finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Audit points for cyber risk management

Overview

Audit field:	**Cyber risk management**
Audit depth:	[Audit/critical assessment][1]
Basis: (non-exhaustive list)	Article 3 para. 2 let. a Banking Act of 8 November 1934 (BA; SR *952.0*) Article 12 paras. 2–4 Ordinance of 30 April 2014 on Banks and Savings Banks (BO; SR *952.02*) Article 9 Swiss Federal Act of 15 June 2018 on Financial Institutions (FinIA; SR *954.1*) Articles 12 para. 4, Articles 68 and 73 Financial Institutions Ordinance of 6 November 2019 (FinIO; SR *954.11*) Margin nos. 13, 50, 52, 53, 58 and 59 FINMA Circular 2017/1 “Corporate governance – banks” Margin nos. 23–26, 40, 61–70 and 104 FINMA Circular 2023/1 “Operational risks and resilience – banks”
Sign-offs:	

Sign-offs:	**Name:**	**Function:**	**Date:**
Auditor:	[Name]	[Assistant / Senior / Manager / Senior Manager / CEO / Partner]	[DD MM YYYY]
Reviewer:	[Name]	[Senior / Manager / Senior Manager / CEO / Partner]	[DD MM JJJJ]

This is the standard work programme that is to be implemented for every intervention under the terms of the audit strategy. It is the responsibility of the audit team to adapt the standard work programme to the specific situation of the institution (size, business model, organisation, processes, risk exposure etc.). If the specified audit procedures are not carried out completely, an appropriate rational for this must be provided in the working paper. Audit procedures marked with an asterisk (*) are not applicable to Category 4 or 5 banks.

[1] Article 10 paras. 2 and 3 FINMA Regulatory Auditing Ordinance of 31 October 2024 (SR *956.161.1*)

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Overall conclusion

<table>
<tr><th>Topic:</th><th>Information / description:</th></tr>
<tr><td>Overall conclusion</td><td>
<table>
<tr><th>Confirmation in audit report:</th><th>Conclusion:</th></tr>
<tr><td>Confirmation that the “Cyber risk management” area was designed adequately.</td><td>Yes (Audit/critical assessment) / No</td></tr>
<tr><td>Confirmation that the institution complied with the stricter requirements ordered by FINMA.</td><td>Yes (Audit/critical assessment) / No</td></tr>
</table>
</td></tr>
<tr><td>Summary of significant findings / notices of reservations and recommendations (see details below)</td><td>[Summary of significant findings / notices of reservations and recommendations]</td></tr>
<tr><td>Audit areas, results and procedures performed by Internal Audit on which audit firm placed reliance (including audit firm’s own assessment)</td><td>[Description]</td></tr>
</table>

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Audit programme: cyber risk management

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
Management of cyber risks considering the principle of proportionality, i.e. taking into account the size, complexity (especially with regard to ICT and outsourcing), structure and risk profile:				
1	Obtain a basic understanding of the institution's general handling of cyber risks, considering the principle of proportionality and the following audit procedures.			
2	Assess the adequacy of the institution's governance in relation to cyber risk (such as regulations, policies, procedures, standard, guidelines, directives, etc.).	Assess the consistency of the strategy for dealing with cyber risks with the institution's policies (such as risk policy, risk management principles, operational risk management, business strategy, ICT and data strategy).		
Integration into overarching operational risk management and strategy, governance and awareness (margin nos. 23–26, 30, 40 and 61 FINMA Circ. 23/1)				
3	Assess whether cyber risks are integrated into overarching operational risk management as a separate taxonomy and thus adequately and comprehensively taken into account, i.e. within the framework of the identification, assessment, limitation and monitoring of operational risks.	Assess relevant risk control instruments (e.g. risk tolerance, audit results and risk and control assessments pursuant to margin no. 30) for cyber risk on the basis of appropriate samples.		
4	Assess whether the board of directors regularly (at least annually) evaluates and approves the risk tolerance for cyber risks in accordance with the risk policy, taking into account the institution's strategic and financial objectives.			
5	Assess whether the board of directors regularly approves a strategy for dealing with cyber risks and monitors its compliance.			
6	Assess the adequacy of the identification of material inherent risks with respect to cyber risks, i.e. if cyber risks are not identified as material inherent risks, assess the plausibility of the explanation provided.	Review, on an appropriate sample basis, the elements for identifying material cyber risks and assess whether potential risks associated with cyber risks are identified and addressed, and whether the assessment of the materiality of inherent risks is in line with the risk tolerance.		
7	Assess the organisational and technical measures taken to raise awareness among employees with regard to their tasks, competencies and responsibilities for the reduction of cyber risks.			
8	Assess the adequacy of the training provided on the topic of cyber security with regard to cyber and/or institution-specific threats and the needs of specific audiences (e.g. for executives, employees with privileged or elevated rights, employees with access to critical data, external personnel [including contractors] etc.).	Assess the operational effectiveness of the controls to ensure (regular) training of employees, key personnel and third parties in the area of cyber security on the basis of appropriate samples.		

