herein, this **ISFA shall** in any case survive the termination or expiration of the last other contractual relationship with **DBG** for a term of 2 years.

Each Party's right to terminate this **ISFA** for good cause ("aus wichtigem Grund") **shall** remain unaffected.

A material breach of **Third-party's** obligations hereunder entitles DBAG and any of DBAG's **affiliate**s to terminate any or all of its other contractual relationships with **Third-party**.

(c) The **Parties** agree that terms printed in bold carry specific meaning as defined in the glossary of this document.

(d) Amendments to this **ISFA must** be made in written form. Each amendment **shall** expressly reference the modified provision of the **ISFA** as a precondition for its validity.

(e) Agreements that the **Parties** may conclude in their business relationship may entail further reaching obligations than those stipulated herein. Such further reaching obligations **shall** govern the respective agreement and do not constitute amendments to this **ISFA**. This **ISFA** does not limit or modify any other agreed rights or obligations.

(f) Agreements already concluded between the **Parties**, or which **will** be included in the future may contain liability provisions. Such liability provisions **shall** not be modified by this agreement, but a breach of this **ISFA shall** constitute a breach of the respective agreements for which **Third-party** is required to fulfil Requirements under this **ISFA**, e.g. for an agreement on development services, the chapter #Development may be agreed to be appliable and thus a breach of the requirements under such chapter would constitute a breach of said agreement, whereas in the same situation other agreements with **Third-party** would not be breached where the chapter #Development was not agreed and thus is not applicable.

(g) **Third-party** may not transfer this **ISFA** or any of its obligations or rights hereunder to any third party without the prior written consent of DBAG.

(h) **Should** one or more provisions of this **ISFA** be or become invalid or unenforceable in whole or part, or contain a gap, this **shall** not affect the validity of the remaining provisions. The invalid or unenforceable provision **shall** be replaced by the **Parties** with a valid and enforceable provision which comes as close as possible to the economic purpose of the invalid or unenforceable provision. In the event of an omission, that valid provision **shall** be deemed agreed which corresponds to what would have been agreed, on the basis of the purpose of the respective contract, had the respective contracting parties given the matter their attention at the outset.

Initials:_____/_____

(i) This Notwithstanding anything else agreed between the **Parties**, this **ISFA** and any dispute relating to this **ISFA shall** be governed by the laws of the Federal Republic of Germany without regard to its conflict of laws principles and the United Nations Convention on the International Sale of Goods.

Notwithstanding anything else agreed between the **Parties**, any dispute arising in relation to this **ISFA shall** be submitted to arbitration by, and finally decided according to the rules of arbitration, of the Chamber of Industry and Commerce of Frankfurt am Main without recourse to the ordinary courts of law. The right of the **Parties** to initiate judicial summary proceedings, as well as injunction proceedings **shall** remain unaffected. The place of arbitration **shall** be Frankfurt am Main. The number of arbitrators **shall** be three (3), at least two (2) of whom **must** be fully qualified lawyers.

2. APPLICABILITY

Requirements that may be applicable for the provisioning of the Services are listed below in sections 5 et seq. in the rows under the table column "Requirement". Their applicability is clustered into categories that are listed under the overarching table column "Chapter". The applicability of a Requirement for a certain chapter is determined by a cross in the table.

The chapters that constitute applicable and binding obligations of the **Third-party** are set forth in Appendix 2 "Applicable Chapters". In agreements concluded after the effective date of this **ISFA** the **parties** of such agreements may determine chapters that **shall** apply and be binding upon **Third-party** regarding the substance matter of each such agreement by making reference to such chapter.

DBG differentiates between the following seven chapters of requirements, which may be explained as follows:

- #Baseline
  Requirements marked as "Baseline" apply only to a narrow scope of services in which the **Third-party**'s personnel **will** have access to **DBG** premises (such as facility services).

- #BaselineExtended

  "Baseline Extended" is applicable to services which are typically not categorized as "Baseline". Requirements for "Baseline Extended" are applicable as determined by a cross in the table.

Additional requirements may be applicable, depending on five specific service types consumed by **DBG** as outlined below.

- #Cloud
  Requirements marked as "Cloud" apply to all cloud-based solutions, including **software as a service**, **platform as a service**, **infrastructure as a service** and other cloud-based solutions.

