EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern

Eidgenössische Finanzmarktaufsicht

EFK-20013 | inkl. Stellungnahmen | 24. November 2020 | FinDel D1/2021

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.20013.913.00407
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern

Eidgenössische Finanzmarktaufsicht

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat eine Prüfung bei der Eidgenössischen Finanzmarktaufsicht (FINMA) durchgeführt, mit dem Ziel, die Effizienz und Wirksamkeit der Aufsicht im Bereich der Cybersicherheit bei Finanzdienstleistern zu untersuchen.

Der Bundesrat hat am 8. Dezember 2017 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) für den Zeitraum 2018–2022 verabschiedet. Zwei der 27 definierten Teilsektoren werden von der FINMA beaufsichtigt: die Finanz- und die Versicherungsdienstleistungen.

Das Gesamtdispositiv in der Schweiz kommt nur zögerlich voran

Die 2017 von der FINMA erlassenen verpflichtenden Vorgaben für Banken und Effektenhändler sind angemessen. Jedoch bestehen seit Jahren Lücken im Gesamtdispositiv der Cyberrisiken. Konkrete Massnahmen kommen aufgrund unklarer Verantwortungen und Kompetenzen allerdings nur zögerlich voran. So befindet sich eine funktionierende Krisenorganisation nach wie vor im Aufbau und auch regelmässige sektorübergreifende Übungen zu Cyberangriffen wurden erst einmal durchgeführt.

Aufsicht richtet sich nach den vorhandenen Mitteln

Die Aufsicht über Cyberrisiken, eines von sechs Hauptrisiken für die FINMA, wurde mit den zur Verfügung stehenden Ressourcen stetig weiterentwickelt. Alle geplanten Aktivitäten in dem Bereich konnten noch nicht durchgeführt bzw. umgesetzt werden. Die FINMA hat dies erkannt und organisatorische sowie formelle Anpassungen Anfang 2020 vorgenommen. Es besteht aber weiterhin das Risiko, dass die Aufsicht nicht den geplanten Aktivitäten folgt, sondern sich an den vorhandenen Ressourcen ausrichtet. Effizienzgewinne könnten bei der Erhebung und Auswertung der Prüfergebnisse erzielt werden.

Meldepflicht der Banken zu Cybervorfällen nur ungenügend eingehalten

Die Meldepflicht in Bezug auf Cybervorfälle haben die Banken nur ungenügend befolgt. Eine Nicht-Meldung hatte keine Konsequenzen für die Beaufsichtigten, obwohl entsprechende Instrumente dafür bestünden. Der FINMA fehlt somit eine wesentliche Quelle zu Cyberrisiken auf Institutsebene.

Dieser Umstand wird dadurch akzentuiert, dass die Banken einen direkten Zugriff der FINMA auf MELANI (Analyse- und Meldestelle des Bundes zur Informationssicherheit) ablehnen. Die von der EFK empfohlene Intensivierung der Vor-Ort-Kontrollen könnte diese Lücken teilweise beheben.

Audit de la surveillance de la cybersécurité chez les prestataires de services financiers

Autorité fédérale de surveillance des marchés financiers

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a mené un audit auprès de l'Autorité fédérale de surveillance des marchés financiers (FINMA) pour examiner l'efficience et l'efficacité de la surveillance dans le domaine de la cybersécurité chez les prestataires de services financiers.

Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale pour la protection des infrastructures critiques pour la période 2018–2022. Deux des 27 secteurs définis sont surveillés par la FINMA : les prestations financières et les prestations d'assurance.

Le dispositif global en Suisse ne progresse que modestement

Emises par la FINMA en 2017, les directives contraignantes pour les banques et les négociants en valeurs mobilières sont appropriées. Cependant, des lacunes existent depuis des années dans le dispositif global des cyberrisques. Les mesures concrètes ne progressent que lentement en raison du peu de clarté des responsabilités et des compétences. Ainsi, une organisation de crise opérationnelle est toujours en cours de mise en place et des exercices intersectoriels réguliers sur les cyberattaques n'ont été menés qu'une seule fois.

La surveillance dépend des moyens disponibles

La surveillance des cyberrisques, l'un des six risques principaux pour la FINMA, a été développée de manière constante avec les ressources disponibles. Toutes les activités prévues dans ce domaine n'ont pas encore pu être réalisées ou mises en œuvre. La FINMA l'a reconnu et a procédé à des adaptations organisationnelles et formelles au début de l'année 2020. Toutefois, il existe toujours un risque que la surveillance ne suive pas les activités prévues, mais soit adapté aux ressources disponibles. Des gains en efficacité pourraient être réalisés dans la collecte et l'évaluation des résultats des audits.

Les banques ne respectent qu'insuffisamment l'obligation d'informer sur les cyberincidents

Les banques n'ont pas assez donné suite à l'obligation de signaler les cyberincidents. Le défaut de déclaration n'a pas eu de conséquences pour les institutions contrôlées, bien que les instruments correspondants existent. Il manque donc à la FINMA une source d'information importante sur les cyberrisques au niveau des institutions.

Cette situation est accentuée par le fait que les banques refusent à la FINMA un accès direct à MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information). L'intensification des contrôles sur place recommandée par le CDF pourrait remédier en partie à ces lacunes.

Texte original en allemand

Verifica della vigilanza sulla cibersicurezza dei fornitori di servizi finanziari

Autorità federale di vigilanza sui mercati finanziari

L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha effettuato una verifica presso l'Autorità federale di vigilanza sui mercati finanziari (FINMA) allo scopo di esaminare l'efficienza e l'efficacia della vigilanza in materia di cibersicurezza dei fornitori di servizi finanziari.

L'8 dicembre 2017 il Consiglio federale ha varato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC) per il periodo 2018–2022. Due dei 27 settori parziali definiti sono sottoposti alla vigilanza della FINMA: i servizi finanziari e i servizi assicurativi.

Il dispositivo complessivo in Svizzera procede a rilento

Le direttive obbligatorie per le banche e i commercianti di valori mobiliari emanate dalla FINMA nel 2017 sono adeguate. Tuttavia, esistono da anni lacune nel dispositivo complessivo sui ciber-rischi. Le misure concrete stanno tuttavia procedendo a rilento a causa di responsabilità e competenze poco chiare. Ad esempio, è ancora in fase di costituzione un'organizzazione di crisi funzionante e le esercitazioni intersettoriali contro i ciberattacchi, che dovrebbero svolgersi regolarmente, sono state effettuate soltanto una volta.

La vigilanza dipende dalle risorse disponibili

La vigilanza sui ciber-rischi, uno dei sei rischi principali per la FINMA, è stata sviluppata ulteriormente in modo costante con le risorse disponibili. In questo settore non sono ancora state realizzate o attuate tutte le attività pianificate. Ciò è stato riconosciuto dalla FINMA, che ha provveduto ad apportare adeguamenti organizzativi e formali all'inizio del 2020. Tuttavia, sussiste ancora il rischio che la vigilanza non segua le attività pianificate, ma si orienti alle risorse disponibili. Si potrebbero ottenere guadagni in termini di efficienza nel rilevamento e nella valutazione dei risultati delle verifiche.

Le banche non hanno sufficientemente rispettato l'obbligo di notifica dei ciberincidenti

Le banche non hanno rispettato a sufficienza l'obbligo di notifica di ciberincidenti. La mancata notifica non ha avuto conseguenze per gli istituti sottoposti alla vigilanza, sebbene sarebbero disponibili adeguati strumenti a tal fine. La FINMA non dispone quindi di una fonte significativa per individuare i ciber-rischi a livello di istituti.

Questa circostanza è accentuata dal fatto che le banche rifiutano l'accesso diretto della FINMA a MELANI (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione). L'intensificazione dei controlli in loco raccomandata dal CDF potrebbe in parte colmare queste lacune.

Testo originale in tedesco

Audit of cybersecurity supervision for financial service providers

Swiss Financial Market Supervisory Authority

Key facts

The Swiss Federal Audit Office (SFAO) carried out an audit at the Swiss Financial Market Supervisory Authority (FINMA) with the aim of examining the efficiency and effectiveness of cybersecurity supervision for financial service providers.

On 8 December 2017, the Federal Council adopted the national strategy for critical infrastructure protection (CIP) for the period 2018 to 2022. Two of the 27 defined sub-sectors are supervised by FINMA: financial services and insurance services.

Overall progress of provisions in Switzerland is slow

The mandatory rules for banks and securities dealers issued by FINMA in 2017 are appropriate. However, gaps have existed for years in the overall cyber-risk provisions and concrete measures are making slow progress due to unclear responsibilities and competencies. For example, a functioning crisis organisation is still being established and regular cross-sectoral exercises on cyberattacks have been conducted only once.

