Deutsche Bank

Third Party Control Obligations

Third Party Control Obligations

Contents

Third Party Control Obligations

1. Introduction

This document contains an indication of control obligations applicable to third parties providing services to Deutsche Bank (DB). While contractual arrangements take precedence, third parties may find this document useful as a point of reference to understand the type of controls that will apply during vendor and service risk assessments at onboarding and periodically while working with DB.

1.1. Interpretation

A supplier, vendor or third-party service provider, for purposes of this document, is any third party that provides a product or service to a member of Deutsche Bank group ("Supplier") including its owners, officers, directors, employees, consultants, affiliates, contractors and subcontractors and any reference to personnel in this document includes its own personnel and the personnel of any subcontractors.

1.2. Applicability

This document should be considered as a DB requirement in case of a Supplier responding to a request for proposal or any other offer to provide goods and services to Deutsche Bank. Suppliers are expected to establish the control obligations set out in this document and continue to monitor at regular intervals their compliance. Where there is a conflict between this document and any local legal and regulatory requirements or any agreements with Deutsche Bank, the local legal and regulatory requirements or the agreement will govern. Upon the start of an engagement with Deutsche Bank, Suppliers should provide a copy of this document to its personnel who will be involved in the risk management of the goods and services and train them accordingly. It should be noted that provision of documentation outlined in this document to DB as part of the Third-Party Risk Management process will be dependent on the risk profile of the service provided to DB.

1.3. Compliance

For the avoidance of doubt, Deutsche Bank will always require that Suppliers fully comply with all applicable laws and regulations in the countries in which they are operating. Where necessary, Deutsche Bank expects Suppliers to respect this document within the context of customs and local law in the country in which they are operating. Suppliers are expected to report promptly any concerns or suspected violations of applicable law or regulations relating to Deutsche Bank.

Whilst this document is not in itself intended to be legally binding, its purpose is to raise awareness of the standards of risk management that Deutsche Bank expects of Suppliers. A failure to meet these control obligations will mean that there are less opportunities to work with Deutsche Bank. The legal obligations between Deutsche Bank and Suppliers will always be set out in the contract between such parties.

1.4. Implementation

Deutsche Bank requires its Suppliers to enter into an agreement with obligations addressing the control obligations listed in this document. For the avoidance of doubt, this document does neither constitute a complete or exclusive list of requirements, nor does it prevent or limit Deutsche Bank in identifying additional risks and asking for additional obligations.

Suppliers are required to participate in Deutsche Bank's vendor risk management process and provide evidence about their established control obligations meeting the requirements as set out in this document.

2. Anti Financial Crime (AFC)

Depending on factors such as the nature of the Supplier and the services being provided, the following controls may be applicable to mitigate the financial crime risk identified as part of DB's third party risk assessment process.

Control Title	Control Description
Code of business conduct	Supplier commits to conduct its business in a legal and ethical manner as demonstrated by Suppliers' policies or Code of Conduct.
Anti-Financial Crime Policy	Supplier prohibits engaging in financial crime including bribery and corruption, money laundering, terrorist financing and proliferation financing and complies with Sanctions regulations and requirements as demonstrated by the Suppliers' policies or Code of Conduct.
Anonymous reporting of violations	To enable employees to speak up, raise concerns, and anonymously report suspected or actual violation of law, regulation, firm policy or employee misconduct, Suppliers' policy should at a minimum include channels to raise concerns for anonymous reporting of suspected or actual breaches of law, regulation, firm policy, or employee misconduct.
Anti-Financial Crime training	To ensure awareness of applicable obligations relating to anti-bribery and corruption, anti-fraud, anti-money laundering, anti-facilitation of tax evasion and sanctions, and whistleblowing channels for employees to raise concerns anonymously, Suppliers' AFC training must cover these topics to ensure employees are equipped to detect and prevent financial crime, and to understand how to escalate when appropriate.
Anti-Facilitation of tax evasion	Where applicable, to mitigate facilitation of tax evasion risk, the Suppliers' policies require compliance with relevant tax laws in jurisdiction(s) where the Supplier operates and provides services to DB.

