INTERNATIONAL MONETARY FUND

IMF Country Report No. 25/296

SWITZERLAND

FINANCIAL SECTOR ASSESSMENT PROGRAM

TECHNICAL NOTE ON CYBER RISK SUPERVISION

November 2025

This paper on Switzerland was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed on October 24, 2025.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

SWITZERLAND

FINANCIAL SECTOR ASSESSMENT PROGRAM

October 24, 2025

TECHNICAL NOTE

CYBER RISK SUPERVISION

Prepared By
Monetary and Capital Markets Department

This Technical Note was prepared by IMF staff in the context of the Financial Sector Assessment Program in Switzerland. It contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

FIGURES

TABLES

Glossary

BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BIS	Bank for International Settlements
CCP	Central Counterparty
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPMI	Committee on Payments and Market Infrastructure
CROE	Cyber Risk Oversight Expectations
CSD	Central Securities Depository
CTP	Critical Third Party
DDPS	Federal Department of Defense, Civil Protection and Sport
DORA	Digital Operational Resilience Act
FADP	Federal Act on Data Protection
FDF	Federal Department of Finance
FDPA	Federal Data Protection Agency
FDPIC	Federal Data Protection and Information Commissioner
FI	Financial Institution
FINMA	Swiss Financial Market Supervisory Authority
FINMASA	Financial Market Supervision Act
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
GovCERT	Government Computer Emergency Response Team
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
NCS	National Cyber Strategy
NCSC	National Center for Cyber Security
NIS	Network and Information systems Security Directive
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
SFMI	Systemically Important Financial Market Infrastructures
SIC	Swiss Inter-bank Clearing System
SIF	State Secretariat for International Finance
SNB	Swiss National Bank
TIBER	Threat intelligence-based Ethical Red Teaming
TTP	Tactics, Techniques and Procedures

EXECUTIVE SUMMARY

Cyber security is recognized as one of the major risks in Switzerland by both authorities and financial market players. With the advancement of digitalization in Switzerland, cyber incidents have been increasing in frequency and sophistication, including in the financial sector. Both the Swiss National Bank (SNB) and the Swiss Financial Market Supervisory Authority (FINMA), the key institutions overseeing cyber risk, are tagging it as a significant threat to the financial sector.

The cyber risk management framework has recently been strengthened, with some major changes still to be implemented. The Financial Sector–Cyber Security Centre (FS-CSC)—a new public-private partnership—helps entities operating in the financial sector share threat intelligence, conduct cyber exercises and tests, assist with incident response, and actively share information. The National Cyber Security Center (NCSC) was established in 2020 to coordinate cyber security matters at the overall country level. Key regulatory initiatives include the Operational Risks and Resilience Circular from 2022 and FINMA's Guidance from 2020 and 2024, which cover the duty to report cyberattacks. Other recent major changes at the legal, institutional, and policy levels will be implemented over the next two to three years, such as amendments to the Information Security Act (ISA) for incident reporting requirements on critical infrastructure (effective in 2025).

Banks' cyber risk supervision relies on external audit firms and to a lesser extent on FINMA's direct onsite supervision, while offsite supervision is limited. The audit work is guided by the "Cyber Risk Management" procedures, which were updated in November 2023, and became operational in 2024. A summary of reported incidents is periodically shared publicly in an aggregated manner. Third-party related cyber incidents accounted for fifty percent and thirty percent of the reported incidents in 2023 and 2024, respectively. Testing practices can be further improved by developing a framework and conducting them more regularly. In recognition of the importance of cyber risk, FINMA should gradually increase its direct onsite supervision.

There is a need for stricter regulation, more effective supervision, and increased coordination in cyber security matters in the financial sector. The financial system is only as strong as its weakest link, therefore, regulation that covers the entire financial system and more effective supervision would not only help the cyber preparedness of the sector but also increase the attractiveness of the Swiss Financial Center (SFC). The scope of relevant regulations should be expanded, beyond banks, to encompass the entire financial sector. The staff resources of FINMA, SNB, and NCSC should be reinforced substantially to adequately monitor cyber risks. Furthermore, coordination among authorities is very important, given the shared responsibilities. For instance, conducting financial stability analysis and cyber resilience stress testing is the mandate of SNB, while FINMA coordinates the supervision of individual entities. Similarly, prosecution of cybercrime is the responsibility of cantonal authorities, while cyber security is addressed by both the federal and cantonal authorities. Enhancing the coordination between FINMA, NCSC, and the Federal Data Protection Agency (FDPA) regarding incident reporting frameworks, as well as formalizing arrangements between FINMA and FDPA would reinforce the cyber risk oversight framework.

Table 1. Switzerland: 2025 FSAP: Key Recommendations		
Recommendation	**Authority**	**Timeframe[1]**
Legal and Regulatory Framework		
1. Strengthen legal measures to facilitate effective supervision of critical third-party service providers to the financial sector (¶18).	FINMA, SIF, NCSC	ST
2. Consider introducing legal measures to empower GovCERT to investigate systemic cyber incidents (¶18).	NCSC	MT
3. Provide adequate resources to GovCERT to ensure effective functioning, including to support the financial sector (¶25).	NCSC	I
4. Extend ICT / cyber and outsourcing regulations to all parts of the financial sector (¶36).	FINMA	ST
5. Consider options to limit further concentration in the SIX group and to de-risk the existing levels of concentration (¶44).	SNB, FINMA	ST
Institutional Elements		
6. Enhance coordination between FINMA, FDPA, and NCSC regarding incident reporting frameworks (¶54).	FINMA, FDPA, NCSC	ST
7. Formalize arrangements between the FDPA and FINMA to enhance further cooperation (¶64).	FINMA, FDPA	ST
Supervisory Arrangements		
8. Reduce the dependence on external auditors and correspondingly increase on-site examinations (¶84).	FINMA	ST
9. Review the on-site supervision policy with an aim to increase FINMA's on-site activity, explore synergies between IT and cyber risk examination units, and strengthen off-site supervision by collecting key risk indicators and data for mapping (¶85).	FINMA	ST
10. Introduce regular reporting to the Board covering the analysis of the threat landscape, type and trend of incidents, regulatory environment, supervisory actions, and material gaps in the preparedness (¶ 85).	FINMA	I
11. Collect, in the form of a regular off-site report, a summary of cyber incidents comprising all categories to better understand the overall threat landscape (¶93).	FINMA	ST
12. Revise the incident reporting regulation to address the gaps, consider the Format for Incident Reporting and Exchange (FIRE) format to make incident reporting template comprehensive, and issue a circular on the topic (¶92).	FINMA	ST
13. Augment resources within SNB to have a complete understanding of the cyber risk profile of Systemically Important Financial Market Infrastructures (SFMI) (¶99).	SNB	I
14. Augment resources in the FINMA Banking-Operational, Cyber, and IT risk unit to improve cyber risk supervision (¶98).	FINMA	I

Table 1. Switzerland: 2025 FSAP: Key Recommendations (Concluded)		
Financial Sector Resilience		
15. Develop a testing framework that is appropriate for the Switzerland market to achieve consistency in the results across institutions (¶108).	FINMA	MT
16. Conduct stress tests with severe but plausible cyber scenarios to assess impact on the financial sector (¶110).	SNB, FINMA	ST
17. Conduct cyber resilience stress tests for the financial sector (¶110).	SNB, FINMA	ST
Selected Cyber Security Considerations at SNB and FINMA		
18. Assess the impact of the Information Security Act (ISA) and take necessary action to comply with its provisions (¶113).	SNB	I
[1] I Immediate (within 1 year); ST Short term (within 1-2 years); MT Medium Term (within 3–5 years).		

INTRODUCTION

1. Cyber risk has increased in Switzerland and has become one of the top risks for the financial sector. The digitalization of the financial sector and adoption of new technologies lead to higher dependencies on third parties, while increasing interconnections have expanded the cyberattack surface. The frequency and sophistication of the cyber incidents within the financial sector has increased and, rightfully, the financial sector authorities—the Swiss National Bank (SNB) and the Swiss Financial Market Supervisory Authority (FINMA)—have tagged cyber risk as a major risk. Cyber incidents reported to the Government Computer Emergency Response Team (GovCERT) have increased significantly over the years, even though such reporting is on a voluntary basis; the actual number of incidents could be much higher. Reporting by individuals accounted for 90 percent of cases and the rest was from corporates.

2. Switzerland has been taking several initiatives to strengthen cyber security, but this is still work in progress. This includes legal measures, setting up and empowering cyber security organizations, improving coordination and encouraging public-private partnership to address the issue. Most of these measures have either a transition period or have been established very recently to gain a meaningful insight into their functioning. Both in terms of institutional arrangements and regulatory and supervisory initiatives, several changes have been made in the right direction but some of them are yet to be fully implemented in view of the transition period. For instance, several provisions in the Operational Risk and Resilience Circular, issued in 2023, have a significant transition time (1–2 years).

3. Several Assessments of Cyber Maturity of Switzerland indicate that despite progress, gaps exist. The Global Cyber Security Capacity Centre (GCSCC) and University of Oxford undertook a review of the maturity of cyber security capacity in Switzerland at the invitation of the authorities. The assessment, published in June 2020, aimed at enabling Swiss authorities to gain an understanding of the country's cyber security capacity, to strategically prioritize investment in cyber security. Another assessment, based on consultations with various stakeholders using the GCSCC's Cyber Security Capacity Maturity Model for Nations (CMM), which defines five dimensions of cyber

security capacity,[1] identified several gaps and made recommendations to address them. Switzerland is ranked on the 27th place in the National Cyber Security Index[2] Rankings and on the 42nd place (2020 report) in the Cyber Security Index published by the International Telecom Union. Recently published Cyber Security Index report in September 2024 places Switzerland in the second tier—"Advancing Category," whereas the first tier already has 45 countries. These suggest that despite progress on several fronts, more needs to be done.

