Level 2

Information Security Principles – Deutsche Bank Group

Table of Contents

1. Introduction

1.1. Preamble

The Deutsche Bank Group (referred hereafter as 'Group' or 'DB Group') prospers on its reputation and the trust that is placed in it by its customers, shareholders, business partners and the wider business community. This reputation is founded upon the Integrity, reliability, and discretion with which the Group conducts all of its relationships and business activities. The Group operates in a business environment with an almost complete dependence on information, which is transported orally and in writing, processed and transmitted by information systems and interconnected computer networks and stored physically and electronically.

It is essential for the Group that the Confidentiality, Integrity and Availability of the Group's information are protected and risk is managed according to the Group's Risk Appetite and in accordance with legal and regulatory requirements. Thereby, the likelihood and/or impact of the corresponding financial, reputational and regulatory risks to the Group are managed.

The Management Board assumes full accountability for the Information Security risks of the Group and thereby delegates responsibilities according to the Information Security Principles and subordinate documents (i.e. IS Policies and IS Procedures). These documents define the frame of reference required to meet the Management Board's objective to manage the security of the Group's information within the Group's Risk Appetite.

1.2. Scope and Objectives

Information is an asset that is essential to the Group's business activities. Consequently, the Group's information needs to be protected independent of its form and across its 'life-cycle', i.e. whenever information is created, processed, transmitted, stored, archived or disposed.

Information Security ('IS') aims to preserve the three Key Security Objectives for information:

- Confidentiality: information is not made available or disclosed to unauthorised individuals, entities, processes and/or technologies;
- Integrity: information is accurate and complete; and
- Availability: information is accessible and usable upon demand by authorised individuals, entities, processes and/or technologies.

This Information Security Principles document ('IS Principles') states the Group's minimum requirements on how to manage Information Security risks to protect the Group's information with regards to Confidentiality, Integrity and Availability, regardless of where and how it is created, processed, transmitted, stored, archived or disposed. The minimum requirements contain IS Control Objectives, IS organisation, and the overall roles and responsibilities.

1.3. Applicability

These principles are applicable to all DB Legal Entities ('Deutsche Bank Group', 'the Group' or 'DB'). It applies to all Businesses, Regional Management and Control Functions (collectively 'Divisions and Functions').

The requirements of this Principle constitute the minimum requirements relating to Information Security for all DB Legal Entities and may be supplemented by additional regional, divisional or local policies and procedures as necessary. In case of a conflict between the IS Principles and local regulatory or legal requirements, the stricter obligation applies.

DB Legal Entities are defined as: Deutsche Bank AG including all its domestic and foreign branches; all subsidiaries (except for investments of short-term nature, typically less than 6 months or for trading purposes), with capital ownership > 50% or with capital ownership 50% or less but controlling influence of a DB Legal Entity.

In this document the term ‘Division and Function’ is used for all organisations affected by this document.

The IS Principles extend to the Group’s partners, vendors, service providers, third parties (excluding customers of the Group) and others if the Group’s information is handled by them. Those accountable for third party engagements must incorporate appropriate provisions into vendor service agreements and contractor agreements to the extent reasonably possible as outlined in the ‘Vendor Risk Management and Intra-Group Outsourcing Principles – DB Group’ and further detailed in the ‘Information Security Requirements for Vendors of Deutsche Bank’ (‘ISRV’) policy.

2. Information Security Management System (ISMS)

The Group has established an Information Security Management System (‘ISMS’) aligned to the international standard ISO/IEC 27001 with strong de-central responsibility and participation.

Each Division and Function is accountable for managing its Information Security risks. To enable effective and efficient Information Security management all Divisions and Functions are responsible for implementing the relevant parts of the ISMS in their area of responsibility (see Section 2.1.2).