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
9	Assess the adequacy of reporting to the executive board (content, frequency etc.) on the development of cyber risks, the effectiveness of key controls and major internal and external incidents.			
10	Assess the results of audit and control procedures performed by Internal Audit and/or other control functions (such as Independent Risk Control) related to cyber security, and review minutes of relevant committees and function meetings			
Tasks, competencies and responsibilities (margin no. 62 FINMA Circ. 23/1):				
11	Assess whether tasks, competencies and responsibilities have been clearly specified within the cyber organisation (e.g. with regard to role description, the organisation, functional distinctions, reporting lines and communication channels).			
12	Assess whether cyber risks are adequately taken into account in the planning and conducting of audits within the scope of Independent Risk Control and Internal Audit. The following in particular must be taken into account: risk analysis and assessment, multi-year planning, international standards applied.			
13	* Assess the independence (see margin no. 62 FINMA Circ. 17/1) of the internal functions in connection with the assessment of the cyber security risk situation.			
Procedures, processes and controls (including continuous development and improvement) (margin no. 62 FINMA Circ. 23/1):				
14	Assess whether the concept for dealing with cyber risks has been drawn up according to internationally recognised standards or practices and covers the specific risk situation and needs of the institution.	Assess the operational effectiveness on the basis of appropriate samples whether the concept for dealing with cyber risks is continuously further developed and improved based on findings from reviews and lessons learned.		
Identification (margin no. 63 FINMA Circ. 23/1):				
15	Assess whether the ICT assets (see margin nos. 53 and 54) and the interfaces with third parties are identified, catalogued and evaluated.	Assess on the basis of appropriate samples that key controls are carried out to ensure the completeness and accuracy of the inventories. For example, the following should be taken into account: • hardware components, • software components: applications (including dependencies),		
16	Assess whether there is a definition of critical data and whether an inventory of such data is maintained (see margin nos. 7, 53 and 54).			

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
17	Assess whether the ICT assets (see margin nos. 7, 53 and 54) are adequately represented in the network infrastructure according to their criticality and need for protection.	• software components: end user software (incl. version control), • assessment of criticality, • storage location of critical data, • interfaces to key external service providers.		
18	Assess the adequacy of procedures, processes and controls for identifying potential cyber threats specific to the institution and assessing possible impacts due to the exploitation of vulnerabilities with regard to the inventoried ICT assets, interfaces with third parties and critical data (see margin nos. 7, 53 and 54).	* Assess on the basis of appropriate samples existing elements for identifying and assessing the cyber threat. Such samples take account of the following aspects as a minimum: the impact of cyber attacks on the institution, the likelihood of occurrence and the risk assessment.		
19	Assess whether the potential threats specific to the institution and the vulnerabilities, and therefore the impact of cyber attacks on the inventoried ICT assets, interfaces with third parties and critical data (see margin nos. 7, 53 and 54) are known and adequately taken into account within the scope of risk assessment.			
Protection (margin no. 64 FINMA Circ. 23/1):				
20	Assess the adequacy of procedures, processes and controls for assigning logical and/or physical access (standard and privileged) to the inventoried ICT assets and interfaces with third parties (see margin nos. 53 and 54).	Assess the operational effectiveness of controls for assigning logical and/or physical access to the critical inventoried ICT assets and critical interfaces with third parties (see margin nos. 53 and 54) on the basis of appropriate samples.		
21	Assess the adequacy of procedures, processes and controls for (periodically) re-checking the logical and/or physical access (standard and privileged) to the inventoried ICT assets and interfaces with third parties (see margin nos. 53 and 54).	Assess the operational effectiveness of the controls for (periodically) re-checking the logical and/or physical access to the critical inventoried ICT assets and critical interfaces with third parties (see margin nos. 7, 53 and 54) on the basis of appropriate samples.		
22	Assess the adequacy of procedures, processes and controls for identifying, managing and monitoring the logical and/or physical access (standard and privileged) to the inventoried ICT assets and interfaces with third parties (see margin nos. 53 and 54).	Assess the operational effectiveness of the controls for identifying, managing and monitoring the logical and/or physical access (standard and privileged) to the critical inventoried ICT assets and critical interfaces with third parties (see margin nos. 53 and 54) on the basis of appropriate samples.		
23	Assess the adequacy of the organisational and technical measures for preventing unauthorised loss of critical data (data loss prevention).	Assess the operational effectiveness of organisational and technical measures for preventing unauthorised loss of critical data on the basis of appropriate samples.		
24	Assess the adequacy of procedures, processes and controls for managing network security (such as zoning, network access control [NAC], firewall, web application firewall [WAF], protection against DDoS, proxy server).	Assess the operational effectiveness of measures for managing network security on the basis of appropriate samples.		