Third Party Control Obligations

Interactions with state-owned entities, government officials or politically exposed persons (PEP) on DB's behalf	Where applicable, to identify and manage potential financial crime risks, particularly bribery and corruption, in relation to the provision of services to DB, the Supplier must disclose all interactions with state-owned entities, government officials or politically exposed persons.
Former or current association, ownership, or shareholding in any form to DB, its subsidiaries, or affiliates	To identify and manage any potential financial crime risks, Supplier must disclose where its management has any association, ownership or shareholding in DB, its subsidiaries, or affiliates.
Associations with current or former public officials in the past 7 years	To identify and manage any potential financial crime risks, particularly bribery and corruption, Supplier must disclose any associations it or its management has with current or former Public Officials within the past seven (7) years.
Jurisdiction(s) involved in providing services	Specific to the services which are being provided to DB, Supplier must provide the list of jurisdiction(s) in/from which it will be providing services to DB, to assess the potential financial crime risks associated with business activity in high-risk jurisdictions.
Transaction monitoring controls	Where applicable, to identify, detect and mitigate potential money-laundering (including tax evasion), and sanctions and embargoes risks by ensuring that policy and procedure documents are in place and cover at a minimum: 1. checks on clients, activities, and products ("due diligence") 2. transaction structure reviews 3. risk-based filtering 4. documentation process including applicable laws and regulations 5. escalation path for "hit results"
Know Your Client (KYC) Controls	Where applicable, to mitigate potential financial crime risks, supplier to demonstrate KYC controls covering at a minimum: 1. Client due diligence: a) definition of client, product, and geographical risk factors b) identification process of contracting party c) identify verification process d) checks on the nature of the client's business
Vendor/client screening activities	Where applicable, to ensure appropriate vendor/client screening is conducted and the outcomes are addressed appropriately, Supplier to provide documents to support vendor/client screening activities, to include at minimum: 1. written procedures

	2. process flow for mapping during screening process 3. escalation processes 4. used screening list(s) have been agreed with DB 5. verification of hit results, 6. remediation actions taken for hit results 7. details of approvals required in the event of a hit 8. requirements for regular reporting
Fraud Prevention	When applicable, the supplier must have: 1. Processes in place to identify, document and address fraud risks which are reviewed on an on-going basis 2. Policy(ies) or procedure(s) which are reviewed on a regular basis that comply with applicable anti-fraud laws and regulations 3. Anti-fraud training to its employees

3. Business Continuity Management (BCM)

The following controls are applicable where potential operational disruption response and recovery risk, in relation to the services to be provided to DB, has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
Crisis management organisation /model	To ensure a timely and coordinated response to crisis situations and disruptive events, Supplier to have a crisis management organisation/model in place.
Business Continuity Plan (BCP)	To enable effective recovery from operational disruptions, Supplier to have a BCP for all processes related to the transaction meeting the following minimum requirements: - planning against the BCM scenarios - definition of roles and responsibilities for maintaining the BCM plan - documentation of Recovery Time Objectives (RTOs) for the services in scope
Business Continuity Plan (BCM Test) requirements	To ensure that the BCP is working in practice to enable effective recovery from operational disruptions, Supplier to conduct a BCM test (recovery test/ test of the BCM Plan) meeting the following minimum requirements: - all recovery strategies of the BCP have been tested in practice - roles and responsibilities for the BCM test have been documented

Third Party Control Obligations

Control Title	Control Description
	- test results have been documented - test has been conducted in the last 12 months
Call tree (or comparable communication channels)	To ensure that staff of the Supplier is informed about disruptive events and related invocation of recovery solutions to enable effective recovery from disruptive events, supplier to have an up-to-date call tree (or comparable communication channels) which has been tested within the last 12 months, meeting the following minimum requirements: - call tree covers all staff relevant for the service in scope - call tree has been tested in the last 12 months - call tree test results have been documented - call tree and call tree test cover DB representative (alternatively DB contact has been tested separately in the last 12 months)
BCM Training	To ensure that Supplier staff are familiar with the application of recovery solutions in case of operational disruptions, Supplier to conduct a BCM Training for the staff involved in the services provided to DB within the last 12 months.

4. Group Data Privacy (GDP)

The following controls are applicable where an inherent risk assessment conducted internally as part of DBs third party risk assessment process has identified that personal data is relevant to the provision of good or services to DB.

Control Title	Control Description
EU personal data processing in a third (non-EU) country	To ensure adherence to EU Data Protection Regulation, Supplier will be asked to attest if EU personal data be accessed, processed and/or stored as part of the service by the supplier, affiliates or any subcontractors in a third (non-EU) country for which the EU Commission has not declared data protection adequacy. Where the response to this question is "Yes", supplier will be asked to attest that EU standard contractual clauses are in place with any affiliates or subcontractors and to attest that a transfer risk assessment has been executed.
EU personal data subject to any law enforcement or government access request	If the response to the above question is 'Yes', the Supplier is asked to advise if they have been subject to any law enforcement or government request for access to or disclosure of EU personal data during the past 3 years. Where relevant, the supplier is asked to comment on whether any requests have been opposed or challenged.
High risk scenarios	To ensure proportionate due diligence across higher risk scenarios, Supplier will be asked to attest if the suppler, affiliate or subcontractor:

Third Party Control Obligations

Control Title	Control Description
	- will physically store EU personal data outside of the EU27 as part of the service. - shall have access to EU personal data related to anti money laundering investigations and related records, email content analytics, criminal convictions and offences from outside of the EU27. - shall have root access management for applications containing EU personal data from a third (non-EU) country for which the EU commission has not declared data protection adequacy.

