DEUTSCHE BÖRSE GROUP

Cloud Usage Policy

Version: 1.5

Valid From Date: 13.10.2025

Last Review Date: 19.08.2025

Notes: This written rule uses gender-neutral and inclusive language. Whenever possible, the generic masculine is avoided and all employees of any gender identity (m/f/d) are addressed.

Content

1. Purpose, Objectives and Basis

1.1. Purpose and Objectives

The purpose of this Policy is to provide general guardrails for the management (incl. usage and deployment) of public cloud services for Deutsche Börse AG (DBAG) and adopting legal entities (LE) of Deutsche Börse Group (DBG).

The objective of this Policy is to outline the scope, roles & responsibilities, processes and requirements, which are mandatory for the management (incl. use and deployment) of public cloud services.

Cloud computing is defined by NIST (Link) as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Cloud services are composed of the three service models Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) and the four deployment methods private cloud, community cloud, public cloud and hybrid cloud. The terms are defined in detail in the definition chapter.

In addition to the below mentioned external Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, the following external requirements are relevant for some of the LEs that are part of the Deutsche Börse Group. If these LEs are using the cloud landing zones provided by DBAG, these external requirements are relevant for the cloud landing zones as well.

BaFin:
- Circular / Rundschreiben 05/2023 – Minimum Requirements for Risk Management / Mindestanforderungen an das Risikomanagement (MaRisk)
- Guidance 02/2024 on outsourcing to Cloud Service Providers / Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbieter

CSSF:
- Circular CSSF 25/883 amending Circular CSSF 22/806 on outsourcing arrangements
- Circular CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597 (regarding Central administration, internal governance and risk management)

EBA:
- EBA/GL/2019/02 – EBA Guidelines on outsourcing arrangements

ESMA:
- ESMA Guidelines on outsourcing to cloud service providers ESMA50-164-4285

MAS:
- Guidelines on Outsourcing (covers also cloud computing)
- MAS Technology Risk Management (TRM) Guidelines
- MAS Notice 655 - Cyber Hygiene
- ABS - Cloud Computing Implementation Guide
- MAS Circular on Cyber Risk of using Public Cloud
- MAS Notice 658 Management of Outsourced Relevant Services for Banks

FCA:
- FG 16/5 Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services
- PRA Supervisory Statement SS2/21 Outsourcing and third party risk management

EDPB (European Data Protection Board, also as successor of WP29):

- Guidance and opinion on Cloud Computing under the GDPR and previous regulation
- Guidelines on supplementary measures

EU Member States Data Protection Regulation (Data Protection Authorities from EU Members):

- Guidance on Cloud Computing under the GDPR as implemented in by national regulations

FINMA:

- Rundschreiben 2018/3 – Auslagerungen bei Banken und Versicherungsunternehmen
- Rundschreiben 2008/21 – Operationelle Risiken Banken insb. Anhang 3; Grundsatz 9 - Umgang mit elektronischen Kundendaten
- Schweizerische Bankiervereinigung (SBVg) Cloud Leitfaden
- Art. 47 Bundesgesetz über die Banken und Sparkassen (BankG) – Bankgeheimnis

DORA (Digital Operational Resilience Act):

- Regulation (EU) 2022/2554 on digital operational resilience for the financial sector

1.2. Basis of this Written Rule

Considering the definitions of the Written Rule Framework Guideline (chapter 3 – Definitions and requirements), this written rule is based on:

X	**External Requirements**	DORA (Digital Operational Resilience Act): Regulation (EU) 2022/2554 on digital operational resilience for the financial sector
X	**High-risk activities**	This Policy prevents operational risks in accordance with risk taxonomy of DBAG by defining appropriate processes and requirements mandatory for the use of cloud services.
X	**Strategy of DBAG**	Cloud Strategy

Table 1: Basis of this Written Rule

2. Functional Scope and Target Groups

2.1. Functional Scope of applicability

Entity	DBAG and adopting LE within DBG
Area	All areas

Table 2: Scope

2.2. Target groups

Target group	Key message
All employees managing, using, or deploying cloud services …	… must know the requirements of this Policy and apply them.

Table 3: Target groups

3. Definitions

This chapter outlines the definitions of a core set of terms used in this Policy.