Supervision depends on available resources

Supervision of cyber-risks, one of the six main risks for FINMA, has been steadily developed with the resources available. Not all of the planned activities in this area have been carried out or implemented yet. FINMA acknowledged this and made organisational and formal adjustments at the beginning of 2020. Nevertheless, there is still a risk that supervision will not be based the planned activities, but will instead depend on the available resources. Efficiency gains could be achieved in the recording and evaluation of audit results.

Banks' duty to report cyberincidents insufficiently respected

Banks have failed to comply adequately with their duty to report cyberincidents. Failure to report has had no consequences for those supervised, even though appropriate mechanisms were in place. FINMA thus lacks a significant source of information on cyber-risks at institution level.

This situation is accentuated by the fact that the banks refuse to allow FINMA direct access to MELANI (Reporting and Analysis Centre for Information Assurance). Intensifying onsite inspections, as recommended by the SFAO, could partially remedy these shortfalls.

Original text in German

Generelle Stellungnahme der Eidgenössischen Finanzmarktaufsicht

Die FINMA bedankt sich bei der EFK für die durchgeführte Prüfung und die konstruktive Zusammenarbeit. Die Empfehlungen geben wertvolle Impulse, die Aufsicht in diesem Bereich weiter zu entwickeln. Cyber-Risiken und Cyber-Sicherheit bei Beaufsichtigten werden seit der Gründung der FINMA mit hoher Priorität überwacht. Dies insbesondere seit mehreren Jahren auch als Top-Risiko im Rahmen des internen Prozesses zur Identifikation und Beurteilung der Risikolage des Finanzplatzes Schweiz. Der erstmals im November 2019 veröffentlichte Risikomonitor der FINMA unterstreicht dies und betrachtet denn "Cyber" als ein Hauptrisiko für Finanzinstitute. Die Bedeutung und besondere Gefährdungslage für den Finanzsektor ist in der Schweiz und weltweit unbestritten. Die FINMA verfolgt bei ihrer Aufsichtstätigkeit entsprechend den rechtlichen Grundlagen generell einen risikoorientierten und proportionalen Ansatz. Das bedeutet einen erhöhten Fokus auf grössere Institute oder bekannte Schwachpunkte. Darauf abgestimmt sind dann die Ressourcenallokation und die Wahl der Aufsichtsmittel. Trotz der anerkannten Verletzlichkeit von kleineren Instituten gegenüber Cyberangriffen, können die Ressourcen der FINMA auch in diesem Bereich nur mit dieser grundsätzlichen Risikoorientierung effizient alloziert werden. Aufgrund der von der FINMA als hoch eingestuften Cyber-Risiken hat die FINMA zu deren Überwachung im 2017 eine dedizierte Querschnittsfunktion geschaffen, die für Cyber-Themen die Fachführung innehat und von einer entsprechenden integrierten Gesamtsicht über die FINMA hinweg profitiert und die Linienaufsicht entsprechend unterstützen kann. Die Ressourcen wurden kontinuierlich aufgebaut. Ein weiterer sukzessiver Aufbau von Ressourcen zur Förderung und Überwachung der Cyber-Sicherheit der Beaufsichtigten wird, wenn nötig, für die Erreichung der Aufsichtsziele erfolgen. Bis jetzt konnten alle geplanten Aktivitäten ausser im Hinblick auf systemweite Übungen termingerecht durchgeführt werden. Die FINMA hat seit langem einen Schwachpunkt der Schweiz in der systemweiten Analyse-, Kooperations- und Koordinationsarbeit zwischen öffentlichem und privatem Sektor identifiziert. Die FINMA fordert beispielsweise schon seit 2016 einen Ausbau dieser systemweiten Arbeit, inklusive übergreifende Szenarioanalysen. Unter der Leitung vom Delegierten des Bundes für Cybersicherheit hat sich die Ausgangslage durch die Etablierung von Koordinationsgremien und eines FS-ISAC (Financial Services Information Sharing and Analysis Center) seit Mitte 2019 verbessert. Eine zentrale Rolle des FS-ISAC wird es dabei sein, insbesondere die Koordination zwischen Behörden und Finanzindustrie und die Durchführung von gezielten Massnahmen wie bspw. Szenarioanalysen bzw. strategische Übungen sicherzustellen. Dadurch soll die Cyber-Resilienz des Finanzplatzes Schweiz weiter gestärkt werden. Ein wichtiges Instrument zur Erkennung von Cyber-Vorfällen ist die Meldepflicht der Beaufsichtigten gegenüber der FINMA. Um die Beaufsichtigten an diese Meldepflicht zu erinnern und zur Konkretisierung, was der FINMA bezüglich Cyber-Attacken gemeldet werden muss, wurde im Mai 2020 eine Aufsichtsmitteilung erlassen. Die Anzahl der Meldungen ist seither merklich gestiegen. Die Entwicklung wird von der FINMA engmaschig verfolgt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Eidgenössische Finanzkontrolle (EFK) hat die Prüfung der Aufsicht der Eidgenössischen Finanzmarktaufsicht (FINMA) über die Cybersicherheit bei Finanzdienstleistern in ihr Jahresprogramm 2020 aufgenommen.

Für diese Prüfung wird die Definition der FINMA für Cyberrisiken (FINMA-RS 08/21 «Operationelle Risiken – Banken») herangezogen, d. h. «Operationelle Risiken in Bezug auf mögliche Verluste durch Cyberattacken». Dies sind Risiken im Bereich der Cybersicherheit, die auf einer kriminellen Aktivität beruhen.

Das Thema Cybersicherheit dominiert in der Finanzindustrie

Das jährlich von Ernst & Young (EY) erhobene Bankenbarometer 2020[1] zeigt, aufgrund einer Umfrage bei 100 Banken in der Schweiz, welche Themen und Aktivitäten aus Sicht der Befragten in den nächsten 6 bis 12 Monaten in der Finanzindustrie eine grosse Bedeutung haben. Cybersicherheit war, ist und bleibt gemäss dieser Umfrage das dominierende Thema bei den Banken. Die Umfrage wird seit 2010 durchgeführt und das Thema Cybersicherheit wurde erstmals 2014 (Rang 3) erhoben. 2015 und 2016 war das Thema auf Rang 2 geführt. Ab 2017 bis heute auf Rang 1.

Das Thema Cyberrisiken und -sicherheit wird von der FINMA seit 2010 als prioritäres und strategisch relevantes Thema geführt. Die grundsätzliche Bedeutung und besondere Gefährdungslage für den Finanzsektor Schweiz und weltweit sind für alle Akteure unbestritten.

FINMA: Organisation und Aufgaben

Die FINMA hat als unabhängige Behörde über den schweizerischen, regulierten privatwirtschaftlichen Finanzmarkt hoheitliche Befugnisse über Banken, Versicherungen, Börsen, Finanzinstitute, kollektive Kapitalanlagen, deren Vermögensverwalter und Fondsleitungen sowie Versicherungsvermittler.

Die FINMA hat den gesetzlichen Auftrag, Finanzmarktkunden – namentlich Gläubiger, Anleger und Versicherte – sowie die Funktionsfähigkeit der Finanzmärkte zu schützen. Davon abgeleitet sind die Aufsichtsaufgaben der FINMA: die Bewilligung, die Überwachung und, wo notwendig, die Durchsetzung des Aufsichtsrechts. Daneben kann die FINMA auf untergeordneter Stufe auch regulieren. Sie bewilligt und beaufsichtigt Finanzinstitute, Finanzprodukte und die Finanzmarktinfrastruktur. Die Aufsicht über die Finanzmarktinfrastruktur teilt sich die FINMA mit der Schweizerischen Nationalbank (SNB). Die FINMA nimmt ihre Aufsichtstätigkeit in einem ganzheitlichen Ansatz mit den Instrumenten Bewilligung, Überwachung, Enforcement und Regulierung wahr. Der Aufsichtsprozess wird durch unterschiedliche Funktionen wahrgenommen sowie durch Prüfgesellschaften als verlängerter Arm der FINMA unterstützt.

[1] https://www.ey.com/Publication/vwLUAssets/ey-bankenbarometer-2020/%24FILE/ey-bankenbarometer-2020.pdf

Die FINMA ist heute wie folgt organisiert:

Abb. 1: Quelle FINMA; Darstellung EFK

Die Organisation der FINMA strukturiert sich in acht Geschäftsbereiche (GB), wovon die folgenden vier für die Überwachung zuständig sind:

- Banken
- Versicherungen
- Märkte
- Asset Management.

Die Gruppe B-OCI (Operationelle, Cyber- und IT-Risiken) ist als Querschnittsfunktion (QF) bei der FINMA für die operationellen Risiken innerhalb des Geschäftsbereichs Banken (GB-B) als auch FINMA-weit für IT-, Cyber-Rrisiken und Outsourcing zuständig. Siehe dazu auch Kapitel 2.1 (Organisation).

