PENTA

FINMA CYBER SECURITY COMPLIANCE ROADMAP

Your definitive roadmap to FINMA cyber risk compliance in 2025

2025

Cyber risks present a significant operational and reputational risk to Swiss financial institutions. In response, FINMA has increased the intensity of its supervision of financial services companies of all sizes and specialty.

Contents

Digital advancements, such as the cloud, are inevitable.

They bring a raft of benefits, capabilities, advantages and possibilities.

But they also bring risk.

The cloud is a complex landscape, which, for heavily regulated industries (such as finance and law, as just two examples) **requires careful navigation.** This is not only from a compliance perspective, but also in terms of safety and security.

Cloud service providers must provide watertight assurance, and in turn, financial institutions need to be able to demonstrate an unerring level of cybersecurity to their customers. **Are you able and equipped to do that?**

If the answer's no, or you're at all unsure, Penta has put together this guide to FINMA cyber risk compliance in 2025. It has been developed to help financial institutions in Switzerland operate with confidence, safe in the knowledge that they are meeting all applicable regulatory requirements — by remaining **safe, secure and compliant.**

Overview

Overview

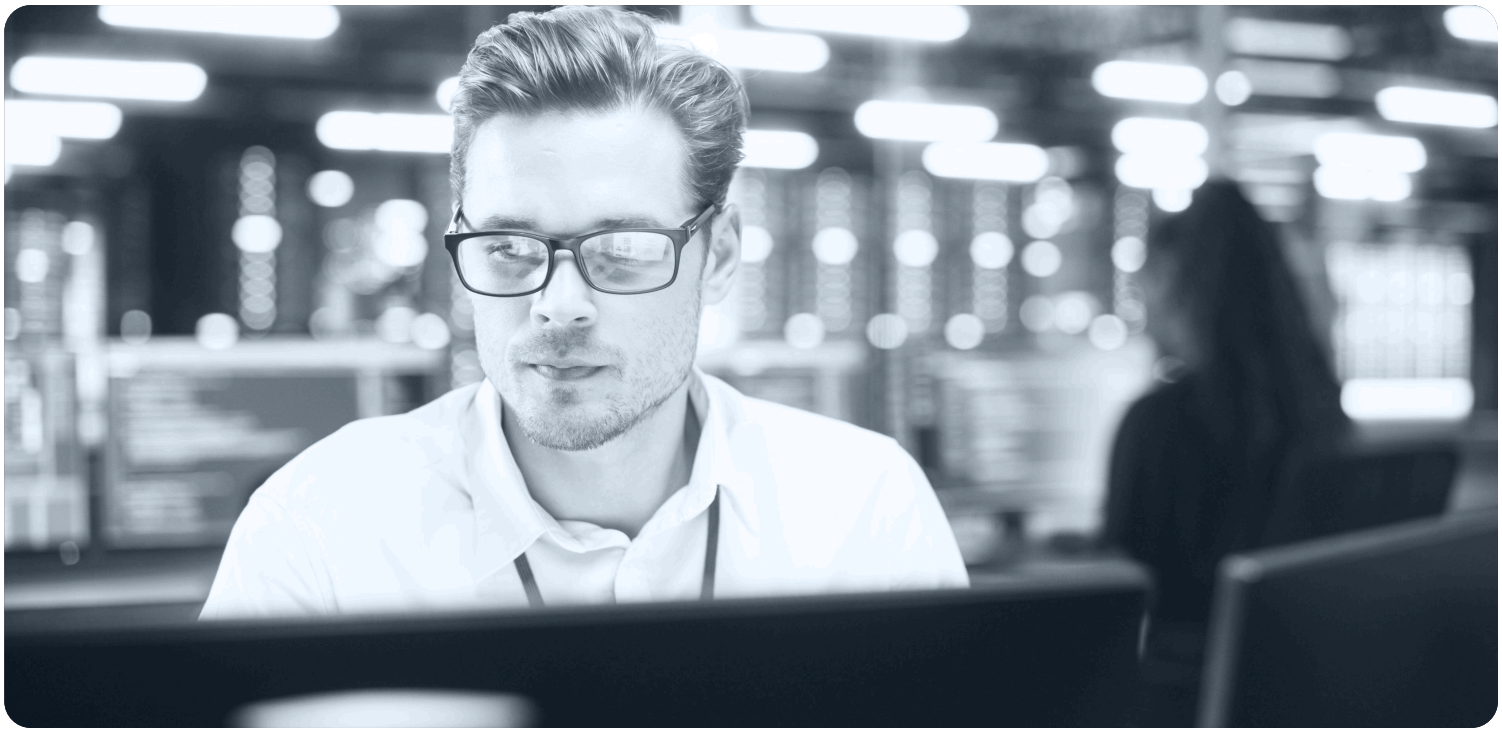
FINMA aims to ensure Swiss financial institutions are not destabilised, which it achieves by assessing the risk position of individual companies.
The main focus of its work is the supervision and protection of the Swiss financial sector and its reputation.