4. This Technical Note (TN) focuses on the cyber risk regulatory and supervisory practices within the financial sector broadly, with specific attention to systemically important banks (SIBs), insurance companies, and financial market infrastructure (FMI)[3]. The assessment considered the institutional arrangements within Switzerland, including legal, organizational, and coordination measures as relevant to the financial sector, cyber risk regulations issued, relevant practices focused on cyber security while licensing entities, cyber risk supervisory practices covering governance, risk management, cyber security, incident reporting, and testing arrangements. The assessment also considered enabling initiatives such as information sharing, awareness building, and public-private partnerships.

5. The TN benefited from answers provided by SNB, FINMA, State Secretariat of International Finance (SIF), and NCSC to the questionnaire, interviews, and discussions with relevant stakeholders, and perusing certain confidential documents in the trust room. The financial sector authorities provided answers to the pre-mission questionnaire explaining the practices and providing documents, including responding to the clarifying questions. The authorities shared some of the sensitive documents and workflows in the trust room. Several publicly available documents including the laws, regulations, and reports were also used.

6. The analysis, conclusions and recommendations are based on standard setters' guidance and international best practices. The principles of sound management of operational risk (PSMOR) and the principles of operational resilience (POR) are those issued by the Basel Committee on Banking Supervision, which cover ICT and cyber risks substantially. The CPMI-IOSCO's cyber resilience guidance provides guidance on cyber security aspects related to FMIs. In addition, the Financial Stability Board's reports on cyber incidents, response and recovery, and third-party risk management provide best practices in this area. IMF's paper on Cyber Risk Supervision[4] as well as the IMF Staff Discussion Note on Cyber Risks and Financial Stability are also useful references.

[1] Cyber security Policy and Strategy, Cyber Culture and Society, Cyber security Education, Training and Skills, Legal and Regulatory Frameworks and Standards, Organizations and Technologies.

[2] These rankings are published by e-Governance Academy Foundation.

[3] This TN has been prepared by Ravikumar Rangachary, Senior Financial Sector Expert, IMF.

[4] https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.

LEGAL AND REGULATORY FRAMEWORK

7. FINMA is the supervisor of a large number of diverse financial institutions (Figure 1 right chart). FINMA is the unified supervisor of banks, insurance companies, securities firms, asset managers, many of which being large, complex, and globally active. Switzerland is also home to a G-SIB (UBS) and one of the top global reinsurers—SwissRe (Figure 1 left chart).

Figure 1. FINMA's Scope of Supervision

FINMA Supervised Entities

Source: FINMA Annual Report 2023.

Systemically Important Financial Institutions and Infrastructure

G-SIB: UBS

D-SIBs: Zürcher Kantonalbank, Raiffeisen, PostFinance

Most important internationally active insurance companies: Swiss Re Group, Zurich Insurance Group

Systemic financial market infrastructure: SIX Group

A. Legal Framework

8. Cyberattacks are considered as criminal activity under the Swiss Criminal Act. According to Article 143 of the Criminal Act, unauthorized access to data processing systems attracts a maximum penalty of three years or a monetary penalty.

9. Various legal acts empower FINMA to supervise financial institutions and market infrastructures and require the respective institutions' boards to identify, mitigate, and monitor all material risks. Even in the absence of specific regulation covering cyber security, FINMA can draw power under these provisions to supervise cyber risks. In respect to financial groups and conglomerates, Article 3 (f)(2) of the Banking Act requires that they must be organized to be able to specifically detect, mitigate, and monitor all material risks.

10. The Financial Market Infrastructure Act (Fin MIA) also casts certain responsibilities on the systemically important FMIs. Article 14 requires systemically important FMIs to operate their IT systems to provide for measures to protect the confidentiality and integrity of information regarding their participants and transactions. Article 23 requires them to fulfil special requirements to protect against the risks they pose to the stability of the financial system, as determined by the SNB.

11. The duty to provide information and to report any incident of substantial importance under the Financial Market Supervision Act (FINMASA) facilitates cyber risk supervision. Article 29 of FINMASA requires that the supervised entities and their audit companies immediately report to FINMA any incident of substantial importance. This requirement is also extended to third parties to whom essential functions of a bank are outsourced; per Article 23 of the Banking Act, FINMA can carry out checks on these outsourced entities at any time. Such a provision is not available for other non-bank supervised entities, constraining FINMA's powers.

12. The Federal Council put into effect the 2024 Information Security Act (ISA), which, apart from federal and cantonal authorities, covers critical infrastructures both in private and public sectors. The financial sector is one of the identified critical infrastructures. There are four ordinances drawing from ISA, namely:

- Information Security Ordinance (ISO),
- Ordinance on Security Checks on Persons (VPSP),
- Ordinance on the Company Security Procedure (VBSV), and
- Ordinance on Federal Identity Management Systems and Directory Services (IAMV).

A cyber security ordinance, which, among other things, specifies the reporting requirement for critical infrastructures in the ISA, is in the works and is scheduled to come into force on April 1, 2025. Some of the provisions are applicable only to federal and cantonal authorities, and not to critical infrastructure, which includes the SNB. The ISA also provides much needed legal backing to some of the activities of the NCSC, particularly about gathering incident reports and access to relevant data.

13. The ISA has been amended to include cyber incident reporting obligation for all identified critical infrastructures, which came into force in January 2025. This requirement for the financial sector will be in addition to FINMA requirements for incident reporting. Importantly, NCSC and FINMA have coordinated their efforts to avoid duplication so far. ISA has also incorporated amendments in other laws with an objective to strengthen cyber security:

- Federal Law on Public Procurement—the NCSC's power to publish certain vendors who do not fix vulnerabilities in their hardware or software within the time limit fixed by NCSC.
- Data Protection Act—the Data Protection Authority can share reports with the NCSC for analyses of incidents.
- Financial Market Supervision Act—FINMA is authorized to share non-publicly available information with other supervisors, NCSC, and SNB.

14. The Federal Council also proposed an amendment to the Data Protection Act (FADP, 2020), which also applies to the financial sector. The revision to the act is prompted by the desire of the authorities to strengthen the law to achieve equivalence with European Union's GDPR and thereby facilitate seamless cross border provision of services. One of the requirements is to

promptly notify the Federal Data Protection and Information Commissioner (FDPIC) in the event of a data security breach.

Assessment and Recommendations

15. Switzerland has made important progress in improving the legal framework. Enacting the ISA, bringing amendments quickly to include cyber incident reporting requirements on critical infrastructure, and revising the FADP (also driven by ensuring equivalence with EU on GDPR related aspects) are notable. Switzerland's federal structure, with Federal Government and Cantons having an important say on legislative matters, coupled with intense public consultation process, can slow down the introduction of new legislation or making major amendments to existing ones.

16. Various components of the ISA, including ordinances issued thereunder, are currently being rolled out and might take some time for fuller implementation. Achieving minimum standard in terms of Information Security Management Systems (ISMS), background check of individuals who are deployed in sensitive position (centralized process at the Government level), background check of critical service providers (centralized process at the Government level, and there is a waiting period of months already), and incident reporting are work in progress. For the SNB being a listed organization in the ISA, they depend on these processes more, compared to FINMA which is not a directly listed entity in the ISA.

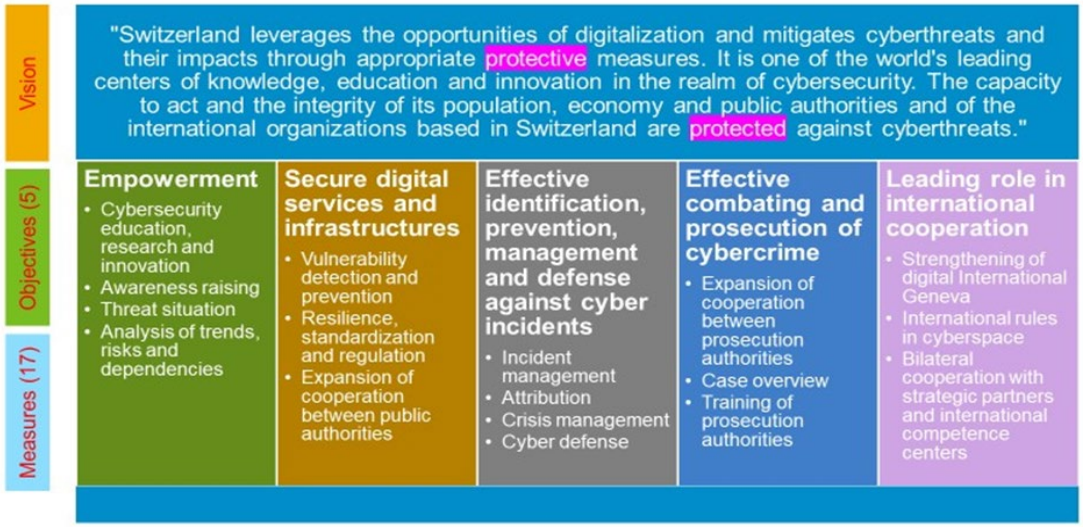
17. Legal measures require strengthening in two areas, namely (i) vesting powers with GovCERT (NCSC) to investigate systemic cyber incidents and (ii) strengthening the powers of the financial sector regulators to effectively supervise critical third parties. At present, although the ISA empowers GovCERT (NCSC) to receive incident reports, the law does not empower it to address a systemic cyber incident by way of investigation, if the victim company does not seek help. Multiple stakeholders expressed their view that in Switzerland, typically the firms behave responsibly, and such situations may not arise. However, it is important to have this power vested with GovCERT (NCSC) to take certain proactive steps without delay, when such incidents have a contagion potential to the whole sector or are judged important to take protective measures, and where the victim is not making a request or does not cooperate. Such powers are generally available in other jurisdictions.

18. Greater oversight over third-party providers is warranted. Third-parties risk management, particularly the risks posed by the critical service providers to the financial sector, has been the focus of various authorities and many countries have legal powers to supervise such entities effectively. In Switzerland, third parties pose significant risk and in the past year, there have been several incidents where third parties have been the target of cyberattacks to steal information from federal agencies as well as the financial sector. FINMA also observes that cyberattacks on third parties are growing and rightly placed outsourcing risk as one of the major risks in its risk assessment. Discussions with various stakeholders also highlight this as a major risk and needs to be addressed. The SNB, FINMA and SIF are already discussing this issue in the light of consultation document released by the Basel Committee on Banking Supervision (BCBS). Appropriate legal measures in this area would help strengthen the supervisor to have effective oversight.

