



structuur

GOVERNANCE RISK *redefined*

“CYBER KRIMINALITÄT”

*...und der Umgang als
Wirtschaftsprüfer und
Berater*

Zürich, 07. November 2017

*Sonja Stirnimann
Dipl. Wirtschaftsprüferin
Internat. Executive MBA FSI HSG
Certified Fraud Examiner
Wirtschaftsmediatorin SKWM*

BACKGROUND

Audit, Finance, Risk, Economic Crime
Non-Compliance & Kommunikation

25
Jahre



Internationaler Tätigkeitsbereich

25
Jahre



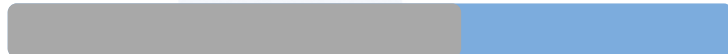
Management & Leadership

20
Jahre



Interne & externe Speakerin,
Referentin, Lehrbeauftragte

15
Jahre



Executive Coaching /
Verhandlungsführung /
Wirtschaftsmediation

15
Jahre



Sonja Stirnimann

Dipl. Wirtschaftsprüferin, zugelassene Revisionsexpertin
Internat. **Executive MBA Financial Services & Insurance** HSG
Certified Fraud Examiner (CFE)
CPCC, Co-Active **Executive Coach** (ICF und CTI)
Wirtschaftsmediatorin SKWM



AGENDA

- Relevanz
- Risiken
- Vorgehen



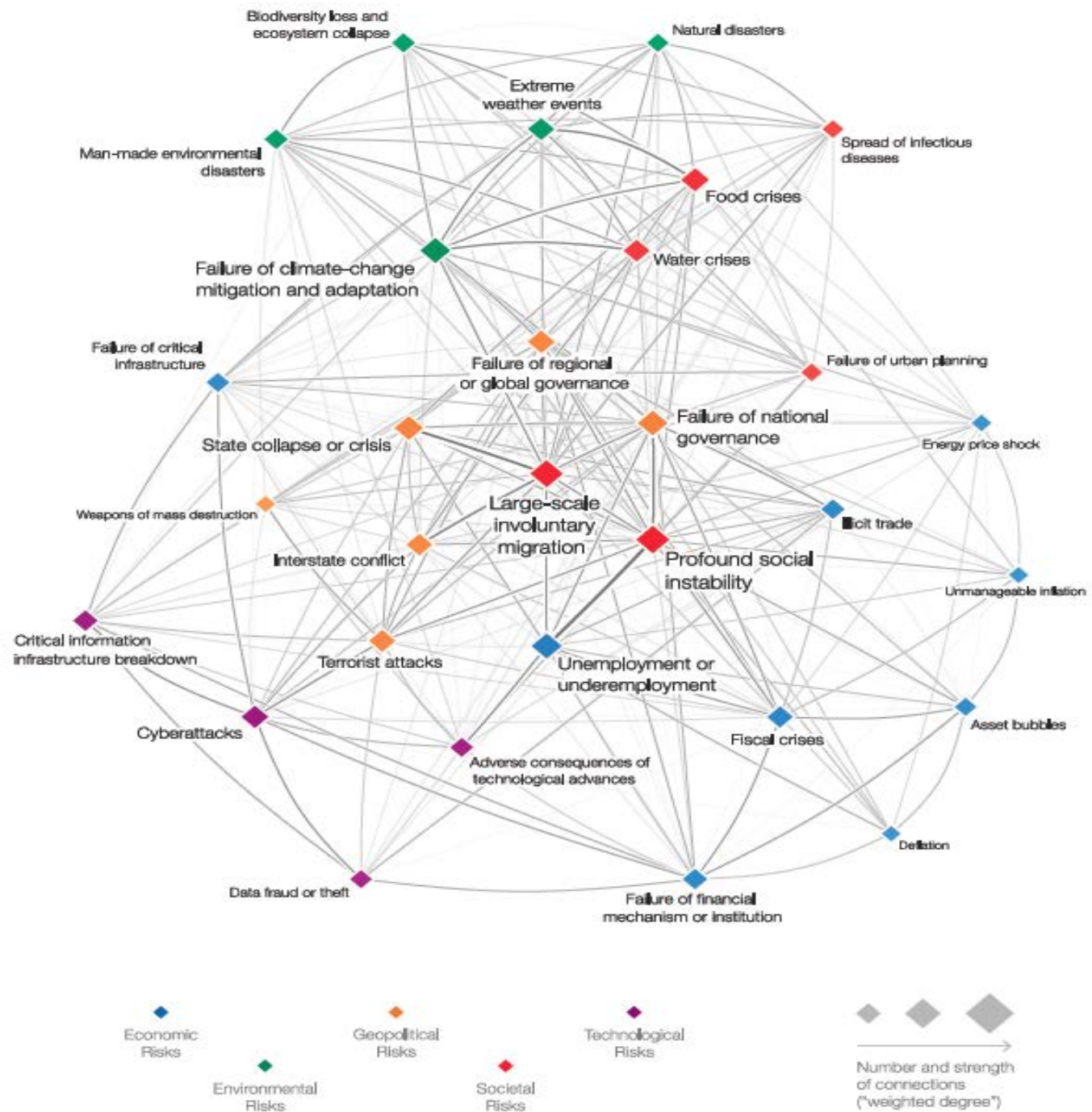
ZIEL





FAKTEN







Top 7 Risiken

Wahrscheinlichkeit

1. *Extreme Wetterereignisse*
2. *Massenhafte ungewollte Migrationsströme*
3. *Grosse Naturkatastrophen*

**4. Gross angelegte
Terroranschläge**

**5. Massiver Vorfall von
Datenbetrug/-diebstahl**

6. Cyber Attacken

7. Illegaler Handel

Auswirkung

1. *Massenvernichtungswaffen*
2. *Extreme Wetterereignisse*
3. *Wasserkrisen*
4. *Grosse Naturkatastrophen*
5. *Versagen bei der Anpassung an Klimaveränderungen*
6. *Grosse unfreiwillige Migrationsströme*
7. *Nahrungsmittelkrise*