Initials:_____/_____

Confidential

- ▪ #Data Outside **DBG**
  Requirements marked as "Data Outside **DBG**" apply to all services that receive, process or store **DBG data** but do not qualify as a cloud solution. This includes all services which enjoy access to **DBG data** or enjoy **privileged access** rights in tools and services utilised by **DBG**.

- ▪ #Infrastructure
  Requirements marked as "Infrastructure" apply to all services which include the provision of infrastructure such as data centres but do not qualify as a "as a service" solution.

- ▪ #Development
  Requirements marked as "Development" apply to all services which include the creation of **information asset**s.

- ▪ #Sub-contracting
  Requirements marked as "Sub-contracting" apply to all **Third-parties** that rely on sub-contracting in the delivery of services to **DBG**.

It is possible, that several chapters may be applied in combination (e.g. "Baseline Extended + Cloud + Sub-contracting").

In the absence of any agreement on the applicability of certain requirements, the following chapter **shall** apply: "Baseline Extended".

Third-party shall procure in written form contracts with each sub-provider being relevant for the provisioning of **Third-party**'s Services to **DBG** terms and conditions that are equivalent to those set forth herein; it remains responsible for its sub-providers' compliance with such terms and conditions.

3. STANDARDS AND **STATE OF THE ART** TECHNOLOGY

The **Third-party shall** ensure that its service provision and organization comply with (i) industry accepted international standards for **information security**, such as the ISO/IEC 270xx framework, the **BSI C5** standard for cloud security, and (ii) the **state of the art** of technology and organizational measures. **State of the art** of technology and organizational measures mean the procedures, equipment and operating methods which application is most effective in achieving the **information security** objectives and legal protection objectives established by law and regulation and by the Framework Agreement and which have been proven effective in practice.

4. AUDIT, ASSESSMENTS AND MONITORING

4.1. AUDITS & ASSESSMENTS

The **Third-party** agrees that services provided to **DBG** are subject to assessments for **Third-Party**'s compliance with the requirements stipulated in this **ISFA**. These assessments may be

Initials:_____/_____

conducted by **DBG** or by another party on behalf of **DBG** as determined by **DBG** (the "**Auditor**").

In conducting these assessments, the **Third-party shall** correctly and comprehensively answer any questionnaire, that **Auditor** makes available to the **Third-party** either directly or via a tool in conducting its assessments. Within three weeks upon receiving **Auditor**'s request, **Third-party will** provide to **Auditor** topical and appropriate evidence (such as policies certificates, standards and implementation evidence; including screenshots, logfiles, etc.).

Third-party grants **DBG** unrestricted rights of inspection and auditing including full access to all relevant business premises, including the full range of relevant devices, systems, networks, information, and data used for providing the outsourced function, including related financial information, personnel, and the service provider's external auditors. The **Third-party shall** ensure that its sub-contractors grant **DBG** equivalent inspection and audit rights. Any audit on **Third-party** premises based on this **ISFA shall** be (i) conducted during **Third-party**'s business hours, (ii) seek to minimize disruptions of **Third-party**'s business, and (iii) take into account the **confidentiality** and security of **Third-party**'s client data and installations. **DBG** or its **affiliate**s **shall** provide reasonable prior notice of an audit under this **ISFA** to the **Third-party**, unless this is not possible due to an emergency or crisis situation.

Notwithstanding anything in any agreement between the **parties**, the **Third-party**, if considered **outsourcing**, grants **DBG** the right to conduct previously announced **penetration tests** regarding its infrastructure and organization which **shall** be conducted by **DBG** or a third party appointed by **DBG** in a best practise manner, including without limitations common **vulnerabilities** and exposures (CVE), or equivalent, reporting.

Should DBG's assessments, audits or **penetration tests** indicate an elevated risk exposure emanating from the **Third-party**'s service delivery, the **Third-party shall** develop and share with **DBG** risk-mitigation plans to remediate the risk and promptly execute such plans until the identified risks are mitigated as agreed with **DBG**.