B. National Cyber Strategy

19. Switzerland has developed National Cyber Strategy (NCS) for over a decade. The first NCS was for the period 2012–2017, and the second strategy for 2017–22. The third and current strategy was approved by the Federal Council and by the Cantons in April 2023. It is no longer limited in time, but it will be updated if the environment or the policy framework changes. However, the NCSC will continue to perform a fundamental review of the strategy every five years to ascertain whether the strategy sets out the right objectives and measures or whether adjustments are needed.

Figure 2. National Cyber Strategy



Source: NCSC - National Cyber Strategy.

20. A Steering Committee has been established to plan and coordinate the implementation of the NCS with representation from multiple stakeholders. The Steering Committee is made up of experts from the various areas of cyber security and aims to integrate the interests of the Cantons, business community, society, universities, and the Confederation. It defines performance indicators for each of the measures to achieve the strategic objectives. The NCSC functions as the steering committee's office and provides regular updates on the implementation status of the strategy and its assessment of the quality of implementation to the Federal Council.

21. The Cantons define their cyber security organization independently, in line with their needs. The Swiss Security Network (SSN) has drawn up the "Recommendation for the implementation of the cantonal cyberorganization", which was adopted by the Conference of Cantonal Justice and Police Directors (CCJPD) in 2020. This document provides guidance to the Cantons including suggestions regarding the appointment of a person responsible for coordinating cyber security-related tasks (cyber-coordinator) and a policy committee at Cantonal Council level. Cooperation with the Confederation is coordinated and promoted by the SSN. An annual report on the status of projects under the cantonal implementation plan is prepared.

22. The NCS is based on an understanding of the subsidiary and partnership role of the state. This means that the state only intervenes when the welfare of the society is seriously threatened, and private actors are unable or unwilling to solve the problem independently. In this case, the state can provide support, create incentives, or intervene through regulation, determining the appropriate measures in close consultation with the actors concerned and striving for close cooperation with them.

23. The role of the SNB and FINMA in implementing the NCS is limited, and the NCSC does not interfere in the supervisory and regulatory activities of FINMA and the SNB. FINMA has strengthened its regulations—notably on incident reporting and operational resilience—and is playing a role in crisis management. The SNB has contributed to establishing the FS-CSC and is a party in setting up crisis management protocols. The strategy document says that the federal office will not take over any supervisory or regulatory tasks from the specialist authorities in individual sectors, which remain responsible for authorization and ongoing operational supervision activities within the industry and for licensed companies regarding sector-specific cyber security requirements. The NCSC works directly with the specialist authorities and provides them with cyber security expertise.

Assessment and Recommendations

24. Cyber security is a cross-cutting issue and different stakeholders, including the Government and financial sector regulators, have major roles to play. It is generally considered a public good and the private sector may lack incentives to look beyond their corporate boundaries. It is important to strengthen public authorities who coordinate cyber security matters, particularly the NCSC. With their elevated status and cross-cutting responsibilities, the resources and authority of NCSC need further strengthening. It is important to appreciate that while there is a role for the private sector in managing idiosyncratic risks, it is for the official sector to address any sector level concentration and negative outcomes of systemic cyber incidents.

25. Having adequate resources in GovCERT (NCSC) will contribute to its effective functioning, including that of supporting the financial sector. The role of the GovCERT (NCSC) has expanded recently and implementing new legislations like the ISA will add to work pressure. Their involvement in resolving systemic cyber incidents, if any, will also demand resources. Having adequate resources in GovCERT (NCSC) will help the financial sector in strengthening its cyber preparedness further.

C. Critical Information Infrastructure Protection

26. The Federal Office of Civil Protection (FOCP) coordinates the activity of identifying and publishing the list of critical infrastructures. The list of critical infrastructures (CI) consists of ten sectors divided into 27 subsectors. The financial sector has been identified as one of the critical infrastructures with financial and insurance services identified as subsectors. A Critical Infrastructure Protection (CIP) strategy has been approved by the Federal Council. The inventory of critical infrastructure elements identifies individual critical infrastructure elements, which includes IT

systems, for planning and setting priorities with regard to risk management and incident response. The CIP inventory is not available in public domain.

27. The Federal Council published the latest Switzerland's National Strategy for Critical Infrastructure Protection in June 2023. The strategy aims to align all the relevant stakeholders, from the federal to the cantonal levels and the private sector, by outlining overarching goals and principles governing the Swiss approach to CIs.

28. The ISA provides that the Confederation supports the operators of critical infrastructures to ensure that network and system interruptions as well as abuses are rare, short-lived and manageable and that the extent of the damage is low. Support in the field of information security includes: (a) the early identification and assessment of threats, hazards, vulnerabilities, and security gaps; (b) the detection of incidents; (c) maintaining and restoring information security after an incident; and (d) the follow-up of incidents (Art.74). The Federal Council designates the federal agencies responsible for these tasks. The designated agencies are permitted to process personal data without notice. According to the ISA, IT resources must be classified within two years of the entry into force of this Act. Technical measures to ensure information security must be implemented within six years of the entry into force of this Act.

D. Scope and Applicability of Regulation

29. The operational, cyber, and IT risk unit in the Banking Division (B-OCI) is responsible for FINMA's supervision of IT and cyber risks. In addition, it is responsible for operational risk and resilience in banks, business continuity, and outsourcing. For the IT and cyber risk area, the Corporate Governance Circular (2017), Operational Risk Circular (2008) now replaced by the Operational Risk and Operational Resilience Circular (2023/1), the Guidance on Incident Reporting (05/2020), and the Outsourcing Circular (2018) are the main regulations and guidance. The applicability of regulations is not uniform. The outsourcing regulation is applicable to banks, insurers and securities firms, and operational resilience regulation and corporate governance regulation are applicable to banks, financial groups, fintech firms and investment firms, while the incident reporting guidance is applicable to all supervised entities. FINMA issues guidance notes to share their supervisory findings, expectations and provide clarification to their principles-based regulatory instructions periodically. In 2024, it issued guidance on supervisory findings, incident reporting and cyber scenario exercises (03/2024) as well as guidance on operational risk to fund management companies and collective investments managers (04/2024).

E. Regulatory Changes Since the Previous FSAP

30. There have been notable developments in terms of regulations in the past five years, focusing on cyber incident reporting and operational risks and resilience. Binding instructions in the form of a circular and guidance are issued when FINMA shares best practices, its interpretations, and certain requirements so as to provide clarity to the supervised entities. In 2020, FINMA issued a guidance on "Duty to report cyberattacks" pursuant to Article 29 para. 2 FINMASA, requiring all supervised entities to report cyber incidents in a timebound manner. The supervised

entities are required to inform FINMA about any medium and above category cyber incident within 24 hours, submit relevant details in a prescribed format within 72 hours and continue to submit follow-through reports till the incident is fully resolved and closed. The guidance states that FINMA will review the possibility of transferring the clarifications to a circular at a later point in time based on experience, accordingly a reference to incident reporting is introduced in the circular on operational risks and resilience. FINMA issued another guidance (FINMA Guidance 03/2024) titled "Findings from FINMA's cyber risk supervision, clarification of FINMA Guidance 05/2020 and scenario-based cyber risk exercises" that provided further clarification regarding the period for reporting, treating incidents at outsourced vendors, and what it takes to fully resolve various categories of incidents and guidance on how to meet various reporting requirements under FINMA and the ISA. In addition, there are reporting requirements under the FADP for incidents resulting in data leakage / loss—irrespective of the risk category of the incident.

31. Standard setters' work is reflected in a new circular issued by FINMA in 2022 on Operational Risks and Resilience. In December 2022, FINMA issued a circular on "Operational Risks and Resilience—banks" (2023/1) which is applicable to banks, financial groups and conglomerates, certain investment firms (proprietary trading and non-proprietary trading) and persons under Article 1b of the Banking Act, reflecting the changes in the environment as well as considering the Principles for Sound Management of Operational Risk (PSMOR) and Principles for Operational Resilience (POR). This principles-based circular replaced the earlier circular issued on operational risk management (2008) and incorporated key elements to achieve operational resilience. The circular addresses governance, risk management, technology risk, business continuity, outsourcing, cyber risk, and operational resilience. While most of it came into effect from January 1, 2024, there is a transition period of one to two years regarding select requirements.

32. FINMA also issued, in 2023, "Audit Points for Cyber Risk Management," to be implemented by auditors for interventions under the audit strategy effective January 1, 2024. The first audit report based on the template will be available in early 2025. The template elaborates several principles-based expectations into detailed assessment points and includes several areas where auditors are required to judge the adequacy of arrangements. As per this template, it is the responsibility of the audit team to adapt the standard work program to the specific situation of the institution (considering size, business model, organization, processes, risk exposure, etc.). If the specified audit procedures are not carried out completely, an appropriate rationale must be provided in the working paper. It is to be seen how this translates into actual audit work in the coming periods.

33. FINMA also issued a guidance on "Operational risk management by fund management companies and managers of collective assets" in 2024. The guidance highlights possible actions to enhance operational risk management, including ICT and cyber risks related aspects.

Insurance Companies

34. The revised operational resilience circular, containing expectations regarding ICT and cyber security, operational resilience, and testing requirements, does not apply to insurance companies. The Insurance Supervision Act requires the Board of Directors to be responsible for

identifying, managing, and mitigating all material risks. The Financial Market Supervision Act (Art-29) provides the legal basis for incident reporting of all licensed and supervised entities, including insurance companies. At the time of licensing, the B-OCI unit provides inputs on ICT and cyber aspects regarding insurance companies as well. Even for larger firms, there are no regulations that are clearly applicable in these areas.

