Operational risk management

• Operational Resilience of Critical Functions: establishing disruption tolerance, preventive remediation measures, Incident and crisis management • Managing risks: ICT, Cyber, Third Party Risk Management, externalised AI • Evolution of banking processes: extension of working hours at stock exchanges, acceleration of the settlement process, integration of the blockchain and AI

Operational Resilience of Critical Functions

8.30 **What is Operational Resilience? How does it differ fundamentally from Business Continuity Management?**
• Difference between BCM objectives (addressing isolated failures) and operational resilience (overcoming a major/general crisis where traditional continuity management measures would be ineffective).
• Operational resilience covers the entire value chain rather than isolated ICT processes and systems.
• Importance of defining and documenting tolerances for each critical function: tolerances should specify the minimum level of service and results required for a critical function to operate during a crisis.
Louis Binswanger, Senior Manager | Risk Consulting, Ernst & Young AG

9.00 **The process of establishing disruption tolerance and minimum service levels in a crisis: rationale, justification, documentation**
• Defining disruption tolerance for critical functions is more complex than initially expected.
• Collecting data to rationalize the defined minimum service level and results.
• Documenting disruption tolerance in a results-based objective statement, along with justifications and additional data/evidence supporting the chosen tolerance level.
• Assessment of work conducted to determine tolerances for critical functions: misunderstandings, poor practices, best practices.
• Practical application of disruption tolerances for critical functions such as payments, securities, and treasury.
Hans Ulrich Bacher, Partner, Head of Risk Consulting, Financial Services, KPMG Switzerland

9.40 **Vulnerabilities and preventive remediation measures**
• Regulatory requirements for identifying vulnerabilities and implementing remediation measures.
• Preventive measures to reduce vulnerabilities (examples) and protective measures.
• Practical application to critical functions such as payments, securities, and treasury.
Louis Binswanger

10.10 **Incident and crisis management: regulator expectations, lessons from crisis experiences in financial intermediaries**
• Requirements for crisis management preparedness.
• Differences between an incident, a crisis, and an attack; isolated failure vs. general crisis.
• Scenario-based preparation.
• Detecting crises.
• How to manage/respond during a crisis and an attack; recovery measures and maintaining normal operations during a crisis.
• Priorities during a crisis.
• Lessons from financial intermediaries that have faced crises.
Louis Binswanger

10.40 Coffee Break

Operational Risk Management

Vulnerabilities, tolerances, mitigation measures, controls, tests, exercises

11.00 **ICT Risk Management**
• Objectives and expectations under Circular 2023/1: inventory, backup recovery and testing, incident controls.
• Mitigation measures.
• Practical application, failures, best/bad practices.
Benjamin Derler, Manager Cybersecurity, Ernst & Young AG

11.30 **Cyber Risk Management**
• Objectives and expectations under Circular 2023/1: vulnerability assessments, penetration testing, exercises.
• Actions to be taken: defining risk appetite and tolerance for cyber risks; introducing key controls within the internal control system; regular review of control effectiveness.
• Specific exercise requirements outlined in FINMA Guidance 03/2024: solutions, best practices.
• Mitigation measures.
• Practical application, failures, best/bad practices.
Alexander Locher, Senior Manager Risk consulting & Internal Audit Financial Services, PwC

12.10 **Managing risks related to critical data**
• Objectives and expectations under Circular 2023/1: identification and categorization of critical data, defining responsibilities for data access rights, due diligence on suppliers, concrete and relevant risk tolerance statements, identification of vulnerabilities.
• Mitigation measures.
• Practical application, failures, best/bad practices.
Beate Fessler, Director, FS Business and Regulatory Transformation, PwC

12.50 Lunch Break

Third Party Risk Management

14.00 **Third Party Risk Management (TPRM): Focus topics for banks and regulators**
• Why Third Party Risk Management matters
• Practical challenges in the management and monitoring of third parties
• Changing regulatory focus: from compliance to operational resilience
• New BCBS principles on TPRM and potential implications for Swiss banks
• Good practice approach for a future-proof TPRM
Hans Ulrich Bacher

New Challenges

14.40 **New operational stakes: risk factors, impacted functions, food for thought**
Market practices require rapid and significant adaptation of operational banking processes (extension of working hours at stock exchanges, acceleration of the settlement process, integration of the blockchain and Artificial Intelligence)
• What factors must be taken into account?
• How to integrate these factors in the analysis of operational risks?
• Who are the impacted stakeholders?
• Which measures should be considered ?
Jérôme Desponds, Consultant in governance, risk management and project organization (former Chief Risk Officer for banks)

15.20 **What are the Swiss and European regulatory requirements for artificial intelligence applications? What precautions should be taken against the risks of outsourced AI?**
• FINMA expectations: governance and responsibility; robustness and reliability; transparency and explainability.
• The new European AI Regulation.
• Risks of outsourced AI: ensuring data remains in Switzerland while AI engines are hosted abroad.
Tomasz Wolowski, Senior Manager, Risk & Regulatory | Compliance & Regulations, PwC

16.00 End of the Conference

ZURICH, TUESDAY 24 JUNE 2025, 8.30-16.00, ZURICH SHERATON HOTEL / ONLINE

ACADEMY & FINANCE

Operational risk management

PRACTICAL INFORMATION

Venue
Zurich Sheraton Hotel
Pfingstweidstrasse 100, Zurich

Visio conference on Zoom
The Zoom link and the documentation will be sent to the participants on 23 June in the afternoon. Academy & Finance provides technical assistance during the conference.

How to register
by phone: +41 (0) 22 849 01 11
by e-mail: info@academyfinance.ch
by post: Academy & Finance SA
3 rue Neuve-du-Molard, CH-1204 Geneva
www.academyfinance.ch

Fees
1160 CHF (+ VAT 8.1%)
Additional registrations from the same company: - 50%

Registration and payment
Payment is made by bank transfer or by credit card. Credit card payments will be debited immediately upon receipt of card details. In any case, we will send you an invoice by email.

Substitution & cancellation policy
Substitutions from the same company are accepted at any time. Cancellation requests must be received in writing, by fax or by post up to the following dates end of business :
- 17 June refund of 90%
- after 17 June no refund will be made for cancellation.

AF1424

REGISTRATION FORM

I register for the seminar "Operational risk management" in Zurich on 24 June 2025.

☐ I will attend in the conference room ☐ I will attend online on Zoom

FIRST PARTICIPANT

Full name.....

Position.....

E-mail.....

SECOND PARTICIPANT (-50%)

Full name.....

Position.....

E-mail.....

Company.....

Address.....

Postcode..... City.....

Tel ..... Mobile.....

Person to which the invoice must be sent for payment:

Name..... Email.....

Bank transfer ☐ Mastercard ☐ VISA ☐

Credit card No : _____/_____/_____/_____ Expiry date : _____/_____

Cardholder.....

Date ..... Signature.....

The organisers reserve the right to amend the programme if, despite their best efforts, circumstances oblige them