4.2. LIVE MONITORING

The **Third-party** agrees that once a service goes live, the **Third-party may** be monitored by **DBG**. The **Third-party shall** support such monitoring by providing reports to **DBG** with content and cadence, as directed by **DBG** from time to time considering **DBG**'s risk exposure and regulatory requirements. **DBG** is entitled to complement the monitoring with automated tools which monitor **Third-party**'s compliance with the requirements stipulated in this **ISFA**.

Should such monitoring indicate an elevated risk exposure for **DBG**, the **Third-party shall** develop and share with **DBG** appropriate risk-mitigation plans, designed to remediate the risk and promptly execute such plans until the identified risks are mitigated.

5. ORGANIZATIONAL REQUIREMENTS

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

5.1 Policies for **information security**

Information security policy and topic-specific policies **shall** be defined and approved by **Third-party's** management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.		X					

5.2 **Information security** roles and responsibilities

Information security roles and responsibilities **shall** be defined and allocated by the **Third-party**.		X					

5.3 Segregation of duties

Conflicting duties and conflicting areas of responsibility **shall** be segregated by the **Third-party**.		X					

5.4 Management responsibilities

Management of the **Third-party shall** require all personnel to apply **information security** in accordance with the established **information security policy**, topic-specific policies and procedures of the **Third-party**.	X	X					

5.5 Contact with authorities

The **Third-party shall** establish and maintain contact with relevant authorities.	X	X					

5.6 Contact with special interest groups

The **Third-party shall** establish and maintain contact with special interest groups or other specialist security forums and professional associations.		X					

5.7 **Threat** intelligence

Information relating to **information security threat**s **shall** be collected and analysed by the **Third-party** to produce **threat** intelligence.		X					

5.8 **Information security** in project management

The **Third-party shall** integrate **information security** into project management.		X					

Initials:_____/_____

Requirement	Chapter						
	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

5.9 Inventory of information and other associated assets

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
An inventory of information and other associated assets, including owners, **shall** be developed and maintained by the **Third-party**.			X	X	X		

5.10 Acceptable use of information and other associated assets

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Rules for the acceptable use and procedures for handling information and other associated assets **shall** be identified, documented and implemented by the **Third-party**.		X					

5.11 Return of assets

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Personnel and other interested parties as appropriate **shall** return all the **Third-party**'s assets in their possession upon change or termination of their employment, contract or agreement.		X					

5.12 Classification of information

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Information **shall** be classified by the **Third-party** according to the **information security** needs of the **Third-party** based on **confidentiality**, **integrity**, **availability, authenticity** and relevant interested party requirements.		X					

5.13 Labelling of information

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
An appropriate set of procedures for information labelling **shall** be developed and implemented by the **Third-party** in accordance with the information classification scheme adopted by the **Third-party**.				X		X	X

5.14 Information transfer

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Information transfer rules, procedures, or agreements **shall** be in place for all types of transfer facilities within the **Third-party** and between the **Third-party** and other parties.							X

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
5.15 Access control							
Rules to control physical and logical access to information and other associated assets **shall** be established and implemented by the **Third-party** based on business and **information security** requirements.		X					
5.16 Identity management							
The full life cycle of identities **shall** be managed by the **Third-party**.			X	X	X	X	
5.17 Authentication information							
Allocation and management of authentication information **shall** be controlled by a management process set up and run by the **Third-party**, including advising personnel on the appropriate handling of authentication information.			X	X	X	X	
5.18 Access rights							
Access rights to information and other associated assets **shall** be provisioned, reviewed, modified and removed by the **Third-party** in accordance with the **Third-party**'s topic-specific **policy** on and rules for access control.			X	X	X	X	
5.19 Information security in Third-party relationships							
Processes and procedures **shall** be defined and implemented by the **Third-party** to manage the **information security** risks associated with the use of **Fourth-party** products or services.							X
5.20 Addressing information security within Third-party agreements							
Relevant **information security** requirements **shall** be established by the **Third-party** and agreed with each **Fourth-party** based on the type of the relationship.							X
5.21 Managing information security in the ICT supply chain							
Processes and procedures **shall** be defined and implemented by the **Third-party** to manage the **information security** risks associated with the ICT products and services supply chain.							X

Initials:_____/_____

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

5.22 Monitoring, review and change management of **Fourth-party** services

The **Third-party shall** regularly monitor, review, evaluate and manage change in **Fourth-party information security** practices and service delivery.							X