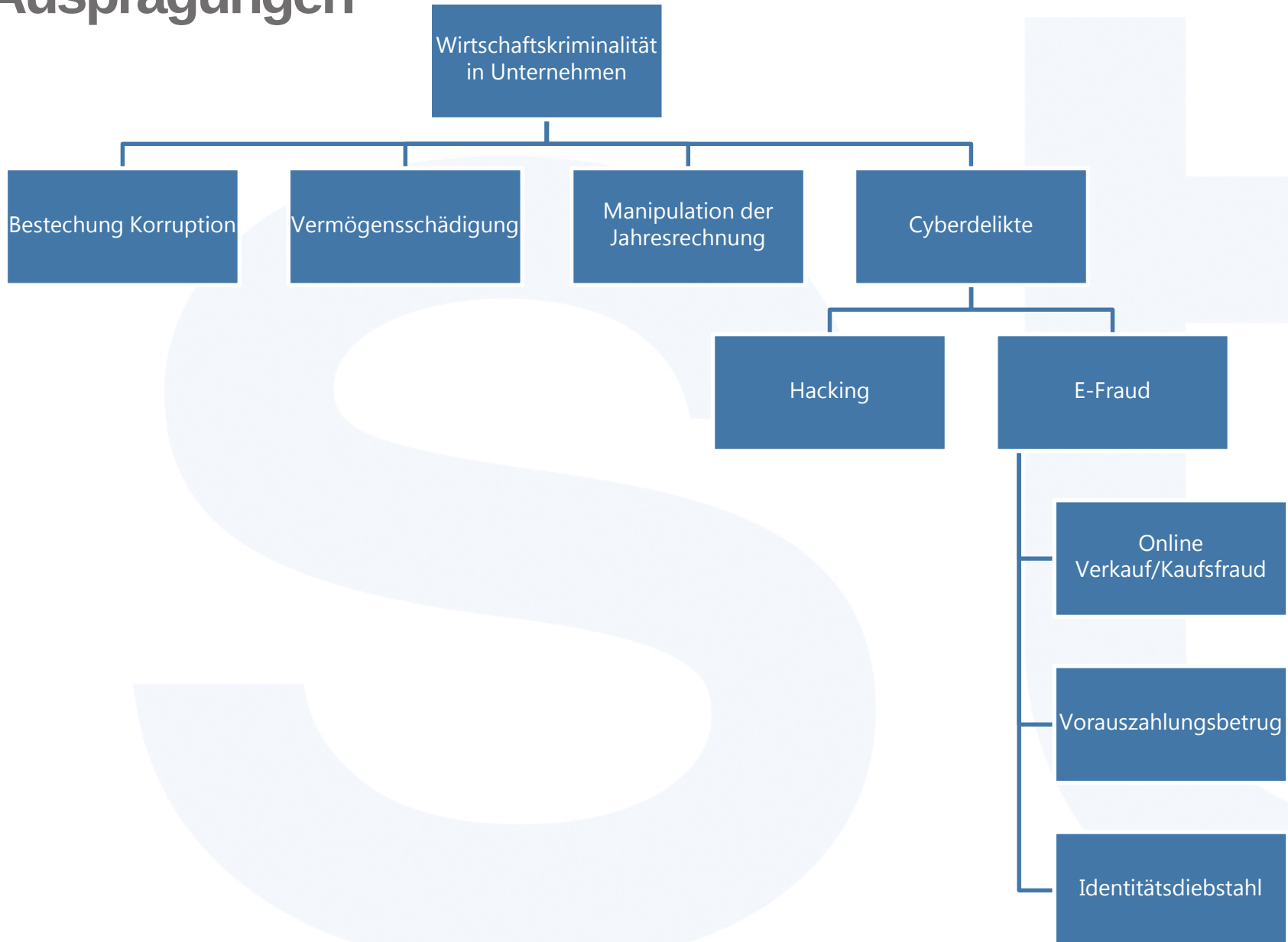


Definition

«Cyber-Risiken sind operationelle Gefahren, die von Informationen ausgehen, die auf Datenträgern und Netzwerken gespeichert sind»



Ausprägungen



Strafrechtliche Behandlung

Unrechtmässiges Verschaffen unkörperlicher Daten
(«Keylogger», «Phishing» Art. 143 StGB)

Unbefugtes Eindringen in ein
Datenverarbeitungssystem (Art. 143bis StGB)

Betrügerischer Missbrauch einer
Datenverarbeitungsanlage (Art. 147 StGB)

Betrug (Art. 146 StGB)

Veruntreuung (Art. 138 StGB)



Strafrechtliche Behandlung

Wirtschaftsspionage:

Verletzung des Fabrikations- oder
Geschäftsgeheimnisses (Art. 162 StGB)

Wirtschaftlicher Nachrichtendienst (Art. 273 StGB).



Risiko Management

Erfolgsfaktor Nr. 1: **SENSIBILISIERUNG**

- 1) Risikoidentifikation**
- 2) Prüfung von Geschäftspartnern**
- 3) Verträge mit Geschäftspartnern**
- 4) Umgang mit Restrisiken**



Haftung I

Ansprüche Dritter (Haftpflicht)

Schadenersatz infolge einer Datenschutz- oder Vertraulichkeitsverletzung & Verletzung des PCI-Datensicherheitsstandards infolge eines zielgerichteten Cyberangriffs = Rechtsverletzung durch digitale Kommunikation

Deckung Abwehrkosten

Vertragsstrafen



Haftung II

Eigenschaden

«Mögliche unbeschränkte und persönlich Haftung
des Leitungsorgans mit dessen gesamten
Privatvermögen»