2.1. Organisation

The ISMS of the Group combines Group-wide and de-central structures:

- Group-wide: the IS Risk Function (‘IRRM-ISR’) and the Chief Information Security Officer (‘CISO’)
- Divisional level: the Divisions and Functions

The design, implementation and operation of the ISMS reflect the nature of the Group and its Divisions and Functions with regard to:

- characteristics of the business
- organisation
- locations
- legal and regulatory requirements
- contractual requirements
- technical environment

2.1.1. Group ISMS

The Group ISMS consists of organisational structures, policies and processes that are performed at group level. The objective of the Group ISMS is to coordinate and consolidate the divisional activities (e.g. via central committees, maintenance of core principles and policies).

The IS Risk Function, the CISO, as well as the Divisions and Functions implement appropriate organisational structures which may include regional representatives. Interfaces between the IS Risk Function, the CISO and the Divisions and Functions ensure effective collaboration to achieve the objectives of the Group ISMS.

The Group undertakes the following activities in establishing, implementing, monitoring, maintaining and improving the Group ISMS:

1. identifying information and their associated Information Security requirements in terms of Confidentiality, Integrity and Availability
2. identifying, assessing and treating IS risks in line with the Group's IS Risk Appetite[1]
3. selecting and implementing controls to mitigate IS risks to an acceptable level of Residual Risk, that is in line with the Group's Risk Appetite
4. monitoring, maintaining and improving the effectiveness of controls associated with the Group's information

To ensure that the Group ISMS effectively protects the Group's information these activities are continually repeated to identify and manage changes in IS risks and/or the IS Risk Appetite aligned to the business objectives. The IS Risk Appetite is the aggregated level of IS risk that the Group is willing to assume within its risk capacity in order to achieve its business objectives.[2]

IS Risk Management targets financial, reputational and regulatory risks by following principles defined in the 'Principles for Managing Operational Risk – DB Group', 'Global Reputational Risk Principles – DB Group' and 'Regulatory Compliance Risk Management Principles – DB Group'. According to the Group's implementation of the Three Lines of Defence ('3LoD') model, the responsibilities for the Group ISMS and the IS Risk Management are split between the 2nd LoD (IS Risk Function) and the 1st LoD (CISO, Divisions and Functions):

- The 2nd LoD defines the Group's IS Risk Appetite Statement and sets the IS Risk Appetite
- The 2nd LoD defines the 'IS Risk Management Framework' in line with the IS Principles
- The 1st LoD manages the IS risks in accordance with the 'IS Risk Management Framework', the Group's IS Risk Appetite Statement and any additional requirements, which may be defined by the 1st Lines of Defence [3]
- The 2nd LoD independently identifies, assesses/challenges and reports on existing and upcoming IS risks

Details on the roles and the responsibilities for the IS Risk Function, the CISO, the Divisions and Functions are given in Section 2.2

[1] The Information Security Key Objectives are used as measurement scales for Information Security related risks. A breach of these Key Objectives is expected to lead to an adverse financial, regulatory and/or reputational impact. Based on impact and likelihood, the risks are projected against the Group's IS Risk Appetite. IS risks, that fall outside the Group's IS Risk Appetite, need to be treated with appropriate IS Risk Treatment Options, i.e. mitigation, acceptance, transfer or avoidance (see Appendix 'Risk Treatment Options').

[2] The IS Risk Function defines qualitative statements underpinned by (quantitative) metrics and corresponding tolerances for monitoring. The Risk Tolerances indicate whether the current risk level measured through a specific metric is acceptable or the risk exceeds the appetite. The implementation of suitable cost-effective controls mitigates unacceptable IS risks. Thereby, the corresponding financial, reputational and regulatory risks to the Group are kept within the Group's Risk Appetite.

[3] Some functions like the IS Risk Function are part of the 2nd LoD organisation. Regardless of their 2nd LoD roles these functions own the IS risks related to their information and therefore must manage them in the same way as the 1st LoD. To simplify wording we do not explicitly state that the 1st LoD requirements must also be fulfilled by these functions.

2.1.2. Divisional ISMS

As part of the Group ISMS each Division and Function designs, implements and maintains a Divisional ISMS with respect to its business context and in compliance with the IS Principles and the Group ISMS. The concept for a Divisional ISMS includes a justification for the appropriateness of the Divisional ISMS, assigned responsibilities and an implementation plan.

