Management of cyber risks: compliance with FINMA's requirements for banks

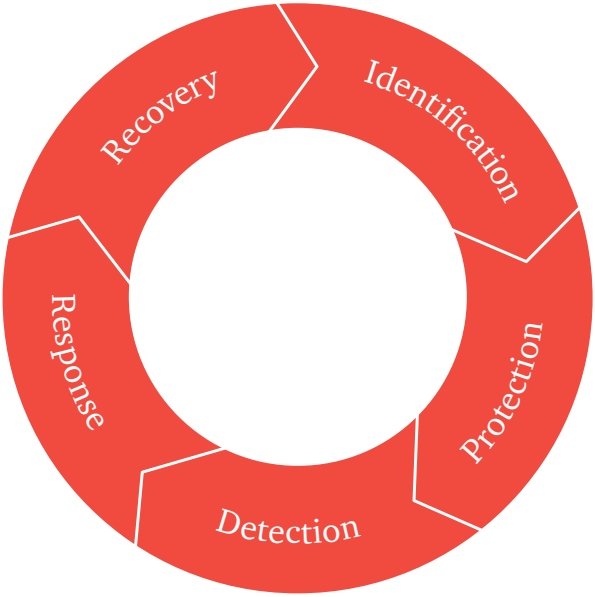
Our recommendations and service offering to help you adjust to the changing regulatory environment

Revised circular on operational risks published

On 1 November 2016, FINMA published a revised version of circular 2008/21 'Operational risks – banks'[1]. The Principle 4 of the updated circular (on technological infrastructure) includes requirements relating to the management of cyber risks. It applies to all banks, regardless of their size or supervisory category, and will enter into force as of 1 July 2017.

New requirements and guidelines set regarding management of cyber risks

Banks must formalise their cyber-risk management strategy, including the definition of roles and responsibilities as well as of the processes to cover the following five dimensions:



pwc

[1] https://www.finma.ch/en/news/2016/11/20161101-mm-rs-corporate-governance-bei-banken/

Overview of FINMA's expectations

FINMA's guidelines - as described in a letter addressed to all banks at the end of August 2016[2] are outlined below:

- Identification and evaluation of cyber risks
  Banks should identify, evaluate and plan remediation actions to get ready to cope with cyber incidents. In particular, they should consider the implementation of a 'threat intelligence' solution and ensure the maintenance of a complete list of their critically important systems and data.
- Protection against cyberattacks
  Banks should implement measures that prevent the unauthorised extraction of data outside of the institution by monitoring data flows; they should also ensure the security of their networks and interfaces with external networks as well as setting up several lines of defence (e.g. to block DDoS attacks).
- Detection of cyberattacks
  Banks should improve their monitoring approaches, which enable them to block any unauthorised penetration of the internal network, detect irregularities in the data flows within the network and handle security alerts effectively; banks should also consider implementing an SIEM solution as a means to improve the systematic logging of cyberattacks.
- Response to cyberattacks
  Banks should define the processes, people and tools required to respond to a cyberattack, notably to maintain normal operational activity; they also should formalise their action plans or overall communications with internal and external stakeholders.
- Restoration of business activities after a cyberattack
  Banks should define the measures required to ensure the restoration of the systems' availability and integrity or to recover corrupted or lost data after a cyberattack; in addition, they should formalise a systematic process and related procedures to launch a forensic inquiry after a significant cyberattack in order to identify the causes and control deficiencies as well as develop an action plan with measures to improve protection against cyberattacks.

Our recommendations to banks

The adoption of the revised circular presents banks with numerous new challenges relating to the management of cyber risks. Based on our experience both as auditors and cyber-security consultants, we recommend the following:

1. Review of your current status: perform a gap analysis
   We recommend performing as of now a gap analysis of your current status against FINMA's new requirements and guidelines relating to cyber-risk management. The objective of such an analysis is to identify which initiatives have to be implemented to ensure compliance. From this perspective, we suggest developing a detailed roadmap, which would also include the prioritisation of the various projects, as well as deadlines. In order to mobilise all of the stakeholders around such an action plan, it is advisable to submit it to the executive board and to the board of directors for approval.
2. Monitoring tools and incident management solutions
   Don't underestimate the complexity and the operating costs incurred in improving monitoring systems. Banks should consider implementing tools that enable them to monitor their infrastructure (in particular, to detect anomalies in data flows). Similarly, to ensure effective, centralised security alerts, we recommend considering the deployment of a central log management tool (SIEM) or capability (SOC). However, we strongly advise evaluating the configuration, maintenance and operating costs of such tools before implementing them. We have often observed that the resources and competencies required to parametrise such solutions and to manage the logs/alerts were not made available and, therefore, the potential benefits from their deployment could not be realised.
3. Threat intelligence: choose a solution adapted to the size of your bank
   We recommend contracting threat intelligence