Cloud service models:

- **Software-as-a-Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.
- **Platform-as-a-Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- **Infrastructure-as-a-Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications.

Cloud deployment methods:

- **Private cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud:** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

- **Public cloud services** refers to all three cloud service models running in a public cloud
- **Public cloud platforms** refers to IaaS and PaaS in the public cloud

- **Cloud applications** refers to applications, self-developed or bought, running on top of the public cloud platforms

- **Cloud Landing Zone is** a pre-defined, secured, multi-area environment that is ready to onboard different workloads and teams in an automated manner. The goal of a landing zone in the Cloud is to have guardrails in place that allow you to onboard different teams and applications and divide them over multiple accounts so that the workloads are secured and isolated and where security controls are managed centrally.

4. Minimum Requirements

This Policy outlines the minimum requirements to which DBAG and/ or adopting LEs within DBG must adhere to ensure public cloud services are appropriately managed.

1. Preconditions for making use of public, DBG-available cloud services

In case a LE within DBG wants to use public cloud services already onboarded by DBAG, the LE must ensure that a valid intercompany contract between DBAG and LE is in place. The intercompany contract allows and governs the usage of cloud services by the LE.

Prior to the use of any cloud service run in a public cloud, it is the responsibility of the business owner of DBAG or the respective LE which wants to make of use the cloud services, to make sure to be compliant with the CSP Secure Landing Zone (SLZ) and associated security baselines.

In addition, the business owner has to make sure to follow other applicable internal processes (e.g., MCP, Outsourcing and CLM) to ensure that technical provisioning and operations are in line with security and regulatory compliance requirements, and to obtain all internal and regulatory approvals which might be required.

The business owner must also consider operations, security, reliability, performance & cost, as well as architecture aspects of the cloud application.

2. Minimum requirements for cloud-based applications

As a minimum, the business owner of a new cloud-based application must:

a. Fill in the Materiality Assessment Questionnaire as part of the MCP or ensure the cloud-based service or application is covered by an existing MCP change; and
b. Fill in the Outsourcing Pre-Assessment; and
c. Document applications as part of the standard application onboarding process, especially including the cloud architecture review as well as the exit action plan and the information security risk assessment; and
d. Utilize cloud services in compliance with the SLZ requirements and associated security baselines.

3. Governance and Lifecycle Management

The Cloud CoE or Cloud Governance, as the case may be, must perform the MCP review and contract reviews. Contract reviews are executed via the Contract Lifecycle Management process.

In case an application or service in the public cloud is not used anymore, the responsible business owner needs to inform Outsourcing, the Cloud CoE and has to decommission the application or service within the application inventory.

4. Cloud Service Provider (CSP) onboarding and contract handling

The onboarding of new CSPs for the service models IaaS and PaaS must be managed by the Cloud CoE in conjunction with other functions like Legal, Outsourcing and Purchasing. The Cloud CoE is also responsible for the ongoing management of the contracts with these CSPs, including the monitoring of the fulfilment of all contractual obligations by the CSPs.

Onboarding of a new CSP for SaaS services is managed by Corporate IT in collaboration with other functions like Legal, Outsourcing, Purchasing and the Cloud CoE. Onboarding of SaaS solutions, outside of SaaS services provided by Corporate IT, is managed by the relevant business owner. The Cloud CoE has to be informed of all CSP SaaS onboardings.

CSP contracts are owned and managed by DBAG unless they are SaaS solutions, outside of SaaS services provided by Corporate IT, and only relevant for a specific Legal Entity or department.

5. Roles and Responsibilities

This chapter provides a high-level overview of cloud-related functions, roles, and their responsibilities.

LEs are advised to leverage the provided secure landing zones but have the that are using the centrally provided cloud services have to leverage the provided secure cloud landing zone but have the flexibility to tailor these roles to their organizational context. A LE that doesn’t use the provided secure landing zone, is not centrally supported and has to ensure adherence to regulatory and security requirements independently.

All responsibilities must be allocated, and activities performed regardless of role title. A LE may not have all the roles outlined below but choose different titles and combine or distribute tasks among other roles.

CSP contracts are owned and managed by DBAG unless they are SaaS solutions, outside of SaaS services provided by Corporate IT, and only relevant for a specific LE or department.