5. Data and Records

The following controls are applicable where potential data and records risk has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
Records creation	If records are created and/or retained by the Supplier on behalf of DB, supplier is asked to attest that they meet the requirements within the "Records Management and Continued Retention Requirements for Third Parties" document which is shared during the sourcing process. Specifically: • For records created by the Supplier on behalf of DB, a list of record types including storage locations and retention periods (incl. triggers where required) and type of services provided for these records (creation, retention, retrieval, disposal) must be shared.
Records retention	Where retention is applicable, Supplier must attest that: • electronic records will be archived in a DB certified Enterprise Approved Electronic Archive (EAEA) or in a certified In Place Archive (an internally developed bank product that brings archiving to the records); • physical records will be retained in adherence with aforementioned document.
Records retrieval	Supplier attests that for records retained by Supplier on behalf of DB, an agreement for accurate and timely retrieval of records is in place and respective documentation will be provided to DB.
Records disposal	Supplier attests that for records retained by Supplier on behalf of DB, a record disposal approach is documented, and evidence is provided to DB that disposal can be executed in line with the aforementioned document.
Storing and/or processing data	Supplier attests to obtain approval in advance from DB through the Third Party Management change request process before storing or processing DB data in or from a new location; or performing new processing activities with DB data.

Third Party Control Obligations

Control Title	Control Description
	Upon request Supplier will provide full transparency and disclosure of all locations where it will store or process DB data; and provide full transparency and disclosure of all processing activities it will perform on DB data.

6. Compliance

The following controls are applicable where potential compliance risk has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
Complaints handling policy/procedure Complaints log/records	If Third Party interacts with clients and handles client complaints, they must have a complaint handling policy/procedure that contains a description of the process for handling client complaints and that corresponds to the standards of the DB Complaints Handling Policy. Additionally, Third Parties must maintain a complaints log/records documenting all complaints from clients as well as the action taken in response to the complaints.
Status Report on Regulatory Reporting Obligation/Performance	Where Third Party provides services that may be mandated to meet specific reporting requirements as mandated by law or regulation in any national, international or supranational organisation, ARM, APA or government agency that is responsible for the financial or non-financial supervision, oversight or regulation of the Bank's activities, they must provide regular overview of the status of the reporting including (but not limited to), breaches, late / amended disclosures, fines and errors.
Escalation framework	Where Third Party is involved in trade and transaction reporting, position reporting and /or regulatory reporting activities, they need to establish an escalation framework to handle reporting breaches, including escalation to management and notifications to regulators where required.
Inside Information	Where Third Party has access to DB Inside Information, they need to acknowledge the rules and regulations and criminal and civil penalties for the misuse of DB's inside information as per the EU Market Abuse Regulation Art 18 "Insider lists" and agree to signing the "EU MAR Art 18 Letter". As per the EU Market Abuse Regulation Art. 18 "Insider lists", issuers of financial instruments and any person acting on their behalf or on their account, shall each take all reasonable steps to ensure that any person with access to inside information acknowledges in writing the legal and regulatory duties entailed and is aware of the sanctions applicable to insider dealing and unlawful disclosure of inside information.

