Swiss Risk Association

3rd-Party Risks
How to manage and define risk appetite?

Zoom Online Meeting
16th March 2021

Speakers

- **Dr. Fedor-Immanuel Rahn**, Senior Manager, zeb
- **Bastian Bahnemann**, Security Assurances Lead FSI DACH, Amazon Web Services
- **Ralf Schüssler**, SRC Regulatory Lead-CH & Tax Governance, Credit Suisse

Swiss Risk Association

Presentation 1 – zeb consultancy

1. What is the general understanding of third-party risks?

2. How can financial institutions deal with them?

3. How can risk appetite be defined or limited?

1 What is the general understanding of third-party risks (1/3)?

Attempt of a definition

Third-party risks are any risks that may arise from the purchase of services by an external party, and which may (negatively) affect institutions in...

1. Compliance with legal or regulatory requirements
2. The soundness or continuity of their banking and payment services
3. Their financial performance or stability

Third-party risks are part of the operational risks and arise in addition solely due to the involvement of a party outside the institution's own organization

1 What is the general understanding of third-party risks (2/3)?

FINMA

FINMA Circular 2018/3, margin nos. 16-21

- Provider-related risks
- Risks of instable service provision
- Economic risks
- Concentration of risks

EBA

EBA/GL/2019/02, margin nos. 64-73

- All risks stated above ✚
- Risks caused by processes, systems, people or external events
- ICT risks (incl. data protection)
- Sub-outsourcing risks
- Risks to lose control
- Reputational risks
- Country risks
- Legal risks
- Compliance risks
- …

Unstructured enumeration

Logical deduction on next page

Swiss Risk Association

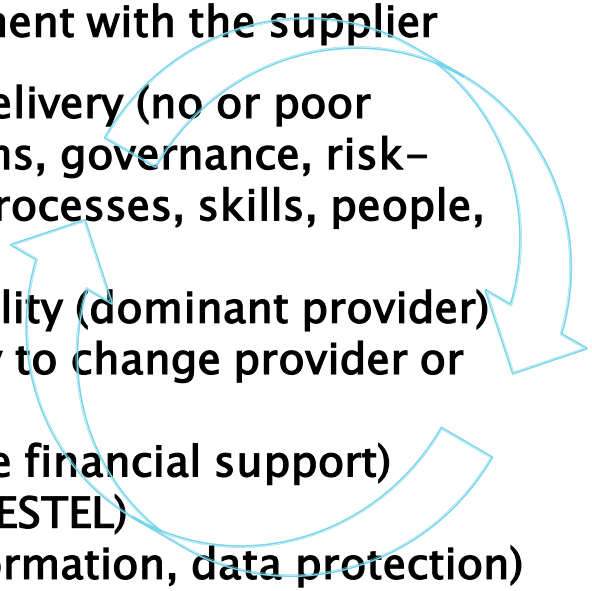
1 What is the general understanding of third-party risks (3/3)?

Process- & know-how-related risks

- Increasing complexity in process execution, operational risks of errors (i.a., interfaces)
- Potential loss of flexibility
- Potential loss of know-how, trade secrets etc.
- Increasing entanglement with the supplier

Provider-related risks

- Inadequate service delivery (no or poor performance), systems, governance, risk-management (ICS), processes, skills, people, expertise
- Reduced substitutability (dominant provider)
- Increased complexity to change provider or re-source service
- Step-in risks (provide financial support)
- Country risks (e.g., PESTEL)
- ICT risks (loss of information, data protection)
- Sub-outsourcing risks
- Reputational risks



Contractual & legal risks

- Legal risks
- Compliance risks
- Contractual risks

Internal risks

- Loss of control
- Concentration
- Accumulation

Not exhaustive, interdependencies and overlaps exist

2 How can financial institutions deal with them (1 / 1)?

Target Operating Model
Outsourcing Mgmt.

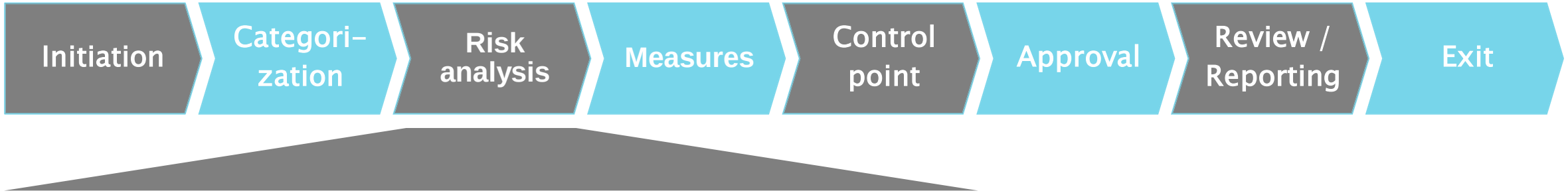
3 How can risk appetite be defined or limited (1 / 3)?

Outsourcing Strategy

- Define a strategic framework and formulate general rules (e.g., “group-outsourcing first”)
- Limit providers to those that meet regulatory requirements (e.g., from FINMA)
- Limit max. no. of contracts per provider to avoid risks of concentration
- Limit locations where provider are headquartered, provide services and store / process data
- Define which services / functions may be outsourced (e.g., internal view “degree of standardization”, “complexity” or external view “number of possible providers available”
- Establish processes which ensure compliance with the outsourcing strategy and limit decentralized decision-making authority

3 How can risk appetite be defined or limited (2/3)?

E2E process view & IT-Support



- Define a scoring model as part of the outsourcing / provider due-diligence that weights information about…
  - Provider in general (company data)
  - Service-related information of the provider (market position, no. of clients, capabilities, IT etc.)
  - Historic collaboration information
  - Outsourcing unit / function or process

Outsourcing…

0-30	Not allowed
31-50	Requires approval
51-70	Requires measures
71-80	Possible

3 How can risk appetite be defined or limited (3/3)?

Set up proper contracts

- Describe the service and its provision in detail
- Define KPIs, KRIs incl. limits and their measurement and reporting ways
- Agree on information obligations (regular and ad-hoc)
- Formulate information and audit rights for internal and external authorities (audit, FINMA)
- Define regulations for data protection and IT security as well as business continuity
- Phrase termination rights, notice periods and support levels after end of the contract
- Restrict or define rules for sub-outsourcing
- Keep contracts up to date
- Review legal / regulatory clauses regularly
- Store and register contacts in a suitable CMS

Dr. Fedor-Immanuel Rahn
Senior Manager

E-mail FRahn@zeb.de
Phone +49.69.719153.413
Mobile +49.160.96946163

Frankfurt Office
Taunusanlage 19
60325 Frankfurt a.M.

BANKING HUB by zeb