Netzwerk
Risikomanagement

Prof. Dr. Bruno Brühwiler, Convenor WG „Core Risk Management Standards“

ISO 31000 UPDATE

Netzwerk Risikomanagement

Roadmap ISO 31000

Start der Entwicklung 2005

Publikation November 2009

Start Revision 2013

Nächste Version Ende 2017

Was ist von der Revision zu erwarten?

Netzwerk Risikomanagement

Was ist Risikomanagement?

Die Revision war gekennzeichnet durch viele und heterogene Sichtweisen über Inhalte und Ausrichtung des Risikomanagements.

Für die Angelsachsen ist Risikomanagement nahe an „Decision making“ (Entscheidungstheorie),.

Die Deutschen z.B. tun sich immer noch schwer mit dem „Sicherheits- / Safety“ Aspekt bei der gegebenen Risikodefinition. Langes Ringen um Kompromisse für einen globalen Konsens.

Netzwerk Risikomanagement

Das Ergebnis der Revision

Die Struktur der ISO 31000 bleibt unverändert:

- Terminologie
- Grundsätze
- Framework
- Prozess

Diese konservative Entwicklung ist gerechtfertigt, weil das Grundkonzept der ISO 31000 sich als zweckmässig erwiesen hat.

Netzwerk Risikomanagement

Beweis: OECD

OECD sagt: ISO 31000 ist de-facto zum Welt-Standard für Risikomanagement geworden.

Andere Regelwerke zu sehr finanzlastig (COSO – SOX, Wirtschaftsprüfung, Bankenregulierung ist Eigenmittelorientiert).

Netzwerk Risikomanagement

Entwicklung eines Reifegradmodells

Basis: die Grundsätze des Risikomanagements:

1. Value creation and protection
2. Integration
3. Structured approach
4. Customized
5. Inclusive
6. Dynamic and responsive
7. Best available information
8. Human and cultural factors
9. Continual improvement

Netzwerk Risikomanagement

Reifestufen: Beispiel „Integration“

- Stufe 1: Passiv

Organisation verfügt kaum über Führungs-instrumente (keine Strategie, keinen Plan) und überlegt somit nicht, was misslingen könnte. Risikomanagement existiert kaum, schon gar nicht als praktizierter Prozess.

(Beispiele: Deutsche Grossprojekte wie Flughafen Berlin, Elbphilharmonie, Airbus 400, politische Projekte)

Netzwerk Risikomanagement

Reifestufen: Beispiel „Integration“

- Stufe 2: Reaktiv

Risikomanagement ist regulatorischen und haftpflichtrechtlich motiviert (man muss um nicht strafbar zu werden), losgelöst Unternehmensstrategie oder operationeller Tätigkeit

Paradebeispiel: THE THREE LINES OF DEFENSE

Netzwerk Risikomanagement

Reifestufen: Beispiel „Integration“

- Stufe 3: Kalkulativ

Risikomanagement wird ins Managementsystem integriert. Ganz typisch dafür ist die Verbindung mit ISO 9001, welches neuerdings risikobasiert gestaltet werden soll.

An sich ist dieser Ansatz richtig, oft mehr system- als inhaltsbezogen.