IT risk presents the fastest-growing risk to that reputation, but mitigation isn't simply a question of ticking boxes and abiding by the rules. Wider picture aside, failure to mitigate IT risk has the potential to be nothing short of catastrophic for your business, which is why compliance isn't the gold standard, **it's the baseline.**

If you do want to look at the wider picture though, the increasing professionalism and agility of criminals continues to keep the financial industry on its toes. After all, a successful attack can lead to outages, the interruption of information and communication, and jeopardise availability, confidentiality and integrity, not to mention outright theft.

Yet, **according to FINMA,** there remains a lack of **risk awareness** amongst FINMA-regulated companies, and cyber processes are often too fragmented to allow for an accurate and comprehensive assessment of the cyber risk situation.

To exacerbate this problem, **security gaps** – which must be identified and mitigated as fast as possible – are constantly emerging.



The nine principle risks in 2025 / The main risk drivers

The nine principle risks in 2025

- Interest rate risk
- Credit risk associated with mortgages
- Credit risk associated with other loans
- Risk of **cyberattacks**
- Risk in the area of combating money laundering
- Risk due to increased impediments to cross-border market access
- The comparative widening of credit spreads
- Outsourcing
- Liquidity and funding risk

So, as you can see, cyber-attacks and outsourcing are two of the nine explicit risks, and, as these are our areas of expertise, they are what we are going to focus on in this report.

The main risk drivers

- Incomplete (or no) response plans for cyber incidents in place, or the effectiveness of these plans is not reviewed.
- Cyber risks not explicitly integrated into the qualitative management of operational risks, which means systematic and comprehensive risk management cannot be guaranteed.
- Cyber risks and their associated risk tolerances not adequately defined, or there is no cyber protection in place.
- Clear cyber security requirements are not set out to service providers, or are not regularly reviewed.

Outsourcing and its associated dangers

Outsourcing

Outsourcing is far from a new concept, but driven by digitisation and a focus on core business activities, the number of outsourced services per institution continues to grow, in parallel with the number of subcontractors.

This has led to more a complex supply chain and, with it, increased risk.