Verantwortung

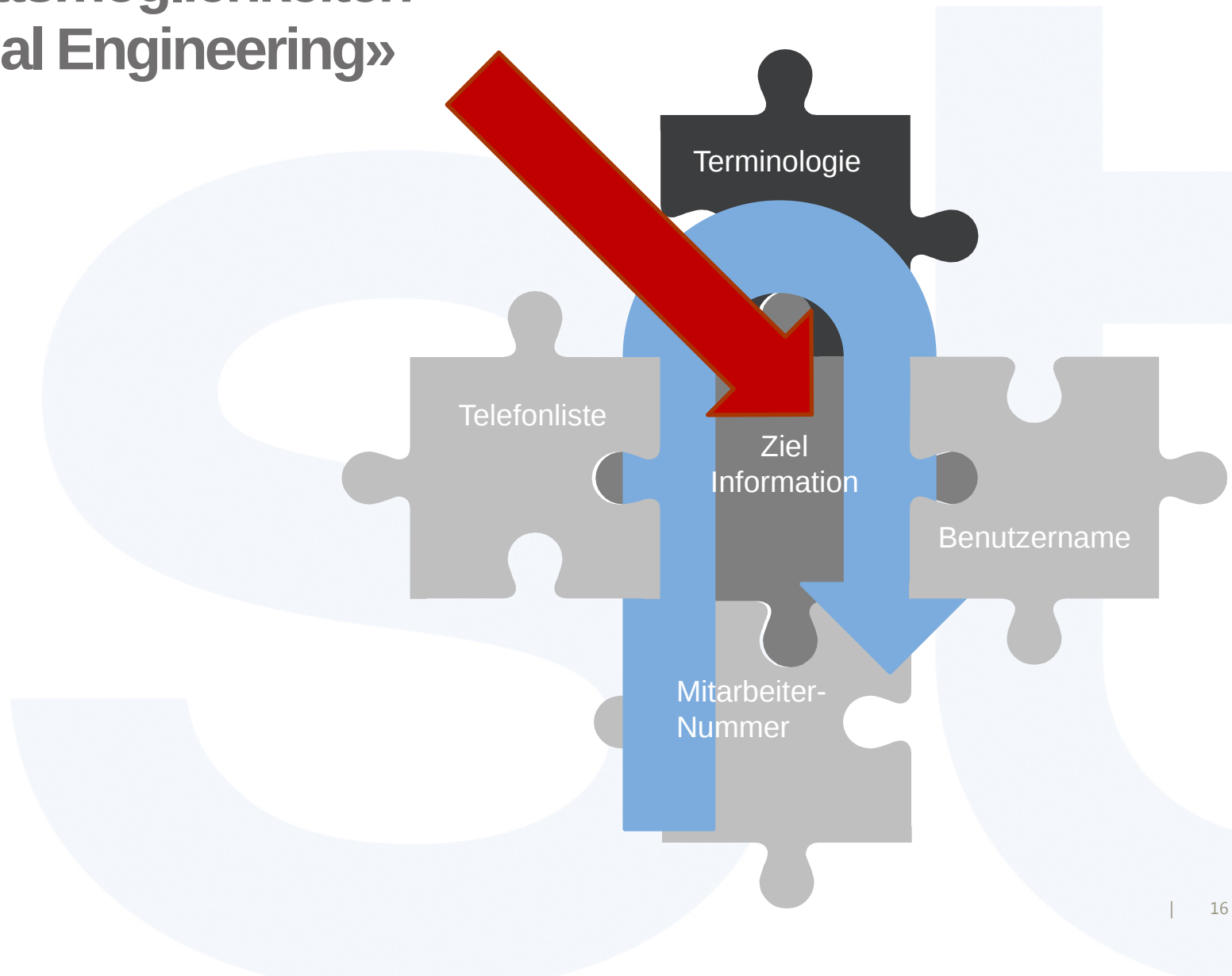
Oberste Leitungsorgane

Die Pflicht des Verwaltungsrates zur Erfassung, Beurteilung und Bewältigung von geschäftlichen Risiken ergibt sich aus seiner Aufsichts- und Strategiekompetenz gemäss Art. 716a Abs. 1 OR.

Gemäss Art. 754 Abs. 1 OR, sind die Organe «für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen»



Eintrittsmöglichkeiten «Social Engineering»





Handlungsfähigkeit I

FraudAidKit™



Die individuelle,
unternehmensspezifische
Anleitung zur
Ereignisbewältigung im Ernstfall
inklusive **Sofortmassnahmen**,
Anleitung zur **Kommunikation**,
Sachverhaltsaufarbeitung sowie
vor- und nachgelagerte
Schulungen für Verantwortliche
und deren Teams.



