



# Zwischen Risikokultur und Risikogovernance

2. Siegener Jahreskonferenz Risk Governance

*Dr. Carsten Steinhoff*

8. Oktober 2014

## Disclaimer

*Diese Präsentation gibt meine eigene Meinung wieder und entspricht nicht zwingend auch der offiziellen Sicht der NORD/LB.*



## Agenda

1. Risikomanagement in der NORD/LB

2. Governance als Proxy einer guten Risikokultur

3. Praxisbeispiele

4. Diskussion



## Herausforderung Risikomanagement



*Wie lässt sich gutes  
**RISIKO**management  
**KULTUREll** verankern?*

## Risiko? Auch eine Kulturfrage!

VERSTÖSSE GEGEN US-SANKTIONEN

*n-tv.de , 26.08.2014*

### Commerzbank soll 650 Millionen Dollar Strafe zahlen



HYPOTHEKENSTREIT

### Deutsche Bank zahlt Millionen an BayernLB

*Handelsblatt, 02.09.2014*

Die Deutsche Bank will laut Insidern einen Millionenbetrag an die BayernLB überweisen – und so den Hypothekenstreit aus der Welt schaffen. Doch damit ist das Thema bei Deutschlands größter Bank noch lange nicht abgehakt.

Im Zentrum des Streits stehen verbriefte Immobilienkredite im Volumen von rund 810 Millionen Dollar, die die BayernLB vor der Finanzkrise von der Deutschen Bank gekauft hatte. Als der US-Häusermarkt kollabierte, erlitt die zweitgrößte deutsche Landesbank damit hohe Verluste. Der Deutschen Bank warf sie daraufhin vor, die schlechte Qualität der zugrundeliegenden Darlehen beim Verkauf bewusst verschleiert zu haben. Deutsche-Bank-Händler hätten zudem explizit auf einen Crash am US-Immobilienmarkt gewettet.

### Deutschlands anerkannteste Berufe Feuerwehreute sind am beliebtesten

*n-tv.de , 26.08.2014*

Beim alljährlichen Berufe-Ranking haben wieder einmal Feuerwehreute und Krankenschwestern die Nase vorn, Manager und Banker zählen zu den großen Verlierern. Eine Überraschung gibt es bei den Beamten.

Feuerwehreute, Krankenschwestern und Altenpfleger genießen laut einer Forsa-Umfrage nach wie vor das höchste Ansehen in der Bevölkerung. Dicht dahinter folgen Ärzte und Polizisten - sowie seit neuerem auch Erzieherinnen in Kindergärten und Kitas.



### JP-Morgan-Ermittlungen ausgeweitet Neuer Ärger für Zockerbank

*N-tv, 01.07.2012*

Etwa 30 Mrd. Dollar Börsenwert vernichtet, dazu ein Milliardenverlust und ein Imageschaden: Das ist die bisherige Bilanz der Zockerei mit riskanten Papieren für die US-Großbank JP Morgan. Aber es kommt noch dicker: Neben der SEC untersucht nun auch der US-Regulierer CFTC die dubiosen Geschäfte und den damit möglicherweise einhergehenden Tatbestand des Betrugs.

LIBOR-SKANDAL

### Ex-Händler bekennt sich schuldig

*Handelsblatt, 19.08.2014*

Bereits im Juni hatte der erste Ex-Händler der Rabobank seine Schuld im Libor-Skandal eingestanden niederländischen Bank schuldig bekannt. Der Umfang des Betrugs sei massiv gewesen.

## Regulierung als Ausweg ?

### EU überflutet Banken mit Vorgaben

Aktuell 400 delegierte Rechtsakte in der Mache – Giegold  
fordert Bündelung in Finanzmarktgesetzbuch

*Börsenzeitung, 06.09.2014*

WIRTSCHAFT REGULIERUNG

*Welt, 03.09.2014*

### Anshu Jain sieht Deutsche Bank als "bedrohte Art"

Führende Banker diskutieren über Europas Weg aus der Krise. Commerzbank-Chef Blessing fordert Eurobonds, Anshu Jain widerspricht. Sein Rezept: Die Politik möge den Wert der Großbank wiederentdecken.