Third Party Control Obligations

Handling of client information	Where Third Party has access to DB proprietary and/or client confidential information, they must have written policies & procedures outlining the minimum requirements for appropriate handling of client confidential information and / or DB proprietary information.
Escalation of breaches	Where Third Party services involve access to client confidential information and/or DB Proprietary information, they must establish a process for escalation of breaches related to accidental leakage or misuse of confidential client information and / or DB proprietary information, which includes, at a minimum, documentation of breaches and sending of notifications to DB in the event of a breach.
Segregation of client assets	Where Third Party services involve holding or handling of client funds and /or taking deposits, Third Party must have written procedures in place documenting the process for segregation of client assets (funds or securities) including (but not limited to) correctly identifying, appropriately segregating, and treating them in accordance with applicable laws, rules and regulations. When handling or holding client funds, Third Parties must also have records of any client's assets held or handled directly or indirectly.
Communications and marketing material	Where Third Party services involve the provision of marketing activities to clients, Third Party must establish a periodic review process to ensure that communications and marketing material meet statutory and regulatory requirements and is clear, fair and not misleading.
Suitability & Appropriateness and Client Classification Policy/Procedure	If Third Party services involve selling, distributing, advising on products or other client-facing services, then the third Party must have - Suitability & Appropriateness Policy/Procedure that contains a definition of the process for ensuring that a product/service sold or advised to a client is suitable/appropriate for the client. Policy/ procedure should cover the fulfilment of related regulatory disclosure and record keeping obligations, and related employee qualification conditions. - Client Classification Policy/Procedure or process, that contains a definition of the process for classifying clients including related documentation/evidencing requirements and approval requirements.
Product Governance Policy/Procedure	If Third Party services involve selling, distributing or advising on products, deposit taking, credit, landing, or activities related to the (co-) manufacturing of products, then Third Party must have a Product Governance Policy/Procedure, that contains a definition of the process for determining the target market of end clients, incl. Distribution channels, for products or services manufactured or distributed.

7. Third Party Security (TPS)

Deutsche Bank Third-Party Security control requirements are aligned with the international standard ISO/IEC 27001.

8. Model Risk

The following controls are applicable where potential model risk to the utilisation of mathematical models in the service to DB including AI models has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
Provision of sufficient information and documentation	Supplier to provide sufficient information and documentation to DB to enable an appropriately skilled validation function replicate the outputs of the quantitative/qualitative model.
Testing results of the model/non-model estimate	To verify the model's accuracy and robustness, to assess potential limitations and the impact of assumptions under various scenarios, Supplier must provide: A. DB independent validation function access to the Suppliers system to perform independent testing of the quantitative/qualitative model; OR, B. Results of testing the quantitative/qualitative model for review by the DB Independent validation function; covering test scenarios specified by the DB independent validation function.
SME contact to address queries	Supplier to provide an appropriate SME contact who can address queries arising during validation or ongoing quantitative/qualitative model estimate lifecycle management.
Validation of the model/non-model estimate by third-party	To ensure the quantitative/qualitative model is validated to confirm that the model is performing as expected, in line with its design objectives and business use and to identify potential model limitations, the Supplier will be asked to attest that either: A. The quantitative/qualitative model estimate will be subject to internal but independent validation with oversight and effective challenge of its development, implementation, and use, against agreed standards and requirements. OR, B. The quantitative/qualitative model estimate will be validated by an independent (external) Supplier.
Share all Supplier validation results with DB	Supplier will provide the results and outcomes of any validation with the DB Independent validation function, including: A. Assumptions and deficiencies (limitations and weaknesses), supported by clear guidance on capabilities, limitations, and uncertainty; and B. Further evidence (such as information on input data /parameters/etc.) to support the validation outcome.

Third Party Control Obligations

Control Title	Control Description
Share evidence of the SAS 70/ SSAE-16/ SOC 1 validation (US only)	The Supplier is to provide evidence to the DB Independent Validation Function of the following (a SAS70/SSAE-16 review (US only) conducted by an independent party may be sufficient) which includes details of: A. Ongoing process controls in place for data inputs impacting the output; and, B. Adequate and appropriate methodology controls considered as part of development and testing; and, C. The implementation being supported by well-defined and documented testing activities; D. Adequate controls in place to prevent unauthorised changes/use.

9. Physical Safety

The following controls are applicable where potential physical safety risk has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
Physical safety audit	Supplier to provide evidence that they and relevant subcontractors which may access / store / handle confidential / strictly confidential data and / or DB assets adhere to robust physical safety and security standards by being audited against a relevant control system standard such as SSAE18 or ISAE3402. An audit report, such as SOC 2 Type II, PCI-DSS or another equivalent independent assessment showing no security-impacting findings may be deemed sufficient. OR In the absence of SOC 2 Type II reports covering all locations storing Confidential / Strictly Confidential data, supplier to provide risk assessments, security policies and concepts, security audit reports and / or relevant industry certifications (e.g. ISO27001:2013) for all the locations (including sub-contractor locations) storing Confidential / Strictly Confidential data.
Permissions and licenses	If the service involves the storage of DB assets outside of DB premises the Supplier (including any sub-contractors assigned to DB) will be asked to provide evidence of relevant permissions regarding physical security, personnel, and vehicle (if involved with transport / handling of DB assets / data) licenses from relevant local legislative authorities.
MAS TRM Guidelines	If the service involves critical systems as defined by the Monetary Authority of Singapore ("MAS") as identified an inherent risk assessment conducted internally as part of DBs third party risk assessment process the Supplier is asked to provide evidence that they meet all regulatory requirements as set by MAS TRM Guidelines related to physical security and environmental controls. Details of MAS TRM Guidelines are available here: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf.