Other Supervised Entities (Other Than FMIs)

35. With the exception of supervised entities that are part of financial groups, and investment firms (both proprietary and non-proprietary), there is no explicit technology or cyber regulation. Similar to insurance companies, only binding regulatory instruction flows from the base Act wherein the Board of Directors have been made responsible for identifying, managing, mitigating and accepting all material risks. At the time of licensing, the Banking Operational Cyber and IT risk unit provides inputs on ICT and cyber aspects. In respect to fund managers and collective investment scheme managers, recently published FINMA guidance provides clarity on expectations.

Assessment and Recommendations

36. There is an urgent need to extend ICT / cyber regulations and outsourcing regulation to all parts of the financial sector. Given that FINMA is responsible for a wide range of supervised entities, it is ideal to issue comprehensive instructions covering all major supervised entities and make certain provisions proportionately applicable, which will help the supervisors as well as the supervised entities.

Financial Market Infrastructures

37. The SIX Group operates various FMIs in Switzerland. The SIX group operated FMIs are the only locally established systemic FMIs, other systemic FMIs are foreign incorporated. While the SNB has the responsibility for SFMIs, FINMA regulates all the FMIs, except for SIX Interbank Clearing (SIC), which is a SNB-operated FMI. Within the general regulatory framework for FMIs, which is governed by the Financial Market Infrastructure Act (FMIA), the Financial Market Infrastructure Ordinance (FMIO), the National Bank Act (NBA), and the National Bank Ordinance (NBO), the SNB designates systemically important FMIs and their systemically important business processes based on the criteria in art. 22 FMIA, based on art. 23 FMIA, issues special requirements that must be fulfilled by systemically important FMIs (in addition to the general requirements stipulated in the FMIA/FMIO), including relating to IT systems. Special requirements relevant for cyber security are contained in the Ordinance to the Federal Act on the Swiss National Bank (NBO) in art. 32 (Management of Operational Risk), art. 32a (Information Security), art. 32b (Business Continuity) and art. 32c (Data Centres). Moreover, special requirements in art. 22 (Governance and Organization), art. 22a (Board of Directors, Senior Management and Internal Audit), art. 27 (Risk Management Principles), art. 31 (Management of General Business Risk), and art. 32d (Outsourcing) are also relevant for certain aspects of cyber security management.

38. The SNB has mandate to oversee SFMI and for SFMIs that are also supervised by FINMA; the two authorities cooperate very closely. For these FMIs, the SNB focuses on assessing

compliance with the special requirements. In the oversight of SFMIs, the SNB places high priority on issues related to operational risk management, including cyber security, and has focused on improving the maturity and the transparency of the cyber security framework in general and in particular in the area of recovery in the case of extreme but plausible scenarios (e.g., by preparing measures in case of a massive ransomware attack). For SFMIs that are operated by the SNB, or on behalf of the SNB, and hence are not subject to supervision by FINMA, the SNB is the sole authority responsible for oversight. FINMA supervises FMIs including SFMI and is planning to strengthen scenario-based testing including red team tests and improve data-based supervisory interventions. Active supervision of cyber risk started in 2017 and has progressively evolved. Moreover, together with FINMA and the FDF, the SNB has been engaged in advancing the financial market authorities' crisis management arrangements for serious operational incidents (including cyber incidents) in the financial sector, and a crisis management handbook has since been developed.

39. In 2018–19, SFMI were asked to carry out a self-assessment under CPMI-IOSCO cyber resilience guideline, but there have been no self-assessments thereafter. Initial self-assessment based on CPMI-IOSCO cyber resilience guidelines provided key insights on gaps, and the SNB and FINMA followed up with SFMI to bridge those gaps. Subsequently, SWIFT's Customer Security Program (CSP) also came into force. The authorities are of the opinion that while at the time of its introduction, CPMI-IOSCO cyber resilience guideline was very unique, over time, other standards like NIST have progressed further, and hence they do not see much value in carrying out self-assessments against CPMI-IOSCO cyber resilience guideline periodically.

40. The SNB has issued an end point security requirement to the participants of the SIC system. Its scope includes all banks (all categories of banks), fintech licenses (at present only 2, there is a proposal to convert such licenses into a payment service provider license going forward) and select insurance companies (which on account of their participation in repo markets is eligible to be part of inter-bank clearing). Compliance with the requirements is mandatory and commencing from 2024 external audit firms need to assess the compliance and provide feedback to the SNB. The requirement has been mapped to SWIFT CSP as well so that compliance could be monitored in an integrated manner.

Assessment and Recommendations

41. The SIX group operates critical FMIs as it plays many key roles in the financial sector. For SIC it is a third-party to the SNB. It operates exchanges and therefore it is a regulator for certain entities; it operates multiple FMIs, each incorporated separately under the supervision of FINMA; it provides market data for the financial sector both within Switzerland and abroad; and also, can provide third-party services to other financial sector entities. It is jointly owned by the financial sector participants locally and abroad. It has acquired Bolsas y Mercados Espaoles (BME) in Spain, has presence in Germany and is looking forward to further expanding its presence. It appears to have assumed such a central role in the financial markets, it would be fair to designate it as a "Too Big to Fail Institution" and strengthen the supervision further.

42. From a technology and cyber security perspective, the SIX group operations entail significant risks to the financial sector and are crucial to day-to-day operations of the financial sector. There are several complexities. For instance, though SIC is a third-party to the SNB, the SNB as SIC System Manager does not conduct independent audit of their service provision, instead it depends on the external auditor's opinion. SIC Board also has a senior official from the SNB, and the oversight is carried out by a different unit. SIC is a critical third-party service provider of a critical infrastructure and is subject to ISA provisions. FINMA does not have either mandate or opportunity to supervise SIC, though it is part of the supervised group. The technology architecture of the SIX group will have a bearing on the operations of SIC. The audit focus areas for the SIX group as well as SIC are determined by the SNB. A systemic cyber incident in the SIX group could potentially have systemic devastating implications.

43. The SIX group has progressed in its journey to strengthen cyber security, but gaps remain. With the supervisory focus on strengthening cyber security, the SNB issued various expectations to be met by the SIX group. One of the major achievements is making their operations ransomware proof. There are contingency arrangements for SIC to carry on with lesser capacity in the event of simultaneously unavailable data centres. The progress in terms of achieving the internally targeted maturity profile falls short for its local and Spanish operations. The maturity level in the Swiss entities is higher compared to the Spanish entities.

44. It is important to consider various options to limit further concentration in the SIX group and de-risk the existing levels of concentration. With their presence in the entire range of market activities, including the provision of market and reference data for settlement to local as well as global financial institutions, the concentration risk is already very high. It is desirable to ensure that concentration levels do not further increase, leveraging existing licensing and oversight powers.

45. Requiring SFMI to carry out self-assessments under CPMI-IOSCO guidelines more frequently would help the supervisors better understand emergence of new gaps arising from implementation of new systems or retirement of existing systems. While the guidelines are about six years old now, they are still relevant to the FMIs as they refer to the PFMI. Works started on the guideline update and a revised version could be in place soon. SFMI can internally map various requirements under regulations issued by the SNB and FINMA, SWIFT's CSP and CPMI-IOSCO cyber guidelines and ensure meeting all requirements.

46. The issuance of end point security requirement mapped with SWIFT's CSP is a welcome step. The approach of the SNB to focus on all participants reflects the potential threat posed by any of the participants to the inter-bank clearing system. This is more needed as the RTGS is used not only to settle larger transactions but also retail payments on a gross basis. The same logic should apply to FINMA's supervision efforts as risk-based approach for cyber should consider the potential of weakest link impacting cyber security.

INSTITUTIONAL ELEMENTS

47. Switzerland is actively promoting its Swiss Financial Center status, including by encouraging digital innovation. The factsheet on 10 years of State Secretariat of International Finance (SIF) rightly captures this by "Support for new, innovative and promising areas (fintech, blockchain, sustainable finance) with a focus on opportunities and risks, but without overregulation" as one of its achievements. The National Cyber Strategy (NCS)[5] is based on an understanding of the subsidiary and partnership role of the state. This means that the state only intervenes when the welfare of the society is seriously threatened, and private actors are unable or unwilling to solve the problem independently. In this case, the state can provide support, create incentives, or intervene through regulation, determining the appropriate measures in close consultation with the actors concerned and striving for close cooperation with them. One of the strategic goals of FINMA for the period 2017-2020 mentioned is that it will push for the removal of unnecessary regulatory obstacles for innovative business models. In a way, public messaging favors private sector solutions to problems, with regulation receiving lower preference or as one of the last resorts. The messaging from the Government has been consistent to indicate that regulations should be need-based and reviewed periodically to ascertain continued relevance.

48. Based on a comparison with other international financial centers, Switzerland has significant room to catch up. Based on the ranking with reference to cyber security index[6] published by ITU for select countries, Switzerland lags peer international financial centers, many of which have significantly more detailed cyber security regulations and a more hands-on supervisory approach (Table 2). Switzerland is placed in Tier 2 while other peer financial centers are placed in Tier 1.

Table 2. Switzerland: Comparison of Cyber Security Index—Select Countries

Country	Cyber Security Index Ranking (2020)	Cyber Security Index Tiers (2024) *
France	9	1
Germany	13	1
Singapore	4	1
United Kingdom	2	1
United States of America	1	1
Switzerland	42**	2

** Number of Tier 1 countries =>45
* ITU publication indicates that Switzerland did not respond to the questionnaire and the ranking is based on publicly available materials.

[5] Source: National Cyber Strategy 2023 (pg 13).

[6] The **Global Cyber Security Index (GCI)** is a trusted reference that measures the commitment of countries to cyber security at a global level—to raise awareness of the importance and different dimensions of the issue. As cyber security has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars—(i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation—and then aggregated into an overall score. (Source: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx).