5.1. Chief Cloud Officer

The Chief Cloud Officer (CCO) is responsible for the DBAG cloud strategy in line with the overall DBG business and IT strategy. For IaaS and PaaS cloud activities, the CCO is responsible for the vendor contracts and vendor relationships. The CCO is accountable for the provisioning of IaaS and PaaS services to DBG IT in accordance with DBAG policies and standards, and with the relevant regulations.

In line with regulatory requirements, multiple cloud officer functions are defined: one Chief Cloud Officer, Corporate IT Cloud Officers, and LE Cloud Officers (where implemented). The Cloud

Officers (CO) manage and monitor the implementation of the cloud services according to legal, security and compliance requirements. The different CO functions have a duty to collaborate to ensure that cloud initiatives are comprehensively in line with applicable regulation.

The CCO is the business owner for the intercompany outsourcing relationship providing the IaaS/PaaS platform services from DBAG to DBG LE. The CCO is **not** responsible for outsourcing relationships from other LEs to DBAG for services running on top of IaaS/PaaS platform services itself, however, keeps responsibility as business owner for the CSP platforms. A detailed description of the responsibilities is covered within the respective SDS. The decision to use the IaaS/PaaS as provided by DBAG remains with the LE.

Furthermore, the CCO is responsible for monitoring the execution of this Cloud Usage Policy as well as for maintaining the Policy according to DBG Policy guidelines.

5.2. Legal Entity Cloud Officer function

LE may implement a Cloud Officer function, which coordinates the assurance of regulatory compliance of cloud usage according to the regulations relevant for the LE. The LE Cloud Officer collaborates with 1st and 2nd lines of defense and guides project teams to make sure risks specific to the use of cloud services are identified, assessed and managed. The LE Cloud Officer provides expertise and supports the oversight of outsourcing activities related to the use of cloud services, the management of the relation to the local regulator incl. potential notification or approval requests with regard to arrangements for the use of cloud services and supports the overall adoption of the cloud strategy within the LE.

5.3. Cloud Centre of Excellence (CCoE)

The Cloud CoE is responsible for the design and the implementation of a framework for standardized IaaS/PaaS cloud usage of Microsoft Azure and Google Cloud Platform (GCP). Integral part of the Cloud CoE is Cloud Platform Engineering (CPE).

The Cloud CoE provides access to and the possibility to use the public cloud services by performing, among others, the following tasks:

- Maintain and publish up-to-date platform security documentation and risk assessments,
- Handle overall billing and cost distribution to the cloud platform users,
- Provide cost management best practice and advice to the cloud platform users,
- Prepare and execute ICT disaster recovery tests on platform level, informing BO of critical applications of such tests
- Implement compliance and security safeguards as outlined in the cloud platform security concepts,
- Drive implementation of adequate security controls in alignment with Group Security,
- Monitor the contractually agreed SLAs per CSP and publish appropriate KPIs,
- Share best practices, including expert advice and training possibilities for all DBG cloud users,
- initial setup and configuration of the public cloud platforms, in line with requirements from security and regulatory compliance
- Drive the monitoring, on an ongoing basis, of the cloud service provider’s performance, including exercising the rights of access, inspection and audit

The onboarding of new CSPs for the service models IaaS and PaaS is managed by the Cloud CoE in conjunction with other functions like Legal, Outsourcing and Purchasing. The Cloud CoE is also responsible for the ongoing management of the contracts with these CSPs, including the monitoring of the fulfilment of all contractual obligations by the CSPs.

5.4. Corporate IT

Corporate IT is responsible for providing SaaS Cloud services to DBG users, including End User Workplace, IT Business Processes and Customer Care services, in line with requirements from security and regulatory compliance analogue to the Cloud CoE responsibilities. These services might be hosted on selected CSP infrastructures or platforms. Additionally, Corporate IT manages and provides the SAP Cloud services – SaaS, PaaS/IaaS – to DBG users.