### Banken stehen vor großen Herausforderungen

**KREDITE** Fremdkapitalfinanzierung mittelständischer Unternehmen  
– aktuelle Entwicklungen und Handlungsalternativen

*Nordwest Zeitung, 05.08.2014*

## Risikokultur

- ... hat viele Facetten (strategisch, operativ, compliance-orientiert)
- ... hat formelle und individuelle Komponenten
- ... ist multidimensional und extrem komplex
- ... ist interdisziplinär (BWL, VWL, Psychologie, Rechtswiss. etc.)
- ... ist eine Kernfrage von Unternehmenskultur und -erfolg



Welches Risikoverhalten wird in / von der Organisation akzeptiert ?

# Voraussetzungen und Gefahrenquellen

## Voraussetzungen



- Gemeinsame **Ziele** / Wertvorstellungen
- **Präsenz** in allen Unternehmensprozessen,
- **transparente Information** / **Kommunikation**  
**Verantwortung** nehmen
- **Präsenz** des Risikomanagement, **Sinn** erkennen!
- Gesunde Risk-Return **Balance**
- Verhalten **verwurzeln**. Fragen und hinterfragen!
- Vorausschauend und verknüpft denken
- **Nachhaltig**

## Gefahrenquellen



- Silos und blinde Flecken
- Markt steuert Risikofunktion, nicht umgekehrt
- Passivität. Warnsignale nicht ernst nehmen
- Über-Sicherheit / Optimismus ⇔ Angstkultur.
- Angst vor schlechten Nachrichten
- Ignorieren / „schönreden“ von Fakten
- Fehlerhafte Entscheidungen nicht korrigieren



## Risikokultur vs. Risikogovernance

	Risikogovernance	Risikokultur
<b>Motivation</b>	Aufsichtsrecht Stakeholder	Intrinsische Motivation „Unternehmertum“
<b>Organisations- / Formalisierungsgrad</b>	Festgelegte Spielregeln niedergeschrieben	Informell / gelebt
<b>Bewertungsmaßstab</b>	Regelbasiert	Offen und ehrlich
<b>Incentivierung</b>	Sanktion bei Regelverstoß	Risikonahme mit Augenmaß und Strategie
<b>Kommunikation</b>	Regelwerk	„Tone from the top“
<b>Autonomie</b>	Leitplanken	Entscheidungsfreiräume
<b>Messbarkeit</b>	Messbar / revisionssicher	Nicht messbar aber erlebbar

*Eigene Darstellung*

Wie lässt sich eine gute Risikokultur in den Bankprozessen leben?

## Lässt sich Risikokultur messbar machen?

Risk Culture Factor Categories	Deloitte	Ernst and Young	IRM <sup>1</sup>	KPMG	McKinsey	PWC	Towers Watson
Acknowledgement of risk (potential for over confidence, level of challenge)			√		√		
Communication (regular risk reporting and escalation of risk issues)			√		√	√	√
Compensation and performance management	√	√	√			√	
IT Systems							√
Leadership ('tone from the top')		√	√	√		√	√
Relationships (between employees)	√						
Respect for risk (potential for gaming the system)					√		
Responsiveness to risk (ability to react to risk issues)					√		
Risk competencies (of employees)	√		√			√	
Risk facilitation (status of risk function and ability to support business)			√	√			
Risk management processes and procedures						√	√
Risk ownership (clear accountabilities)			√	√		√	
Structure of organisation and governance	√	√	√				√