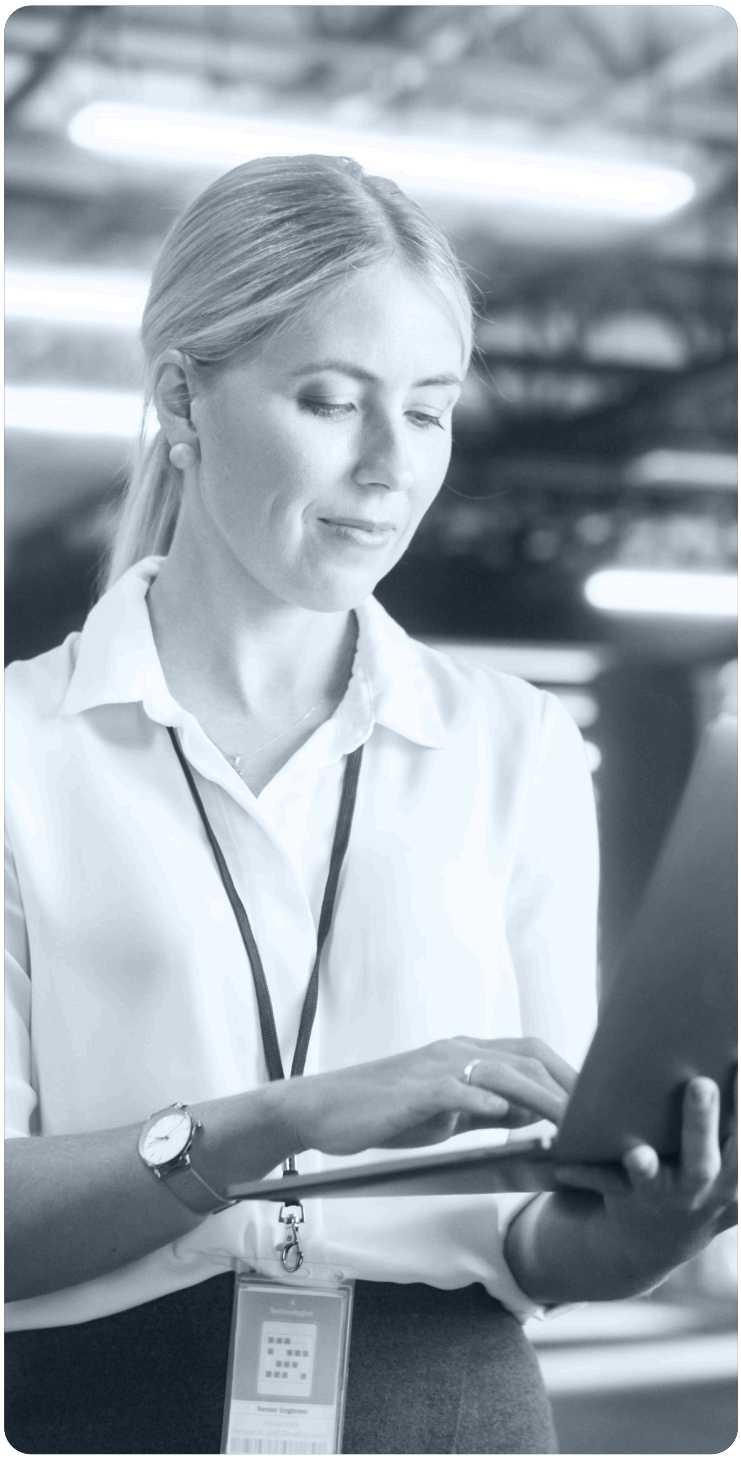
Outsourcing offers several (not insignificant) benefits, including **increased flexibility, innovation, and improved operational resilience.**

But, as newly identified by FINMA, outsourcing critical functions to third parties has become a major operational risk.

It cites that **a third of all cyberattacks** on financial institutions occur through third-party providers, and adds that disruptions or failures in critical functions handled by third-party providers could, in extreme cases, **threaten wider financial market stability.**

This is because, it says, many institutions rely on a small group of providers for critical functions, such as cloud services.

This concentration **increases the sector's dependence** on these providers, and any disruption or unauthorised access could seriously affect the Swiss financial market as a whole.



Commonly outsourced processes include payments (outsourced by two-thirds of banks) and IT infrastructure and operations (outsourced by 80% of banks and 60% of insurers).

As a result, these institutions are highly dependent on third parties to deliver their services.

However, they remain responsible for overseeing these providers and ensuring that necessary actions are taken when issues arise.

Effectively managing and monitoring service providers and their associated risks is therefore **crucial for maintaining operational integrity.**

Organisations cannot delegate responsibility for proper business conduct, and this extends to outsourcing.

Instead, they must **develop the expertise** to manage outsourced functions effectively and take swift action when necessary.

FINMA notes that many institutions **need to improve their understanding** of supply chains and associated risks.

It says that — worryingly — in some cases, outsourcing risks are **not properly identified,** let alone monitored or controlled.

FINMA’s cyber threat landscape: latest insights (2023–2024)

FINMA's cyber threat landscape: latest insights (2023–2024)

Cyber threats remain one of the top operational risks for Switzerland's financial sector.

FINMA reports a 30% year-on-year increase in successful or partially successful cyberattacks.

