Cyber Maturity Assessment (CMA) für Banken

Laut den Aufsichtsbehörden im In- und Ausland stellen Cyberattacken auf Finanzunternehmen ein aufkommendes Risiko für die Finanzstabilität ihrer Länder dar. Um die statutarischen und aufsichtsrechtlichen Ziele zu erfüllen, müssen diese Behörden die Cyber-Sicherheit und Abwehrmechanismen des Finanzsektors besser verstehen. Hierzu haben verschiedene Aufsichtsbehörden Assessments bei Banken durchgeführt.

Was ist CMA für Banken?

CMA für Banken ist ein Tool, das vom Information Protection & Business Resilience Team der KPMG entworfen wurde. Es vermittelt einen Überblick über die Bereitschaft der Banken, auf Cyberattacken zu reagieren.

CMA für Banken geht auf sechs Schlüsselbereiche ein, die in kürzester Zeit und auf fünf Reifegrad-Stufen einen umfassenden und ausführlichen Einblick in die Cyber-Sicherheit eines Unternehmens geben.

Die sechs Schlüsselbereiche, die mit dem CMA-Tool für Banken behandelt werden, sind:

- Leadership and Governance
- Human Factors
- Information Risk Management
- Business Continuity
- Operations and Technology
- Legal and Compliance

Welche Vorteile bringt CMA für Banken?

Die von KPMG entworfene CMA für Banken soll CxOs/CISOs dabei unterstützen, entweder ein umfassendes neues Konzept zu erstellen oder den Fortschritt eines bereits existierenden Konzepts mit klaren Meilensteinen zu überwachen. Die drei Hauptziele im Bereich IT-Sicherheit sind wie folgt:

1. Einbettung einer IT-Risikomanagement Kultur:

- Daten sollen als wichtiges Kapital behandelt werden, sowohl in der eigenen Unternehmenskultur als auch in jener der Dienstleister und Drittanbieter des Unternehmens.
- Rechenschaftspflicht für die Risikolage von Informationen auf Verwaltungsratsebene.
- Risikoauswirkungen auf Shared Services werden so behandelt, wie in den Vereinbarungen mit diesen externen Dienstleistern festgelegt.

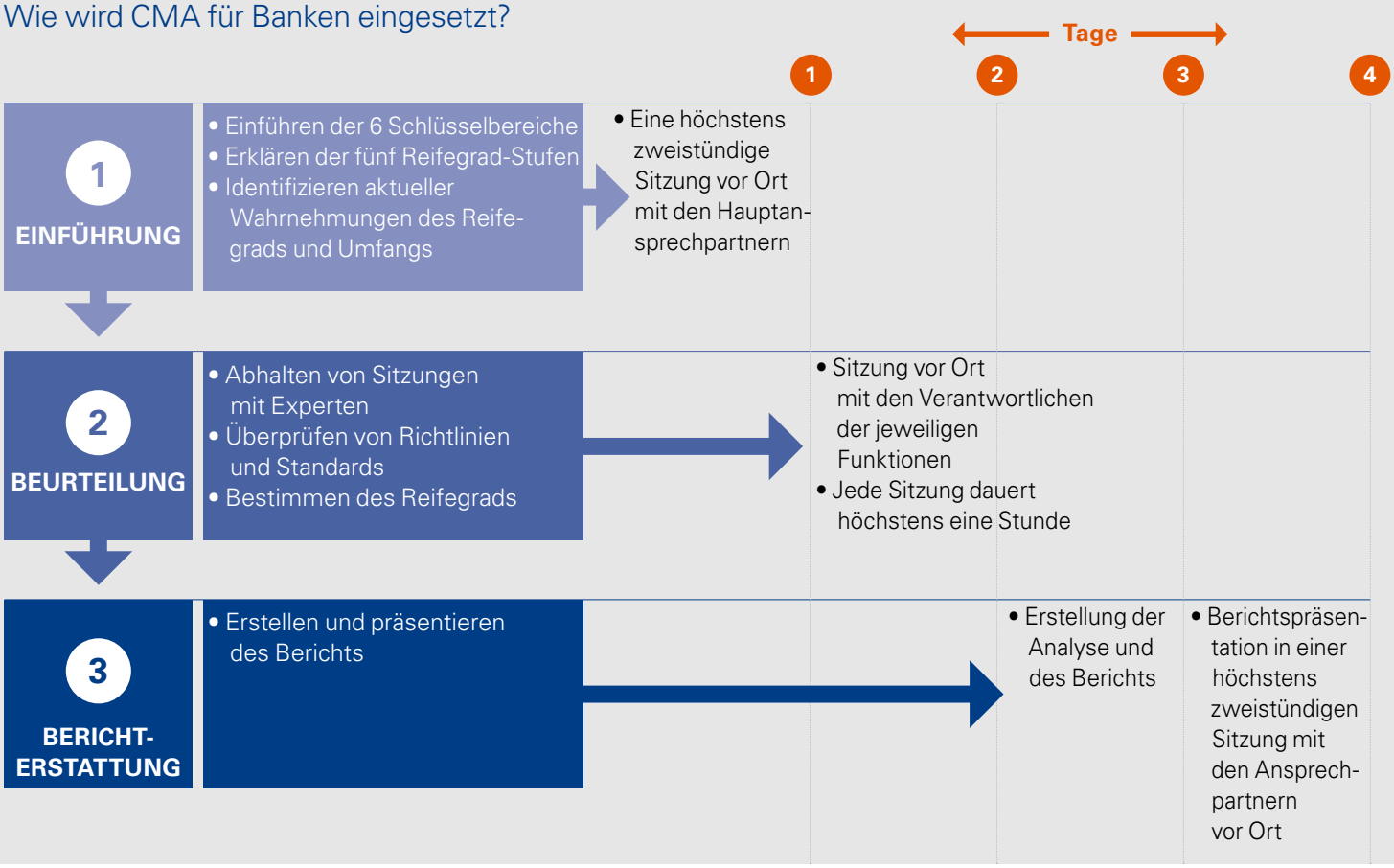
2. Umsetzung optimaler Verfahren zur Informationssicherung:

- Dienstleister und sonstige Drittanbieter setzen allumfassende Verfahren zur Informationssicherung ein.
- Eine systematische Überwachung von Netzwerken, Systemen und Schnittstellen erlaubt es, Gefahren besser zu erkennen und entsprechende Gegenmassnahmen zu treffen.

3. Wirksame Compliance

- Zur Einhaltung von rechtlichen Anforderungen seitens des Unternehmens muss eine wirksame Compliance eingesetzt werden.
- Die Einhaltung wird durch voneinander unabhängige interne und externe Überprüfungen nachgewiesen.

Wie wird CMA für Banken eingesetzt?



Der Beurteilungsprozess besteht aus drei einfachen Schritten, die z.T. vor Ort ausgetragen werden.

- Transparenz und die Einbindung von Fachwissen sind der Schlüssel zu einer erfolgreichen Beurteilung.
- Es handelt sich hierbei nicht um eine Prüfung, sondern um eine schnelle Beurteilung der sechs Schlüsselbereiche, um die Ausgereiftheit jedes Bereichs zu identifizieren. Auf diese Weise sollen Sicherheitslücken und verbesserungswürdige Bereiche erkannt werden, um schliesslich für jeden Bereich den gewünschten Reifegrad zu erreichen.
- Um Informationen über jeden der Bereiche sammeln zu können, sind Sitzungen mit den Verantwortlichen jeder der in der folgenden Tabelle genannten Funktionen nötig. Jede Sitzung dauert höchstens eine Stunde.

Funktion	Rolle	Wichtigste Aufgaben
HR	Leitung HR oder vergleichbare Rolle	• Sicherheitsschulung und -bewusstsein • Sicherheitskultur • Talentmanagement: Fachkenntnisse im Bereich IT-Sicherheit
IT	Leitung IT oder vergleichbare Rolle	• Verwaltung der Identitäten und Zugriffsrechte • Begrenzung von Bedrohungen und Schwachstellen • Sicherheit im Bereich der Netzwerke und Applikationen
Interne Prüfung	Leitung interne Prüfung oder vergleichbare Rolle	• Prüfungsrahmen im Bereich IT-Sicherheit • Überwachung der Feststellungen und deren Behebung
Risikomanagement	Leitung Risikomanagement oder vergleichbare Rolle	• IT-Risikomanagement • Outsourcing Dienstleistern • Business Continuity
Recht	Leitung Recht oder vergleichbare Rolle	• Three lines of defense • Transfer finanzieller Risiken • Gesetzeskonformität

Kontakt:

KPMG AG
Badenerstrasse 172
Postfach 1872
CH-8026 Zürich

Matthias Bossardt
Partner, IT Advisory
T: +41 58 249 36 98
E: mbossardt@kpmg.com

Gerben Schreurs
Partner, Forensic
T: +41 58 249 48 29
E: gschreurs1@kpmg.com

Jean Paul Ballerini
Senior Manager, IT Advisory
T: +41 58 249 55 64
E: jballerini@kpmg.com

Roman Haltinner
Senior Manager, IT Advisory
T: +41 58 249 42 56
E: : rhaltinneri@kpmg.com