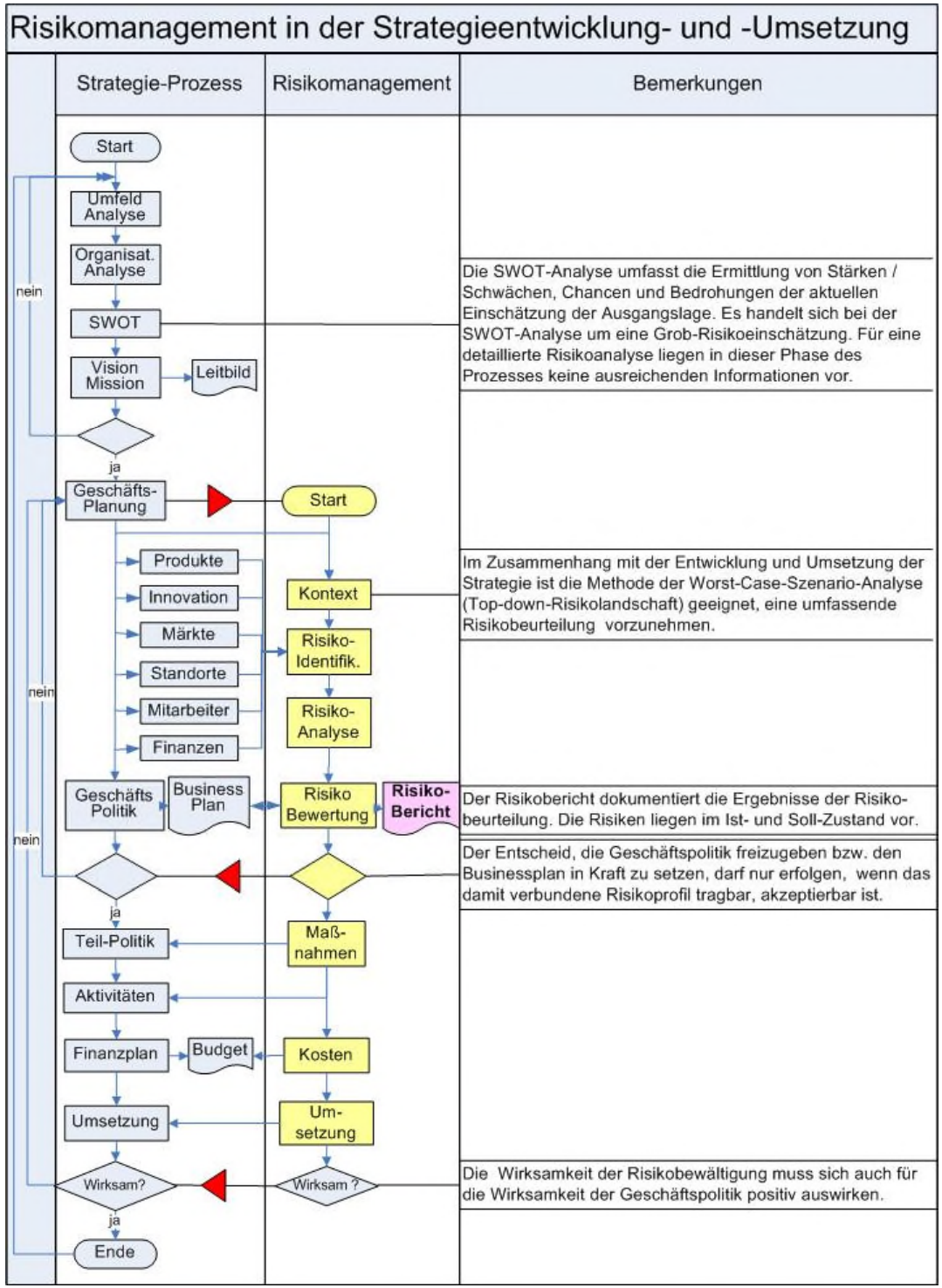
(Erfahrungen mit risikobasiertem Denken: Alles ist Risiko)

Netzwerk Risikomanagement

Reifestufen: Beispiel „Integration“

- Stufe 4: Proaktiv

Risikomanagement wird mit den strategischen Zielen und mit den operationellen Tätigkeiten eng verknüpft. Es geht darum, die Chancen der Unternehmensstrategien gegen Bedrohungen abzuwägen (Güterabwägung). Somit werden Strategie und Verlustrisiko nicht gegeneinander ausgespielt.



Netzwerk Risikomanagement

Paradebeispiele der Nicht-Beachtung:

- UBS
- Volkswagen
- Swissair

Netzwerk Risikomanagement

Reifestufen: Beispiel „Integration“

- Stufe 5: Reif

Entspricht einerseits der Kombination von Stufe 3 und 4, berücksichtigt zusätzlich die Schnittstellen zwischen den verschiedenen Applikationen von Risikomanagement

Netzwerk Risikomanagement

Schnittstellen

Netzwerk Risikomanagement

Revision ISO 31000:2017

- Nicht spektakulär
- Gleiche Struktur (Wiedererkennungswert)
- Immer noch sehr allgemein gehalten
- Nicht zertifizierbar
- ISO 31000 ist skalierbar mit den Reifegraden und damit für die Weiterentwicklung des Risikomanagements top-geeignet