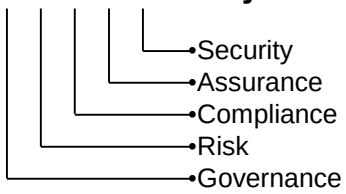
Aduno Group
the smart way to pay

Recent developments in technology regulation

Rainer Kessler, IT & Operations GRCAS Project Manager



Overview

- Background and the global dimension
- Local example: operational risk and technology regulation
- Important further developments
- Excerpt of some key questions in the tech. regulation context
- Q & A

Background and the global dimension

BANK FOR INTERNATIONAL SETTLEMENTS

http://www.bis.org/publ/bcbs223.pdf

Internal Audit http://www.bis.org/publ/bcbs292.pdf

Three Lines of Defense

Operational Risk

Line of defence	Examples	Approach
First line	Front Office, any client-facing activity	Transaction-based, ongoing
Second line	Risk Management, Compliance, Legal, Human Resources, Finance, Operations, and Technology	Risk-based, ongoing or periodic
Third line	Internal Audit	Risk-based, periodic

MAS Monetary Authority of Singapore

Key Resources

- TRM Guidelines
  Download PDF(497.42 KB)
- Checklist for TRM Guidelines
  Download XLSM(114.76 KB)
- Response to Public Feedback for Consultation Paper - TRM Guidelines
  Download PDF(514.06 KB)
- Instructions on Incident Notification and Reporting to MAS
  Download PDF(264.76 KB)
- Incident Report Template
  Download DOCX(45.29 KB)
- FAQs - Notice on TRM
  Download PDF(403.80 KB)
- Response to Public Feedback for Consultation Paper - Notice on TRM
  Download PDF(481.81 KB)

Public Law 107–204
107th Congress

An Act

To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

July 30, 2002
[H.R. 3763]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Sarbanes-Oxley Act of 2002".

Sarbanes-Oxley Act of 2002. Corporate responsibility. 15 USC 7201 note.

	Internal facing	External facing
Secret	Special regime on the level of 2FA	Special regime additional to 2FA
Confidential	1FA	2FA
Internal	1FA	Will be 2FA for practicality reasin, not because of security req.
Public	1FA	1FA

Cf. important further developments…

NIST-Level 3 versus NIST-Level 4

MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: E-Authentication Guidance for Federal Agencies

NIST National Institute of Standards and Technology

U.S. Department of Commerce

Aduno Group
the smart way to pay

Local example: operational risk and technology regulation

finma
Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA-Circ. 08/21	20.11.08 (amended 27.03.14)	Operational risks at banks	Capital adequacy requirements for operational risks within the banking sector

Allegato 1

Classificazione degli ambiti di attività conformemente all'art. 93 cpv. 2 OFoP

Allegato 2

Panoramica della catalogazione dei tipi di eventi

Allegato 3

Trattamento dei dati elettronici dei clienti

FINMA-Circ. 08/7	20.11.08 (amended 06.12.12)	Outsourcing – banks

III. Informationstechnologiesysteme und Unterhalt

- Datenaufbewahrung
- Betrieb und Unterhalt von Datenbanken
- Betrieb von Informationstechnologie-Systemen
  - Ausarbeitung eines Informationstechnologie-Projektes zur anschliessenden Integration in den Betrieb der Bank
  - Auftrag zur Software-Entwicklung
  - Erwerb von Software-Lizenzen
  - Support von Software
  - Wartung technischer Geräte, von Systemen (Informationstechnologie usw.) und von Software

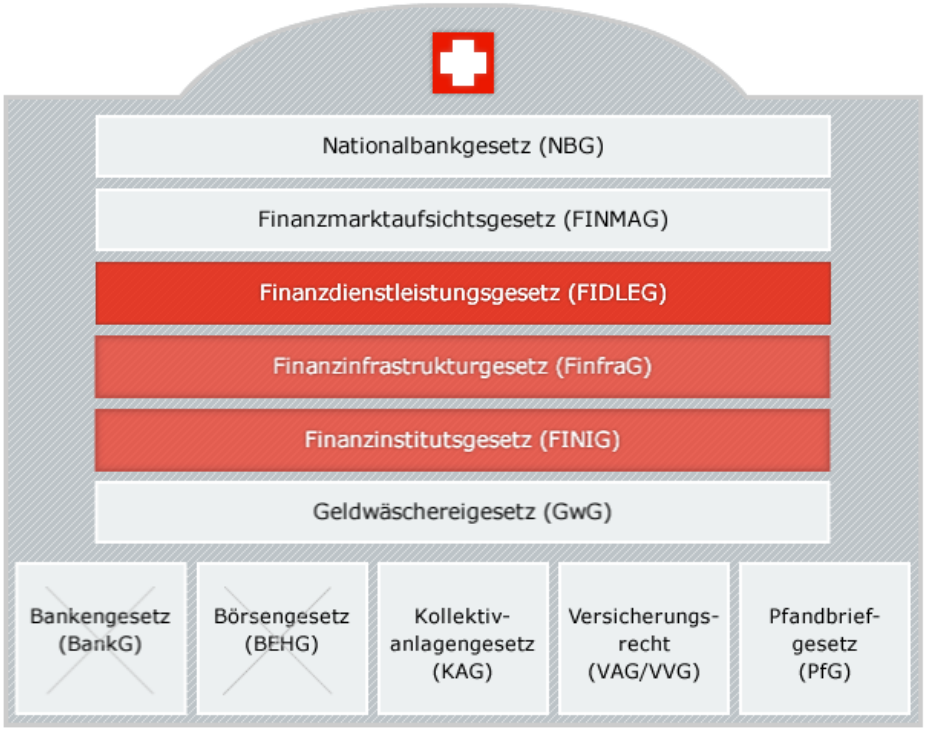
▪ ▪ ▪

FINMA-Circ. 08/10	20.11.08 (amended 03.12.14)	Self-regulation as a minimum standard	Self-regulation recognised as a minimum standard by the Swiss Financial Market Supervisory Authority

Recommendations for Business Continuity Management (BCM) of August 2013: limited to subsections 4.4 "Business Continuity Management Strategie", 4.5.1 "Business Impact Analysis" and 4.5.2 "Business Recovery Options 7

Aduno Group
the smart way to pay

Important further developments



Aduno Group
the smart way to pay

Excerpt of some key questions in the tech. regulation context

1. When is data considered “identifying”?
2. What level of anonymization is enough?
3. How to document clients’ agreements for cross-border data processing (e.g., opt-in vs. opt-out)?
4. How to treat persons with different relationships to a company (e.g., employee vs. client or supplier vs. client)?
5. How to provide global services to a local (bank) client?
6. How to respect different cultures regarding data protection or information security?
7. When (by what criteria) starts a supplier or business-partner relationship to become an outsourcing relationship?
8. How to react to clients’ sometimes carless behavior with their personal data?
9. How to deal with virtualization and cloud services?
10. Which sound practice to follow, if, e.g., article 7 Swiss Data Protection Law should be combined with appendix 3 FINMA circular 2008/21?
11. How to deal with risk appetite and risk tolerance in the technology context?
12. …


R
T
Y
U
Redo
Undrln
D
Q
&
A
J
Find
C
V
B
N
Copy
Paste
Bold