2.2. Roles and Responsibilities

2.2.1. IS Risk Function (2nd LoD)

The IS Risk Function is the 2nd LoD Risk Type Controller for the IS Risk Type as per the Group's Non-Financial Risk Taxonomy. Therefore, this function is responsible for:

- defining the Risk Taxonomy for the IS Risk Types
- setting the Risk Appetite for IS risks, in accordance with the Group's Risk Appetite Statement including qualitative statements as well as metrics and tolerances
- establishing an effective Risk Management Framework within the IS Risk Type including setting and monitoring of minimum control standards (i.e. Key Controls):
  - maintaining the 'IS Principles' for the Group including the IS Control Objectives
  - maintaining the 'IS Risk Management Framework' for the Group
  - developing and providing IS risk trainings and awareness measures for the Group
- challenging, assessing and reporting risks within the IS Risk Type:
  - coordinating the identification and harmonised assessment of Group-wide top IS risk scenarios (Group Top IS Risk process)
  - overseeing IS risks in 3rd party vendor relationships (IS Risk Third Party Governance)
  - challenging 1st LoD's assessments of IS risks (Risk and Control Assessments Challenge)
- monitoring the Group-wide adherence to IS risk tolerances
- performing 2nd LoD controls complementary to the 1st LoD controls:
  - overseeing relevant IS policies derived by 1st LoD
  - challenging Divisional ISMS regarding design & operational effectiveness (IS Vetting)
  - challenging 1st LoD's Risk and Control Assessments of controls in terms of design & operational effectiveness for IS risk exposure
- establishing independent Non-Financial Risk governance of IS risk, and reporting into the Group Non-Financial Risk Committee ('NFRC')

The IS Risk Function has a veto right for Group-wide IS topics (1st LoD) that are not in line with the defined IS Risk Appetite and/or IS Principles in regard to: IS Policies and Procedures, IS processes and IS services and IS technical solutions. If the IS Risk Function is vetoing, it needs to state the violated aspect(s) of the IS Risk Appetite statement and/or the IS Principles, the risks resulting from the violation and the expected consequences of the violation. The IS Risk Function informs all relevant stakeholders (including Group Audit) and addresses the veto to the Non-Financial Risk Committee ('NFRC'). If the veto cannot be solved by the NFRC, it is brought to attention of the Management Board.

2.2.2. Chief Information Security Officer (1st LoD)

The Deutsche Bank Chief Information Security Officer ('CISO') as a 1st LoD role is in charge of maintaining an appropriate level of Information Security protection Group-wide and end-to-end relative to the Risk Appetite defined by the IS Risk Function as 2nd LoD. As central owner of Information Security for the Group, the CISO develops and drives the implementation of the IS strategy and ensures that Group's information assets are adequately protected by

- Identifying, establishing and maintaining information security architecture and solutions that are integrated within the Group's IT architecture
- Mitigating identified and assessed IS risks by remediation actions or risk acceptance
- Providing security consulting and compliance services to the business divisions and functions
- Ensuring adherence to global and local regulatory IS frameworks and law/regulations in driving IS programs
- Developing and managing the Group's global IS policies and selected Group IS procedures
- Communicating a consistent view of Group's IS posture to internal/external committees by being the central point of contact

2.2.3. Divisions and Functions (1st LoD)

Each Division and Function is the 1st LoD Risk Owner for the IS risks related to its business or function. It is ultimately accountable for managing these risks. Particularly, each Division and Function is responsible for:

- designing, implementing and maintaining a suitable Divisional ISMS with respect to its business context and in compliance with the Group's requirements issued by the 2nd LoD functions as well as by the CISO; including ensuring compliance with legal and regulatory requirements for information handling
- managing all IS risks in their business/processes with an end-to-end process view within the defined IS Risk Appetite and in accordance to the 'IS Risk Management Framework'
- identifying, establishing and maintaining 1st LoD controls in line with the Group-wide requirements
- mitigating identified and assessed risks within the Risk Appetite by remediation actions, insurances, risk acceptances or ceasing/reducing business activities

The head of the respective Division or Function is ultimately accountable and therefore must be adequately involved in these activities.