Quelle: Institute of Operational Risk (2013), S. 15

## Agenda

1. Risikomanagement in der NORD/LB

2. Governance als Proxy einer guten Risikokultur

3. Praxisbeispiele

4. Diskussion

① Governance- Risk- Compliance

② Expertenschätzungen

③ Den Scope verbreitern

## Beispiel I

# Governance- Risk- Compliance

- Akteure zusammenbringen
- Konventionen schaffen
- Akzeptanz erhöhen

## Herausforderung Risikomanagement

### *Schwere Schäden verhindern*

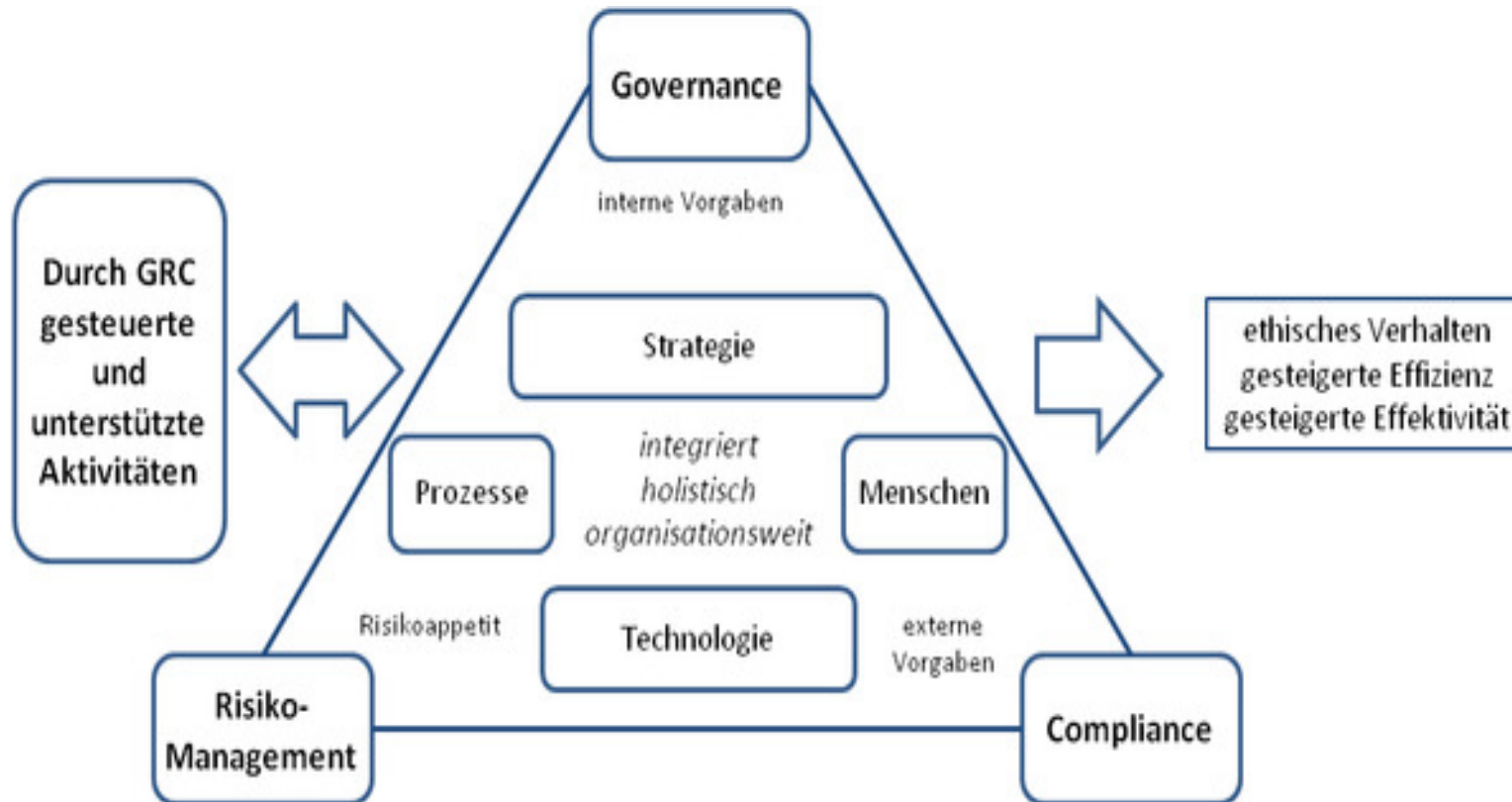
1. Vor der Welle schwimmen
2. Sensibel sein für Trends und schwache Signale
3. Gezielt Prophylaxe betreiben