[2] In November 2015, FINMA requested that supervisory category 3 banks fill in a self-assessment questionnaire on their ability to combat cyber risks. 27 banks active in Switzerland›s financial market submitted their self-assessments to FINMA at the end of January 2016. At the end of August 2016, FINMA disclosed the anonymised results, as well as its analysis, to all Swiss banks.

services to assist you in anticipating and proactively protecting your organisation by mitigating the risk of cyberattacks. Depending on the size of your organisation, such solutions (prices can differ significantly) may be replaced by regular reports compiled by threat intelligence specialists. This is a pragmatic alternative that ensures you a minimum level of compliance.

4. Consistence of your security framework: have a risk-based approach to information security and cybersecurity
   Since 2015, most Swiss banks have rolled out their own framework to ensure the confidentiality of their clients' data (in compliance with FINMA circular 2008/21 Appendix 3 on handling of electronic client identifying data). The measures implemented allowed them to reduce the risk of data leaks, in particular. FINMA's new requirements mean that banks will now have to find an appropriate response to protect themselves against cyberattacks. In this context, it is crucial to deploy and spread a consistent risk-based approach to information security and cybersecurity.

How PwC can help

As a multi-disciplinary firm, we are uniquely placed to help clients adjust to the changing regulatory environment. We have developed a range of services to help you cope with regulatory challenges, including:

- Gap analysis
  We have established a comprehensive methodology designed to assess your readiness against cyberattacks and the maturity level of your cyber capabilities, and to identify gaps against FINMA's requirements. Our proven, field-tested gap analysis templates include 50+ controls grouped into the following six areas: strategy, identification, protection, detection, response and recovery.
- Definition of compliance roadmap and action plan implementation monitoring
  We have already helped numerous clients define compliance action plans. Such plans typically include: identified gaps, the relating regulatory requirements, the list of activities to be undertaken to bridge identified gaps, suggested business owners and impacted stakeholders, proposed timeline and estimate of costs. Besides, one of the key challenges faced by organisations undergoing transformational regulatory compliance programmes is managing the complexity, the interdependencies and the sequencing of activities. To deal effectively with this challenge, we've developed easy-to-use project management templates specifically designed for this kind of evaluation (e.g. project status or detailed progress report).
- Assistance in the implementation of compliance actions
  We have developed strong expertise in advising our clients on compliance strategies, reviews and assurance. We can assist in implementing a broad variety of actions to achieve compliance with FINMA's requirements by mobilising our network of cyber specialists: e.g. elaboration of your cyber-risk management strategy / policy, due diligence assessments of third parties regarding cyber-risk management, review of your protection capabilities against cyber threats, review of your cyber-threat detection capabilities or definition of your cyber-attack response and recovery processes.

Here are some further services taken from our service catalogue that might be of interest to you in your compliance journey:

- Threat intelligence services
  Our active cyber defence team is comprised of handpicked analysts with a background in network defence and intelligence services. Our range of services enables proactive protection from the business risk of targeted attacks and includes: Threat intelligence reporting: valuable insights into sectors and targets, sector threat profiles, tactical and strategical bulletins, etc. Feeds and collaboration: real time threat intelligence and information sharing with other organisations, at fixed costs. Directed research: customised threat intelligence for your business, research on the 'dark web' for imminent threats or attacks, etc.
- Cyber-risk assessment
  We have a wealth of experience in helping our clients assess their cyber risks. We can help you identify, analyse, evaluate and prioritise your cyber risks. In particular, we have developed an automated tool enabling you to present the results of your cyber-risk assessment in a dynamic matrix.

- Security assessment services
  Our services include vulnerability assessments and penetration testing. We can leverage our global methodology and a tailored set of software to best match the context of your organisation to identify currently known vulnerabilities in your environment. For penetration testing, we use a tailored approach to each client situation to undertake realistic tests and determine the business impact of the exploitation of identified vulnerabilities and configuration errors.

Contacts

Reto Haeni
Cyber Security Partner and Leader
PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

Yan Borboën
Partner, Cyber Security
+41 79 580 73 53
yan.borboen@ch.pwc.com

Nicolas Vernaz
Leader Data Protection and Regulatory Compliance
PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com