2.2.4. Group Audit (3rd LoD)

The 3rd LoD provides independent and objective assurance on the effectiveness of risk management, internal controls and governance processes (internal audit).

2.3. Control Objectives, Controls and Key Controls / Minimum Control Standards

The IS Risk Function as 2nd LoD establishes mandatory IS Control Objectives as documented in the attachment to this document. The CISO defines Controls to achieve the IS Control Objectives. From these Controls, the IS Risk Function selects certain 'Key Controls' as minimum control standards for monitoring IS risks.

2.4. Rule-Setting Documents

2.4.1. IS Principles

The IS Principles sets the frame of reference for the Group ISMS in terms of organisation, processes, control domains and objectives.

2.4.2. IS Policies and Procedures

The CISO develops and owns the IS Policies and IS Procedures to detail the IS Principles. The CISO furthermore ensures accuracy and appropriate coverage of the IS Policies and IS Procedures against the Control Objectives within their remit. This includes regional/country, divisional and local IS Policies and IS Procedures, if required.

Table 1 shows the hierarchy of IS-related Policies and Procedures from a Group-wide view.

Owner	IS Risk Function (2nd LoD)	the CISO (1st LoD)	Divisions & Functions (1st LoD)
Level 2	IS Principles	-	-
Level 3	IS Risk Management Framework	Group-wide IS Policies (region/country IS Policies)	Divisional IS Policies (region/country IS Policies)
Level 4	IS Risk Management Procedures	Group-wide IS Procedures (region/country IS Procedures)	Divisional IS Procedures (region/country IS Procedures)

Table 1: Hierarchy of IS-related Policies and Procedures (Group-wide view)

2.5. Processes

2.5.1. IS Risk Management

Each Division or Function has the ownership of the information regarding its business and therefore it is the Risk Owner of the related IS risks. The IS Risk Management is detailed in the 'IS Risk Management Framework' and comprises the following activities:

1. Risk Identification and Assessment: Each Division or Function identifies and assesses the risks related to its information. This bottom-up approach is complemented by a top-down approach driven by the IS Risk Function to aggregate and harmonise the identified and assessed IS risks at the Group level ('Group Top IS Risk Process').
2. Risk Treatment: Each Division or Function decides on the treatment of its IS risks in accordance with the defined IS Risk Appetite (see Appendix 'Risk Treatment Options') the Group's IS Strategy, the Key Controls and Group-wide (technical) IS solutions. The appropriate risk treatment is selected in a cost-effective manner, i.e. by comparing the costs and efforts of implementing controls versus the benefits derived, while ensuring that legal and regulatory requirements are met.
3. Risk & Control Monitoring and Reporting: Each Division or Function monitors their owned IS risks and reports the identified risks to the IS Risk Function, the CISO and its management. This includes the treatment measures and residual risks as well. Furthermore, it periodically self-assesses its IS risks as well as the design and operational effectiveness of the controls. The IS Risk Function monitors the metric tolerances and independently reports on the IS Risk Profiles of the Divisions and Functions.

As part of the continual improvement, the CISO as well as each Division or Function review and improve implemented controls. The reviews are supported by the risk-driven challenges performed by the IS Risk Function.

2.5.2. Group Top IS Risk Process

The IS Risk Function coordinates the Group Top IS Risk Process which strives for consistency in identifying and assessing the top IS risks of the Group. The process compiles a list of relevant IS risk scenarios based on:

- input from the Divisions and Functions
- information on emerging IS risks from internal and external sources

The IS risk scenarios are discussed with experts in the Group and managers responsible for Information Security from the Divisions and Functions. To determine the residual risks, mitigating measures are mapped against the identified top IS risks. The Group Top IS risks are incorporated into the report for the Non-Financial Risk Management. Additionally, it provides a basis for senior management communication of top IS risks and for investment decisions.

2.5.3. Risk & Control Assessment (R&CA) and Challenge

As required by Group Operational Risk Management, each Division or Function periodically assesses the IS risks and the design & operational effectiveness of the controls in their business and processes. The Risk & Control Assessment ('R&CA') adopts a bottom-up approach in identifying relevant risks and related control weaknesses. If required risk treatment is initiated.

