Business Information Risk Officer – 6-9 months fixed-term assignment

Experience level : Intermediate
Entity : Bank Syz
Office : Geneva

Why join us for this assignment? This short-term assignment offers a unique opportunity to contribute quickly and visibly to the bank's operational resilience and risk management framework. Working closely with senior stakeholders across Information Security, IT, Operations and control functions, you will help strengthen key governance processes, support critical initiatives, and gain hands-on exposure to the risk environment of a Swiss private bank.

As Business Information Risk Officer, you will play a hands-on role in identifying, assessing, mitigating and monitoring non-financial risks across the bank's operational, technological and support functions. Acting as a first line of defense, you will support the CSO in strengthening the bank's infrastructure, governance, policies, processes and services, ensuring they remain resilient, well-controlled and aligned with internal risk appetite and Swiss regulatory expectations.

This is an ideal assignment for a pragmatic risk professional who enjoys working across functions, engaging with stakeholders, and delivering tangible outcomes within a defined timeframe. You will partner closely with IT, Cyber Security, Physical Security, Operations, Central File, Client Reception and Procurement, while coordinating with second-line functions, including Risk Control, Compliance and Internal Audit as required.

Key responsibilities

Business & Operational Risk Management

- Identify, assess, and monitor non-financial risks across COO-owned functions, including IT, Operations, Central File, Client Reception and Procurement
- Maintain and enhance risk and control assessments across the CSO perimeter, including key risk indicators and mitigation plans aligned with the bank's risk appetite

Operational Resilience, Business Continuity & Disaster Recovery

- Update and maintain Business Impact Analyses for critical banking functions and processes, ensuring documentation is clear, practical and actionable
- Support the review, testing and improvement of Business Continuity and Disaster Recovery Plans with relevant business stakeholders, in coordination with the CSO
- Support the bank's operational resilience framework, ensuring continuity of critical services under severe but plausible scenarios in collaboration with the CSO
- Monitor dependencies on people, processes, technology, premises, and third-party providers and adequately documented within the ERM tools (ie. OPCIS)

Access Management & Recertification

- Manage periodic access recertification campaigns for the core banking system and other relevant bank-managed applications, ensuring timely follow-up and clear stakeholder coordination

Change Risk

- Partner with IT and Information Security to assess risks linked to system changes, migrations, and incidents

Outsourcing & Third-Party Risk

- Assess and monitor risks related to outsourced services and critical suppliers, in coordination with procurement and IT

Change & Project Risk Assessment

- Assess operational, access, and resilience risks arising from new products, process changes, and system implementations

Governance, Reporting, Audit & Stakeholder Management

- Act as the primary point of contact for internal and external auditors for all audits covering the COO perimeter; coordinate, supervise, and contribute to audit activities, including planning, walkthroughs, evidence collection, and management responses for all COO division-related audits
- Liaise with second-line risk control and internal audit to ensure alignment with the bank's control framework and regulatory expectations

Your profile

- 5–7 years' experience in operational, IT, or business risk, including 2+ years in financial services or IT audit
- Experience conducting Business Impact Analysis interviews and maintaining Business Continuity Plans
- Solid knowledge of FINMA, LPD operational risk frameworks, BCM/DR, and outsourcing requirements
- Experience with third-party/vendor assessments (ISAE reports) and operational controls
- Good understanding of IT, information security, and ITIL frameworks
- Proven experience in access management, including recertifications and segregation of duties
- Strong analytical and problem-solving skills, balancing business priorities with risk
- Ability to challenge audit findings and provide pragmatic recommendations
- Project and change management experience, including complex operational or IT initiatives
- Knowledge of critical functions, business impact analyses (BIA), and operational resilience
- Curious and motivated to contribute quickly, while gaining deeper exposure to private banking operations and resilience practices
- Strong written communication in French and English for reports, policies, and governance documentation

Personal competencies:

- Results and solution-oriented with the ability to lead change
- Analytical and problem-solving skills, balancing business needs with risk
- Able to explain security and risk topics to non-technical audiences
- Confident and credible, willing to challenge findings when necessary
- Discreet, loyal, and able to handle sensitive information with integrity
- Pragmatic, resilient, and able to work under pressure
- Highly organized, rigorous, and attentive to detail

- Able to integrate rapidly into a new environment and deliver practical results within a short assignment timeframe

Language requirements:

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

Education:

- Bachelor's degree in Computer Science, Management or equivalent
- Current relevant professional certification in Information Security (CISSP, CISA, CISM) highly appreciated