### *Geeignete Rahmenbedingungen setzen!*

1. Was ist OpRisk, was nicht?
2. Wer ist verantwortlich für dieses OpRisk?
3. Wie arbeiten die Verantwortlichen optimal zusammen?
4. Wie kann das Framework eine gute Risikokultur erzeugen und ausbauen?



# Forschungsrahmen „Governance-Risk-Compliance“

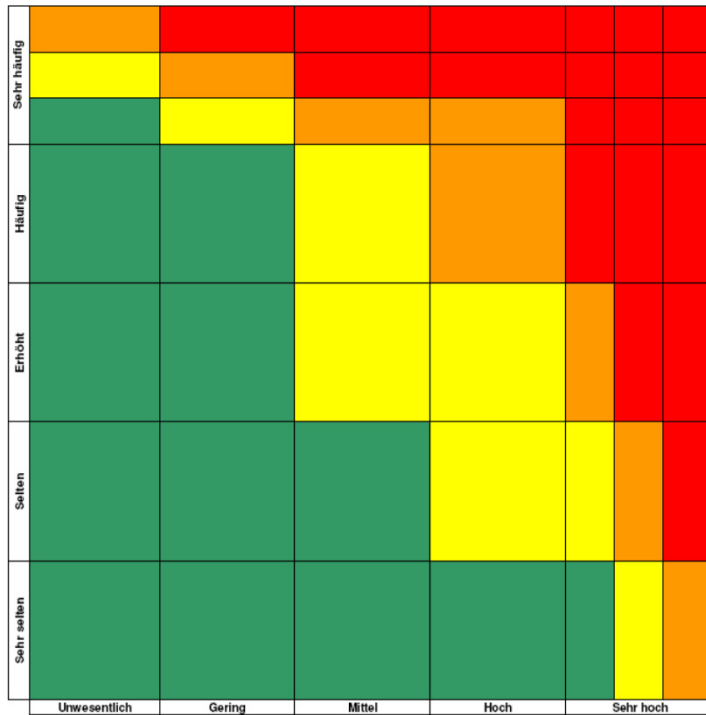


Quelle: Racz et al., 2010

# Risikomatrix als zentrales Instrument

**Eintrittswahrscheinlichkeit**

- Geschätzte Wahrscheinlichkeit
- Angemessenheit / Wirksamkeit
- Beurteilung Fall



- Bankweit einheitliches **Bewertungsinstrument** für alle Arten operationeller Risiken
- Zentrales **Berichts- und Steuerungswerkzeug**
- Definition einheitlicher **Risikotoleranzen** im Sinne von **Eskalationsstufen**

- Auswirkung**
- Finanzieller Verlust > x
  - Reputationsverlust
  - Verstoß gegen gesetzliche Vorschriften
  - Verletzen interner Guidelines
  - Verlust der Steuerungsfähigkeit