5.23 **Information security** for use of cloud services

Processes for acquisition, use, management and exit from cloud services **shall** be established by the **Third-party** in accordance with the **Third-party**'s **information security** requirements.		X					

5.24 **Information security incident** management planning and preparation

The **Third-party shall** plan and prepare for managing **information security incident**s by defining, establishing and communicating **information security incident** management processes, roles and responsibilities.	X	X					

5.25 Assessment and decision on **information security event**s

The **Third-party shall** assess **information security event**s and decide if they are to be categorized as **information security incident**s.	X	X					

5.26 Response to **information security incident**s

Information security incidents **shall** be responded to by the **Third-party** in accordance with the documented procedures.	X	X					

5.27 Learning from **information security incident**s

Knowledge gained from **information security incident**s **shall** be used by the **Third-party** to strengthen and improve the **information security** controls.	X	X					

5.28 Collection of evidence

The **Third-party shall** establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to **information security event**s.		X					

5.29 **Information security** during disruption

The **Third-party shall** plan how to maintain **information security** at an appropriate level during disruption.			X	X	X		X

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

5.30 ICT readiness for business continuity

Requirement							
ICT readiness **shall** be planned, implemented, maintained and tested by the **Third-party** based on business continuity objectives and ICT continuity requirements.			X	X	X		X

5.31 Legal, statutory, regulatory and contractual requirements

Requirement							
Legal, statutory, regulatory and contractual requirements relevant to **information security** and the **Third-party**'s approach to meet these requirements **shall** be identified, documented and kept up to date.		X					

5.32 Intellectual property rights

Requirement							
The **Third-party shall** implement appropriate procedures to protect intellectual property rights.			X			X	

5.33 Protection of records

Requirement							
Records **shall** be protected by the **Third-party** from loss, destruction, falsification, unauthorized access and unauthorized release.			X	X		X	X

5.34 Intentionally left blank

5.35 Independent review of **information security**

Requirement							
The **Third-party**'s **shall** ensure that its approach to managing **information security** and its implementation including people, processes and technologies is reviewed independently at planned intervals, or when significant changes occur.			X	X	X		

5.36 Compliance with policies, rules and standards for **information security**

Requirement							
Compliance with the **Third-party**'s **information security policy**, topic-specific policies, rules and standards **shall** be regularly reviewed by the **Third-party**.		X					

5.37 Documented operating procedures

Requirement							
Operating procedures for **information processing facilities shall** be documented and made available by the		X					

Initials:_____/_____

Third-party to personnel who need them.							

Initials:_____/_____

6. PEOPLE REQUIREMENTS

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

6.1 Screening

Background verification checks on all candidates to become personnel **shall** be carried out by the **Third-party** prior to joining the **Third-party** and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	X	X					

6.2 Terms and conditions of employment

The **Third-party shall** ensure that employment contractual agreements state the personnel's and the organization's responsibilities for **information security**.	X	X					

6.3 **Information security** awareness, education and training

The **Third-party shall** ensure that personnel and relevant interested parties receive appropriate **information security** awareness, education and training and regular updates of the organization's **information security policy**, topic-specific policies, and procedures, as relevant for their job function.	X	X					

6.4 Disciplinary process

A disciplinary process **shall** be formalized and communicated by the **Third-party** to take actions against personnel and other relevant interested parties who have committed an **information security policy** violation.	X	X					

6.5 Responsibilities after termination or change of employment

Information security responsibilities and duties that remain valid after termination or change of employment **shall** be defined, enforced and communicated by the **Third-party** to relevant personnel and other interested parties.	X	X					

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten- ded	Cloud	Data Outside DBG	Infra- structure	Develop -ment	Sub- contracti ng

6.6 **Confidentiality** or non-disclosure agreements

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infrastructure	Development	Subcontracting
The **Third-party shall** ensure that **confidentiality** or non-disclosure agreements reflecting the **Third-party**'s needs for the protection of information are identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	X	X					

6.7 Remote working

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infrastructure	Development	Subcontracting
Security measures **shall** be implemented by the **Third-party** when personnel are working remotely to protect information accessed, processed or stored outside the **Third-party**'s premises.		X					

