1. **Purpose**

The purpose of this concept is to outline the requirements for corporate governance, risk management and internal control system ICS, and internal audit.   
The bank ensures that all employees possess the necessary risk understanding and attention.

1. **Legal and Regulatory Basis**

The basis of this concept consists of the following regulations:

* Rundschreiben FINMA 2017/01 Corporate Governance - Banken
* Rundschreiben FINMA 2008/21 Operationelle Risiken - Banken
* Rundschreiben FINMA 2023/01 Operationelle Risiken und Resilienz - Banken

1. **Organization and Responsibilities**

The bank places high importance on an effective risk management structure, recognizing it as a key factor in ensuring long-term success. Core elements of this framework include a transparent and comprehensive information policy, along with a well-balanced approach to managing and monitoring risks within the institution. This commitment underpins the bank’s efforts to build a resilient and sustainable risk management culture.

**The Three Lines of Defense Model**

The bank's risk management framework is structured around the Three Lines of Defense model, designed to enable the systematic identification and monitoring of risks. The first line of defense, as well as the compliance and risk management functions (both forming the second line of defense), are organizationally separated at the executive management level. The internal audit function, reporting directly to the board of directors, constitutes the third line of defense.

**Board of Directors**

The Board of Directors (BoD) establishes the overarching principles for risk management, including risk appetite and additional risk-related policies, as outlined in the primary risk governance framework. The BoD is also responsible for monitoring and regularly reviewing the adequacy and effectiveness of internal controls, including the risk and compliance management functions.

The BoD approves limits and reviews transactions involving significant strategic risks, provided these exceed the authority of the executive management. It ensures that it does not engage in operational activities that might compromise its oversight responsibilities.

The BoD is accountable for establishing and maintaining internal controls in the areas of operational risks, critical data, and Business Continuity Management (BCM). These responsibilities include:

* Annual approval of the risk inventory and risk appetite, particularly in the case of significant changes.
* Regular approval and oversight of strategies for ICT, cyber risks, critical data, and BCM.
* Authorization of critical functions and interruption tolerances as part of operational resilience.

**Executive Management**

The Executive Management (EM) is responsible for operational revenue and risk management. It approves the policies for identifying, assessing, measuring, limiting, and monitoring risks and ensures the availability of a suitable technological infrastructure. The EM provides periodic reports to the Board of Directors (BoD) on overall bank risks and compliance with risk policy guidelines. It also informs the BoD about measurement methods, models, and their implications for risk management.

The EM oversees the operational risk management processes and performs the following key tasks:

* Identifying and evaluating operational risks within the risk inventory in collaboration with the Risk Management department
* Promoting risk awareness among employees to mitigate risks
* Reporting to the BoD on the effectiveness of implemented controls
* Establishing and ensuring processes and controls for critical data with respect to confidentiality, availability, and integrity
* Analyzing cyber-attacks on critical ICT components and data and reporting significant incidents to FINMA

Additionally, the EM critically reviews operational risk reports, coordinates with the risk control function, and initiates necessary actions. It approves potential losses per the competency framework, adjusts the operational risk concept, and oversees emergency and crisis management. The EM keeps the BoD informed about the risk situation and acts immediately on high-impact incidents.

To fulfill its responsibilities, the EM is empowered to organize the necessary committees as required.

**First Line of Defense**

The risk owners, comprising the business units, form the first line of defense and are accountable for the profits and losses associated with the risks they undertake. They are responsible for the continuous and proactive management of these risks. Additionally, they ensure ongoing compliance with all risk policy requirements and consistently perform systematic control tasks on a regular basis.

**Second Line of Defense**

**Risk Control**

The bank’s Risk Management unit (Risk Control) serves as the risk control authority, functioning as the second line of defense. It is responsible for the comprehensive and systematic monitoring and reporting of both individual and aggregated risk exposures.

Risk Management reports directly to the CRO (a member of the Executive Management). The CRO ensures that Risk Control has access to the necessary human and technical resources, as well as the relevant information required to fulfill its responsibilities effectively.

Risk Control is organized according to the principle of independence. Specifically, this means that Risk Management staff operate independently of the bank’s revenue-generating activities. Furthermore, Risk Control holds unrestricted rights to request, access, and review any information or documentation needed to carry out its duties.

The tasks include among others:

* Participation in setting risk limits, aligned with the bank's risk tolerance and stress test results, to support operational management by the Executive Management
* Identification and monitoring of risks, ensuring adherence to risk policy guidelines and limits, including the implementation and quality control of risk measurement methods, stress tests, and scenario analyses
* Monitoring of risks and execution of risk measurement defined in the internal control system ICS

**Third Line of Defense**

It conducts independent reviews and evaluations of the adequacy and effectiveness of the organizational structure and business processes, with a particular focus on the internal control system (ICS) and the bank’s risk management framework.

1. **Risikomanagement**

**Identification**

Operational risks are identified and classified using a market-oriented approach. These risks are mitigated through corresponding controls and are aligned with the regulatory guidelines outlined in FINMA Rundschreiben 2008/21 and 2023/01, which provide standards for managing operational risks and ensuring resilience.

**Definitions and risk assessment methodology**

Operational risks are assessed comprehensively based on several perspectives: risk appetite, inherent risk, residual risk, and effective risk.

* Risk Appetite refers to the maximum level of risk the bank is willing to accept, determined by combining the likelihood of occurrence and the potential severity of an event.
* Inherent Risk represents the level of risk in the absence of any mitigating controls.
* Residual Risk refers to the remaining risk after implementing controls.
* Effective Risk is the periodically updated residual risk, recalculated by Risk Management based on recent incidents and key risk indicators (KRIs).

1. **Internes Kontrollsystem IKS**

The bank uses an internal control system tool, which provides an integrated overview of operational risks and the corresponding control inventory. By linking identified risks to their respective controls, it ensures a comprehensive and transparent view of both risks and control measures.

The Risk Control is responsible for maintaining and managing the control inventory. In close collaboration with risk and control owners, it makes necessary adjustments whenever required.

* The control inventory contains all critical information related to the execution of controls, including at minimum:
* A detailed description of each control,
* The frequency of control execution,
* The designated control owner, and
* The corresponding link to the relevant operational risk.

The Risk Management department is responsible for executing key controls and monitoring their compliance and implementation by the respective business units. This ensures that the bank’s operational risks are managed systematically and proactively.