Verbindliche Vorgaben für Banken und Effektenhändler zu Cyberrisiken führt die FINMA erstmals 2017 im Rundschreiben «FINMA-RS 08/21 «Operationelle Risiken – Banken» auf. Das Rundschreiben wird zudem von Versicherungen sowie banknahen oder sehr grossen Verwaltern von Kollektivvermögen als Orientierungsrahmen bei Prüfungen beigezogen.

Anforderungen bzgl. Cybersicherheit gegenüber einer zentralen Finanzmarktinfrastruktur wurden separat aufgrund des Finanzmarktinfrastrukturgesetzes verfügt.

Cyberrisiken sind für die FINMA eines von sechs Hauptrisiken

Gemäss dem im Dezember 2019 von der FINMA publizierten Risikomonitor[2] sind Cyberrisiken mittelfristig eines von sechs Hauptrisiken für die Beaufsichtigten und den Schweizer Finanzplatz. Die sechs Hauptrisiken sind:

- Niedrigzinsumfeld
- Immobilien- und Hypothekarmarktkorrektur
- Cyberrisiken
- Wegfall des LIBOR
- Geldwäscherei
- Marktzugang.

Exkurs – Was genau bedeutet Cyber[3]?

Cyber: Wortbildungselement mit der Bedeutung «die von Computern erzeugte virtuelle Scheinwelt betreffend», insbesondere «Cyberspace». Im weiteren Sinne wird mit «Cyber» die (virtuelle) Welt referenziert, die mithilfe von vernetzten Computern gebildet wird. Insofern kann gefolgert werden, dass «Cyber» als Begriff für «vernetzte Computer», demzufolge «internet-vernetzte Computer» verwendet wird.

Cybersicherheit verfolgt entsprechend das Ziel, den Cyberspace bzw. die Teilnehmenden am Cyberspace vor Cyberattacken zu schützen. Sicherheit ist dabei definiert als «unerwünschte Effekte zu kontrollieren», in idealtypischer Ausprägung eine risikofreie Situation zu schaffen bzw. eine Situation, in der (sämtliche) Risiken kontrolliert sind.

Cyberattacken: von aussen (durch einen einzelnen Angreifer (Hacker), durch eine Institution o. ä.) zum Zweck der Sabotage oder der Informationsgewinnung geführter Angriff auf ein Computernetzwerk. Diese Definition impliziert, dass Cyberangriffe «von aussen» induziert sind und damit im Kontext der vorsätzlichen oder kriminellen Handlungen anzusiedeln sind. Damit werden Sorglosigkeit, Fahrlässigkeit im internen Organisationskontext tendenziell ausgeschlossen. Dennoch muss weiterhin berücksichtigt werden, dass ein Cyberangriff sehr wohl auch «von innen» (vorsätzlich oder mit krimineller Absicht) erfolgen kann, z. B. durch Infektion oder Kompromittierung von Systemen über technische oder personelle Angriffsvektoren. Im der englischen Sprache wird insbesondere zwischen «Safety» (Schutz gegen Versagen, Bruch oder Unfall) und «Security» (Zustand der Sicherheit, frei von Gefahr oder Bedrohung zu sein) unterschieden, wobei diese Wörter auf Deutsch einfach durch «Sicherheit» übersetzt werden.

[2] https://www.finma.ch/de/dokumentation/finma-publikationen/berichte/risikomonitor/
[3] Quellen: www.merriam-webster.com; www.lexico.com; www.duden.de

1.2 Prüfungsziel und -fragen

Der Fokus der Prüfung liegt in der Beurteilung der Effizienz und Wirksamkeit der Aufsicht der FINMA über die Cybersicherheit bei Finanzdienstleistern aufgrund von aufsichtsrechtlichen Anforderungen der Cyberrisiken gemäss Rundschreiben «FINMA-RS 08/21 «Operationelle Risiken – Banken».

Die folgenden Fragen werden behandelt:

- Ist die Aufsicht über die Finanzdienstleister im Bereich Cyberrisiken effizient und wirksam?
- Ist die Aufsicht über das Zahlungsverkehrssystem SIC effizient und wirksam?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roger Lanicca (Revisionsleiter) und André Vuilleumier sowie von InfoGuard (externer Dienstleister) von Januar bis April 2020 durchgeführt. Sie erfolgte unter der Federführung von Andreas Baumann. Die Ergebnisbesprechung hat am 15. April 2020 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

Das systemisch bedeutsame Zahlungsverkehrssystem Swiss Interbanking Clearing (SIC), welches von der Schweizerischen Nationalbank (SNB) betrieben wird, gehört zu der kritischen Infrastruktur, wurde aber nicht geprüft. Die SNB untersteht nicht dem Aufsichtsbereich der EFK. Das SIC ist weder bewilligungspflichtig noch steht es unter der Aufsicht der FINMA. Verschiedene Gesprächspartner beurteilen das SIC als eines der primären potenziellen Ziele in Bezug auf Cyberangriffe im Finanzsystem.

Weitere Komponente, die ebenfalls eine systemische oder kritische Rolle im erweiterten Rahmen der Cybersicherheit bei Finanzdienstleistern spielen, bspw. Telekommunikation, Strom, Outsourcing Partner, Softwareanbieter etc. sind nicht Bestandteil des Prüfumfangs.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von der FINMA erteilt. Die gewünschten Unterlagen (sowie die benötigte Infrastruktur) standen dem Prüfteam zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 19. August 2020 statt. Teilgenommen haben seitens der FINMA der Direktor, die Leiterin Geschäftsbereich Strategische Grundlagen, der Leiter Geschäftsbereich Banken, die Leiterin Interne Revision und der Leiter Querschnittsfunktion B-OCI. Seitens der SNB hat der Leiter Überwachung teilgenommen. Von der EFK vertreten waren der Direktor, der Mandatsleiter, der Federführende und der Revisionsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Geschäftsleitung bzw. dem Verwaltungsrat obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Effizienz und Wirksamkeit der Aufsicht

2.1 Organisation der FINMA

Verantwortlich für die Umsetzung der Aufsichtstätigkeit bei den Banken sind die rund 30 Aufseher bzw. Key Account Manager (KAM). Bei grösseren Instituten sind teils eigenständige Teams für die Aufsicht eines Instituts zuständig. Bei kleineren sind die KAM für mehrere Institute gleichzeitig verantwortlich. Die Überwachungstätigkeit erfolgt auf Basis der Aufsichtskategorien, die die Aufsichtsintensität bestimmen. Dabei berücksichtigt die Überwachungstätigkeit u. a. auch die aufsichtsrechtlichen Prüfungen der externen Prüfgesellschaften, die als verlängerter Arm der FINMA agieren.

Die dedizierte Querschnittsfunktion «Operationelle, Cyber- und IT-Risiken» (B-OCI) innerhalb des Geschäftsbereichs Banken (GB-B) wurde 2017 gegründet. B-OCI fungiert als Kompetenzzentrum für die operationellen Risiken im Geschäftsbereich Banken sowie FINMA-weit für die Themen IT, Cybersicherheit und Outsourcing. Dies beinhaltet u. a. die Durchführung und Unterstützung von eigenen Vor-Ort-Kontrollen in verschiedenen Geschäftsbereichen, eine Auskunftsstelle von ad-hoc-Fragen oder aber auch für eine geschäftsbereichsübergreifende Sensibilisierung des Themas (Schulungen) Cyberrisiken innerhalb der FINMA. Die Querschnittsfunktion B-OCI steht zur Unterstützung der KAM zur Verfügung, wenn es um die fachlich und technisch anspruchsvolle Beurteilung der Cyberrisiken geht.

In den Jahren 2018 und 2019 konnten im Bereich Cyberrisiken wegen der Ressourcenknappheit nicht alle geplanten Aktivitäten durchgeführt werden. So wurden verschiedene konzeptionelle oder analysierende Aufsichtstätigkeiten verschoben oder sind ganz entfallen.

Die Mitarbeitenden von B-OCI sind auch in Projekten (FINMA-Vertretung bei bundesweiten Projekten), Ausschüssen und Weiterbildungen (Referententätigkeiten) engagiert. Ausserdem ist das Thema Cybersicherheit zurzeit auf Bundesebene in der Umsetzungsphase (Krisenorganisation, sektorübergreifende Übungen und Szenarien etc.) mit Beteiligung von B-OCI-Mitarbeitenden.

Zudem kommen im Finanzbereich laufend neue Technologien und Geschäftsmodelle dazu, welche, besonders im IT-Bereich, ein vertieftes fachliches Verständnis und Miteinbezug von B-OCI erfordern.

Im Bereich Cyberrisiken befindet sich die FINMA aktuell in einer Übergangsphase und hat aufgrund der Bedeutung und Aktualität des Themas ab 2020 organisatorische und formelle Anpassungen vorgenommen. So wurde die Gruppe Cybersicherheit innerhalb der Querschnittsfunktion B-OCI von einer auf zwei Vollzeitstellen erhöht und es wurden spezifische Fachkonzepte zur Aufsicht im Bereich Cybersicherheit erstellt.