6.8 **Information security event** reporting

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infrastructure	Development	Subcontracting
The **Third-party shall** provide a mechanism for personnel to report observed or suspected **information security events** through appropriate channels in a timely manner.		X					

Initials:_____/_____

7. PHYSICAL REQUIREMENTS

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

7.1 Physical security perimeters

Security perimeters **shall** be defined and used by the **Third-party** to protect areas that contain information and other associated assets.			X	X	X	X	

7.2 Physical entry

Secure areas **shall** be protected by the **Third-party** by appropriate entry controls and access points.		X					

7.3 Securing offices, rooms and facilities

Physical security for offices, rooms and facilities **shall** be designed and implemented by the **Third-party**.		X					

7.4 Physical security monitoring

Premises **shall** be continuously monitored by the **Third-party** for unauthorized physical access.		X					

7.5 Protecting against physical and environmental **threat**s

Protection against physical and environmental **threat**s, such as natural disasters and other intentional or unintentional physical **threat**s to infrastructure **shall** be designed and implemented by the **Third-party**.			X	X	X		

7.6 Working in secure areas

Security measures for working in secure areas **shall** be designed and implemented by the **Third-party**.		X					

7.7 Clear desk and clear screen

Clear desk rules for papers and removable storage media and clear screen rules for **information processing facilities shall** be defined and appropriately enforced by the **Third-party**.				X		X	

7.8 Equipment siting and protection

Equipment **shall** be sited securely and protected by the **Third-party.**			X	X	X		X

Initials:_____/_____

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

7.9 Security of assets off-premises

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Off-site assets **shall** be protected by the **Third-party**.			X	X	X		X

7.10 Storage media

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Storage media **shall** be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the **Third-party**'s classification scheme and handling requirements by the **Third-party**.		X					

7.11 Supporting utilities

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Information processing facilities shall be protected by the **Third-party** from power failures and other disruptions caused by failures in supporting utilities.			X	X	X		X

7.12 Cabling security

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Cables carrying power, data or supporting information services **shall** be protected by the **Third-party** from interception, interference or damage.			X	X	X		X

7.13 Equipment maintenance

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Equipment **shall** be maintained correctly by the **Third-party** to ensure **availability**, **integrity authenticity** and **confidentiality** of information.			X	X	X		X

7.14 Secure disposal or re-use of equipment

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Items of equipment containing storage media **shall** be verified by the **Third-party** to ensure that any sensitive da**ta** and licensed software has been removed or securely overwritten prior to disposal or re-use.		X					

Initials:_____/_____

8. TECHNOLOGICAL REQUIREMENTS

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
8.1 User endpoint devices							
Information stored on, processed by or accessible via user endpoint devices **shall** be protected by the **Third-party**.			X	X		X	X
8.2 Privileged access rights							
The allocation and use of **privileged access** rights **shall** be restricted and managed by the **Third-party**.			X	X			
8.3 Information access restriction							
Access to information and other associated assets **shall** be restricted by the **Third-party** in accordance with the established topic-specific **policy** on access control.			X	X			
8.4 Access to source code							
Read and write access to **source code**, development tools and software libraries **shall** be appropriately managed by the **Third-party**.			X	X		X	
8.5 Secure authentication							
Secure authentication technologies and procedures **shall** be implemented by the **Third-party** based on information access restrictions and the topic-specific **policy** on access control.		X					
8.6 Capacity management							
The use of resources **shall** be monitored and adjusted by the **Third-party** in line with current and expected capacity requirements.			X	X	X		
8.7 Protection against malware							
Protection against malware **shall** be implemented and supported by the **Third-party** by appropriate user awareness.		X					

Confidential

Initials:_____/_____

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

8.8 Management of technical **vulnerabilities**

Requirement							
Information about technical **vulnerabilities** of information systems in use **shall** be obtained by the **Third-party**, the **Third-party**'s exposure to such **vulnerabilities shall** be evaluated and appropriate measures **shall** be taken.			X	X		X	X

8.9 Configuration management

Requirement							
Configurations, including security configurations, of hardware, software, services and networks **shall** be established, documented, implemented, monitored and reviewed by the **Third-party**.		X					

