# Management von Cyberrisiken: wie Banken die Anforderungen der FINMA einhalten

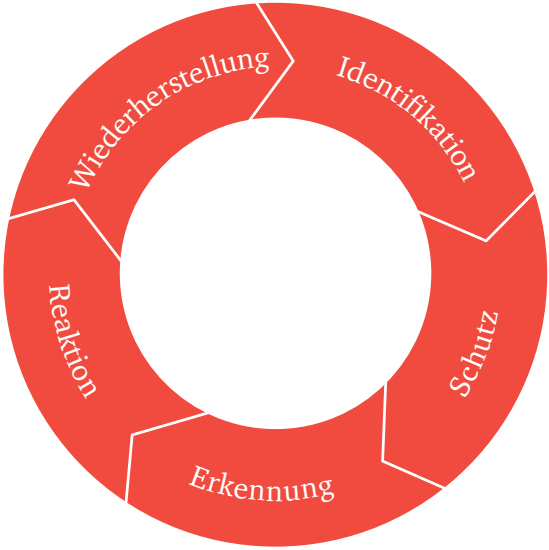
Unsere Empfehlungen und Dienstleistungen unterstützen Sie dabei, sich an das ändernde regulatorische Umfeld anzupassen.

## Revidiertes Rundschreiben über operationelle Risiken veröffentlicht

Am 1. November 2016 veröffentlichte die FINMA eine revidierte Version des Rundschreibens 2008/21 «Operationelle Risiken – Banken». [1] Der Grundsatz 4 (über die technologische Infrastruktur) des aktualisierten Rundschreibens beinhaltet Anforderungen, die sich auf das Management von Cyberrisiken beziehen. Er tritt am 1. Juli 2017 in Kraft und gilt für alle Banken, unabhängig von ihrer Grösse oder Aufsichtskategorie.

## Neue Anforderungen und Richtlinien hinsichtlich des Managements von Cyberrisiken festgelegt

Banken müssen ihre Strategie für das Management von Cyberrisiken formalisieren, einschliesslich der Definition der Rollen und Aufgaben sowie der Prozesse. Damit werden die folgenden fünf Dimensionen abgedeckt:




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

pwc

## Die Erwartungen der FINMA

FINMA, Die Ende August 2016 allen Banken per Brief mitgeteilt wurden, [2] sind folgende:

- Identifikation und Bewertung potenzieller Cyberrisiken
  Banken müssen Abhilfemassnahmen identifizieren, bewerten und planen, um sich für die Bewältigung von Cybervorfällen zu rüsten. Insbesondere sollten sie die Einführung einer Threat-Intelligence-Lösung erwägen, um stets eine vollständige Aufstellung ihrer besonders wichtigen Systeme und Daten zu garantieren.
- Schutz vor Cyberattacken
  Banken müssen Massnahmen ergreifen, die die unbefugte Extraktion von Daten ausserhalb des Finanzinstituts verhindern, indem die Datenflüsse überwacht werden. Sie müssen auch die Sicherheit ihrer Netzwerke und Schnittstellen mit externen Netzwerken garantieren und mehrere Verteidigungslinien einrichten (z.B. zum Blockieren von DDoS-Angriffen).
- Erkennung von Cyberattacken
  Banken müssen ihre Überwachungsansätze verbessern, die es ihnen ermöglichen, jegliches unbefugte Eindringen in ihr internes Netzwerk zu blockieren, Unregelmässigkeiten bei den Datenflüssen innerhalb des Netzwerks zu erkennen und effektiv mit Sicherheitswarnungen umzugehen. Banken sollten auch erwägen, eine SIEM-Lösung als Mittel zur Verbesserung der systematischen Erfassung von Cyberattacken umzusetzen.
- Reaktion auf Cyberattacken
  Banken müssen die Prozesse, Personen und Instrumente definieren, die für die Reaktion auf eine Cyberattacke notwendig sind, insbesondere zur Wahrung des normalen Geschäftsbetriebs. Sie müssen auch ihre Massnahmenpläne oder die gesamte Kommunikation mit internen oder externen Interessenvertretern formalisieren.
- Wiederherstellung des Geschäftsbetriebs nach einer Cyberattacke
  Banken müssen die erforderlichen Massnahmen definieren, um zu garantieren, dass die Verfügbarkeit und Integrität der Systeme sowie korrumpierte oder verloren gegangene Daten nach einer Cyberattacke wiederhergestellt werden können. Ausserdem müssen sie einen systematischen Prozess und dazugehörige Abläufe formalisieren, um nach einer bedeutenden Cyberattacke eine forensische Untersuchung einzuleiten. Auf diese Weise können die Ursachen und Kontrollschwächen identifiziert und ein Massnahmenplan zur Verbesserung des Schutzes vor Cyberattacken entwickelt werden.