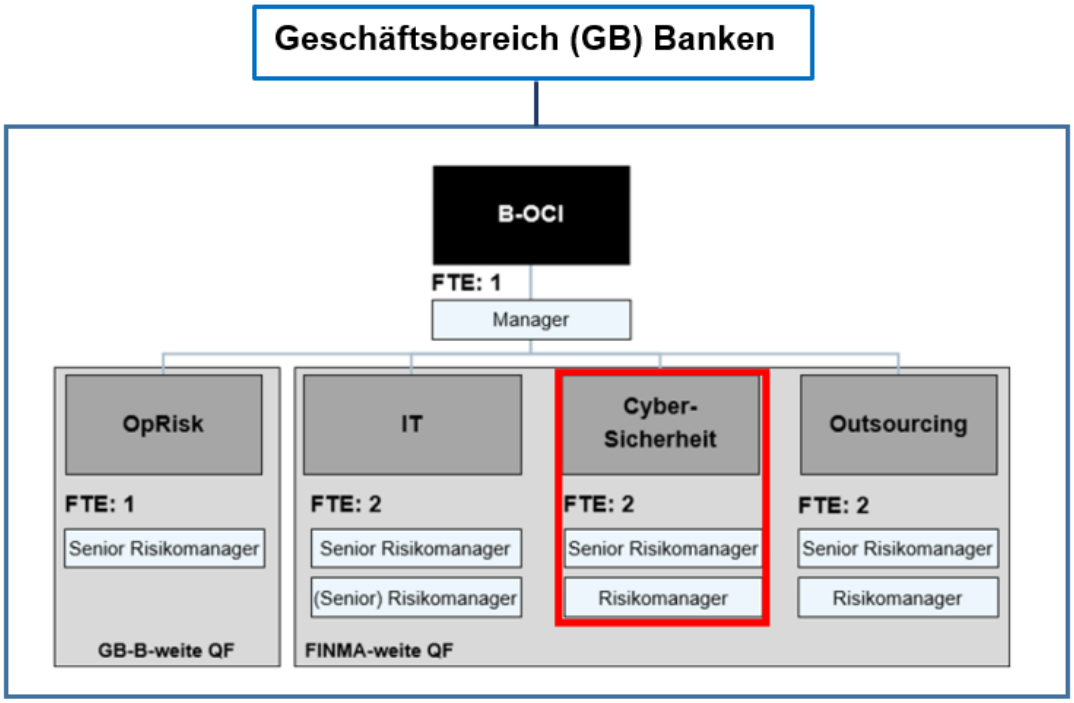

Abb. 2: Soll-Funktionsstruktur B-OCI ab 2020; Quelle FINMA

Übergreifendes und themenspezifisches Fachkonzept Cybersicherheit

Um bei der fachlich und technisch anspruchsvollen Aufsicht im Bereich Cybersicherheit auch andere bzw. weitere Geschäftsbereiche der FINMA zu unterstützen, stellte sich bei einer internen Umfrage heraus, dass auch von anderen Geschäftsbereichen Bedarf nach Unterstützung für diesen Bereich besteht.

Im Hinblick auf diese Mandatserweiterung wurde Ende 2019 von B-OCI ein übergreifendes Fachkonzept[4] sowie themenspezifische Fachkonzepte[5] u. a. für Cybersicherheit erstellt.

Die Ziele der jeweiligen Strategieperiode werden in die Jahresziele pro Geschäftsjahr heruntergebrochen. Die Allokation von Ressourcen erfolgt basierend auf den gesetzlichen Schutzzielen und relativ zur Bedeutung anderer Risiken. Cyberrisiken und die Etablierung von B-OCI bilden einen Schwerpunkt im Jahr 2020.

Im Rahmen des Fachkonzeptes ist auch ein Benchmark zur Aufsichtspraxis gemäss Rundschreiben «FINMA-RS 08/21 «Operationelle Risiken – Banken» zu Cybersicherheit, mit dem Ziel einer Maturitätsanalyse gemäss National Institute for Standards and Technology (NIST) Cybersecurity Framework, vorgesehen und im Entwurf vorhanden.

Die praktische Etablierung des Fachkonzepts erfolgte bereits vor der formellen Implementierung, es wurden jedoch noch nicht alle geplanten Aktivitäten aus dem Fachkonzept Cyberrisiken vollumfänglich umgesetzt.

[4] Das Fachkonzept gewährt einen Überblick über grundsätzliche Aspekte der Tätigkeit von B-OCI wie Ziele, Anspruchsgruppen, Organisation und Ressourcen, Leistungsauftrag sowie Fach- und Aufsichtsinstrumente.

[5] Themenspezifische Fachkonzepte: Diese konkretisieren die Anwendung der Fach- und Aufsichtsinstrumente für die Fachthemen Operationelles Risiko, IT, Cybersicherheit und Outsourcing. Weiter werden die themenspezifischen Fachkonzepte um sog. Benchmarks ergänzt. Die Benchmarks stellen die Grundlage für ein konsistentes Vorgehen im jeweiligen Thema dar und bilden die Basis für eine Maturitätsanalyse. Quelle: FINMA.

Beurteilung

Die FINMA und der Bereich Cyberrisiken stehen aufgrund der Wichtigkeit und Aktualität des Themas organisatorisch vor Herausforderungen. Cyberrisiken war, ist und wird ein bestimmendes Thema bzw. Risiko bei den Beaufsichtigten bleiben.

Die um die Cyberrisiken im Fachkonzept definierten Aktivitäten sind sinnvoll und tragen zum Schutz bei. Wenn einzelne, wie festgestellt, nicht durchgeführt werden können, bspw. wegen limitierten Ressourcen, hat dies einen Einfluss auf die Qualität und Wirksamkeit der Cyberaufsicht. Obschon per 2020 organisatorische und formelle Anpassungen vorgenommen wurden, erscheinen die Ressourcen und Aktivitäten im Bereich Cyberrisiken nicht ausgewogen, um diese wie geplant durchzuführen bzw. zu unterstützen.

Es gilt zu berücksichtigen, dass in den nächsten Jahren aufgrund des Fachkonzepts, das als angemessen beurteilt wird, nebst bestehenden noch zusätzliche Aktivitäten und Unterstützungen geplant sind und das für weitere und mehrere Geschäftsbereiche gleichzeitig. Dies wird zu einer erhöhten Nachfrage nach Unterstützung von B-OCI führen.

2.2 Vorgaben bzw. aufsichtsrechtliche Anforderungen

Konkrete aufsichts-rechtliche Anforderungen zu Cyberrisiken führt die FINMA erstmals 2017 im Rundschreiben «FINMA-RS 08/21 «Operationelle Risiken – Banken» auf. Der Risikomanagementgrundsatz zur Technologieinfrastruktur erfasst ab dieser Zeit explizit auch IT- und Cyberrisiken. Diese Anforderungen basieren auf dem international anerkannten NIST-Rahmenwerk.

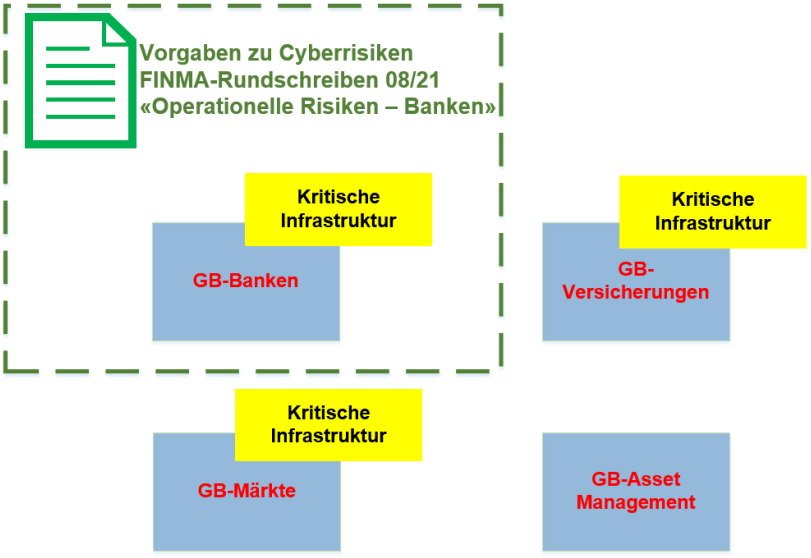

Abb. 3: Gültigkeitsrahmen der Vorgaben zu Cyberrisiken aufgrund des Rundschreibens

Das Rundschreiben ist direkt für alle Banken und Effektenhändler verpflichtend und wurde gegenüber einer zentralen Finanzmarktinfrastruktur verfügt. Für Versicherungen, Fondsleitungen und Verwalter von Kollektivvermögen ist es nicht verpflichtend.

Gemäss FINMA befolgen grössere Fondsleitungen bzw. Verwalter von Kollektivvermögen oder solche innerhalb einer Bankengruppe das RS 08/21 in vielen Fällen auch freiwillig.