Around one in three of these incidents originated from external service providers, reflecting the persistent vulnerabilities introduced through outsourcing and third-party IT services.

Malware and unauthorised access were the most common attack methods, with smaller institutions such as independent asset managers and non-affiliated insurance intermediaries increasingly being targeted.

Email remains the most prevalent entry point, particularly for business email compromise (BEC) and CEO fraud.

Distributed Denial of Service (DDoS) attacks also resurged in multiple waves, often financially or ideologically motivated.

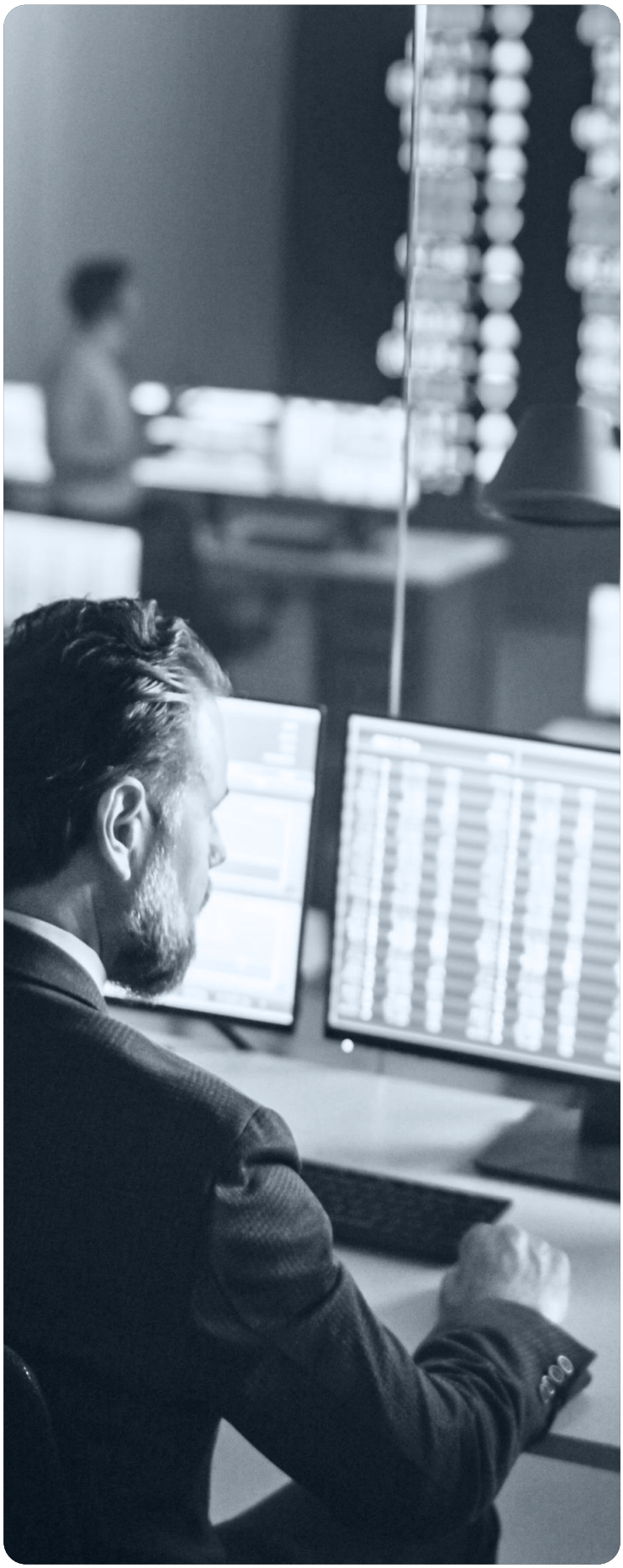
Alarmingly, supply chain attacks—including those targeting cloud providers—continue to rise and accounted for nearly 30% of all reported incidents.

FINMA underlines the need for better lifecycle management of IT infrastructure, enhanced security policies with third parties, and faster detection and response capabilities.

These are critical to protecting core business operations and client data.

Who do FINMA’s cyber security guidelines apply to?

Who do FINMA's cyber security guidelines apply to?



Most Swiss financial services and businesses operating in the Swiss financial market require authorization.

