FINMA Circular 2018/3

Outsourcing (Banks, Insurance companies and selected Financial Institutions under FinIA)
Versus ISO/IEC 27001:2022 & ISAE 3402 Type 2

Requirements Mapping

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
I. Purpose	none	This circular defines the supervisory requirements applicable to outsourcing solutions at banks, insurance companies and financial institutions as per Margin nos. 5, 6.1 and 6.2. in terms of appropriate organisation and risk limitation.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG
II. Definition of terms	none	A company is understood to mean an institution that falls within this circular's scope of application as per no. III. Outsourcing within the meaning of this circular occurs when a company mandates a service provider to perform all or part of a function that is significant to the company's business activities independently and on an ongoing basis. Significant functions are those that have a material effect on compliance with the aims and regulations of financial market legislation.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
III. Scope of application	none	This circular applies to: • Banks and securities firms with a registered office in Switzerland as well as Swiss branches of foreign banks and securities firms; • Insurance companies with their registered office in Switzerland and branches of foreign insurance companies requiring authorisation to commence business operations under Articles 3 and 6 Insurance Supervision Act (ISA) (initial authorisation) or authorisation for individual elements of the business plan under Article 4 in conjunction with Article 5 ISA (authorisation for changes); • Managers of collective assets with their registered office in Switzerland and Swiss branches of a foreign manager of collective assets and fund management companies with their registered office and a head office in Switzerland; • Self-managed SICAVs. The requirements are to be applied taking into account the institution's size, complexity, structure and risk profile.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG
IV. Admissibility	A. Joint provisions	Subject to the exceptions outlined below (Margin nos. 8–13.3), all significant functions may be outsourced. Direction, supervision and control by the supreme governing body, central executive management functions and functions that involve strategic decision-making may not be outsourced, nor may decisions concerning the commencement and termination of business relationships. Companies in supervisory categories 1–3 have an autonomous control body in the form of a separate risk control and compliance function. For companies in supervisory categories 4 and 5, it is sufficient for a member of executive management to be assigned responsibility for these functions. Operational risk management and compliance tasks may be outsourced in all supervisory categories.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
IV. Admissibility	B. Insurance companies	Under Article 4 para. 2 let. j in conjunction with Article 5 para. 2 ISA, the outsourcing of significant functions and the partially admissible outsourcing of control functions are relevant to the business plan and thus require authorisation. The scope of permitted outsourcing of management and control functions is wider for insurance captives than other insurance companies. The following are admissible: • outsourcing the management of direct and reinsurance captives with their registered office in Switzerland (including central executive management functions) to companies appropriately specialised in the management of captives; • outsourcing the management of branches of foreign direct insurance captives within the group or to companies appropriately specialised in the management of captives. Such outsourcing must not restrict the function of the general agent in accordance with supervisory law provisions (Arts. 17 and 18 Insurance Supervision Ordinance, ISO)	not applicable

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
IV. Admissibility	C. Managers of collective assets, fund management companies and SICAVs	In addition to the tasks that cannot be outsourced under Margin no. 8, the following tasks in particular must also be performed by the financial institution itself: • Managers of collective assets: the portfolio and risk management of at least one collective investment scheme or the assets of at least one occupational pension scheme respectively (Art. 26, para. 1 FinIA). • Fund management companies: the management of the investment fund and associated tasks, such as the valuation of investments or the decision on the issue of units (Art. 35 para. 1 FinIA). Moreover, the head office in Switzerland may not be adversely affected by outsourcing. The same applies for self-managed SICAVs by analogy.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.
V. Requirements for outsourcing companies	A. Inventory of outsourced functions	An inventory of outsourced functions must be drawn up and kept up to date at all times. It must contain a description of the outsourced function and indicate the service provider (including subcontractors), the service recipient and the unit responsible within the outsourcing company (see Margin no. 20). Insurance companies keep this inventory in conjunction with business plan form J. Financial institutions under Margin nos. 6.1 and 6.2 and securities firms keep this inventory within the context of their organisational principles (Art. 17 para. 3 FinIO).	Covered by ISO/IEC 27001:2022 clause 4. cluse 6 and cluse 8 as well as annexure controls.

V. Requirements for outsourcing companies	B. Selection, instruction and monitoring of the service provider	The service specifications must be agreed in line with the aims of the outsourcing and documented before the agreement is signed. This includes conducting a risk analysis that takes account of the main economic and operational considerations as well as the associated risks and opportunities. The service provider must be chosen with due regard to, and subject to checks of, its professional capabilities as well as its financial and human resources. Where multiple functions are outsourced to the same service provider, the concentration of risk must be taken into account. Furthermore, the eventuality of a change of service provider and the possible consequences of such a change must be considered when deciding to outsource and selecting the service provider. The service provider must offer a guarantee of permanent service provision. Provision must be made for insourcing the outsourced function or transferring it to another service provider in an orderly manner. The duties of the company and the service provider must be contractually agreed and delimited, in particular with regard to interfaces and responsibilities. The outsourced function must be integrated into the company's internal control system. The main risks associated with the outsourcing must be systematically identified,	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.