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
25	Assess the adequacy of procedures, processes and controls for managing infrastructure security (e.g. endpoint detection & response (or XDR), anti-virus software etc.).	Assess the operational effectiveness of measures for managing critical infrastructure on the basis of appropriate samples.		
26	Assess the adequacy of procedures, processes and controls for ensuring standard configuration and system hardening (baseline configuration and hardening) of the inventoried ICT assets and continuous compliance thereof.	Assess the operational effectiveness of measures for standard configuration and system hardening for critical systems on the basis of appropriate samples.		
27	Assess the risk-based approach to the timely closure of security gaps (patching) and addressing of misconfigurations (configuration change) in systems, applications and underlying infrastructure.	Assess the operational effectiveness of measures for closing major or critical security gaps in critical systems on the basis of appropriate samples.		
28	Assess the adequacy of provisions for protecting the confidentiality, integrity and availability of stored and transferred critical data.	Assess the operational effectiveness of measures for protecting the confidentiality, integrity and availability of stored and transferred critical data, e.g. by means of encryption, on the basis of appropriate samples.		
Logging and detection (margin no. 65 FINMA Circ. 23/1):				
29	Assess whether anomalies (e.g. abnormal behaviour) and security events are timely identified by means of continuous monitoring of the ICT and potential effects of such incidents adequately assessed.			
30	Assess whether default values for permissible network operations and the expected data flows for users and systems (e.g. with regard to data flows between different network zones and interfaces between the ICT systems) are technically defined via SIEM use cases and assess the processes for keeping these up to date.			
31	Assess whether the critical inventoried ICT assets and their use by employees and third parties are systematically and continuously monitored.	Assess on the basis of appropriate samples whether all critical inventoried ICT assets and business applications supply log data to a central system and these are appropriately analysed to identify cyber incidents.		
32	Assess the adequacy of the technical measures for identifying cyber incidents on the basis of defined cyber risk scenarios (so-called use cases).			
33	Assess whether the procedures and directives for the detection of cyber incidents are regularly updated and tested.			
Response (margin nos. 66 and 68 FINMA Circ. 23/1):				
34	Assess the adequacy of the response plan for addressing identified cyber incidents, in particular how this is coordinated with internal and external stakeholders and which support is required from external bodies in the event of an incident.	Assess on the basis of appropriate samples whether the response plan was efficiently and promptly executed in the event of an incident or test.		

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
35	Assess the adequacy of the processes for the timely analysis, documentation and classification of reports from the detection systems (so-called events).	Assess the operational effectiveness of the processes for the analysis and classification of events from the detection systems (so-called events).		
36	Assess the adequacy of processes and measures (e.g. so-called playbooks) for containing and mitigating cyber attacks.			
37	Assess whether the points from FINMA Guidance 05/2020 "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA" are taken into account in the response plan.	Assess the operational effectiveness on the basis of appropriate samples of successful and partially successful cyber attacks and whether the reporting process was complied with in accordance with FINMA Guidance 05/2020 "Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA"		
Recovery (margin no. 67 FINMA Circ. 23/1):				
38	Assess the adequacy of the periodic assessment of and improvements to response and recovery processes.	Assess the operational effectiveness on the basis of appropriate samples concerning whether appropriate lessons have been documented and implemented for previous incidents.		
39	Assess the adequacy of the recovery processes in order to guarantee a prompt recovery of the systems after a cyber attack.	Review on the basis of appropriate samples whether the recovery processes after a cyber attack have been verified by means of appropriate tests (so-called walk-throughs, tabletop exercises).		
Vulnerability assessments, penetration tests and risk-based, threat intelligence-related scenario cyber exercises (margin nos. 69 and 70 FINMA Circ. 23/1):				
40	Assess the adequacy of the processes for regularly conducting vulnerability assessments, penetration tests and scenario cyber exercises on the basis of the institution-specific threat landscape.			
41	Assess whether vulnerability assessments and penetration tests are regularly conducted on all ICT assets accessible over the internet and at least for systems necessary for the provision of critical processes or that contain critical data.			
42	Assess the adequacy of institution-specific provisions and processes for dealing with identified weaknesses and their risk-based removal.	Review on the basis of appropriate samples whether high and critical weaknesses identified in vulnerability assessments and penetration tests are removed within the defined period.		
43	Assess the adequacy of the technical and personnel resources for ensuring the initiation, implementation and risk-based implementation of vulnerability assessments, penetration tests and scenario cyber exercises.			

No.	Procedures for audit depth "critical assessment":	Additional procedures for audit depth "audit":	Procedures performed/findings	WP ref.:
44	Assess whether the results of cyber exercises are suitably documented and reported.			

****