8.10 Information **deletion**

Requirement							
Information stored in information systems, devices or in any other storage media **shall** be deleted by the **Third-party** when no longer required.		X					

8.11 Data masking

Requirement							
Data masking **shall** be used by the **Third-party** in accordance with the organization's topic-specific **policy** on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.			X	X			

8.12 Data leakage prevention

Requirement							
Data leakage prevention measures **shall** be applied by the **Third-party** to systems, networks and any other devices that process, store or transmit sensitive information.		X					

8.13 Information backup

Requirement							
Backup copies of information, software and systems **shall** be maintained and regularly tested by the **Third-party** in accordance with the agreed topic-specific **policy** on backup.		X					

Initials:_____/_____

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

8.14 Redundancy of **information processing facilities**

Information processing facilities shall be implemented by the **Third-party** with redundancy sufficient to meet **availability** requirements.			X	X	X		

8.15 Logging

Logs that record activities, exceptions, faults and other relevant events **shall** be produced, stored, protected and analysed by the **Third-party**.			X	X		X	

8.16 Monitoring activities

Networks, systems and applications **shall** be monitored for anomalous behaviour by the **Third-party** and appropriate actions taken to evaluate potential **information security incidents**.			X	X	X		

8.17 Clock synchronization

The clocks of information processing systems used **shall** be synchronized to approved time sources by the **Third-party**.		X					

8.18 Use of privileged utility programs

The use of utility programs that can be capable of overriding system and application controls **shall** be restricted and tightly controlled by the **Third-party**.			X	X	X		

8.19 Installation of software on operational systems

Procedures and measures **shall** be implemented by the **Third-party** to securely manage software installation on operational systems.			X	X	X		

8.20 Networks security

Networks and network devices **shall** be secured, managed and controlled by the **Third-party** to protect information in systems and applications.		X					

8.21 Security of network services

Security mechanisms, service levels and service requirements of network services **shall** be identified, implemented and monitored by the **Third-party**.		X					

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
8.22 Segregation of networks							
Third-party shall ensure that groups of information services, users and information systems are segregated in the **Third-party**'s networks.		X					
8.23 Web filtering							
Access to external websites **shall** be managed by the **Third-party** to reduce exposure to malicious content.				X			
8.24 Use of cryptography							
Rules for the effective use of cryptography, including cryptographic key management, **shall** be defined and implemented by the **Third-party**.		X					
8.25 Secure development life cycle							
Rules for the secure development of software and systems **shall** be established and applied by the **Third-party**.		X					
8.26 Application security requirements							
Information security requirements **shall** be identified, specified and approved by the **Third-party** when developing or acquiring applications.		X					
8.27 Secure system architecture and engineering principles							
Principles for engineering secure systems **shall** be established, documented, maintained and applied by the **Third-party** to any information system development activities.		X					
8.28 Secure coding							
Secure coding principles **shall** be applied by the **Third-party** to software development.			X			X	
8.29 Security testing in development and acceptance							
Security testing processes **shall** be defined and implemented by the **Third-party** in the development life cycle.			X			X	
8.30 Outsourced development							
The **Third-party shall** direct, monitor and review the activities related to outsourced system development.		X					

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

8.31 Separation of development, test and production environments

Requirement	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contracting
Development, testing and production environments **shall** be separated and secured by the **Third-party**.			X	X		X	

8.32 Change management

Changes to **information processing facilities** and information systems **shall** be subject to **Third-party**'s change management procedures.		X					

8.33 Test information

Test information **shall** be appropriately selected, protected and managed by the **Third-party**.			X			X	

8.34 Protection of information systems during audit testing

Audit tests and other assurance activities involving assessment of operational systems **shall** be planned and agreed between the tester and appropriate management of the **Third-party**.			X			X	

9. ADDITIONAL REQUIREMENTS

Requirement	Chapter						
	Baseline	Baseline Extended	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contracting

9.1 Change of **Information Security** Contact

Changes in the nomination of the **Third-party**'s **Information Security** contact **shall** be communicated to **DBG,** including name, mail address and phone number		X					

9.2 Changes in the internal controls system

Significant changes in the **Third-party**'s internal controls system affecting **information security shall** be communicated to **DBG should** the **Third-party** be considered **outsourcing**.		X					