# Konsolidierung von Berichtswegen

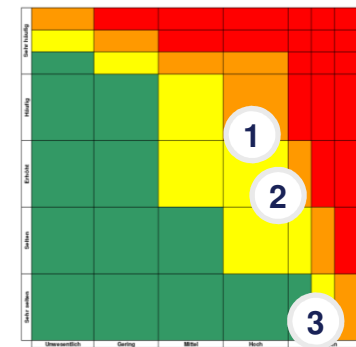


Risikokategorie	Risikostatus				Aktuelle Themen
	Ent1	Ent2	Ent3	Ent4	
Personal	🟡	🟢	🟢	🟢	Lorem ipsum dolor sit amet
Externe Dienstleister	🟡	🟡	🟢	🟡	voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no
Höhere Gewalt / Sachschäden / Gebäudesicherheit	🟢	🟢	🟢	🟢	-
Informationssicherheit / Technologie / Datenschutz	🟡	🟢	🟢	🟢	voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no
Geldwäscheprävention/ Fraud Compliance	🟢	🟢	🟢	🟢	-
Kapitalmarkt Compliance	🟢	🟢	🟢	🟢	-
Rechtsänderungsrisiko	🟡	🟢	🟢	🟢	Lorem ipsum
Prozesse / Abläufe / Bearbeitungsfehler	🟢	🟢	🟢	🟢	-

### Summary

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

	Schäden und Risikopotenziale (in TEUR)		
	Losses	EL	VaR
Total			
Ent 1			
Ent 2			
Ent 3			
Ent 4			