Beurteilung

Die aufsichtsrechtlichen Anforderungen werden als angemessen beurteilt.

Im Sinne des Aufsichtszwecks der FINMA sowie in Anbetracht, dass mit der zunehmenden technischen Vernetzung der Finanzmarktteilnehmer die Risiken bezüglich Cyberattacken steigen, ist eine Ausweitung der Adressaten notwendig.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der FINMA, die aufsichtsrechtlichen Anforderungen betreffend Cyberrisiken neben Banken und Effektenhändler auf weitere Beaufsichtigte wie bspw. Versicherungen auszudehnen.

Stellungnahme der FINMA

Die FINMA findet die Empfehlung sinnvoll und wird dieser nachkommen. Die dafür nötigen Schritte (passendes Regulierungsgefäss sowie Regulierungsvorlage) werden analysiert und bis Mitte 2021 festgelegt.

2.3 Risikoanalyse

Risikoanalyse – FINMA

Der erstmals im November 2019 von der FINMA publizierte Risikomonitor nennt Cyberrisiken als eines von sechs Hauptrisiken für die Beaufsichtigten und den Schweizer Finanzplatz über eine mittlere Frist.

Der Risikomonitor ist eine Synthese eines internen Prozesses der aus dem Risikobarometer und den daraus abgeleiteten Massnahmen besteht.

Der Risikobarometer wird zweimal jährlich erstellt. Eine Kategorisierung und Gewichtung findet aufgrund einer qualitativen Beurteilung statt und ergibt eine Gesamtbeurteilung. Gemäss FINMA sind zurzeit 28 Risiken definiert, wovon sechs als Hauptrisiken aufgeführt sind.

In Verbindung mit dem Risikobarometer listen die Massnahmen die abgeschlossenen, laufenden und geplanten Aktivitäten auf.

Der Risikobarometer wird halbjährlich und die Massnahmen werden jährlich der Geschäftsleitung präsentiert. Cyberrisiken wurden im Risikomonitor erstmals 2014 aufgeführt und seit 2015 als Hauptrisiko beurteilt.

Ein formeller Prozessbeschrieb ist zum Prüfungszeitpunkt nicht vorhanden, gemäss FINMA aber zurzeit in Ausarbeitung.

Beurteilung

Die Risikoanalyse bzw. der Prozess dazu werden als angemessen beurteilt. Das Thema Cyberrisiken ist zu Recht als eines der Hauptrisiken identifiziert worden.

Risikoanalyse – Beaufsichtigte

Das Bewusstsein für das Thema hat sich bei der FINMA und bei den Beaufsichtigten positiv entwickelt. Eine vollumfängliche Umsetzung eines schweizweit wirksamen Dispositivs gegen systemweite Cyberattacken ist noch offen.

Die risikoorientierte Aufsicht der FINMA für die Beaufsichtigten umfasst fünf Aufsichtskategorien und ein internes Institutsrating (auf der Basis aller der FINMA zur Verfügung stehenden Informationen). Die Risiken eines beaufsichtigten Unternehmens werden anhand des individuellen Ratings und der Kategorisierung bestimmt. Für die Aufsichtstätigkeit ist die Informationsgewinnung von entscheidender Bedeutung.

Die Aufsichtskategorisierung erfolgt über verschiedene Kriterien (z. B. Bilanzsumme). 2018 gibt es 269 bewilligte Banken. Die folgende Tabelle gibt eine Übersicht über die unter der Aufsicht stehenden Banken:

Kategorie	Eigenschaften	Risiko	Anzahl
1	Äusserst grosse, bedeutende und komplexe Marktteilnehmer	Sehr hoch	2
2	Sehr bedeutende, komplexe Marktteilnehmer	Hoch	3
3	Grosse und komplexe Marktteilnehmer	Bedeutend	26
4	Marktteilnehmer mittlerer Grösse	Durchschnittlich	60
5	Kleine Marktteilnehmer	Tief	178

Tabelle 1: Quelle FINMA; Darstellung EFK

Die Risikoanalyse und Prüfstrategie zur Cybersicherheit werden entlang der Prüfpunkte im Prüffeld Informatik definiert. Dabei erarbeitet die Prüfgesellschaft auf Basis einer Risikoanalyse einen Vorschlag (Prüfstrategie) zuhanden der für die jeweilige Bank zuständigen Aufsichtsperson, dem KAM. Gemäss FINMA übernimmt die Querschnittsfunktion B-OCI im Hinblick auf die Risikoanalyse und Prüfstrategie die Fachführung für Institute der Aufsichtskategorien 1, 2 und teilweise 3für den Teil Cyberrisiken. Bei den Instituten der Aufsichtskategorien 4 und 5 erfolgt grundsätzlich keine explizite Unterstützung bei der Risikoanalyse und Prüfstrategie durch B-OCI. Im Fall von Empfehlungen bzw. Beanstandungen mit hoher Kritikalität (Schweregrad) zum Thema Cybersicherheit kann B-OCI die Risikoanalyse und Prüfstrategie auch bei Instituten der Aufsichtskategorie 3 unterstützen. Die Unterstützung der jeweiligen KAM durch B-OCI erfolgt u. a. deswegen, weil das Thema Cyberrisiken sehr technisch und dynamisch ist.

Für die Aufsichtskategorien 4 und 5 wird B-OCI nur nachträglich bei wesentlichen Vorfällen im Bereich Cyberrisiken beigezogen. Spezifische Cyberrisiken für mittlere und kleinere Banken wurden u. a. auch explizit anlässlich von Geschäftsleitungssitzungen benannt.

Zudem wird im Rahmen des am 1. Januar 2020 eingeführten Kleinbankenregimes für bestimmte Banken der Kategorie 4 und 5, die besonderen Anforderungen (z. B. hohe Liquidität oder Kapitalisierung) erfüllen, die Kontrollintensität reduziert, d. h. es findet keine jährliche aufsichtsrechtliche Prüfung mehr statt. Die aufsichtsrechtlichen Vorgaben bleiben jedoch bestehen. Gemäss FINMA wurden 64 Institute zum Kleinbankenregime zugelassen.

Beurteilung

Aufsichtstätigkeiten bei Banken der Kategorie 3, 4 und 5 werden nicht aktiv von Fachspezialisten von B-OCI begleitet. Dies sind 98 % der beaufsichtigten Banken. Aus Sicht der EFK bestehen auch für diese Kategorien Abhängigkeiten und Einflussnahme auf den Finanzplatz Schweiz, speziell bei einem gleichzeitigen Cyberangriff auf mehrere mittlere und/oder kleinere Banken. Cyberrisiken können sowohl die Stabilität von Einzelinstituten als auch jene

des Finanzplatzes Schweiz gefährden. Durch die technische Vernetzung und den Datenaustausch zwischen den Instituten ergibt sich eine breitere Angriffsfläche, die durch Cyberattacken ausgenutzt werden kann, indem anfälligere Teilnehmer angegriffen werden.

Die Kategorisierung der Banken bzw. die Risikobeurteilung nach quantitativen Kriterien sind im Bereich der Cyberattacken nur bedingt sinnvoll, da bereits das Ausnutzen einer einzelnen Schwachstelle für einen erfolgreichen Angriff ausreichen kann.

Die aufsichtsrechtliche Praxis sollte auf alle Aufsichtskategorien ausgeweitet, intensiviert und weiterentwickelt werden, um dem Stellenwert der Cyberrisiken zu entsprechen und der dynamischen Natur gerecht zu werden. Damit können die Aufsichtsziele noch effektiver und effizienter verfolgt werden.

2.4 Meldepflicht Beaufsichtigte

Im Rahmen der Einführung von spezifischen Cybervorgaben gemäss Rundschreiben wurde von der FINMA darauf verzichtet eine Meldepflicht für Cybervorfälle aufzunehmen. Diese unterliegen der allgemeinen Meldepflicht gemäss Finanzmarktaufsichtsgesetz (FINMAG) Art. 29. Darin sind die Beaufsichtigten verpflichtet, der FINMA unverzüglich Vorkommnisse zu melden, die für die Aufsicht von wesentlicher Bedeutung sind.

Gemäss FINMA und Branchenvertretern wurden bis anhin nicht alle relevanten Fälle mit Bezug zu Cybervorfällen gemeldet. Die Gründe können unterschiedlich sein, entweder sind die Vorgaben zu unpräzise, was genau gemeldet werden muss, oder die Banken haben kein Interesse, der FINMA ihre Schwachstellen mitzuteilen.

Bei der Risikoanalyse sind Meldungen zu Cybervorfällen ein wichtiges Hilfsmittel, um die Bedrohungslage ganzheitlich (Lageradar) aber auch auf Institutsebene vorzunehmen. Dies hat u. a. einen Einfluss auf das Risikorating.