This, in most cases, is granted by FINMA.

Any individual or company that wants to manage clients' money, use investors' money, underwrite insurance policies, or set up and manage a collective investment scheme, needs FINMA authorization.

Authorised companies then become supervised.

FINMA supervision varies in intensity – it can range from intensive, ongoing supervision to a simple act of registration, after which FINMA will only step in if it receives reports of inappropriate conduct.

Under certain circumstances, service providers must join a private self-regulatory organisation instead.

To check whether an individual, company or financial product is authorised, search for its name here.

Where to start / Immediate reporting to FINMA: how it works

How to mitigate internal and third-party cyber threats

Swiss banks need to guard their infrastructure against attacks in many forms, including (but by no means limited to) phishing, malware and disruption to the availability of computers.

All banks and securities dealers that fall under FINMA's jurisdiction must adopt an "integrated and systematic" approach to countering threats from the virtual world.

This must include specific measures for governance, identification, protection, detection, response and recovery of threatened systems and services in connection with cyber risks and attacks.

Immediate reporting to FINMA

If your FINMA-regulated company is affected by a cyber-attack, you must inform FINMA through your responsible (key) account manager within 24 hours of detection, and carry out an initial assessment of its severity.

If FINMA finds out that you're operating (knowingly or unknowingly) without authorisation – which includes not reporting back to it in the event of a cyber attack within the specified time – it will investigate the matter. If it finds evidence that this has happened, it can launch **enforcement proceedings** and impose measures "of varying severity" which may even include closing down the company.

A report (as outlined below) should then be submitted via the **FINMA web-based survey and application platform, within 72 hours.**

Guidance on what should be included in a cyber attack report to FINMA

- Name of institution
- Contact person including contact details (telephone and email address)
- Date/time of submission to FINMA
- Date/time when attack was discovered
- Date/time of attack (if already known)
- Description of cyber attack and current status
- Initial assessment of the severity of the cyber attack (see *'determining the severity of a cyber attack,* below)
- Severity trend (selection)
  - decreasing
  - stable
  - increasing
- Affected entities (affected organisational unit(s) within the institution or service provider)
- Affected protective goals (multiple selection)
  - confidentiality
  - integrity
  - availability
- Affected critical functions, business processes or assets
  - affected information
  - technology infrastructure
  - facilities or personnel

- Affected number of customers (current status)
- Vectors of attack (multiple selection)
  - email
  - web-based attack
  - brute force attack
  - identity theft
  - removable media
  - loss/theft of devices
  - exploitation of software vulnerability
  - exploitation of hardware vulnerability
  - other [please define]
- Type of attack (description) (e.g.)
  - DDoS
  - unauthorised access
  - malware
  - misuse/improper use of technology infrastructure etc
- Administrative, operational and/or technical countermeasures with expected time to effectiveness
- Communication measures (what, to whom, when)

It's important to note that if, after the report has been submitted, there are new **developments or assessments** relating to the same attack, a new report must be submitted within the (renewed) deadline of 72 hours.

For cyber attacks defined as **high or severe** (see *'determining the severity of a cyber attack'*, below) once the case has been processed, FINMA expects a "conclusive root cause analysis" to be submitted.

This must include:

- an analysis
- reason for the success of the attack
- impact of the attack on the observance of regulations, operations and customers
- mitigating measures to address the consequences of the attack.

For severe cyber attacks, proof and analyses of the proper functioning of the crisis organisation must also be submitted.

For cyber attacks with a medium severity level, a conclusive root cause analysis is sufficient.