Top Risks	
# 1	
# 2	
# 3	



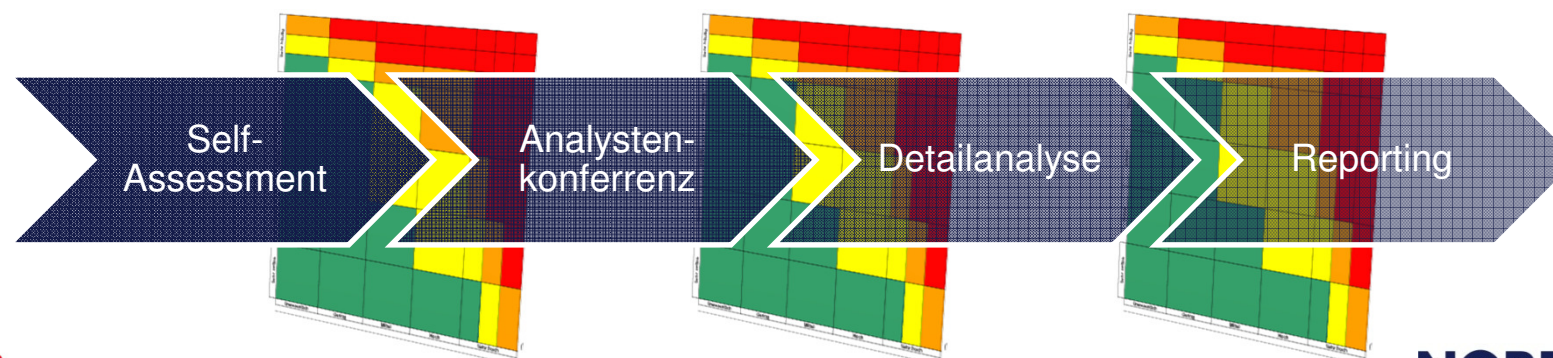
## Beispiel II

# Expertenschätzungen

- Expertise nutzen
- Prävention anregen

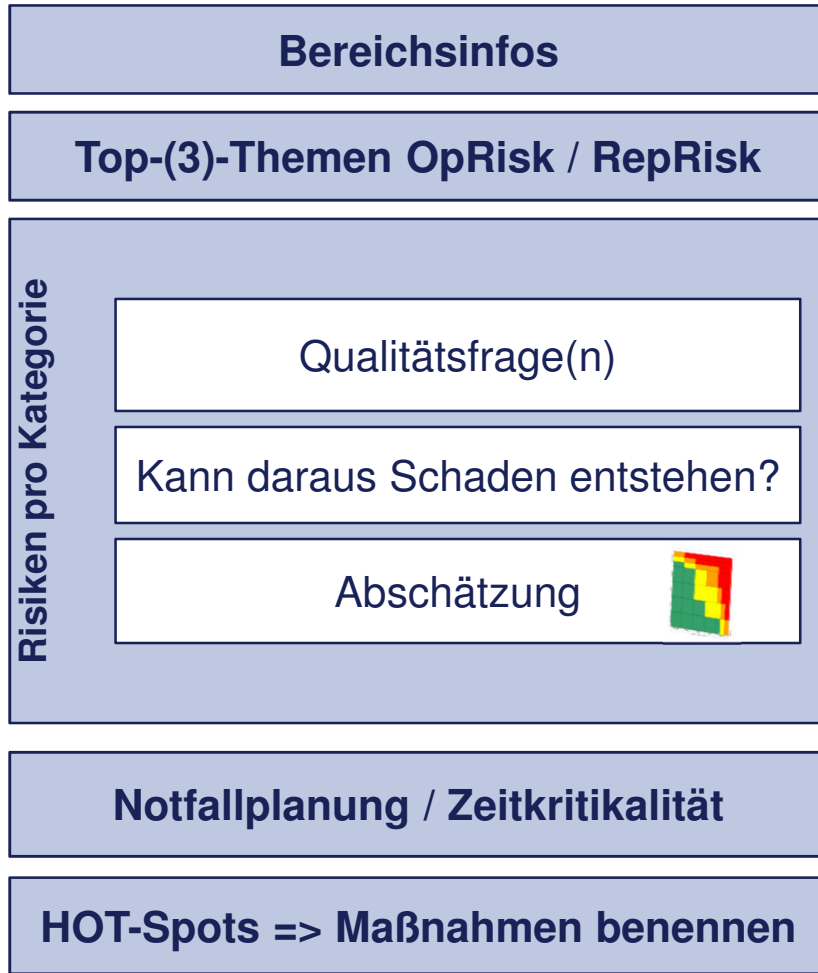
## Expertise nutzen – Datensammlungen konsolidieren

- **Fragebogenbasierte** Analysen in einer Methode gebündelt
- **Risikorientierter Ansatz**, Unterstützt durch Entscheidungsbäume
- Automatisierte und manuelle **Plausi-Checks**
- **Akzeptanz und Datenqualität erhöhen** durch:
  - Eine gebündelte Datenerhebung
  - Risikoorientierte Abschichtung
  - Gemeinsamer Auftritt
  - Konsolidierte Datenhaltung und Reporting
  - „Zweitverwendung“ von Daten





# Datensammlung konsolidieren



### Risikoprofil Bereich xyz

Department	xyz	
Losses	10 Severe Findings	2

#### Incidents

Cause	Incident	Action	Closed
Loss			
Loss			
Finding			

#### Assessment Profile

Category	Value
HR	0
Outso	0
Fraud / AML	5000
...	500

#### Critical Questions

Topic	Status
1. Internal Fraud	
2. AML	

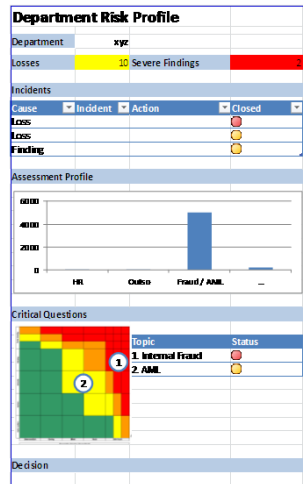
*weitere Daten*

#### Decision



# Verknüpfung zum Gesamtmodell

## Risk Profile



## 2. Scenario Analysis

**Possible Gaps / Action**

**Quantify Impact**

- Worst Case: WSK %, Schadenhöhe €
- Normal Case: WSK %, Schadenhöhe €
- Lucky Case: WSK %, Schadenhöhe €