A. Institutional Arrangements

49. The Federal Council looks at cyber security under three domains—cyber security, cyber defense, and cyber prosecution. The NCSC is responsible for cyber security. Intelligence services and armed forces are responsible for cyber defense and cyber prosecution falls mostly under cantonal authorities. At the national level, the Federal Council is the highest authority, and it has established a Cyber Core Group to support this activity. A National Cyber Strategy Steering Committee comprising a wider section of representatives monitors the progress in implementation of NCS and the federal cyber security delegate—who is also the head of NCSC, provides support to the committee. The FDF is ultimately responsible for the financial sector and has a unit supporting cyber security developments under its Insurance Division. The SIF also deals with crisis management as well as international cooperation on the topic and involves the SNB and FINMA in this process.

50. The NCSC was set up under the Ordinance on Protecting against Cyber Risks that entered into force on July 1, 2020, as approved by the Federal Council. The tasks of the NCSC include: (i) operating a national contact point on cyber risks that centralizes and analyses reports from the federal administration, economic sectors, cantons and general population; (ii) running the national Computer Emergency Response Team (GovCERT); (iii) managing the federal administration's specialized IT security service; and (iv) assisting different offices in implementing the NCS, and developing, implementing and evaluating standards and regulations in the field of cyber security.

51. The NCSC's role has been elevated and relocated effective from January 1, 2024. The NCSC became a federal office (Federal Office for Cyber Security) and was transferred from the FDF to the Federal Department of Defense, Civil Protection and Sport (DDPS), thereby increasing their stature and visibility within the country. The NCSC has a staff of 67, out of which 12 staff are earmarked for the GovCERT function. They are responsible for all the critical infrastructure sectors, federal agencies, and cantonal authorities. They collaborate actively with the industry and the regulators though they do not assume any regulatory role. A Federal Office of Information Security is currently being established to look after the Federal Council's and other federal authorities' information security needs, which is likely to be activated by mid-2025. Until then the NCSC will carry on these tasks.

52. One of the notable developments in Switzerland is the setting up a Financial Sector Cyber Security Center (FS-CSC), as a public-private partnership. The FS-CSC is set up as an association of currently 171 members from the financial sector on a voluntary basis and supported by the SIF, SNB, NCSC and FINMA and started its operation in 2022. Members pay an annual fee, which supports the activities and participate in working groups set up on various topics. The FS-CSC plays an important role in facilitating information sharing among financial sector entities, building awareness, developing guidelines on select areas to provide guidance to its members, conducting exercises and tests, and dealing with systemic cyber crises. The SNB is a full member of the steering board and FINMA, SIF and the NCSC sit in the steering board as participating members without vote, considering their supervisory roles.

53. A Federal Data Protection Agency (FDPA) has been set up to implement the new Federal Act on Data Protection (FADP). The FDPA is headed by Federal Data Protection and Information Commissioner (FDPIC) and among other things requires reporting of incidents involving data privacy issues including from the financial sector. FINMA is exempt from the provisions with regard to its supervisory activities, though the act will be applicable to the processing of data related to their own employees.

Assessment and Recommendations

54. Coordination among FINMA, NCSC and FDPA regarding incident reporting will help in reducing the regulatory burden on the financial sector. FINMA's incident reporting framework came into force with the 2020 guidance. There are incident reporting requirements under the new ISA as well as FADP, though with some variance in terms of threshold, nature of incident, and scope of application. Also, the information requirement by respective agencies may differ. It is important to coordinate these activities well and introduce a technical solution to ensure minimal regulatory burden on the financial sector. NCSC is currently coordinating with the authorities in this regard.

B. Computer Emergency Response Teams

55. The GovCERT, as an integral part of the NCSC, provides specialist technical services in analyzing and managing cyber threats. The GovCERT (NCSC) is the official CERT of the Switzerland's government and is a member of FIRST (Forum of Incident Response and Security Teams), of the European Government CERTs (EGC) group and of the International Watch and Warning Network (IWWN). Its constituency is the network of the Swiss Federal Administration (Government) as well as the private and public sectors in Switzerland. It supports critical infrastructure operators, the public sector, and the Swiss business location with technical information on current cyberthreats and with the management of cyber incidents. The GovCERT (NSCS) also works in close collaboration with the police authorities. This cooperation covers both the exchange of information and the support with technical analyses.

56. Cyber incidents reported to the NCSC have exhibited a steady growth over the past five years. Figure 3 depicts the number of cyber incidents reported to the NCSC from 2019 to 2023. Cyber incidents reported increased by more than 100 percent during 2020-21 and thereafter moderated to 59.0 percent and 38.6 percent for the years 2021-22 and 2022-23. Cyber incidents reported during the first half of 2024 stood at 34789 (19048 during the first half of 2023), exhibiting a growth of 82.6 percent over corresponding period of the previous year. 90 percent of reports came from individuals and the rest from corporates.

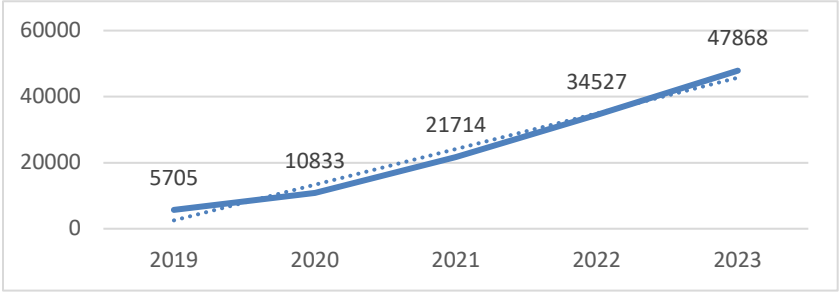
57. In the past two years, Switzerland has faced several notable cyberattacks. These include (i) the distributed denial of service (DDoS) attacks[7] on Swiss organizations and authorities in the first two weeks of June 2023; (ii) ransomware attack[8] on a software company 'Convevis', a provider of

[7] NCSC Analysis Report dated October 30, 2023.

[8] The Federal Council—the portal of the Swiss Government—report dated November 14, 2023.

software solutions for public administrations, the financial sector and companies in industry and logistics; (iii) a malware campaign[9] known as 'Poseidon campaign' targeting Swiss macOS internet users, and (iv) hacker attack[10] on 'Xplain' a major provider of IT services to national and cantonal authorities.

Figure 3. Switzerland: Cyber Incidents Reported to NCSC (2019–2023)



Source: NCSC.

Assessment and Recommendations

58. The GovCERT (NCSC) has been playing an important role in monitoring the threat landscape, issuing advisories, helping in handling incidents, and generally supporting initiatives to strengthen cyber security. The range of activities performed by the GovCERT (NCSC) along with the broader NCSC is notable. The NCSC has undergone several administrative changes in the past few years. NCSC have now assumed the role of single point contact for mitigating cyber risks of the country. The GovCERT (NCSC) actively coordinates its activity with its international peers.

59. The GovCERT (NCSC) needs to be strengthened with adequate resources and legal powers. Resource constraint and inadequate legal powers may hamper the effective functioning of the GovCERT (NCSC), having a bearing on the financial sector as well. The GovCERT (NCSC) currently has a strength of 12 FTEs, which is very low compared to its responsibilities. The growing frequency and sophistication of cyberattacks will make its role expand further in the future. Its responsibilities in implementing ISA provisions that are yet to be fully implemented, and addressing the challenges of varying cyber maturity of different sectors underscores the need for urgent augmentation of their resources. In a comparable country within Europe, a national CERT will easily have 100+ FTEs to discharge their responsibilities. As indicated earlier, the GovCERT (NCSC) also needs to have sufficient legal powers to address systemic cyber incidents proactively.

C. Coordination Across Authorities

60. The Federal Council published a report titled "Digital Finance: Areas of Action 2022+" in February 2022 identifying 12 specific areas of actions.[11] As regards cyber security, the Federal

[9] Technical analysis of Poseidon campaign targeting Swiss internet users published by NCSC on July 11, 2024.

[10] Data analysis report published by NCSC on March 7, 2024.

[11] Digital finance: areas of action 2022+, Bern, Feb 2022 published by the Federal Council.

Council instructed the FDF (NCSC), together with competent offices (SIF, FINMA and SNB) to continuously monitor the threat situation and the state of progress regarding cyber security in the financial center, and to expand the mechanisms for combating financial cybercrime. The specific areas of action also included several ICT and data security related aspects.

61. Formal agreements help in enabling better coordination and cooperation among agencies. Tripartite agreement between the FDF, the SNB and FINMA facilitates cooperation among agencies, particularly in a crisis. The bipartite agreement between the SNB and FINMA facilitates coordination among them, notably regarding supervision of SFMI, financial stability analysis, and crisis coordination. However, the cooperation between the SNB and FINMA could further be enhanced by (i) coordinating their activities regarding supervision of SFMI by mutually inviting the other agency for meetings with the SFMI; (ii) the SNB may invite FINMA for the supervisory discussions with the Swiss Inter-bank Clearing system (SIC) even though SIC does not come under their purview in order to get a fuller picture on the functioning of SIX; and (iii) coordinating the supervisory activities further.

62. The NCSC plays an important role in the national cyber security preparedness and particularly that of critical infrastructure such as the financial sector. Both the SNB and FINMA coordinate with the NCSC well during normal times as well as during a crisis. The NCSC, the SNB and FINMA, as well as SIF, also sit on the steering board of the FS-CSC either as a member or an affiliate.

Assessment and Recommendations

63. The tripartite agreement among the FDF, SNB and FINMA and the bipartite agreement between the SNB and FINMA are the good bases for cooperation and coordination among these agencies, although there is scope for improvement. The SNB and FINMA have responsibilities related to SFMIs and in this, they cooperate already. The SNB's role in financial stability necessitates close coordination with FINMA in cyber security matters, such as stress testing under a severe but plausive cyber scenario or conducting a cyber resilience stress testing. Under the tripartite agreement, a steering committee has been established that meets semi-annually to discuss strategic coordination; a committee on financial crises (CFC) that coordinates the preparatory efforts for crisis managements, and a sub-group on operational crises that focuses on operational matters, including developing a crisis management handbook, cooperating at the operational level and facilitating conduct of exercises. While the focus on handling crises is understandable, there is scope for improving the role of these committees during normal times, for example, by articulating a cyber security strategy for the financial sector, periodical assessment of threat landscape, nature of cyber incidents, changes within their organizations that may have a bearing on the crisis preparedness, providing directions to the operational teams, adequacy of regulations and supervisory focus, and lessons to be learned from other sectors.