Die EFK hat im Rahmen der Prüfung eine Statistik zu den Meldungen ab Einführung der Vorgaben mit Bezug zu Cybervorfällen eingefordert, jedoch waren diesbezüglich keine Informationen verfügbar. Ebenso nicht verfügbar waren Statistiken zu aufsichtsrechtlichen Zwangsmitteln aufgrund von Verletzungen der Meldepflicht in Bezug auf Cybervorfälle.

Eine Aufsichtsmitteilung wurde im Verlauf der Prüfung auf der FINMA-Webseite publiziert[6]. Darin wird u. a. detailliert erläutert, was und wie genau gemeldet werden muss. Sie beinhaltet keinen Hinweis auf Sanktionen im Falle eines Verstosses gegen die Meldepflicht.

Beurteilung

Ohne entsprechende und ausreichende Meldungen zu Sicherheitsvorfällen fällt es schwer, Fakten und Zahlen zur Risikolage (sowohl für einzelne Banken als auch für den Finanzplatz) zu erheben, was wiederum hinderlich ist, um daraus entsprechende Massnahmen abzuleiten. Ein ganzheitlicher Lageradar würde z. B. bei der Melde- und Analysestelle Informationssicherheit (Melani) vorliegen, die FINMA hat jedoch wegen der kategorisch ablehnenden Haltung ihrer Beaufsichtigten keinen Zugriff darauf.

Eine aufsichtsrechtliche Mitteilung als Erinnerungsschreiben zur Meldepflicht von Cybervorfällen wird aus Sicht der EFK positiv beurteilt, sie sollte aber auch die Folgen bzw. verwaltungsrechtlichen Zwangsmittel bei einer Verletzung der Meldepflicht aufführen. Die

[6] https://www.finma.ch/de/dokumentation/finma-aufsichtsmitteilungen/ (7 mai 2020)

Meldungen und deren Qualität haben einen direkten Einfluss auf das Risikorating auf Institutsebene und den ganzheitlichen Lageradar.

Empfehlung 2 (Priorität 2)

Die EFK empfiehlt der FINMA, die Vorgaben zur Meldepflicht stärker zu untermauern. Notfalls auch unter Anwendung der aufsichtsrechtlichen Zwangsmittel die ihr gemäss Finanzmarktaufsichtsgesetz zur Verfügung stehen.

Stellungnahme der FINMA

Bis anhin wurden nur vereinzelt Cyber-Vorfälle direkt von Beaufsichtigten an die FINMA gemeldet. Aufgrund dessen hat die FINMA Massnahmen ergriffen. Insbesondere hat die FINMA im Mai 2020 eine Aufsichtsmitteilung zur Meldung von Cyber-Vorfällen basierend auf der allgemeinen Auskunfts- und Meldepflicht gemäss Art. 29 FINMAG veröffentlicht. Dabei präzisiert diese Aufsichtsmitteilung die Erwartungshaltung der FINMA zur Meldung von Cyber-Vorfällen. Diese Meldung von Cyber-Vorfällen auf Institutsebene komplementiert eine halbjährliche gesamtheitliche Risikolage durch MELANI zu Handen der FINMA. Die FINMA beobachtet die Anzahl eingehender Meldungen von Cyber-Vorfällen auf Basis der neuen Aufsichtsmitteilung genau. Die Anzahl Meldungen von Cyber-Vorfällen haben sich seit Einführung der Aufsichtsmitteilung merklich erhöht. Die Folgen bzw. die verwaltungsrechtlichen Zwangsmittel bei einer Verletzung der Meldepflicht gemäss Art. 29 FINMAG sind den Beaufsichtigten allgemein bekannt. Aufgrund dessen kommen wir vorläufig zum Schluss, dass die FINMA aktuell genügend Massnahmen ergriffen hat, um die Meldedisziplin der Beaufsichtigten zu erhöhen. Eine Eskalation im Sinne der Empfehlung wäre im Einzelfall, oder falls die Meldungen generell wieder rückfällig würden, zu prüfen. Daher wird auf Basis der Entwicklung der Meldungen bis Ende 2021 beurteilt, inwiefern weitere Massnahmen hinsichtlich Einhaltung der Meldedisziplin notwendig sind. Die Empfehlung wird somit weiterverfolgt, wenn die Aufsichtsmitteilung zur Meldung von Cyber-Vorfällen vom Mai 2020 nicht die erwartete Wirkung zeigt. Wenn die Wirkung zufriedenstellend erscheint, wird die Empfehlung mit den im Mai 2020 getroffenen Massnahmen als umgesetzt beurteilt.

2.5 Aufdeckungsmassnahmen und Prüfungen

Externe Prüfgesellschaften

Die jährlichen aufsichtsrechtlichen Prüfungen der externen Prüfgesellschaften haben die Einhaltung der FINMA-Vorgaben bspw. im Hinblick auf Cyberrisiken zum Ziel. Die Wahl einer durch die Eidgenössische Revisionsbehörde zugelassenen Prüfgesellschaft obliegt den Beaufsichtigten. Letztere mandatieren und bezahlen die Prüfgesellschaften.

Diese Konstellation und Abhängigkeit der FINMA von den externen Prüfgesellschaften im Rahmen der Prüfungstätigkeit sind bekannt. Einerseits von der FINMA selbst, andererseits durch einen Bericht des Internationalen Währungsfonds von 2019[7].

Ab Frühjahr 2020 werden die Prüfberichte durch die Prüfgesellschaften strukturiert über die EHP (Erhebungs- und Gesuchsplattform) eingereicht. Bis zum Frühjahr 2020 erfolgte die Berichterstattung nicht strukturiert.

[7] IMF Country Report Nr. 19/183 – Financial Sector Assessment Program (https://www.imf.org/en/Publications/CR/Issues/2019/06/26/Switzerland-Financial-Sector-Assessment-Program-47045)

Die Aussagekraft der Berichterstattung durch die Prüfgesellschaften über die durchgeführten Prüftätigkeiten (Tiefe, Gewichtung etc.) weist eine hohe Varianz auf. Eine Analyse der Daten und eine Auswertung der Berichterstattung durch die FINMA ist sehr aufwendig.

Die Aussagekraft und Anwendbarkeit der im Rahmen der aufsichtsrechtlichen Basisprüfung erfolgten Berichterstattung ist für eine Datenanalyse in Bezug auf die sich verändernde Bedrohungslage sehr aufwendig. Die Berichterstattungen formulieren teilweise stark abstrahierende Aussagen zum Prüfgebiet Informatik inklusive Umgang mit Cyberrisiken und -attacken (Analyse von fünf zufällig ausgewählten Prüfberichten aus dem Jahr 2017).

Zugriff auf Arbeitspapiere und die temporären Beanstandungen und Empfehlungen des Fachprüfers der externen Prüfgesellschaft könnte die FINMA bei Bedarf einfordern, tut sie aber nicht. Die FINMA führt kein Benchmarking über die Aussagekraft der Berichterstattung der Prüfgesellschaften im Bereich Informatik inklusive Umgang mit Cyberrisiken durch.

Gemäss FINMA (Fachkonzept) erfolgt für Institute der Aufsichtskategorien 1 und 2 eine Analyse der Prüfberichterstattung zum Umgang mit Cyberrisiken durch B-OCI. Bei Instituten der Aufsichtskategorie 3 orientiert der jeweilige KAM proaktiv B-OCI im Falle von Empfehlungen und Beanstandungen im Hinblick auf Cybersicherheit mit hoher Kritikalität. Weiter erfolgt die Unterstützung der Institute der Kategorien 4 und 5 grundsätzlich nur bei wesentlichen Vorfällen im Rahmen von institutsspezifischen Abklärungen oder beim Fallmanagement.

Die Unterstützung erfolgt u. a., weil das Thema Cyberrisiken sehr technisch und dynamisch ist und eine Beurteilung der durch die externen Prüfgesellschaften rapportierten Beanstandungen und Empfehlungen für diesen Bereich durch den jeweiligen KAM schwierig ist. Eine Vorgabe, wann der KAM bei Beanstandungen oder Empfehlungen bei Banken der Aufsichtskategorien 4 und 5 B-OCI informiert, gibt es nicht. Es ist eine Bringschuld und liegt im Ermessen des jeweiligen KAM.

Selbstbeurteilung (Self-Assessment)

Ein weiteres Aufsichtsinstrument sind Selbstbeurteilungen im Bereich Cybersicherheit, die durch die Beaufsichtigten selber vorgenommen werden. Die FINMA hat in den Jahren 2016 und 2018 jeweils bei Banken der Aufsichtskategorie 2 und 3 eine Selbstbeurteilung zu einem bestimmten Thema im Bereich Cyberrisiken verlangt. Bis zum heutigen Zeitpunkt hat die FINMA keine Selbstbeurteilungen für Banken der Aufsichtskategorien 4 und 5 durchführen lassen. Gemäss FINMA wurden die Resultate und Erkenntnisse aus den erwähnten Selbstbeurteilungen den Banken der Aufsichtskategorie 4 und 5 per Brief zugestellt.