Duration Jahre

## 4. Back-Loop

## 3. Model

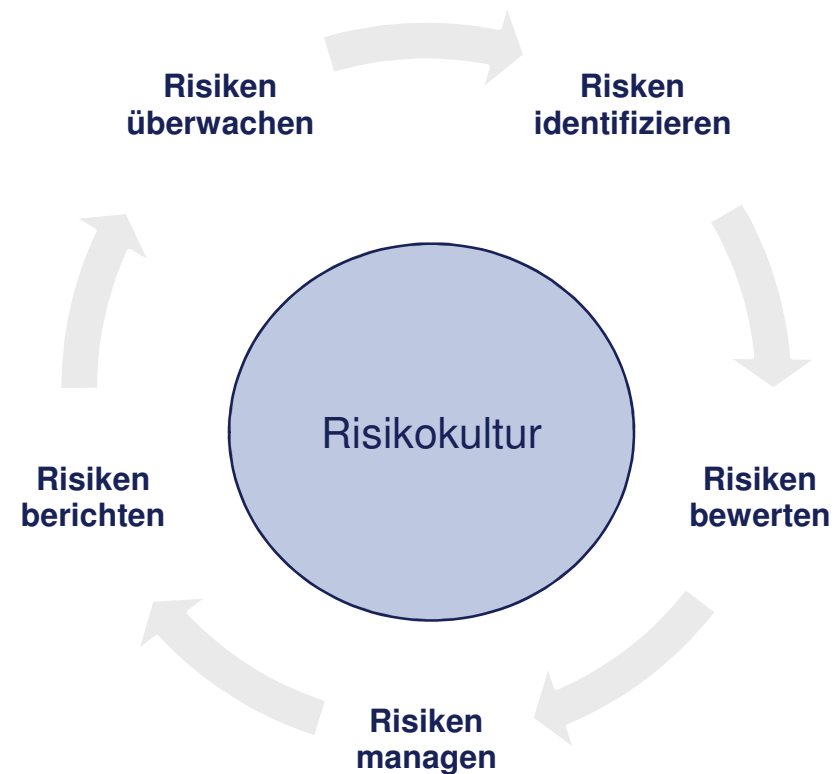
**Decisions**

**LDA-Model**



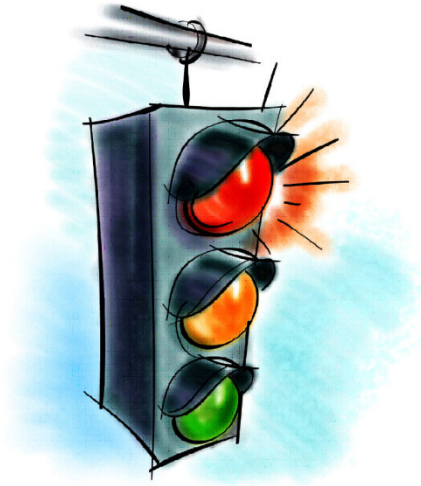
## Risikodialog mit externen Daten verbessern

- Benchmarking, Umfeldanalyse, Trends erkennen
- Stresstesting
- Szenarioanalysen / Lessons Learned
- Versicherungsanalysen
- GFA Fraud
- Reputationsrisiken beurteilen
- ...





## Quick wins mit Risikoindikatoren



- Breites Themenspektrum
- Sind vom Risiko her abgeleitet
- Werden Quartalsweise erhoben
- Beinhalten Qualitative wie quantitative Elemente
- Maßnahme wenn  $\neq$  grün
- Einfach, kostengünstig, effektiv!