64. Coordination and cooperation between FINMA and FDPA may be formalized in the form of a MOU to further enhance the cooperation. Such an arrangement can help in understanding of mutual responsibilities, ways to minimize regulatory burden, and streamlining operational processes.

SUPERVISORY ARRANGEMENTS

A. Supervisory Priorities

65. FINMA publishes its strategic goals every four years, after approval from the Federal Council, and the current strategy covers the period 2021–24. Among the ten strategic goals are: (i) ensure that financial institutions maintain the highest risk management standards and promote responsible corporate governance (FINMA identified cyberattacks as one of the most significant risks faced by the financial sector in its Risk Monitor), (ii) seek to ensure that financial institutions remain robust in the light of forthcoming structural developments and clients are able to benefit from new opportunities without being exposed to additional risks (the rapid pace of digitalization has been identified as one of the challenges), and (iii) promote innovation in the Swiss financial center (when applying existing rules to innovative business models and products, FINMA takes a pragmatic and forward-looking approach. FINMA ensures that regulation and supervision do not pose unnecessary obstacles to innovation and are designed in a technology-neutral way, so that innovative business models and products have a fair chance on the market) can be considered relevant for assessing ICT / cyber risk.

66. FINMA identifies cyber risk as a major risk every year since it was added to the Risk Monitor in 2019. The published Risk Monitor creates transparency both for supervised institutions and the wider public about how FINMA fulfils its statutory responsibilities. It provides an overview of what FINMA believes are the most important risks currently facing supervised institutions over a time horizon of up to three years. This is supplemented by a Risk Barometer, which is an internal document. Seven risks remain the same as in the previous year: interest rate risks, credit risks associated with mortgages, credit risks associated with other loans, credit spread risks, risks of cyberattacks, risks in combating money laundering and risks due to increased impediments to cross-border market access. The cyber risk trend over the last five years is shown in Table 3.

Table 3. Switzerland: Trend of Cyber Risk in the Financial Sector

Year/ Trend	2019	2020	2021	2022	2023
Cyber risk	New	(↑)	(→)	(→)	(→)

Source: FINMA Risk Monitor. The trend of each risk for the next three years is indicated by way of an arrow (increasing, remained same, decreasing.

67. Outsourcing risk has been added to the list of main risks in the Risk Monitor in 2023. This underscores the importance of outsourcing and third-party risk management within the Swiss financial sector. There have been a few impactful cyberattacks on the service providers (example include Xplain attack.) where significant amount of data was exfiltrated and published in the dark web. This has raised an alarm not only in the financial sector but also in other critical sectors. The NCSC also considers this as an emerging risk area where concerted action is needed. FINMA notes that outsourcing has continued to grow in recent years due to digitization and the focus by financial institutions on their core business. FINMA recognizes that while outsourcing offers many advantages, such as flexibility, innovation, and improved operational resilience, interruptions and

outages of critical functions and key service providers can also pose significant risks and in extreme cases, they could affect the stability of the financial market.

B. Supervisory Processes

68. Cyber risk supervisory processes were strengthened notably post 2020. FINMA recognized that dependency on ICT continued to rise in 2020, driven by digitalization strategies pursued by the supervised institutions and intensified by the pandemic-driven extensive shifts towards home-office working. FINMA therefore assessed this risk to be even higher than in the previous year. Consequently, FINMA further augmented its resources to monitor institutions across three areas: (i) the analysis of the threat, (ii) ongoing supervision and (iii) incident management or eventually crisis management. This approach allowed for consistent FINMA-wide monitoring of the cyber risks faced by all supervised institutions.

69. Following the complete revision of the Circular "Operational risks and resilience", FINMA updated its supervisory practice regarding cyber risks in 2023. In November 2023, FINMA provided additional guidance to the Audit firms carrying out regulatory audit related to cyber security. The changes enter into force for audit periods ending in 2024 and will be the focus of future supervisory activity.

70. The supervision of cyber risk, along with operational risk and resilience, ICT risks, outsourcing and business continuity are carried out by a small unit. The Operational, Cyber and IT risks unit (B-OCI) within the Risk Management department, which is located under Banks Division. Though the unit is located within the Banks Division, for cyber and ICT risks as well as outsourcing, the responsibilities are FINMA-wide, that is, the unit is responsible for all the supervised entities. The unit has responsibilities including: (i) contribute to developing regulations; (ii) assessing the threat landscape; (iii) onsite and offsite supervision; (iv) incident reports and follow up; (v) receiving external regulatory audit reports and perusing them identify supervisory concerns and following up; (vi) assisting in licensing process by providing comments on the ICT / cyber security requirements; and (vii) coordination and cooperation with other agencies both within Switzerland and internationally. A unit focusing on AI is located within the Insurance Division with FINMA-wide responsibility.

71. FINMA is currently examining carving out all specialized risk units that perform horizontal reviews to be placed in a separate division, at the same hierarchy level as Banks or Insurance division. The current arrangement of having the risk management department located within Banks Division and making them responsible for FINMA-wide responsibilities poses administrative and logistical challenges. This change, when implemented, will help in strengthening the supervisory activities further.

72. The NIST framework is leveraged in articulating the regulation. FINMA uses the NIST framework for framing its regulation and in general, financial sector entities in Switzerland are aware of the NIST framework and many use it. Some of the major banks leverage other standards as well, namely, ISO and COBIT.

73. The B-OCI maintains specific documents describing the supervision process on ICT and cyber risks. A list of relevant documents as follows:

- Supervision concept of B-OCI.
- Technical concepts of B-OCI on ICT and cyber risks.
- Benchmarks on ICT and cyber risks.
- On-site inspections policy.

74. On-site inspection policy provides guidance on the conduct of onsite examinations, which are categorized as deep dive, supervisory review, and joint reviews. Deep dives are typically conducted for a day by visiting the supervised entity. Supervisory reviews are conducted for a maximum of four days and joint reviews are conducted along with international regulators on a need basis. The onsite examination visits are planned annually by a central unit based on the major risks identified in the Risk Barometer and considering the proposals made by the key account managers. Review manager accompanies the onsite team of cyber specialists to ensure that supervisory policies and processes are adhered to, and the key account manager also joins the team. For the year 2023, eleven supervisory reviews and three deep dives were carried out.

75. External audit firms have a larger role in the Swiss financial market since FINMA and the SNB mandate regulatory audits, carried out by audit firms regularly. The number of onsite examinations conducted by FINMA vis-à-vis regulatory audits performed by the external auditors is given in Table 4. External auditors do most of the work, with FINMA slowly increasing their on-site visits over the period. In in-depth audits, FINMA plays a role in determining the scope of the audit. At times, depending on the scope determined there are push-backs from the supervised entity if the costs have a significant bearing on their audit budget, and rarely is the scope reviewed by FINMA again so that such a situation is avoided. FINMA also review the draft audit reports. All the external audit reports are submitted to FINMA and the B-OCI staff review these reports on a regular basis but with priority given to larger and systemic entities. All regulatory audits do not assist in completing the 'Benchmark', and that is why only 32 'Benchmarks' are available even though the number of regulatory audits is larger. In all the examination reports issued by FINMA, a notification to the effect that examination is not an audit, and its scope, focus and purpose differ.

76. The top ten risks identified by the audit firms provide key insight on the position of cyber risk as part of the top risks (Table 5)**.** For all category 1 and 2 banks, cyber is either top risk or second top risk. For category 3 banks, for 15 banks, it is either top risk or second top risk, similarly 25 and 43 banks in categories 4 and 5 respectively. In addition, ICT risk, operational resilience, business continuity and outsourcing risk also placed in top 10 risks notably. All these risks are closely related to cyber risk.

Table 4. Switzerland: FINMA Onsite Examination Activity and External Auditors' Regulatory Audits on ICT and Cyber Risks			
Year	FINMA On-site Exams	Regulatory Audit by External Audit firms	Of which In-depth Audit
2020	4	212	29
2021	14	229	21
2022	19	218	18
2023	17	211	18
Source: FINMA.			

Table 5. Switzerland: Summary of Audit Findings—Cyber Risk among Top 10 Risks										
	Rank 1	**Rank 2**	**Rank 3**	**Rank 4**	**Rank 5**	**Rank 6**	**Rank 7**	**Rank 8**	**Rank 9**	**Rank 10**
Category 1	1									
Category 2	2	1								
Category 3	7	8	3	1	3	2			1	
Category 4	14	11	3	10	5	2		1	4	
Category 5	22	21	18	16	14	12	6	7	1	6
Total	46	40	24	27	22	16	6	8	6	6
Source: FINMA.										

77. In November 2023, FINMA issued 'Audit Points for Cyber Risk Management' as part of standard audit program to be carried out by external auditors. This document elaborates the regulatory expectations in a systematic way to assist the auditors to perform their task and achieve consistency in results. This will become applicable for audits conducted for the period 2024 and onwards. It is expected that such a systematic approach may lead to a greater number of findings initially and lead to better compliance over time. For instance, some of the supervisory examination visits produced better results than auditors, as observed by FINMA.

78. The B-OCI prioritizes their supervisory activity in a risk-based manner, focusing significant efforts on GSIB, DSIBs and SFMI. FINMA categorizes banks into five categories, Category 1 & 2 being GSIB and DSIBs, Category 3, 4 and 5 banks are based on size; some Category 3 banks are large. After banks, its priority are security firms and insurance companies, followed by other supervised entities. As a rule of thumb rule, FINMA has better understanding of the digital risk profile of large banks, SFMI and large insurance companies. They depend on external auditors for the other entities.