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

9.3 Security incident notification

In the event of a security incident which may have compromised or has the potential to compromise **DBG data**, **DBG shall** be notified by the **Third-party** without undue delay. The notification **must** contain information on the disruption, on possible cross-border effects as well as on the technical framework conditions, in particular the suspected or actual cause, the information technology affected, the type of facility or installation affected as well as the critical service provided and the effects of the disruption on this service. Beyond the initial notification, **Third-party shall** reporting continue at least daily for the complete duration of the incident and cover at least the requirements of the initial notification. Notifications **must** be made/send to: +352 243 33555 and cert@deutsche-boerse.com. Vice versa, **Third-party shall** also provide a 24/7 emergency contact (mail and phone) to **DBG**.		X					

9.4 Audit and Information Rights

Third-party shall grant unrestricted audit and information rights by a) **DBG**'s 1st, 2nd or 3rd Line of Defense, b) **DBG**'s **Third-party** risk team, c) external auditors acting either on behalf of **DBG** and d) supervisory authorities or external auditors acting on behalf of the supervisory authorities.		X					

Initials:_____/_____

Confidential

Requirement	Chapter						
	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting

9.5 Annual Reports

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Third-party, if considered **outsourcing** and if the risk picture mandates it, **shall** submit an annual report on its overall security risk profile, covering at least relevant security risk scenarios and corresponding risk treatment strategies, as well as material incidents.		X					

9.6 **Fourth-Parties**

Requirement	Baseline	Baseline Exten-ded	Cloud	Data Outside DBG	Infra-structure	Develop-ment	Sub-contrac-ting
Third-party shall submit a list of all **Fourth-parties** involved in the delivery of services to **DBG** and therefore sub-outsourcings. It **shall** update that list without undue delay when **Fourth-parties** utilised in the service delivery are changed. If the **Third-party** is considered **outsourcing**, changes in the **Fourth-party** selection **shall** be made contingent on **DBG**'s approval.		X					

10. GLOSSARY

This glossary lists items that carry specific meaning in this **ISFA**.

Term	Definition
Affiliate	means any person that, directly or indirectly, controls, is controlled by or is under common control with such Party; the term "control" means the possession of (i) 50% or more of the voting rights in the general meeting of a person or (ii) the power, directly or indirectly, whether by contract or ownership, to direct or cause the direction of the management and affairs of a person, including investment decisions.
Authenticity	means the property that an entity is what it claims to be.
Availability	means the property of being accessible and usable on demand by an authorised entity.
BSI C5	means the C5 criteria catalogue (Cloud Computing Compliance Criteria Catalogue) by Bundesamt für Sicherheit in der Informationstechnik/ Federal Office for **Information Security** (BSI) specifies minimum requirements for secure cloud computing.
Confidentiality	means the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
DBG	Refers to Deutsche Börse Group, a group of companies comprised of Deutsche Börse AG (DBAG), 60485 Frankfurt and its Affiliates (within the meaning of § 15 Aktiengesetz).
DBG Data	means **DBG** information in electronic form that can be stored and processed by a computer. It (i) belongs to **DBG** (ii) is provided to **DBG** or (iii) originates from **DBG**.
Deletion	means a way of removing a file from a computer's file system and securely overwriting it.
Fourth-party	means parties that do not have a direct relationship with **DBG** but are utilised by the **Third-party** in the service provision to **DBG**.
Information asset	means information such as data, values or documents, and **information processing facilities** such as networks, systems and applications.
Information Processing Facilities	means any information processing system, service or infrastructure supporting business processes considering the physical location housing it.
Information Security	means the preservation of **confidentiality**, **integrity**, **availability**, and **authenticity** of information.
ISFA	means this **Information Security** Framework Agreement.
Information Security Event	means an identified occurrence of a system, service or network state indicating a possible breach of **information security policy** or failure of controls, or a previously unknown situation that can be security relevant.
Information Security Incident	means a single or a series of unwanted or unexpected **information security events.**
Information Security Management System (ISMS)	means a management system that defines the methodology, rules, procedures, measures, and control measures for protection of information in the organisation pursuant to the ISO standard series ISO/IEC:27001.

