FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Cyberrisiken

Institutsspezifische Ausbildung auf Stufe Verwaltungsrat

Zürich, Dezember 2017

Dr. Eugen Haltiner,
vormals Verwaltungsratspräsident FINMA

Daniela Stehli-Wiederkehr
Inhaberin und Geschäftsführerin Fachschule für Bankwirtschaft AG

Grobkonzept

Workshop Stufe Verwaltungsrat: Cyberrisiken

Zielsetzungen

- Beantwortung relevanter Fragestellungen auf Stufe Verwaltungsrat
- Vermittlung der Ausgangslage:
  - FINMA-RS 2008/2: Änderungen gültig seit 1. Juli 2017
  - Umgesetzte Massnahmen und Prüfungsergebnisse
- Aufzeigen möglicher Bedrohungsszenarien und Risiken
- Ermittlung Handlungsbedarf für weitere Schutzmassnahmen

Methodik

- Wissensvermittlung mittels Fachbeiträgen und Erfahrungsaustausch
- Fallstudie zur Ermittlung eines möglichen Handlungsbedarfs

Ablauf

Workshop Stufe Verwaltungsrat: Cyberrisiken

Ablauf der Tagung

▪ Einleitung	VRP/CEO	15`
▪ Ausgangslage		
▪ Aufsichtsrechtliche Bestimmungen	Eugen Haltiner	15`
▪ Erfahrungen Bank, Prüfungsergebnisse	Bankvertreter	15`
▪ Umgesetzte Massnahmen und Ausblick	Bankvertreter	15`
▪ Cyber Attacken und Bedrohungsszenarien	Externer Referent	45`
▪ Fragestellungen «what if …»	Verwaltungsrat	45`
▪ Präsentation und Schlussfolgerungen	Verwaltungsrat	45`
		Total 210`

Cyberrisiken

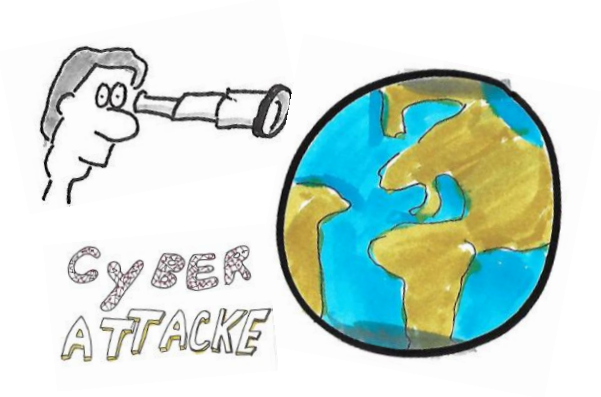
Ablauf: Institutsspezifische Ausbildung auf Stufe Verwaltungsrat

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Grobkonzept

Institutsspezifische Ausbildung auf Stufe Verwaltungsrat

finma



Risikomanagement-Konzept für den Umgang mit Cyberrisiken

- Neue regulatorische Vorgaben
  - Verwundbarkeitsanalysen
  - Penetration Testing
- Bisher umgesetzte Massnahmen