79. FINMA uses a tool called 'Benchmark' to assess the cyber maturity of its supervised entities. This excel-based document provides guidance to the examiners in assessing the maturity of the supervised entities by clearly linking it to various requirements in the Operational Risk and Resilience circular, related expectations from the supervised entity and guidance regarding how to assess the respective areas. The observations of the supervisors are captured in a free text format. Using a weighted average score a heat map is generated for each of the major components of the

circular indicating the level of maturity as well as a composite heatmap. To complete the 'Benchmark' sufficient information is needed and that is available mostly for category 1 & 2 banks, SFMI, category 3 banks, and insurance companies subjected to onsite examination by FINMA. Thus, FINMA has completed such 'Benchmark' for 32 supervised entities all together. Such information is not available for the rest of the supervised entities.

80. In addition, FINMA carries out occasional surveys to gather relevant information. Recently, a survey of small and medium-sized insurance companies was conducted to enable a better assessment of the state of readiness of supervised institutions' cyber- specific risk management. FINMA will define further specific supervisory measures based on the survey. It also wrote to a set of insurance companies whose cyber-preparedness was considered leaving scope for improvement. Similarly, a detailed survey was conducted on the topic of outsourcing. The survey questions included various ICT aspects as well. A memorandum summarizing the outcome of the survey was prepared and shared with the management. The survey clearly indicates that the third-party risks are increasing, particularly cloud adoption has increased steadily.

81. FINMA holds regular meetings with IT and Cyber teams of Category 1 and 2 banks and technical discussions as needed. These discussions help FINMA to keep abreast of developments in the IT / Cyber work areas and to follow up on the progress made in complying with regulatory action points as well as regulations. The results of such engagements are also reflected in the 'Benchmark' exercise.

82. FINMA regularly shares with supervised institutions and the public current risks and potential attack vectors as well as methods based on the cyberattacks reported to it. Two such reports are Risk Monitor and Cyber Dossier. While Risk Monitor provides a list of top risks which are considered as a principal risk by FINMA on an annual basis, Cyber Dossier provides details about incidents reported and their analysis. One of the observations made recently by FINMA was that third-party service providers and smaller firms accounted for a larger share of incidents.

83. On-site inspections of critical third-party service providers are occasionally carried out by FINMA. As per Article 23 of the Banking Act, if a bank outsources essential functions to other natural or legal persons, they are subject to the information and reporting obligation in accordance with Article 29 of FINMASA. FINMA can carry out checks on these persons at any time, only in relation to the outsourced function. Such enabling provisions are not there for non-banks. Currently the SIF, SNB and FINMA are discussing ways in which the regulatory and supervisory practices around third-party risk management could be further strengthened. The equivalent of the EU's Digital Operational Resilience Act (DORA) and its provisions are also considered, but authorities feel such a complex arrangement may not be warranted for Switzerland.

Assessment and Recommendations

84. Supervision is heavily dependent on external auditors; that is detrimental to effective supervision and needs to change. It is important for supervisors to have insights on the digital risk profile of the supervised entities, which is facilitated by on-site examinations. FINMA articulating its

audit objective to the auditors for Category 1 & 2 banks and perusing the audit reports of other categories of banks may not be sufficient. The dependence on external auditors needs to be reduced and on-site supervisory visits need to be augmented.

85. There is a need to review the on-site supervision policy, look at synergies between IT and cyber risk examination units, and strengthen off-site supervision. Cyber risk and outsourcing risk (which is closely related to cyber risk) are considered high risk categories in the Risk Barometer. On cyber risk supervision, currently there are no regular off-site reports gathering key risk indicators, gap assessments, mapping related information, etc., that allow obtaining a better understanding of digital landscape of the financial sector. There is also a lack of visibility on these risks in respect of category 4 & 5 banks in particular. Under onsite supervision policy, onsite examinations may be conducted in the form of deep dive (one day), supervisory review (maximum of four days) and joint review (with international regulators). The limitation of the duration of examinations may undermine the effectiveness of such assessments. Some of the recommendations are:

- Cyber security is as strong as the weakest link and hence supervision needs to be strengthened further for category 3, 4 and 5 banks and other financial sector entities. The intensity and frequency of the onsite visits need to increase, considering the heightened and persistent levels of cyber risk. The artificial caps on examination periods may be reviewed and suitably modified.
- There is a potential to increase synergies by combining the IT and Cyber teams together as these topics are very closely interrelated.
- Offsite supervision needs to be strengthened by requiring regular reporting to obtain better understanding and maintaining digital risk profile of entities.
- It is important that supervised entities provide regular information to their respective Boards on this important area, covering analysis of the threat landscape, type and trend of incidents, regulatory environment, supervisory actions as well as material gaps in the preparedness.

C. Incident Reporting Arrangements

86. Requirements under Article 29 of FINMASA already mandate supervised entities and the audit companies that conduct audits on them to report to FINMA any incident that is of substantial importance. This applies to technology and cyber incidents too. Prior to cyber risk becoming a major risk for the financial sector, reporting of IT and cyber incidents were rare.

87. FINMA's guidance issued in May 2020 indicates the responsibilities of supervised institutions and introduced a reporting template, and classification requirements. FINMA extended this guidance to all supervised entities and used an IT application to collect such incidents. The framework requires supervised entities to report all cyber incidents that are categorized as medium and above on an individual basis. Initial report in the form of an email or a phone call to the key account manager must be made in 24 hours, followed by submission of the incident reporting template duly filled in 72 hours, considering working days. In cases of critical incidents, the number

of days is counted including the bank holidays and weekend. Subsequently, the report must be updated till a final closure is achieved.

88. FINMA published a summary of incidents reported for the benefit of informing the public as well as the supervised entities in cyber dossier. From the commencement of cyber incident reporting in late 2020, FINMA has provided information on the number and type of incidents, category of supervised entities impacted, and an analysis of such incidents on its website.

89. Based on the experiences gained over past three years, FINMA issued a new guidance note in 2024 reflecting the supervisory expectations regarding incident reporting. The guidance note summarizes the common errors noticed by FINMA in receiving such reports and provides clarity to supervised entities and clarifies the requirements accordingly. This is likely to further improve the quality of such reporting.

90. FINMA's cyber incident reporting format does not capture certain critical elements, such as details about amounts of losses incurred or potential losses for each incident. The current practice of collecting incident information does not therefore provide the quantum of losses suffered by the supervised entities.

91. FINMA's reporting indicates certain categories of institutions are more often successfully targeted. Some of the trends shared by FINMA include (i) smaller institutions are successfully attacked more often, (ii) insurers (around 30% of attacks) and asset managers (around 20%) are more often becoming the focus of successful cyberattacks compared to the past and to banks, and (iii) successfully attacking companies via service providers has continued. FINMA uses such reporting to reiterate the need for the financial institutions to keep carefully monitoring the current threat level, react quickly if needed and continuously test their own infrastructure for any vulnerabilities. In all, about 280 incidents have been reported to FINMA since the introduction of such reporting. The incidents reported by banks, insurers, asset managers and market infrastructure stood at 78, 60, 147, and 3 respectively. Compared to 74 incidents reported in 2023, until October 2024, 54 incidents have been reported.

Assessment and Recommendations

92. FINMA should upgrade the instructions for incident reporting from the current guidance to a full-fledged circular. At present, FINMA elaborates the incident reporting requirements in the Circular on Operational Risks and Resilience. FINMA is aware that FSB is looking at the cyber incident reporting practices and templates and has issued a consultation document in October 2024 proposing a new reporting format for cyber incidents. This template and best practices are expected to bring in convergence in regulatory expectations, and Switzerland have multiple licensed entities operating globally it would be desirable to reflect the finalized the Format for Incident Reporting Exchange (FIRE) format for incident reporting.

93. FINMA must collect a summary of cyber incidents comprising all categories to understand the overall threat landscape better in the form of a regular off-site report.

Currently, cyber incidents below the threshold for reporting to FINMA are not divulged to FINMA on a regular basis. As a result, FINMA is considering only the individually reported cyber incidents for its supervisory purposes. It is necessary that FINMA gets a complete picture of all cyber incidents impacting the financial sector. This return can be designed to capture different types of cyber incidents, the quantum of losses incurred by the supervised entity, amount of customer losses, and the number of such incidents for each type on at least quarterly basis. This can be used to obtain a complete picture for regulatory and supervisory purposes.

D. Supervisory Resources

94. FINMA's resources in the B-OCI are inadequate. The unit has nine staff apart from the head of the unit, with one FTE responsible for operational risk and operational resilience, three FTEs each looking after ICT, Data, and cyber risks and two FTEs with responsibility to supervise outsourcing risk. Other factors to consider are (i) the number of supervised entities; (ii) need to strengthen off-site supervision, (iii) implementation of various elements of operational resilience circular, (iv) extending the circular to other segments of the financial sector, (v) strengthening outsourcing regulations, (vi) increasing the number and duration of onsite examinations, (vii) revision of the incident reporting circular, and (viii) cyber risk being one of the top risks consistently over years.

95. The SNB's resources in oversight unit are limited with current responsibilities to oversee the SFMI, and the gap is expected to increase as new security requirements come into force. The SNB's oversight unit prioritizes its work to monitoring the SIX group predominantly. The unit also is responsible for designating SFMI, prescribing special requirements under the Act, deciding on the scope of external audit, perusing the audit findings and following up, perusing the internal audit reports and having ongoing dialogue with the SFMI. End point security requirements issued by the SNB to the SIC participants, and the requirement therein to obtain a certificate from external audit firms in respect of all the participants will increase the workload significantly. The requirement will translate into perusing 300 such certificates from Auditors and following up with the banks for remedial action where there are gaps by the Banking Operations Department. This might also lead to some banks opting to participate in clearing indirectly, and the paperwork related to that also needs to be considered.

96. The need for strengthening assessing systemic cyber risk as part of financial stability analysis will entail additional work for both the SNB and FINMA. This will include coordination measures, research, design of such exercises, monitoring and finalizing outcomes and follow-ups.

Assessment and Recommendations

97. Given the range of institutions under supervision, and the work areas planned, the staff in FINMA focused on this work area is inadequate and needs to be augmented. Considering the size of the Swiss Financial Center the supervisory resources (of the ten focusing on operational risk, IT and cyber, three resources are focused on cyber) are grossly inadequate. Due to

ongoing work pressure, always there is a tendency to prioritize the activities to a sub-optimal level. In cyber risk, one needs to consider the weakest link will determine the security posture.