The IS Risk Function regularly conducts independent challenges of the assessments. It gathers business intelligence and builds an expected risk profile (from internal and external sources) which serves as a baseline. The IS Risk Function prepares a challenge report and submits it to the corresponding division. Feedback is analysed and follow-ups are performed where applicable. If required, the IS Risk Function escalates issues to the Non-Financial Risk Committee.

2.5.4. IS Vetting

The IS Risk Function performs vettings of Divisional ISMSes challenging their design and implementation/operation as defined in the 'IS Risk Management Framework'. The cycle for design vettings follows the review cycle defined in the 'Principles for DB Policies and Procedures – DB Group'. For operational vetting a risk-prioritised 3-year cycle has to be followed.

IS Vetting is coordinated between the IS Risk Function and the CISO Policy Office to comply with the requirements defined in the 'Information Security Policy Governance'.Findings and their resolutions are tracked in accordance with the 'Operational Risk Management Policy'.

2.5.5. Non-Compliance

The Group's Issue Management & Risk Acceptance processes apply to non-compliances to the IS Principles. The IS Risk Function should veto if IS Policies and IS Procedures are not in line with the IS Principles (see Section 2.2.1).

The CISO establishes a non-compliance process regarding its Group-wide IS Policies and IS Procedures. Legal and regulatory requirements must not be circumvented. The CISO ensures completeness and accuracy of IS Policies and IS Procedures. The same applies to regional and country IS Policies and IS Procedures.

2.5.6. IS Trainings and Awareness

The IS Risk Function develops and provides global IS trainings (based on identified required competences) and awareness measures. The training process follows a structured approach and training activities are formally documented. The CISO provides complementary specialist trainings.

2.6. Improvements

The IS Risk Function, the CISO, and the Divisions and Functions improve the design & operational effectiveness of the Group ISMS and its components (as defined in chapter 2.1.1) based on triggers such as Risk & Control Assessments (R&CA), IS Vettings, IS Assessments, benchmarks, certifications or audits.

Appendix 1 Glossary of Terms

Topic	Description	Source
Availability	Availability is the property of being accessible and usable upon demand by authorised individuals, entities, processes and/or technologies.	ISO/IEC 27000 (slightly modified)
Confidentiality	Confidentiality is the property information is not made available or disclosed to unauthorised individuals, entities, processes and/or technologies.	ISO/IEC 27000 (slightly modified)
Control	A control is a measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk.	ISO/IEC 27000
Control Objective	A control objective is a statement describing what is to be achieved by implementing controls.	ISO/IEC 27000
Committee	A Committee is a forum with decision-making authority established by a body, (an) individual(s) or a forum with respective responsibility for a task and corresponding authority to assign such responsibility.	Committee Governance Policy
Division	The Divisions (or 'Business Divisions') as per the current organisational structure of the Group.	./.
Divisional ISMS	Implementation of the ISMS within a Division or Function.	./.
Function	The term 'Function' as used in this document refers to one of Deutsche Bank's Infrastructure Functions or Regional Management. Infrastructure Functions cover a wide range of departments, including departments relating to personnel, financial reporting, technology and operations and other aspects of the Bank's infrastructure.	./.
Information	Information is an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of knowledge of the employees. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.	ISO/IEC 27000
Information Security ('IS')	Information Security is the preservation of Confidentiality, Integrity and Availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	ISO/IEC 27000
Information Security Management System ('ISMS')	The ISMS is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve Information Security.	ISO/IEC 27000