For the SaaS solutions provided by Corporate IT, Corporate IT is responsible for the onboarding, the vendor and contract management as well as ensuring the technical provisioning and operations in line with requirements from security and regulatory compliance. If different functions within DBG, including the Cloud CoE, purchase a SaaS solution outside of SaaS solutions provided by Corporate IT, this function is responsible for the onboarding, the vendor and contract management as well as ensuring the technical provisioning and the operations in line with security and regulatory compliance requirements.

Onboarding of a new CSP for SaaS services is managed by Corporate IT in collaboration with other functions like Legal, Outsourcing, Purchasing and the Cloud CoE. Onboarding of SaaS solutions, outside of SaaS services provided by Corporate IT, is managed by the relevant business function. The Cloud CoE has to be informed of all CSP SaaS onboardings.

5.5. Purchasing

Purchasing is involved in the onboarding process of new CSPs. They support the conduct of the vendor risk assessment as part of the outsourcing risk assessment. Purchasing monitors the vendors and shares relevant alerts with the Cloud CoE.

5.6. Enterprise Architecture & Digital Innovation

Enterprise Architecture and Digital Innovation (EA&DI) is responsible for managing cross product-line and future-state architecture, and facilitates, sets and promotes Technology Standards. It also seeks to define more detailed technology strategies and develop intentional innovation capabilities & competencies. EA&DI ensures critical stages of activity along the path to successful innovation are not neglected.

Minimum architecture requirements can be found in the EA Guideline.

5.7. Cloud Governance

Cloud Governance manages the regulatory and mandatory requirements for cloud services and maintains the cloud control catalogue. Cloud Governance contributes to a secure and compliance cloud secure landing zone by performing, among others, the following tasks:

- Provide the LEs with all information reasonably required to determine and assess regulatory compliance stemming from the use of IaaS/PaaS cloud services
- Control the geographic regions where cloud services are run and data is stored in the cloud, in line with regulatory requirements
- Facilitate a centralized review of cloud initiatives and relevant documents throughout the MCP review
- Informing Regulatory Outsourcing Management on changes to sub-outsourcers of the CSPs.

5.8. Group Security

Group Security manages the Mandatory Control Framework (MCF) (link), which must be used for the onboarding of all public cloud services. The MCF is the collection of all security controls, which are used to generate the Security Scope Document (SSD). The SSD is the basis for the risk assessment together with the security document. The creation of the security document and the SSD is the responsibility of the business owner of the service or application which is moving workloads into the public cloud.

5.9. Chief ICT Risk Officer / CISO

Chief ICT Risk Officer / CISO is a department under the Chief Risk Officer and is the 2nd line of defense function providing the ICT Risk Framework including Information Security in Deutsche Börse AG. In its capacity as a control function, Chief ICT Risk Officer / CISO sets DBG's framework for ICT risk, which includes information security management, provides governance and control over the associated management system, and evaluates the resulting risk posture.

5.10. Core Infrastructures Services

Core Infrastructure Services operates central security services like authentication services, key management, vulnerability and compliance scanning, web-application firewalls etc. for infrastructure and applications independent if they run on-premise or in a public cloud. Additional, Core Infrastructure Services is responsible for central network services e.g., DNS, proxy, and firewalls for the on-premise as well as for public cloud infrastructure.

5.11. Group Legal

Group Legal supports the negotiations with CSPs and provides advice on contractual compliance with regulatory requirements.

5.12. Regulatory Outsourcing Management

The Outsourcing Management teams from the regulated LE, in close cooperation with Regulatory Outsourcing Governance, are responsible for the overall Outsourcing Framework and related processes. The Outsourcing Management teams from the regulated LEs conduct the necessary steps of the Outsourcing process of planned cloud activities relevant for the LEs as well as maintain the central Outsourcing register in alignment with the CCO.