Handlungsfähigkeit II

FraudAidKit™ Prozess

```
graph LR; A[Sensibilisierung Awareness] --> B[Implementierung Tools]; B --> C[«Run the firm» Unterhalt Maintenance]; C --> D[Alarmierung Help]; D --> E[Abwicklung Support];
```

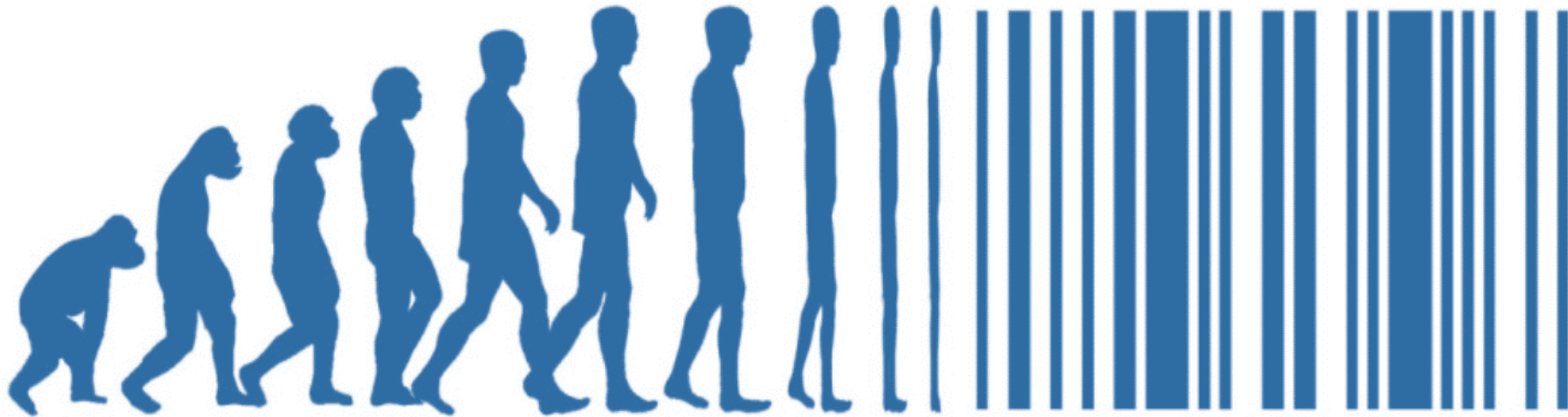
Sensibilisierung
Awareness

Implementierung
Tools

«Run the firm»
Unterhalt
Maintenance

Alarmierung
Help

Abwicklung
Support



Verhalten = Anpassungsprozess an Bedingungen



«Food for thoughts»

- a) Gibt es ein Notfallszenario für wirtschaftskriminelle Ereignisse, Non-Compliance und Cyber-Angriffe?
- b) Wann wurde dieses Szenario zum letzten Mal getestet?
- c) Kennen Sie die Experten welche Sie in solchen Ereignissen unterstützen können?
- d) Wurde ihre Risikolandschaft auf die aktuellen Entwicklungen überprüft?

«Food for thoughts»

Was ist zu tun?

Bis wann?

Wichtige Adressen

Ihre Experten im Ereignisfall:

www.melani.admin.ch

[https://www.fedpol.admin.ch/fedpol/de/
home/kriminalitaet/cybercrime.html](https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime.html)

ZIEL
ERREICHT?



Handlungsfähig

Sensibilisiert

Angeregt

structuul

GOVERNANCE RISK *redefined*

*Structuul unterstützt natürliche Personen und Unternehmen bei der Beantwortung sensibler Fragestellungen und während Krisen in den Bereichen **Governance, Risk & Compliance und Kommunikation**.*

Sie ist spezialisiert auf die Prävention und Aufarbeitung von Krisensituationen, Wirtschaftskriminalität und Non-Compliance im nationalen und internationalen Umfeld.

Structuul AG
+41 41 511 21 71
www.structuul.ch