## Unsere Empfehlungen an Banken

Die Umsetzung des revidierten Rundschreibens stellt Banken vor zahlreiche Herausforderungen hinsichtlich des Managements von Cyberrisiken. Aufgrund unserer Erfahrung als Bilanzprüfer und Berater für Cybersicherheit empfehlen wir Folgendes:

1. Prüfen Sie Ihren aktuellen Status
   Führen Sie eine GAP-Analyse durch. Wir empfehlen Ihnen, nicht länger zu warten und eine GAP-Analyse durchzuführen. Ermitteln Sie Ihren aktuellen Status im Hinblick auf das Management des Cyberrisikos im Vergleich zu den neuen Anforderungen und Richtlinien der FINMA. Das Ziel einer solchen Analyse besteht darin, herauszufinden, welche Initiativen ergriffen werden müssen, um die Compliance sicherzustellen. Ausgehend von diesen Erkenntnissen empfehlen wir Ihnen, einen detaillierten Plan zu entwickeln, der auch die Priorisierung der verschiedenen Projekte sowie Zeitpläne enthält. Damit dieser Massnahmenplan von allen Interessenvertretern unterstützt wird, ist es empfehlenswert, den Plan der Geschäftsleitung und dem Verwaltungsrat zur Genehmigung vorzulegen.
2. Überwachungswerkzeuge und Lösungen für das Management von Vorfällen
   Unterschätzen Sie nicht die Komplexität und die Betriebskosten, die durch die Verbesserung der Überwachungssysteme anfallen. Banken sollten Implementierungswerkzeuge in Betracht ziehen, mit denen sie ihre Infrastruktur überwachen können (um insbesondere Anomalien in Datenflüssen festzustellen). Um

[2] Im November 2015 ersuchte die FINMA Banken der Aufsichtskategorie 3, einen Selbstbewertungsfragebogen auszufüllen, um ihre Fähigkeit zur Bekämpfung von Cyberrisiken zu beurteilen. Von den Banken, die am Schweizer Finanzmarkt tätig sind, haben 27 bis Ende Januar 2016 ihre Selbstbeurteilung eingereicht. Ende August 2016 teilte die FINMA die anonymen Ergebnisse sowie deren Analyse allen Schweizer Banken mit. ((Kleinere Schrift))

effektive, zentralisierte Sicherheitswarnungen zu garantieren, empfehlen wir die Einführung eines zentralen Sicherheitsinformations- und Ereignismanagements (Security Information and Event Management, SIEM) oder eines Zentrums für EDV-Sicherheit (Security Operations Center, SOC). Wir empfehlen jedoch dringend, die Konfigurations-, Instandhaltungs- und Betriebskosten solcher Instrumente vor deren Implementierung zu analysieren. Wir haben oft festgestellt, dass die für die Parametrisierung solcher Lösungen und die Verwaltung der Protokolle/Warnungen notwendigen Ressourcen und Kompetenzen nicht bereitgestellt wurden und deshalb der «angestrebte» Nutzen der Lösungen nicht realisiert werden konnte.

3. Threat-Intelligence: Wählen Sie eine Lösung, die der Grösse Ihrer Bank angepasst ist
   Wir empfehlen Ihnen, Threat-Intelligence-Dienstleistungen in Anspruch zu nehmen, die Ihnen dabei helfen, Bedrohungen frühzeitig zu erkennen und Ihr Unternehmen proaktiv zu schützen, indem sie das Risiko von Cyberattacken mindern. Je nach der Grösse Ihres Unternehmens können solche Lösungen (Preise können stark variieren) durch regelmässige Berichte von Threat-Intelligence-Spezialisten ersetzt werden. Es handelt sich hier um eine pragmatische Alternative, die Ihnen ein Mindestmass an Compliance garantiert.
4. Zusammensetzung Ihres Sicherheitsrahmens: Verwenden Sie einen risikobasierten Ansatz für Informations- und Cybersicherheit
   Seit 2015 haben die meisten Schweizer Banken ihren eigenen Massnahmenrahmen umgesetzt, um die Vertraulichkeit ihrer Kundendaten zu sichern (in Übereinstimmung mit FINMA-Rundschreiben 2008/21, Anhang 3, über den Umgang mit elektronischen Kundenidentifikationsdaten). Die eingeführten Massnahmen ermöglichten es ihnen vor allem, das Risiko von Datenverlusten zu verringern. Die neuen Anforderungen der FINMA bedeuten, dass die Banken nun eine geeignete Antwort finden müssen, um sich vor Cyberattacken zu schützen. In diesem Zusammenhang ist es sehr wichtig, einen konsequenten risikobasierten Ansatz für die Informations- und Cybersicherheit umzusetzen und zu verbreiten.