Prüfberichte

- Interne Prüfberichte
- Externe Prüfberichte

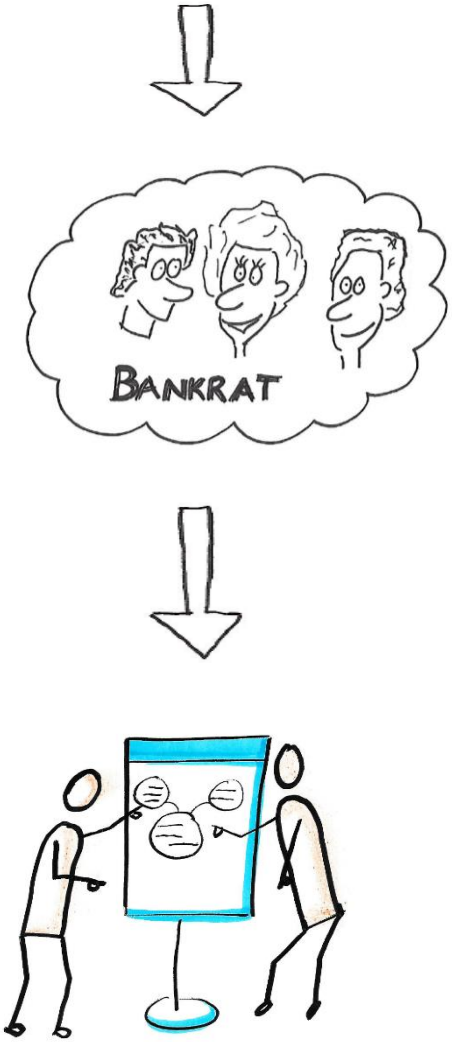
Umweltanalyse Externer Referent

- Bedrohungsszenarien
- Cyberattacken

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Grobkonzept

Institutsspezifische Ausbildung auf Stufe Verwaltungsrat



Fragestellungen und Fallstudien

- Eintretenswahrscheinlichkeit und Gefährlichkeit verschiedener Szenarien?
- Schutzwirkung bisher getroffener Vorkehrungen?
- Führungsorganisation?

Präsentationen und Schlussfolgerungen

- Handlungsbedarf
- Ziele und Massnahmen

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Cyberrisiken

FINMA-RS 2008/21Rundschreiben «Operationelle Risiken Banken» (mit Änderungen in Kraft ab 1.Juli 2017)

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

FINMA-RS 2008/21 Rundschreiben «Operationelle Risiken Banken» (mit Änderungen in Kraft seit 1.Juli 2017)

Randziffer 135.6 – 135.12

- Die Geschäftsleitung hat zudem ein Risikomanagement-Konzept für den Umgang mit Cyber-Risiken zu implementieren. Dieses Konzept hat mindestens die folgenden Aspekte abzudecken und eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Festlegung von Aufgaben, Rollen und Verantwortlichkeiten zu gewährleisten:
  - a. Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme,
  - b. Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IT-Systeme,
  - c. Zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis eines Prozesses zur systematischen Überwachung der Technologie-infrastruktur,

FINMA-RS 2008/21Rundschreiben «Operationelle Risiken Banken» (mit Änderungen in Kraft ab 1.Juli 2017)

- d. Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacken in Abstimmung mit dem BCM,
- e. Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen.

- Die Geschäftsleitung lässt zum Schutz der kritischen und/oder sensitiven Daten und IT-Systemen vor Cyber-Attacken regelmässig Verwundbarkeitsanalysen (Analyse zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken) und Penetration Testings (Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der Technologie-infrastruktur, um unberechtigten Zugang zu dieser Technologieinfrastruktur zu erhalten) durchführen. Diese müssen durch qualifiziertes Personal mit angemessenen Ressourcen durchgeführt werden.

Cyberrisiken

Umweltanalyse

Fragestellungen und Schlussfolgerungen

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Umweltanalyse und Fragestellungen

1. **Umweltanalyse**
   Externer Referent, z. B. Vertreter Bund, Swisscom oder IT-Security-Firma

2. **Konkrete Fragestellungen an den Verwaltungsrat (Beispiele)**
   - Verunstaltung Website einer Bank
   - Website gehackt und Kundendaten gestohlen
   - DDoS-Attacke mit Erpressung
   - E-Banking-Trojaner gegen Kunden der Bank
   - Verschlüsselungs-Trojaner gegen die Bank
   - Gezielte Spionage-Angriff (APT) gegen die Bank

Präsentationen und Schlussfolgerungen

3. **Gruppenarbeit mit anschliessender Präsentation**
   - Wie hoch schätzen Sie die Eintretenswahrscheinlichkeit und die Gefährlichkeit der Szenarien für die Bank ein? Welche Risiken sind damit verbunden?
   - Wer löst bei Eintritt eines solchen Ereignisses welche Massnahmen aus (Führungsorganisation)?
   - Sind vorsorgliche Schutzmassnahmen zu treffen? Versicherbarkeit?
   - Juristische Abklärungen (Involvierung Rechtsdienst, Polizei und Strafbehörde)

4. **Handlungsbedarf, Ziele und Massnahmen**
   1. …
   2. …

FSB
FACHSCHULE FÜR BANKWIRTSCHAFT

Wir freuen uns auf Ihre Kontaktaufnahme.

Fachschule für Bankwirtschaft AG
Waffenplatzstrasse 64
CH-8002 Zürich

T +41 44 433 14 84
M +41 79 351 90 00
dstehli@fsbz.ch | www.fsbz.ch