		monitored, quantified and controlled. A unit within the company must be named as responsible for monitoring and controlling the service provider. The latter's services must be monitored and assessed on an ongoing basis so that any necessary measures can be taken promptly. To this end, the company must ensure that its agreement with the service provider grants it the necessary rights of instruction and control	

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
V. Requirements for outsourcing companies	C. Outsourcing within a group or conglomerate	With regard to the requirements set out in Margin nos. 16–21 and 32–35, relationships within the group or conglomerate may be considered to the extent that the risks typically associated with outsourcing are demonstrably absent or certain requirements are not relevant or are met in some other way.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.
V. Requirements for outsourcing companies	D. Responsibility	The company remains accountable to FINMA in the same way as it would if it performed the outsourced function itself. Proper business conduct must be assured at all times.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.
V. Requirements for outsourcing companies	E. Security	Where security-relevant functions are outsourced (particularly in information technology), the company and the service provider must contractually agree security requirements. The company must monitor compliance with these requirements. The company and the service provider must draw up a security framework to ensure that the outsourced function can continue to be performed in an emergency. In doing so, the company must apply the same degree of care and attention as it would if it performed the outsourced function itself.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments.

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
V. Requirements for outsourcing companies	F. Audit and supervision	The company, its audit firm and FINMA must be able to verify the service provider's compliance with supervisory regulations. They must have the contractual right to inspect and audit all information relating to the outsourced function at any time without restriction. Auditing may be delegated to the service provider's auditors if these are adequately qualified. Where this is done, the company's audit firm may use the findings of the service provider's auditors for its audit. The outsourcing of a function must not make supervision by FINMA more difficult, in particular if the function is outsourced to another country. If the service provider is not supervised by FINMA, it must enter into a contractual obligation with the company to provide FINMA with all the information and documentation concerning the outsourced functions, which are necessary for FINMA's supervisory activities. If auditing is delegated to the service provider's auditors, their report must be supplied, on request, to FINMA as well as to the outsourcing company's internal auditors and audit firm.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls A.12, A.13, A.14 and A.17) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments by third parties.

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
V. Requirements for outsourcing companies	G. Outsourcing abroad	Outsourcing to another country is admissible if the company can expressly guarantee that it, its audit firm and FINMA can assert and enforce their right to inspect and audit information. The possibility of restructuring or resolving the company in Switzerland must be assured. Access to the information required for this purpose must be possible in Switzerland at all times.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments by third parties.

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
V. Requirements for outsourcing companies	H. Agreement	The outsourcing must be based on a written agreement or an agreement in some other format that can be evidenced in text form. In addition to naming the parties and describing the function, this agreement must also contain the following as a minimum (Margin nos. 33–34): The company must ensure that it is informed about the use or replacement of subcontractors for significant functions at an early stage and has the possibility of terminating the outsourcing in an orderly manner in accordance with Margin no. 18.1. Where subcontractors are used, they must also be bound by the obligations and guarantees on the part of the service provider that are necessary to comply with this circular. The agreement must include measures to ensure implementation of the requirements set out in this circular, in particular in Margin nos. 21, 24, 26, 29, 30 and 31. The company must specify the internal approval procedures for outsourcing projects as well as the responsibilities for signing outsourcing agreements.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 (Management System Controls clause 4 to 10 as well as annexure controls) by independent body at Phoenix Technologies AG including ISAE 3402 annualy assessments by third parties.

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
VI. Conditions and exceptions	none	In justified cases, FINMA may impose conditions on a company or grant a company partial or total exemption from compliance with this circular. Institutions as defined in Articles 47a to 47e CAO as well as institutions under Article 1b BA assess and decide on the relevance and application of the requirements set out in Margin nos. 17–18.1 within the scope of the risk analysis described in Margin no. 16. Institutions as defined in Articles 47a to 47e CAO as well as institutions under Article 1b BA are exempt from the requirement set out in Margin no. 18.1 as far as the insourcing of outsourced functions is concerned. For institutions as defined in Articles 47a to 47e CAO as well as institutions under Article 1b BA, the implementation of Margin no. 20 can take place by way of regular reporting by an independent auditor, taking account of Margin no. 27. This reporting must allow an assessment to be made of the most significant risks associated with the outsourcing and the control activities undertaken by the service provider.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG

Chapter	Sub Chapter	Requirements	Covered by / Compliant with
VII. Transitional provisions	none	This circular applies directly to outsourcing relationships entered into or altered by banks and securities firms after its entry into force. Existing outsourcing relationships entered into by banks and securities dealers prior to the circular's entry into force must be adapted within a transition period of five years from its entry into force such that they meet the requirements of the new circular. For insurance companies, the circular applies to initial authorisations from its entry into force. It applies to authorisations for changes from the time when a change to the business plan is submitted or communicated to FINMA for approval. For financial institutions as per Margin nos. 6.1 and 6.2, the circular applies to initial authorisations from its entry into force. It applies to authorisations for changes from the time when a change is submitted or communicated to FINMA for approval, but no later than a year after its entry into force.	Covered by contractual negotiations between customer and service provider and certified due to ISO/IEC 27001:2022 by independent body at Phoenix Technologies AG