Beurteilung

Die Aufsichtstätigkeit wird zu einem wesentlichen Teil von externen Prüfgesellschaften vollzogen. Es besteht das Risiko, dass die relevanten Informationen anlässlich der aufsichtsrechtlichen Berichterstattung nicht umfassend wiedergegeben sind. Teilweise sind stark abstrahierende Aussagen des Prüfgebiets Informatik inklusive Umgang mit Cyberrisiken und -attacken in nicht strukturierter Form enthalten. D. h. der Bericht kann ohne vollständigen Erkenntnisse aus den fachlichen Prüfungshandlungen verfasst werden, was gravierende Mängel beinhalten kann.

Die risikoorientierte Aufsicht und Unterstützung durch B-OCI (Kategorien 1, 2 und teilweise 3) erfolgt hauptsächlich bei Banken, die entsprechende Ressourcen und Know-how bereitstellen, nicht aber bei mittleren und kleinen Banken, die organisatorisch und technisch weniger Möglichkeiten haben. Die fachliche Unterstützung durch B-OCI kann nur erbracht werden, wenn der KAM informiert.

Vor-Ort-Kontrollen

Seit 2018 führt die FINMA im Bereich Cyberrisiken eigene Prüfungen, sog. Vor-Ort-Kontrollen (VOK), durch, um sich ein eigenes Bild machen zu können. Gemäss FINMA führt B-OCI im Hinblick auf die Institute der Aufsichtskategorien 1 bis 3 eine Übersicht über Empfehlungen und Beanstandungen mit hoher Kritikalität im Bereich Cybersicherheit aufgrund der jährlichen aufsichtsrechtlichen Prüfungstätigkeiten der externen Prüfgesellschaften. Diese dienen u. a. als Grundlage für die Planung von VOK bei diesen Instituten.

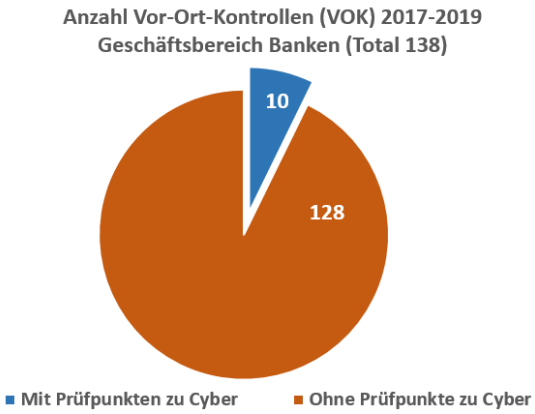

Abb. 4: Quelle FINMA; Darstellung EFK

Anzahl und Umfang der Prüfungen zum Themenbereich Cyberrisiken haben zugenommen. 2018 wurden fünf VOK im Bereich Operationelle Risiken (inkl. Umgang mit Cyberrisiken) durchgeführt. 2019 führte die FINMA erstmals ausschliesslich für den Bereich Cyberrisiken fünf VOK durch.

Bis zum jetzigen Zeitpunkt wurden in den Aufsichtskategorien 4 und 5 keine VOK durchgeführt. Siehe dazu die Abbildung 4.

Beurteilung

Vor-Ort-Kontrollen der FINMA als Regulator haben ein anderes Gewicht als Prüfungen, welche von den durch die Beaufsichtigten selbst mandatierten und bezahlten Prüfgesellschaften durchgeführt werden. Anzahl und Umfang der eigenen Vor-Ort-Kontrollen im Bereich Cyberrisiken sind trotz Zunahme noch auf einem tiefen Niveau.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt, das Thema Cybersicherheit innerhalb der bestehenden Anzahl Vor-Ort-Kontrollen stärker zu gewichten.

Stellungnahme der FINMA

Die Anzahl der Vor-Ort-Kontrollen und gegebenenfalls von der FINMA mandatierten Prüfbeauftragten im Bereich der Cyber-Risiken wird weiter erhöht.

2.6 Datenerhebung und -analyse

Die Aufsichtstätigkeit im Bereich Cyberrisiken sieht verschiedene Aktivitäten vor, bei denen geprüft wird, inwieweit die Vorgaben eingehalten werden.

Im Rahmen der Prüfungsvorbereitung wurden u. a. Analysen und Statistiken der letzten Jahre spezifisch für den Bereich Cyberrisiken nach den Vorgaben aus dem Rundschreiben zu folgenden Punkten angefordert:

- Analysen der Ergebnisse aus den Aufsichtsprüfungen
- Statistiken über die Meldepflicht der Banken (FINMAG Art. 29)
- Statistik über Sanktionen aufgrund von Beanstandungen (gem. FINMAG Art. 30 eröffnet die FINMA ein Verfahren, wenn sich Anhaltspunkte für Verletzungen aufsichtsrechtlicher Bestimmungen ergeben).

2018 wurde von B-OCI einmalig eine Auswertung der Prüfergebnisse 2017 für die Aufsichtskategorien 2 und 3 spezifisch für den Bereich Cyberrisiken gemacht. Diese erfolgte unter grossem Aufwand von Hand. Die Aufsichtskategorie 4 wurde nicht bis auf Ebene der aufsichtsrechtlichen Anforderungen ausgewertet.

Auf übergeordneter Ebene hat die FINMA Ende 2019 eine Datenstrategie genehmigt, welche u. a. definiert, wie Daten erhoben und analysiert werden sollen. Zurzeit ist innerhalb der Gruppe B-OCI keine Datenstrategie inkl. systematischer Datenerhebung und -analyse aus den Aufsichtstätigkeiten im Bereich Cyberrisiken vorhanden und im Fachkonzept beschrieben.

Seit 2019/20 übermitteln die externen Prüfgesellschaften Informationen wie bspw. die Resultate ihrer Prüfung sowie Risikoanalysen via elektronische Erhebungs- und Gesuchsplattform (EHP).

Beurteilung

Die fachliche Unterstützung im Bereich Cyber durch Spezialisten (B-OCI) fokussiert, auch aus Ressourcengründen, auf die Banken der Kategorien 1, 2 und teilweise 3.

Eine unabhängigere, umfassendere, effizientere und wirkungsvollere Steuerung der Aufsichtstätigkeit bringt einen klaren Mehrwert und Nutzen. Das setzt jedoch strukturierte Datenanalysen und Statistiken zu den Ergebnissen aus den aufsichtsrechtlichen Tätigkeiten und Massnahmen voraus. Dies über sämtliche Aufsichtskategorien und auch über einen längeren Zeitraum, z. B. um Trends und Muster zu erkennen.

Des Weiteren unterstützen Datenanalysen die Risikoanalyse und Prüfprogramme von den externen Prüfgesellschaften für das folgende Jahr, wenn etwa eine Häufung von Beanstandungen oder Empfehlungen zu einem bestimmten Bereich festgestellt werden. Zusätzlich kann die Qualität der Berichterstattung der verschiedenen Prüfgesellschaften miteinander verglichen werden.

Voraussetzung für ein effizientes Reporting ist, dass gegenüber den externen Prüfgesellschaften verbindliche Vorgaben für die standardisierte Eingabe der erforderlichen Daten bestehen.

Empfehlung 4 (Priorität 2)

Die EFK empfiehlt, die Prüfergebnisse detailliert und strukturiert einzufordern. Damit würde es möglich, entsprechende Analysen und Statistiken aus der Erhebungs- und Gesuchsplattform aufzubereiten. Dies sollte auch im Fachkonzept umschrieben und definiert werden.

Stellungnahme der FINMA

Jede aufsichtsrechtliche Prüfung mündet in einen Prüfbericht, den die Prüfgesellschaften der FINMA übermitteln. Dabei werden die Prüfergebnisse über die Erhebungs- und Gesuchsplattform der FINMA strukturiert eingereicht. Bei der Analyse dieser Prüfergebnisse stehen für die FINMA die Feststellungen und Beanstandungen der Prüfgesellschaften zur Umsetzung der aufsichtsrechtlichen Anforderungen im Fokus. Diese werden bei den Aufsichtskategorien 3 bis 5 derzeit vom jeweiligen Key Account Manager analysiert und bei Bedarf an die Fachspezialisten, z.B. auch im Bereich Cyber-Risiken eskaliert. Bei den Aufsichtskategorien 1 und 2 nimmt die Querschnittsfunktion zur Überwachung von Cyber-Risiken die Analyse direkt vor. Die Empfehlung wird angenommen und wie folgt umgesetzt: Als kurzfristige Massnahme wird die Querschnittsfunktion zukünftig diese Prüfergebnisse über sämtliche Aufsichtskategorien hinsichtlich Feststellungen und Empfehlungen direkt auswerten. Diese Anpassung wird im Fachkonzept umschrieben und dokumentiert. Zudem wird das Prüfprogramm zur ”Informatik”, welches auch die Prüfpunkte zu den Cyber-Risiken beinhaltet, einer inhaltlichen Prüfung unterzogen und wo nötig angepasst bzw. erweitert.