Topic	Description	Source
Information Security risk ('IS risk')	An IS risks is an effect of uncertainty on Information Security objectives; it is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation. The Group has defined a IS Risk Type with several subtypes.	ISO/IEC 27000
Information System	An information system is a application, service, information technology asset, or other information handling component.	ISO/IEC 27000
Integrity	Integrity is the property of safeguarding the accuracy and completeness of information and technologies.	ISO/IEC 27000
IS Policy	IS related Policy	./.
IS Principles	Information Security Principles (this document)	./.
IS Procedure	IS related Procedure	./.
IS risk	See 'Information Security risk'	./.
IS Risk Type	The IS Risk Type covers IS risks as per the Group's Non-Financial Risk (NFR) Taxonomy.	./.
ISO/IEC 27000 family	The ISMS family of standards is intended to assist organisations of all types and sizes to implement and operate an information security management system (ISMS).	ISO/IEC 27000
ISO/IEC 27000	The international standard ISO/IEC 27000 gives an overview and coins vocabulary for the ISMS family of standards (ISO/IEC 27000 family); we refer to the latest edition 2016.	ISO/IEC 27000
ISO/IEC 27001	The international standard ISO/IEC 27001 sets the requirements for an ISMS; we refer to the latest edition 2013.	ISO/IEC 27001
Key Controls	The Key Controls for a Risk Type define what, as a minimum, each Risk Owner needs to do in order to mitigate its related risks and to meet the relevant Control Objectives. For Information Security risks, 'Minimum Control Standard' is synonymous to 'Key Controls.'	./.
Minimum Control Standard	see 'Key Controls'	./.
Non-Financial Risk Committee ('NFRC')	The NFRC mandate is to ensure the oversight, governance and coordination of the Non-Financial Risk management in the Deutsche Bank Group on behalf of the Management Board and to establish a cross-risk and holistic perspective of the key Non-Financial Risks of the Group.	Principles for Managing Operational Risk – DB Group

Topic	Description	Source
Policy	Policies are the third highest ranking documents in the DB Policies and Procedures hierarchy; they implement associated Fundamentals and Principles while: i) providing additional specifications and guidance reflecting the requirements of a particular business division, infrastructure function, legal entity or jurisdiction; or ii) providing statements, specifications and guidance for a business or infrastructure subject matter concerning the whole DB Group on a global or local basis.	Principles for DB Policies and Procedures – DB Group
Principles	Principles are the second highest ranking documents in the DB Policies and Procedures hierarchy; they implement DB's fundamental values and provide guidance and information to facilitate the application and enforcement of DB's strategic objectives, governance and principal requirements from management, on a given topic. They apply to and bind affected employees of DB Group on a global basis.	Principles for DB Policies and Procedures – DB Group
Procedure	Procedures are the fourth-ranking documents in the DB Policies and Procedures hierarchy; they implement associated Fundamentals, Principles and Policies while: i) providing detailed process-related descriptions or unit-specific organisational processing rules for a particular business division, infrastructure function, legal entity or jurisdiction; or ii) providing detailed specifications and guidance for a business- or infrastructure subject matter concerning the whole DB Group on a global or local basis.	Principles for DB Policies and Procedures – DB Group
Risk	A risk is an effect of uncertainty on objectives.	ISO Guide 73
Residual risk	A Residual Risk is the risk remaining after risk treatment.	ISO Guide 73
Risk Appetite	The Risk Appetite is the aggregated level of risk that DB is willing to assume within its risk capacity in order to achieve its business objectives.	Principles for Managing Operational Risk – DB Group
Risk Tolerance	Risk Tolerance is a quantitative measure based on forward looking assumptions that allocates DB's risk appetite to business lines, legal entities, specific risk categories, concentrations, and, as appropriate, other levels. Tolerance is typically used in relation to risks for which DB has no material appetite (mainly non-financial risks). Limits most typically refer to risks for which DB needs to accept a certain level of exposure in order to achieve its objectives (mainly financial risks).	Principles for Managing Operational Risk – DB Group
Risk Type Controller ('RTC')	A Risk Type Controller is an independent 2nd LoD control functions, they control specific non-financial Risk Types as per the NFR Risk Taxonomy.	Principles for Managing Operational Risk – DB Group

Topic	Description	Source
Risk Owner	A Risk Owner is the person or entity with the accountability and authority to manage a risk. As a Risk Owner each Division and Function is accountable for managing IS risks within its field of responsibility.	ISO Guide 73/ Principles for Managing Operational Risk – DB Group
Rule-Setting Documents	Rule-Setting Documents refers to Fundamentals, Principles, Policies and Procedures.	./.