Determining the severity of a cyber attack

Determining the severity of a cyber attack

FINMA cyber attack severity definition criteria

Severe **Extensive and prolonged damage to protective goals (availability, integrity, confidentiality) of critical assets present or expected.**

- Availability: critical assets are not available in the medium to long term (failure > 200 % of the RTO9)
- Confidentiality/integrity: sensitive information affected to (almost) full extent
- Financial implications or damage to the institution's reputation, endangering its existence
- Overcoming the cyber attack requires the activation of the crisis organisation (BCM)

High **Protective goals (availability, integrity, confidentiality) of critical assets are substantially damaged or threatened.**

- Availability: critical assets are not available in the medium term (failure >= RTO)
- Confidentiality/integrity: sensitive information and/or critical information for the business process affected to a large extent
- Considerable financial implications or damage to the institution's reputation
- Overcoming the cyber attack requires the engagement of external resources

Medium **Direct harm or threat to the protective goals (availability, integrity, confidentiality) of critical assets.**

- Availability: critical assets are not available in the short term (failure > 50% of the RTO)
- Confidentiality/integrity: sensitive information substantially affected.
- Perceptible financial implications or damage to the institution's reputation
- The cyber attacks can be overcome internally with the resources available

Defining critical assets and their potential respective cyber attacks

Sensitive/confidential information such as customer identification data, insurance contracts, data in connection with the settlement of claims or benefits processing, minutes of meetings of the board of directors or executive board, strategy information, HR data.

- Attacks on protective goals via unauthorised data access either from within the company or externally, leakage of data, data theft, alteration of data.

Technology infrastructure necessary for performing a critical function (i.e. hardware, software, network infrastructure.)

- Attacks on protective goals via (D)DoS, loss/theft of storage media with confidential information, ransomware.

Facilities essential for the provision of critical functions (i.e. data centre, branches, back office premises).

- Attacks on protective goals by disrupting or deactivating the protective measures in place to regulate authorised access to sensitive areas.

Personnel employees who perform critical functions or contribute significantly to these such as e.g. executive board, traders, client advisers, as well as key personnel (i.e. employees with elevated rights, system administrators, security staff, accounting).

- Attacks on protective goals via social engineering (such as spear phishing), insider threats, identity theft, and extortion.

FINMA audit points for cyber risk management

FINMA audit points for cyber risk management

Below is a guide to what FINMA deems to be an acceptable cyber risk management audit.

Procedures for audit depth "critical assessment":

1 ☐

Learn how the institution handles cyber risks, including how much importance they place on them, and how they go about auditing them.

2 ☐

Discuss whether the institution's cyber risk governance is fit for purpose (including regulations, policies, procedures, standards, guidelines, and directives).

3 ☐

Assess whether cyber risks are properly taken into account within wider operational risk management – such as the identification, assessment, limitation and monitoring of operational risks.

4 ☐

Does the board of directors regularly (at least once a year) review the institution's tolerance for cyber risk? Both to make sure they are in line with the wider risk policy, and to take into account strategic and financial objectives?

5 ☐

Does the board of directors regularly approve cyber risk strategies and monitor compliance?

6 ☐

If cyber risks are not identified as material inherent risks, assess whether the explanation provided is satisfactory and clear.

7 ☐

Assess cyber risk training for employees, including formal and informal sessions on their ability and responsibility to reduce cyber risk.

8 ☐

Assess whether cyber risk training is appropriately tailored for different roles within the institution (including executives, employees with access to privileged data, third parties and contractors).

9 ☐

Assess whether the executive board receives sufficient reports on cyber risks, including frequency of reports and information around the development of cyber risks, the effectiveness of key controls and major (internal and external) incidents.

10 ☐

Assess the results of audit and control procedures performed by Internal Audit and/or other control functions (such as Independent Risk Control) relating to cyber security, and review the minutes of relevant committees and function meetings.

11

Are specific tasks, competencies and responsibilities clear for each role in the institution with regards to cyber risks - including role description, the organisation, functional distinctions, reporting lines and communication channels.

12

Are cyber risks adequately taken into account in audits by the Independent Risk Control and Internal Audit? The following, in particular, must be taken into account: risk analysis and assessment, multi-year planning, the application of international standards.

13

Assess whether the institution's concept of cyber risk matches that of internationally recognised standards or practices, and if it is specific enough to match the needs and risks of the institution.

14

Assess whether ICT assets and interfaces with third parties are identified, catalogued and evaluated.

15

Is there a definition of critical data, and is there an inventory of that data?

16

Assess whether ICT assets are adequately represented in the network infrastructure, according to how important they are and their need for protection.

17

Are the procedures, processes and controls for identifying potential cyber threats specific to the institution adequate? And are they able to assess the impacts of a cyber attack, such as the theft of critical data, communication with third parties and ICT assets?