3 Die Aufsicht über das Zahlungssystem – Swiss Interbanking Clearing System (SIC)

Die FINMA bewilligt und beaufsichtigt u. a. die Finanzmarktinfrastruktur. Die Aufsicht über systemisch bedeutsame Zahlungs- und Abwicklungssysteme teilt sich die FINMA mit der SNB.

Eine Ausnahme ist die Interbank Clearing AG und das von ihr betriebene Interbankenzahlungssystem SIC. Dieses ist weder bewilligungspflichtig noch steht es unter der Aufsicht der FINMA, da das System von der SNB betrieben wird. Genauer gesagt wird es von SIX im Auftrag der SNB betrieben.

Im Gegensatz zur FINMA hat die SNB keine hoheitlichen Befugnisse bei der Ausübung ihrer Aufsichtstätigkeit. Die Teilnahme und die sich daraus ableitenden Rechte und Pflichten sind vertraglich bzw. privatrechtlich geregelt.

Das SIC ist auch eine kritische Infrastruktur.

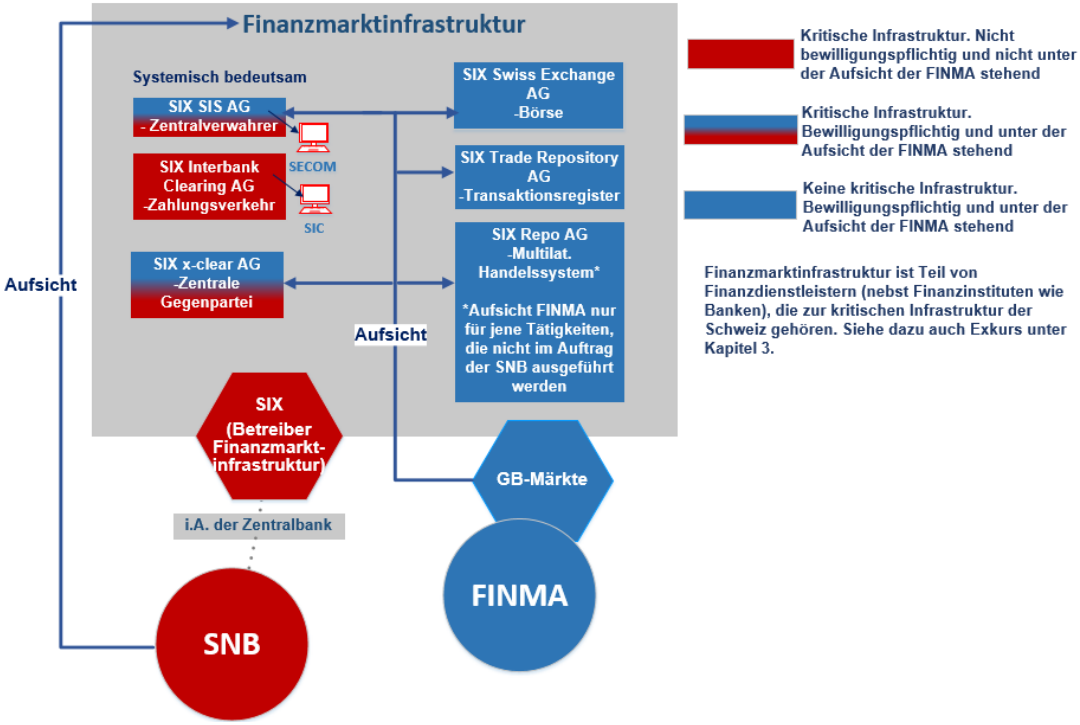

Abb. 5: Darstellung EFK

Im Rahmen dieser Prüfung wurde die SNB separat angefragt, das Zahlungssystem SIC in die Prüfungshandlungen miteinzubeziehen. Dies unter dem Gesichtspunkt, dass die SNB nicht dem Aufsichtsbereich der EFK unterstellt ist. Die SNB hat der EFK schriftlich mitgeteilt, dass eine Prüfung ihrer Aufsichtstätigkeit durch die EFK aus gesetzlichen Gründen nicht möglich ist.

Die EFK stellte fest, dass im Rahmen der Informationsbeschaffung bei Gesprächen mit verschiedenen Experten und der Analyse von Fachdokumenten, das Zahlungssystem SIC als eines der primären potenziellen Ziele in Bezug auf Cyberangriffe im Finanzsystem wahrgenommen wird. Diese Hinweise sind gemäss Absprache direkt an die SNB weitergeleitet worden.

Beurteilung

Da keine Prüfungshandlungen vorgenommen worden sind, kann keine Beurteilung erfolgen.

EXKURS: «systemrelevant» vs. «systemisch bedeutsam» vs. «kritische Infrastruktur»

Systemrelevant:

Definition der systemischen Relevanz aufgrund der Analyse der «too big to fail» (TBTF)-Problematik (Bericht Expertenkommission 2010 z. Hd. des Bundesrats):

Ein Unternehmen ist dann als systemrelevant zu kategorisieren, wenn es

(i) Leistungen erbringt, die für die Volkswirtschaft unverzichtbar sind und

(ii) andere Marktteilnehmer diese Leistungen nicht innerhalb einer Frist ersetzen können, die für die Volkswirtschaft tragbar ist. Konkrete Kriterien der Grösse, der Marktkonzentration, der Vernetzung sowie der mangelnden Substituierbarkeit ermöglichen die praktische Anwendung dieser Definition. Gegenwärtig sind in der Schweiz ausserhalb des Bankensektors keine Unternehmen als TBTF einzustufen.

Die SNB stellt die systemrelevanten Banken durch Verfügung fest.

Systemisch bedeutsam:

Ausschliesslich Finanzmarktinfrastrukturen, von denen Risiken aufgrund bestimmter Kriterien für die Stabilität des Finanzsystems ausgehen können, werden als systemisch bedeutsam bezeichnet.

Die SNB stellt die systemisch bedeutsamen Finanzmarktinfrastrukturen und deren systemisch bedeutsamen Geschäftsprozesse durch Verfügung fest.

Kritische Infrastruktur:

Gemäss dem Bundesamt für Bevölkerungsschutz (BABS) sind von zentraler Bedeutung zur Aufrechterhaltung der Volkswirtschaft insbesondere Dienstleistungen wie die Versorgung der Bevölkerung mit Bargeld, die Abwicklung des Zahlungsverkehrs, die Kapitalisierung Dritter (z. B. Kreditvergabe und Handelsfinanzierung), die Entgegennahme von Einlagen oder die Sicherstellung der Preisstabilität. Ohne Zugang zu Bargeld oder Kapital, ohne die Möglichkeit, Einlagen zu tätigen und Zahlungen abzuwickeln, kann die Schweizer Wirtschaft nicht oder nur sehr eingeschränkt funktionieren. Bereits ein kurzfristiger Ausfall des Bankensystems kann zu grossen volkswirtschaftlichen Schäden führen. Ein gut funktionierender Bankensektor ist daher Voraussetzung für sämtliche wirtschaftliche Tätigkeiten und den Erhalt der Lebensgrundlagen der Schweizer Bevölkerung.

Innerhalb des Teilsektors Banken stehen zum einen diejenigen Institute im Vordergrund, die im Rahmen der «too big to fail»-Thematik als systemrelevant bezeichnet wurden. Zum anderen erbringen aber auch die Finanzmarktinfrastruktur-Betreiberin sowie die SNB essenziell wichtige Funktionen.

Die übergeordnete Koordination und Umsetzung liegt beim Bundesamt für wirtschaftliche Landesversorgung und beim BABS.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 1. Januar 2018, SR 614.0
Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (FINMAG) vom 22. Juni 2007, SR 956.1
Verordnung der Eidgenössischen Finanzmarktaufsicht über die Datenbearbeitung (Datenverordnung-FINMA) vom 8. September 2011, SR 956.124
Verordnung über die Aufsichtsorganisationen in der Finanzmarktaufsicht (Aufsichtsorganisationenverordnung, AOV) vom 6. November 2019, SR 956.134
Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG) vom 19. Juni 2015, SR 958.1
Verordnung über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturverordnung, FinfraV) vom 25. November 2015, SR 958.11
Bundesgesetz über die Schweizerische Nationalbank (Nationalbankgesetz, NBG) vom 1. Januar 2020, SR 951.11
Verordnung zum Bundesgesetz über die Schweizerische Nationalbank (Nationalbankverordnung, NBV) vom 1. Januar 2020, SR 951.131
Bundesgesetz über die Banken und Sparkassen (Bankengesetz, BankG) vom 1. Januar 2020, SR 952.0
Verordnung über die Banken und Sparkassen (Bankenverordnung, BankV) vom 1. Januar 2020, SR 952.02

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).