Appendix 2 Abbreviations

Topic	Description
3LoD	Three Lines of Defence
CISO	Chief Information Security Officer
COO	Chief Operating Office
FRR	financial, reputational and regulatory
IRRM	Information and Resilience Risk Management
IS	Information Security
ISMS	Information Security Management System
ISR	IS Risk Function
ISRV	Information Security Requirements for Vendors of Deutsche Bank
IS risk	Information Security risk
LoD	Line of Defence
NFR	Non-Financial Risk
NFRC	Non-Financial Risk Committee
ORM	Operational Risk Management
R&CA	Risk & Control Assessment
RTC	Risk Type Controller

Appendix 3 Risk Treatment Options

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The four basic risk treatment options are:

Risk Treatment Option	Description
Acceptance	take the particular risk
Mitigation	modify the particular risk by reducing the likelihood and/or the impact
Transfer	share the particular risk with another party or parties (including contracts and risk financing)
Avoidance	decide not to be involved in, or to withdraw from, an activity in order not to be exposed to the particular risk

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the financial, reputational and regulatory impact of the risk. Treating IS risks has different effects on the likelihood and impact of the Group's financial, reputational and regulatory (FRR) risks. The following table shows the effects:

Risk Treatment Option	Likelihood of FRR Risks	Impact of FRR Risks
Acceptance	no change	no change
Mitigation[4]	reduce likelihood	reduce impact
Transfer	no change	reduce impact
Avoidance	eliminate completely	eliminate completely

[4] In general, (preventive) controls primarily reduce the likelihood of FRR risks. However, controls may also reduce or only reduce the impact of risk exposure.

Appendix 4 Reference Documents

The following documents can be referenced to learn more about neighbouring topics and sub-ordinate subjects:

- Archive Principles – DB Group
- Corporate Governance Fundamentals – DB Group
- Data Leakage Management Policy – DB Group
- Electronic Communication Systems Principles – DB Group
- Group Information Security Management System (ISMS)
- Information Classification Policy – DB Group
- Information Security Policy Governance
- Information Security Requirements for Vendors of Deutsche Bank (ISRV)
- Information Security Risk Management Framework – DB Group
- Information Security Roles & Responsibilities – DB Group
- Operational Risk Management Policy
- Principles for DB Policies and Procedures – DB Group
- Principles for Managing Operational Risk – DB Group
- Records Management Principles – DB Group
- Risk Appetite Statement – DB Group
- Risk Management Principles – DB Group

Appendix 5 Document History

Version	Date	Author	Change Reason
0.1	22-Aug-2016	T.Staehle/R. Fischlin	Initial Draft
0.2	02-Sept-2016	T.Staehle/R. Fischlin	Draft for first stakeholder review
0.3	23-Sept-2016	T.Staehle/R. Fischlin	Revised draft, control objectives added
0.31	06-Oct-2016	T.Staehle/R. Fischlin	control objectives moved to attachment
0.4	16-Nov-2016	T. Staehle/C. Wittmann	integrated feedback from mandatory Stakeholder Review
0.5	23-Feb-2017	T. Staehle/C. Wittmann	Finalisation for next release
1.0	20-Mar-2017	T. Staehle/C. Wittmann	Finalisation after second review

Document Title	Information Security Principles - DB Group
Language	English
English Title	
Translation	No
Classification	Principle (Level 2)
Policy Producing Function	Information & Resilience Risk Management
Document Author	Tobias Staehle (tobias.staehle@db.com)
Document Approver	Carsten-B Fischer (carsten-b.fischer@db.com)
Portfolio Owner	Andy Murphy (andy.murphy@db.com)
Document Contact	Christine Monkowius
Legal or Regulatory Requirement	Yes
Functional Applicability	Deutsche Bank Group
Geographic Applicability	Global
Original Issue Date	08 January 1998
Last Review Date	30 March 2017
Next Review Date	30 March 2018
Version	5.0