5.13. Business Owner

For each cloud usage a responsible representative must be identified as the business owner (BO) of the service. The BO must obtain all required approvals and be compliant with all relevant company policies as well as regulatory requirements. This means, among others, that the BO has to:

- Trigger the outsourcing assessment and if the BO is also the Information Owner, the information classification,
- Ensure that all required service definition statements are in place for the outsourced service,
- Oversee that all required risk assessments are executed and collect corresponding evidence,
- Collect relevant LE board approvals if required by the Outsourcing and Material Change Processes
- Monitor and oversee the outsourcing relationships,
- Ensure that Business Continuity Management is fully covered,
- Execute ICT disaster recovery tests for critical applications,
- Use the resilience setup provided by the Cloud CoE, esp. with regards to RPO / RTO

Prior to the use of any cloud-based applications, it is the responsibility of the Business Owner of the LE which wants to use the cloud services, to follow the internal processes (e.g., MCP, Outsourcing and CLM) to ensure that technical provisioning and operations are in line with security and regulatory compliance requirements, and to obtain all internal and regulatory approvals which might be required. The Business Owner must also consider operations, security, reliability, performance & cost, as well as architecture aspects of the cloud application.

In case the business owner does not belong to DBAG but to another LE, the BO has to ensure that there is an outsourcing agreement, e.g., an SDS, and oversight in place between the LE and DBAG.

If different functions within DBG purchase a SaaS solution outside of what is provided by Corporate IT, the BO is responsible for the vendor and contract management as well as technical provisioning and operations in line with security and regulatory compliance requirements.

Nevertheless, this Cloud Usage Policy still fully applies, which means that the CCO needs to be informed by the BO and that an MCP incl. Outsourcing Pre-Assessment, and subsequent risk assessments if required, is conducted.

5.14. IT Product Organization

The IT product teams are responsible to run services in the cloud, e.g., application operations, according to all security and compliance requirements as outlined by the applicable DBG policies and standards.

All product IT teams must use the DBG secure landing zone that is provided centrally.

5.15. Data Protection

Data Protection advises the BO on

- GDPR requirements,
- Other applicable personal data protection regulation and guidelines of data protection authorities related to Cloud computing, in particular related to contractual requirements[1],
- The necessary organizational protective measures,
- Data protection by design and default requirements,
- Appropriate safeguards for potential transfer to or access from a third country outside of the European Union, and on Transfer Impact Assessment where applicable.

The BO needs to document Cloud usage within the DBG record of processing activities while Data Protection monitors the data protection compliance of the Cloud usage within its second line control activity. In case of a higher risk processing of personal data within a Cloud usage, the BO mandatorily needs to conclude a Data Processing Impact Assessment and involve Data Protection for advice.

5.16. Internal Audit / Collaborative Cloud Audit Group

Internal Audit is a permanent function that, as the third line of defense, delivers independent, objective assurance and consulting services designed to add value and improve Deutsche Börse Group's operations. Internal Audit of DBAG, ECAG, CBF and CBL participate in the Collaborative Cloud Audit Group (CCAG) which performs Cloud vendor audits for the European financial industry in a joint format.

5.17. Business Continuity Management

Business Continuity Management supports the Cloud Officers and business owners to ensure contingency planning for time critical services operated in cloud environments. This includes direct involvement in the relevant process steps, in particular contributing in assessing continuity risk and giving expert advice where needed. BCM provides a documented framework to assess requirements towards services and to ensure contingency planning and testing. This serves to ensure the continuing suitability, adequacy, and effectiveness of contingency arrangements.

[1] The CSP acts in general as a processor acc. art. 28 GDPR

6. Appendix

6.1. Contact Information

Written Rule Owner: Head of Unit Cloud Governance

6.2. Document History

Document History

Version	Date	Changes & Background
1.0	24.02.2020	Initial version
1.1	20.10.2021	Annual review
1.2	25.11.2021	Adjusted role description for 3.1.10 and 3.1.11
1.3	10.10.2022	Annual review, added role descriptions 3.1.14, 3.1.15, 3.1.16
1.4	27.03.2024	Minor updates for 3.1.3, 3.1.6, 3.4, 3.5,
1.5	01.10.2025	Minor update in light of Written Rules Framework Guideline implementation and organizational changes.

Coordination before publication

Version	Date	Task	Function
1.5	19.08.2025	**Creator**	Cloud Governance
	19.08.2025	**Content Review**	Cloud Governance
	29.08.2025	**Content Confirmation**	HoU Cloud Governance

Approvals

Version	Date	Task	Function
1.5	13.10.2025	**Approval**	Chief Cloud Officer

6.3. Related Written Rules

Superordinated Written Rules	• *N/A*
Subordinated Written Rules	• *N/A*

***** END OF DOCUMENT *****