## Wie PwC helfen kann

Dank unserer branchenübergreifenden Erfahrungen sind wir bestens positioniert, um unseren Kunden bei der Anpassung an das sich ändernde regulatorische Umfeld zu helfen. Wir haben eine Reihe von Dienstleistungen entwickelt, um Ihnen zu helfen, die regulatorischen Herausforderungen zu bewältigen. Diese sind unter anderem:

- GAP-Analyse
  Wir haben eine umfassende Methodik entwickelt, die speziell erstellt wurde, um Ihre Vorbereitung auf Cyberattacken und den Reifegrad Ihrer Cyberfunktionen zu bewerten und Lücken im Hinblick auf die FINMA-Anforderungen zu ermitteln. Unsere bewährten, praxiserprobten GAP-Analyse-Vorlagen umfassen mehr als 50 Kontrollen, die in folgende sechs Bereiche eingeteilt werden: Strategie, Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung.
- Definition einer Compliance-Roadmap und Überwachung der Umsetzung des Massnahmenplans
  Wir haben bereits zahlreiche Kunden dabei unterstützt, Compliancemassnahmenpläne zu definieren. Solche Pläne umfassen typischerweise: identifizierte GAPs; die dazugehörigen regulatorischen Anforderungen; die Aufstellung der Massnahmen, die zur Überbrückung der identifizierten Lücken zu treffen sind; vorgeschlagene Fachverantwortliche und betroffene Interessenvertreter; vorgeschlagene Zeitplanung und Kostenschätzung. Eine der zentralen Herausforderungen, denen sich Unternehmen bei Veränderungen von regulatorischen Complianceprogrammen gegenübersehen, ist der Umgang mit der Komplexität, den Interdependenzen und der Sequenzierung von Massnahmen. Um diese Herausforderung effektiv zu bewältigen, haben wir einfach zu verwendende Projektmanagementvorlagen entwickelt, die eigens für diese Bewertung bestimmt sind (z.B. Projektstatus- oder detaillierter Fortschrittsbericht).

- Unterstützung bei der Umsetzung von Compliancemassnahmen
  Wir haben eine hohe Kompetenz in der Beratung unserer Kunden in Bezug auf Compliancestrategien, Überprüfungen und Sicherheit entwickelt. Indem wir unser Netzwerk von Cyberspezialisten mobilisieren, können wir bei der Implementierung vieler verschiedener Massnahmen helfen, um die Einhaltung der FINMA-Anforderungen zu erreichen: z.B. Ausarbeitung Ihrer Managementstrategie bzw. -politik für das Cyberrisiko; Due-Diligence-Bewertungen von Drittparteien hinsichtlich des Managements des Cyberrisikos; Prüfung Ihrer Schutzfähigkeit gegenüber Cyberbedrohungen; Prüfung Ihrer Kompetenzen, Cyberbedrohungen zu erkennen; oder Festlegung Ihrer Reaktion auf Cyberattacken und des Wiederherstellungsprozesses.

Es folgen noch einige andere Dienstleistungen aus unserem Serviceangebot, die auf Ihrem Weg zur Einhaltung von FINMA-Anforderungen von Interesse sein könnten:

- Threat-Intelligence-Dienstleistungen
  Unser spezialisiertes Cyberabwehrteam besteht aus handverlesenen Analysten mit Erfahrung in Netzwerkabwehr und Nachrichtendiensten. Unser Dienstleistungsangebot ermöglicht einen pro aktiven Schutz vor dem Unternehmensrisiko gezielter Angriffe und umfasst: Threat-Intelligence-Berichterstattung: wertvolle Einblicke in Sektoren und Ziele, Bedrohungsprofile für Sektoren, taktische und strategische Mitteilungen usw. Informationsströme (Feeds) und Zusammenarbeit: Austausch von Threat-Intelligence und Informationen in Echtzeit mit anderen Unternehmen, zu Fixkosten; zielgerichtete Recherchen: personalisierte Threat-Intelligence für Ihr Unternehmen, Recherchen auf der «dunklen Seite» nach unmittelbaren Bedrohungen oder Attacken usw. Consulting: interner Datenverkauf, Optimierung der Datenentwicklung, Analytiker eingebetteter Intelligenz usw.
- Cyberrisikobewertung
  Wir verfügen über grosse Erfahrung in der Unterstützung unserer Kunden, ihre Cyberrisiken zu bewerten. Wir können Ihnen helfen, Ihre Cyberrisiken zu identifizieren, zu analysieren, zu bewerten und zu priorisieren. Insbesondere haben wir ein automatisiertes Instrument entwickelt, das es Ihnen ermöglicht, die Ergebnisse Ihrer Cyberrisikobewertung in einer dynamischen Matrix darzustellen.
- Dienstleistungen zur Sicherheitsbewertung
  Unsere Dienstleistungen umfassen Schwachstellenanalysen und Penetrationstests. Wir können unsere globale Methodologie und massgeschneiderte Softwareprodukte wirksam einsetzen, um sie dem Kontext Ihres Unternehmens anzupassen und derzeit vorhandene Schwachstellen in Ihrem Umfeld zu identifizieren. Für unsere Penetrationstests verwenden wir für jede Kundensituation einen eigenen Ansatz, um realistische Tests durchzuführen. So bestimmen wir, wie sich ein Ausnutzen der identifizierten Schwachstellen und Konfigurationsfehler auf Ihr Geschäft auswirken könnte.

## Kontakte


**Reto Haeni**
Partner und Leiter Cybersicherheit, PwC Digital Services
+41 79 345 01 24
reto.haeni@ch.pwc.com

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

**Nicolas Vernaz**
Leiter Cyberdatenschutz und Erfüllung gesetzlicher Auflagen, PwC Digital Services
+41 79 419 43 30
nicolas.vernaz@ch.pwc.com