Business Risk Manager – COO Office

Experience level : Intermediate
Entity : Bank Syz
Office : Geneva

The Business Risk Manager within the Chief Operating Officer "COO" division is accountable for the implementation of a comprehensive risk and control framework within the 1LOD COO functions, which will be designed and developed by and in close collaboration with the Chief Risk Officer and the Head of Internal Controls. Acting as a first line of defence, the role supports that the bank's infrastructure, governance, policies, processes, and services are resilient, well-controlled, and aligned with internal risk appetite and Swiss regulatory expectations.

The position partners closely with the various departments within the 1LOD COO function (such as IT, information security, physical security, facilities, operations, client reception, procurement, etc) acting as central interface within the first line of defence and in collaboration with the second line of defence.

Key responsibilities

- Identify, assess, and monitor risks associated to relevant COO owned processes
- Maintain controls framework for the relevant functions and processes, in line with the bank's internal/external regulation and risk appetite
- Regularly review and enhance the control framework, oversee its implementation and monitor the effectiveness of controls by the relevant control owners
- Closely collaborate with the key stakeholders within the COO function for the definition of action plans to mitigate residual risks and address control gaps
- Proactively escalate material incidents and control weaknesses to the COO, Chief Risk Officer and Head of Internal Controls

Governance, Reporting, Audit & Stakeholder Management

- Serve as a trusted risk partner to COO management and key stakeholders
- Act as central interface within the first line of defence for COO function and the second line of defence
- Key point of contact for internal and external auditors for the COO function
- Coordinate reporting on COO risk management matters to management committees

Change & Project Risk Assessment

- Under the guidance of the Chief Risk Officer, coordinates the implementation of operational, access, and resilience risk mitigation measures arising from new products, process changes, and system implementations

Operational Resilience, Business Continuity & Disaster Recovery

- Together with the Chief Risk Officer and Chief Security Officer, maintain and proposes updates to the Business Impact Analyses (BIA) to identify vulnerabilities, critical functions, and potential threats
- Under the guidance and in collaboration of the Chief Risk Officer and the Chief Security Officer identify document and test critical functions, review BCP' and DRP's
- Coordinate in collaboration with the Chief Security Officer Crisis exercises planning

- Coordinate in collaboration with the Chief Security Officer Crisis exercises planning
- Support the bank's operational resilience framework, with the aim to ensure continuity of critical services under severe but plausible scenarios in collaboration with the Chief Risk Officer and Chief Security Officer
- Monitor dependencies on people, processes, technology, premises, and third-party providers and adequately documented within the ERM tools (ie. OPCIS)

Access Management & Recertification controls

- Manage access recertification for COO-owned or managed applications, including Lombard Odier (LO) related services
- Support and guide managers in performing Entra-based access recertification for all COO departments and support functions, acting as a point of contact and facilitator; exclude Front Office roles (managed by the BRM Front team). Excluding the technical aspects of the Entra IAM platform and recertification tooling which remains under the responsibility of the Security function

Outsourcing & Third-Party Risk controls

- Assess and monitor risks related to outsourced services and critical suppliers, in coordination with the Chief Risk Officer, the procurement function and IT

Your profile

- 5–7 years of experience in the banking sector, preferably in risk & control, audit or BRM role
- Strong understanding of regulatory requirement applicable to the banking sector, banking processes and operational, IT risks and resilience
- Solid knowledge of FINMA regulatory expectations and banking auditors' requirements (1st and 2nd line of defence organizational requirements notably in the compliance, data protection, operational risk, resilience, BCM/DR, and outsourcing fields)
- Good understanding of information security frameworks (ITIL,) and third-party assurance reports (ISEA/SOC)

Soft skills:

- Highly organized, rigorous, and able to manage multiple priorities
- Appetite for transversal projects and enhancing collaboration intra-teams and stakeholders
- Excellent communication skills, French & English, both in verbal and writing
- Innovative mindset, able to identify opportunities for process improvement and operational efficiency
- Solution-oriented, and comfortable working under time pressure
- Credible and confident when interacting with stakeholders of all levels

Language requirements:

- Excellent verbal and written command in French and English, German an asset

Education & Certifications:

- Bachelor's degree in business, or computer science, or equivalent
- Professional certification in Information Security (CISSP, CISA, CISM, auditor, or similar) highly appreciated