10. Sustainability

The following controls are applicable where potential sustainability risk has been identified in an inherent risk assessment conducted internally as part of DBs third party risk assessment process.

Control Title	Control Description
EcoVadis or equivalent Environmental Social and Governance (ESG) rating	Supplier to provide an EcoVadis or equivalent ESG rating.
Human rights policies and programme	To ensure the Supplier adheres to the human rights standards, including prevention and remediation of adverse impacts, also in line with requirements of the German Supply Chain Due Diligence Act (SCDDA), Supplier should have policies or a programme in place to manage human rights related risks covering the following areas: - measures to assess and manage risks within your operations and supply chain - prohibition of the use of forced, compulsory, bonded, involuntary, or trafficked labour and measures to identify and respond to human rights-related violations - measures to prevent the use of child labour in your operations and supply chain and mechanisms to detect this should occur - grievance mechanism in place that can be easily accessed by employees, suppliers, and other people the supplier interacts with through its operations (e.g. members of the community) - measures to ensure that employees can choose to join labour unions, workers' councils, or other collective bargaining organisations - measures to ensure fair and timely payment of wages - measures to promote non-discriminatory working practices, including ensuring that there is no discrimination on the basis of race, class, nationality, religion, age, disability, gender, marital status, sexual orientation, union membership or political affiliation - process or mechanism to identify and respond to human rights-related violations within your operations or supply chain
Human Rights implementation	Supplier must evidence the implementation of the Human Right policy by demonstrating the following (when applicable): - Ensure all employment terms are available and accessible to employees - Provision of regular training program on ESG (environmental, social and governance) matters - Ensure health & safety policy, procedures and/or practices are in place

Third Party Control Obligations

Control Title	Control Description
	- Ensure appropriate, clean, secure, and safe living conditions to employees fitted with appropriate emergency requirements and containing adequate facilities - Ensure no breach of obligations related to the payment of tax or social security contributions
Environmental risks	To identify, assess and reduce environmental risks associated with the activities performed, also in line with requirements of the German Supply Chain Due Diligence Act (SCDDA), Supplier should have policies or a programme in place to manage environmental risks covering the following areas: - measures to assess and manage environmental risks within your operations and supply chain - procedures to manage and dispose of hazardous material (if applicable)

11. Subcontractors

Suppliers will be asked to declare use of subcontractors as part of the risk assessment process, for higher risk transactions the following controls will apply. The supplier will also be asked to provide details of the subcontractors which will be used as part of the third party risk management framework.

Control Title	Control Description
Subcontract any of its rights or obligations	Supplier must inform DB of the intention to subcontract any of its rights or obligations provided for in this arrangement to another supplier. At all times the supplier retains accountability to DB for the delivery of the arrangement.
Supplier risk management process or framework	Supplier must evidence that they have a third-party risk management framework in place covering items such as determination of their supplier's criticality, due diligence, risk management, ongoing monitoring, management, Transition / Exit / Termination Plans & Strategy are considered, where applicable.
Integrity assessment checks on their third-party population	Supplier must provide evidence that they perform integrity assessment checks on their own supply chain considering things like adverse media, sanctions, embargos, politically exposed people, conflicts of interest.
Financial stability checks on your third-party population	To ensure the supply chain are financially stable and not at risk at causing interruption to DB services, Supplier must provide evidence that they perform financial stability checks on their own supply chain.
Material subcontractors' requirements	A subcontractor is considered to be material where: • they receive onward disclosure of DB Client or employee data or other sensitive DB data (e.g. Financial data); or, • they perform licensed financial services activities in relation to the services delivered to DB (e.g. acting on or making decisions or commitments on behalf of DB, direct client interactions); or,

Third Party Control Obligations

Control Title	Control Description
	• there is a direct service extension to the subcontractor or an issue related to a subcontractor would directly result in a disruption of a measurable portion of the overall services; or, • they have unsupervised access to DB facilities or access to DB production systems. The Supplier is requested to demonstrate for each material subcontractor: • compliance with local privacy laws and regulations (GDP); • there is an Anti-Financial Crime (AFC) framework in place; • they undertake employee background screening (HR); and • they have implemented and tested Business Continuity Management (BCM) Plans.