98. There is a need to augment resources within the SNB to address additional work areas and to have a complete understanding of the risk profile of SFMI. The current resources will not be sufficient to handle the upcoming work assignments and lack of resources will reflect on the quality of work.

E. Enforcement

99. When it comes to enforcement, FINMA does not have legal powers to levy monetary penalties. Powers to levy non-monetary penalties exist, but to date, there have been no cases of use. FINMA as a supervisor does not enjoy the powers to levy monetary penalty generally and the same applies to ICT / cyber risk. Non-monetary penalties can be levied if the supervisors substantiate grounds for such a penalty and recommend it to the Enforcement Division. If such requests are found maintainable, the Enforcement Division conducts its own investigations to reach a conclusion. Once the Enforcement Division has enough proof of violation of legally binding instructions, it can levy a non-monetary penalty. This can be challenged in courts by the supervised entities. There had been no enforcement activity following cyber related incidents as part of an enforcement procedure related to cyber risk so far. FINMA as well as other governmental organizations are very clear that victims of cyberattacks should not be penalized. This is a context factor and relates to the legal framework in general, and the penal code and its application.

Assessment and Recommendations

100. There is a need to empower FINMA to levy monetary fines. In technology and cyber risk areas, the expectation is that the supervised entities will behave responsibly and manage their individual institution risk carefully and will not pose a threat to interconnected systems where they participate. However, irresponsible behavior may have serious consequences for the financial sector. In such circumstances, levy of monetary fines would act as a disciplining factor. There are several high-profile IT / cyber-related monetary penalties levied by major regulators.

101. It is important to use the powers available to impose non-monetary penalties judiciously. Non-monetary penalties act as messages from the supervisor not only to the affected institutions but other institutions as well. In deserving cases, FINMA must pursue this route to strengthen cyber security of the sector.

FINANCIAL SECTOR RESILIENCE

A. Information Sharing Arrangements

102. The FS-CSC plays a crucial role in information sharing among financial sector participants. The FS-CSC is a public-private partnership, with membership from banks, insurance companies and other supervised entities. In Switzerland, the private sector tends to cooperate more

with mutual trust. This has facilitated information sharing among the members. The presence of FINMA, SNB, SIF and NCSC help in extending the support of the authorities to this initiative.

103. The FS-CSC is a young organization supported by volunteers nominated by its members and reasonable time needs to be given to assess whether this is successful. The FS-CSC was established only in 2022. They have collaborated with the FS-ISAC to collect information at tactical and operational level. The steering board and various working groups are capable of discussing strategic information shared on an ongoing basis.

B. Cyber Exercises and Testing

104. Operational resilience circular (2023/1) mandates red team testing exercises, in addition to regular vulnerability assessments and penetration testing. While vulnerability assessments and penetration testing requirements are already implemented, red team testing expectations are built in. In selected cases, a few supervised entities (as guided by FINMA) have carried out red team testing with the help of audit firms. FINMA does not have a testing framework published (in the lines of CBEST or TIBER-EU). However, FINMA indicated that it would expect banks to hire professional firms to conduct red team testing going forward. Annual Report 2021 indicated that FINMA has also carried out some cyber exercises. Firstly, the processes for detecting and responding to a cyberattack were tested by means of tabletop exercises, which simulate attack scenarios. Secondly, FINMA commissioned specialists to conduct scenario-based tests under controlled conditions and in consultation with the institutions.

105. The FS-CSC conducts operational exercises as well as strategic exercises regularly. The SNB, FINMA, SIF and NCSC participate annually in strategic tabletop exercises organized by the FS-CSC, which are focusing primarily on measures to mitigate the impact of a systemic cyber-attack on the Swiss financial sector. In addition to the strategic level the FS-CSC also organizes regular operational exercises for the financial sector. A successful first operational cyber exercise for the Swiss financial center with over 100 participants from the member institutions, was carried out on November 27, 2023. FINMA has considered participation of category 3 and 4 banks in such operational and strategic exercises as meeting the requirements under the operational resilience circular.

Assessment and Recommendations

106. Operational Risk and Resilience circular covers only banks and financial groups. There is a need to extend the circular to other parts of the financial sector in a proportional manner there by extending the testing framework to all sections of the financial sector.

107. FINMA may consider developing a testing framework that is appropriate for the Switzerland's market to achieve consistency in the results across institutions. Currently, there is no preferred testing framework that has been indicated by FINMA with the belief that the banks will be able to decide their own scope considering their own digital presence. However, for supervisors it is also important to compare the results and ensure minimum quality. In this regard, developing a testing framework suitable for Switzerland is necessary.

C. Systemic Analysis and Concentration Risk

108. FINMA's supervision is primarily focused on individual entities and not the sector as whole, whereas the SNB is vested with the responsibility to contribute to financial stability. FINMA's risk monitor covers some sectoral views. Recent survey on outsourcing carried out by FINMA also provided a systemic view of dependence on critical service providers. The SNB's recent financial stability report covered recent cyber security-related work of standard setters. The SNB also covers cyber security aspects in its annual report. However, stress tests considering cyber scenarios or cyber resilience stress testing are not carried out.

Assessment and Recommendations

109. Further work is needed in strengthening financial stability analysis relating to cyber. FINMA, using its supervisory reporting and outcome, needs to identify systemic elements of cyber risk (say concentration risk in terms of technology, services, geography, etc., and emerging areas of systemic risk). The SNB and FINMA need to coordinate their activities to carry out cyber resilience stress tests at periodic intervals to assess the systemic gaps as well as institution-specific gaps in the preparedness. The SNB may consider severe but plausible cyber scenarios while conducting stress tests to identify potential financial stability implications.

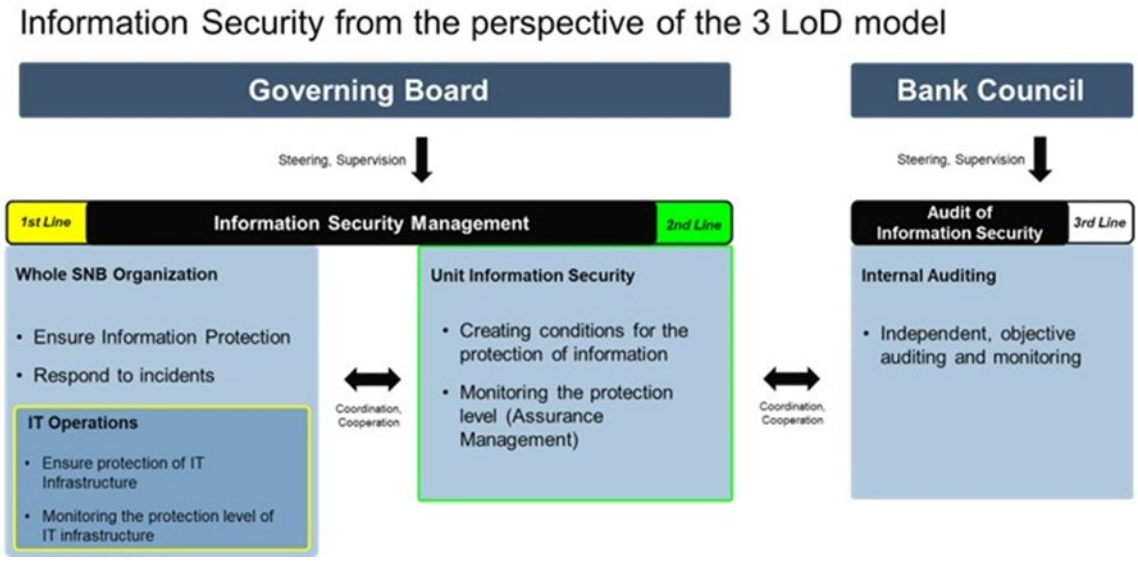
SELECTED CYBER SECURITY CONSIDERATIONS AT SNB AND FINMA

A. Swiss National Bank

110. The SNB considers operational and cyber risks as major risks and has developed a cyber security strategy for its own operations. The SNB's cyber security strategy sets out the overarching cyber security objectives including adopting a holistic approach, focus on current and future initiatives on cyber security, the use of widely accepted standards, aim for full protection at non-targeted attacks, aim at a high degree of protection against targeted attacks, strengthen response and recovery, regularly review the status, focus and progress of the measures. These are broken down into various focused actions.

111. The SNB follows a three lines of defense approach in managing cyber risks (Figure 4). The SNB is strengthening its own cyber security posture and is currently in the process of implementing an identity and access management (IAM) solution, which has progressed substantially, with few more elements to be still integrated. The SNB is yet to implement a full-fledged data leak prevention system, though some elements are already in place. It is careful about cloud adoption, with limited usage of cloud as of now, though the SNB is preparing itself if there is a need to increase its cloud usage.

Figure 4. SNB's Organization Structure Supporting Cyber Risk



Source: SNB

Assessment and Recommendations

112. The SNB is subject to the newly enacted ISA and its various provisions. The SNB is an organization listed in the ISA, and being part of the federal agencies category, it is subject to all the ordinances issued thereunder. Background check to be carried out for individual posted in sensitive areas relating to cyber security by the designated federal agency and such checks to be carried out regarding critical third-party service providers may pose some challenges in implementation. The SNB is also subject to incident reporting requirements under the ISA and needs to report cyber incidents to NCSC. Hence, there is a need to assess the impact of the ISA and take necessary action to comply with its provisions.

B. FINMA

113. FINMA also has a cyber security strategy, which was first approved by the management and the Board of Directors in 2022. The revision of the strategy will be brought to the attention of the Executive Board (via the annual safety report) and the Board of Directors (via management reporting) at the appropriate stage. An external cyber security assessment takes place every two years (for the first time now in 2024) to assess the maturity of cyber security. The results and measures were presented to the Board of Directors in September 2024. It is targeting a maturity level of 3.5 out of 4, though currently they are yet to reach that level, despite progress made. The NIST and ISO standards are leveraged internally.