18

To what extent do risk assessments know about, and appropriately take into account, potential threats, vulnerabilities and the impact of cyber attacks, such as the theft of critical data, communication with third parties and ICT access?

19

Does ICT have adequate procedures, processes and controls for granting access to the inventoried ICT assets and interfaces with third parties?

20

Are there adequate procedures, processes and controls for periodically rechecking the access to the inventoried ICT assets and interfaces with third parties?

21

Assess the procedures, processes and controls for managing and monitoring access to the inventoried ICT assets and interfaces with third parties.

22

To what extent are there adequate organisational and technical measures to prevent critical data theft?

23

Are the procedures, processes and controls for managing network security adequate? Consider zoning, network access control [NAC], firewall, web application firewall [WAF], protection against DDoS, and proxy servers.

24

Assess the adequacy of procedures, processes and controls for managing infrastructure security (such as endpoint detection & response (or XDR), and anti-virus software).

25

Do the procedures, processes and controls ensure standardised baseline configuration and system hardening of ICT assets? Do they also ensure ongoing compliance after configuration?

26

Assess the risk-based approach to the timely closure of security gaps (patching) and addressing of misconfigurations (configuration change) in systems, applications and underlying infrastructure.

27

With regards to systems, applications and underlying infrastructure, to what extent are security gaps (patching) closed in a timely manner? Equally, assess whether misconfigurations are addressed in a similarly timely manner.

28

Assess the adequacy of provisions for protecting the confidentiality, integrity and availability of stored and transferred critical data.

29

Are anomalies and security events identified in a timely manner by continually monitoring the ICT, and are the potential effects of these incidents adequately assessed?

30

Are the default values for permissible network operations and the expected data flows for users and systems (such as data flows between different network zones and interfaces between the ICT systems) technically defined via SIEM? Discuss the process for keeping these values up to date.

31

Are the critical inventoried ICT assets and their use by employees and third parties systematically and continuously monitored?

32

Assess the adequacy of the technical measures used to identify cyber incidents using cyber risk scenarios (also known as use cases).

33 ☐

Assess whether the procedures and directives for the detection of cyber incidents are regularly updated and tested.

34 ☐

Assess the adequacy of the response plan that addresses identified cyber incidents, and in particular how this is coordinated with internal and external stakeholders. Discuss what support is needed from external bodies in the event of an incident.

35 ☐

Is there timely analysis, documentation and classification of reports from the detection systems (also known as events)?

36 ☐

Are there adequate processes and measures (such as playbooks) in place for containing and mitigating cyber attacks?

37 ☐

Assess whether the requirements from FINMA Guidance 05/2020 “Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA” are taken into account in the response plan.

38 ☐

Are response and recovery processes assessed and improved regularly and adequately?

39 ☐

Assess whether there is an adequate process in place to promptly recover systems after a cyber attack?

40 ☐

Are there regular and adequate vulnerability assessments, penetration tests and scenario cyber exercises based on the institution-specific threat landscape?

41 ☐

Assess whether vulnerability assessments and penetration tests are regularly conducted on all ICT assets accessible over the internet. Are they adequately conducted for the systems necessary for the provision of critical processes, and those that contain critical data?

42 ☐

Once identified, are risks and weaknesses addressed and removed satisfactorily?

43 ☐

Are there sufficient technical and personnel resources for the initiation, implementation and risk-based implementation of vulnerability assessments, penetration tests and scenario cyber exercises?

44 ☐

Assess whether the results of cyber exercises are suitably documented and reported.

Next step

Next step

By conducting vulnerability assessments and penetration testing, your company will be able to proactively identify and mitigate security risks before they can be exploited by attackers.

- Work collaboratively with reputable professionals to perform regular assessments and tests to identify potential weaknesses in your systems and networks.

- Use the findings to evaluate the effectiveness of your existing controls.

- Develop and implement a remediation plan to address identified vulnerabilities and flaws.

> **Cyberattacks pose a very real threat to businesses of all sizes—and this threat is only increasing.**
>
> **To ensure your security and compliance, it is important to follow FINMA's guidance to the letter.**