Initials:_____/_____

Infrastructure as a Service	means the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Integrity	means the property of accuracy and completeness.
"must"/"will"	means the implementation of/adherence to the requirement is mandatory.
"Modification"	means any amendment or change to this **ISFA**.
Outsourcing	means **outsourcing** as defined in (i) the EBA Guidelines on **Outsourcing** Arrangements (EBA/GL/2019/02), and (ii) the Minimum Requirements for Risk Management (MaRisk) circular by BaFin.
Parties	**Third-Party** and **DBG**
Penetration Test	means a security assessment which aims to identify the security **vulnerabilities** on the target systems that can be exploited by attackers.
Platform as a Service	means the capability provided to the user is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Policy	Intentions and direction of an organisation, as formally expressed by its top management.
Privileged Access	means users that need multiple accounts, some of which enjoy additional rights to perform administrative tasks, for example.
"shall"	Indicates a mandatory responsibility not subject to exceptions.
"should"	means that the implementation of/adherence to the requirement is mandatory, unless there is an unreasonable technological effort involved or a business justification for not implementing the requirement exists, is documented and available for review.
Software as a Service	means the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Source Code	Human readable code written in a specific code language.
State of the Art	means the **state of the art** as outlined in the "Guideline **State of the art** Technical and organizational measures" 2021, released by the European Union Agency for Cybersecurity (ENISA) in cooperation with the TeleTrusT – IT Security Association Germany

Initials:_____/_____

Third-party	means a legal or natural person having a direct relationship to **DBG**, usually through a contract as supplier or service partner.
Threat	means a potential cause of an unwanted incident which can result in harm to a system or organisation.
Vulnerability	means a weakness of an asset or control that can be exploited by one or more **threat**s.

- Signature Page Follows -

Initials:_____/_____

Deutsche Börse AG

Eschborn, _____   Eschborn, _____

Signature   Signature

Name: Name:

Position: Position:

[*Supplier*]

Place, date   Place, date

Signature   Signature

Name: Name:

Position: Position:

APPENDIX 1: **Affiliate**s

This list of DBAG **Affiliate**s may be amended by DBAG, eligible for amendment are companies that qualify as **affiliate**s under § 15 et sec. Aktiengesetz.

List of DBAG Affiliates:

Börse Frankfurt Zertifikate AG

Börse Frankfurt Zertifikate AG Central Functions & others

Clearstream Australia

Clearstream Banking AG

Clearstream Banking London

Clearstream Banking Luxembourg Central Functions & others

Clearstream Banking SA

Clearstream Banking SA Singapore Branch

Clearstream Banking SA Singapore Branch Central Functions & others

Clearstream Fund Centre AG

Clearstream Global Security Services Ltd. Cork

Clearstream Global Security Services Ltd. Cork Central Functions & others

Clearstream Holding AG

Clearstream International SA

Clearstream Operations Prague s.r.o

Clearstream Operations Prague s.r.o Central Functions & others

Clearstream Services

Clearstream Services SA

DBAG Cash

DBAG London

DBAG Paris

Deutsche Börse Beteiligungen GmbH

Deutsche Börse Digital Exchange Central Functions & others

Deutsche Börse Photography Foundation GmbH

Deutsche Börse Services s.r.o.

Initials:_____/_____

Deutsche Börse Systems Inc (USA)

Deutsche Börse Systems Inc (USA) Central Functions & others

European Commodity Clearing AG

Eurex Clearing AG

Eurex Clearing AG Prague

Eurex Frankfurt AG

Eurex Frankfurt AG Singapore Branch

Eurex Global AG

Eurex Global AG Central Functions & others

Eurex Repo GmbH

European Energy Exchange AG

Lux CSD SA

Regis-TR SA Limited

Regis-TR UK Limited

Regulatory Services GmbH GER

Regulatory Services GmbH UK Branch

Stoxx Limited Frankfurt

Stoxx Limited London

Stoxx Limited New York

Stoxx Limited Tokyo

Stoxx Ltd Switzerland

Stoxx Ltd. Prague

Initials:_____/_____

APPENDIX 2: Applicable Chapters

The following Chapters are applicable and constitute binding obligations of Third-party:

[Pls insert]

APPENDIX 2: Applicable Chapters