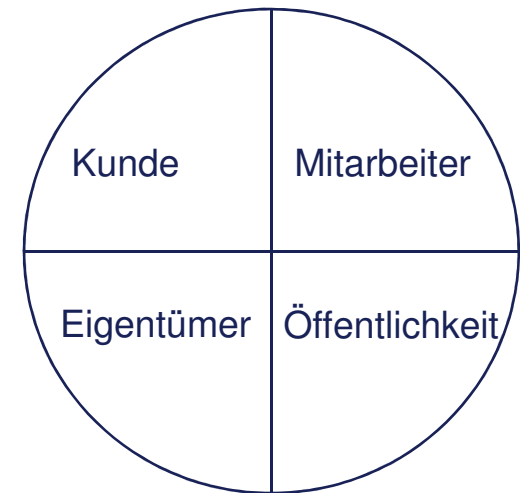
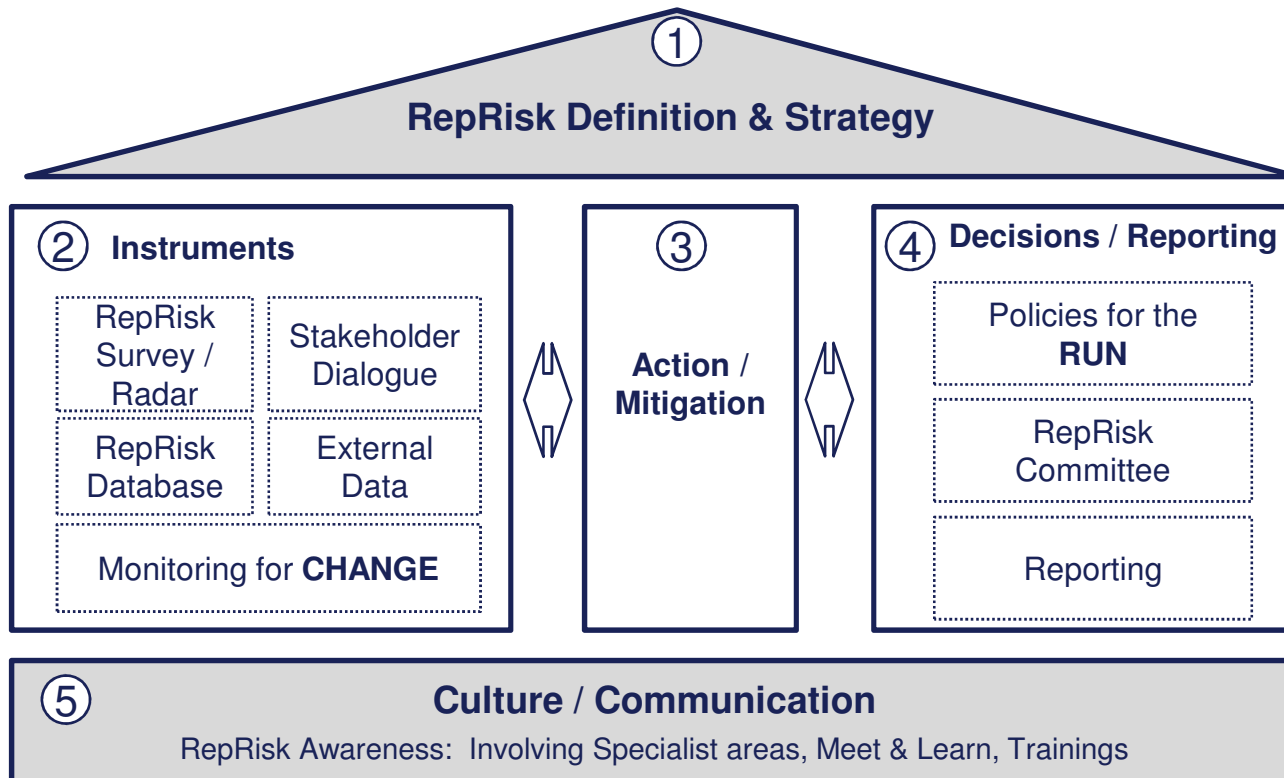


## Beispiel III

# Den Scope verbreitern

- Reputationsrisiko
- Stress 2.0

# Reputationsrisiken



Quelle: Steinhoff / Sprengel (2014)



## Enterprise Risk Management als Ziel ???



(inverse) Stresstests

Inter / Intra- Korrelationen

Belastungs-/  
Bedrohungsszenarien

Sanierungsindikatoren

## Agenda

1. Risikomanagement in der NORD/LB
2. Governance als Proxy einer guten Risikokultur
3. Praxisbeispiele
4. Diskussion



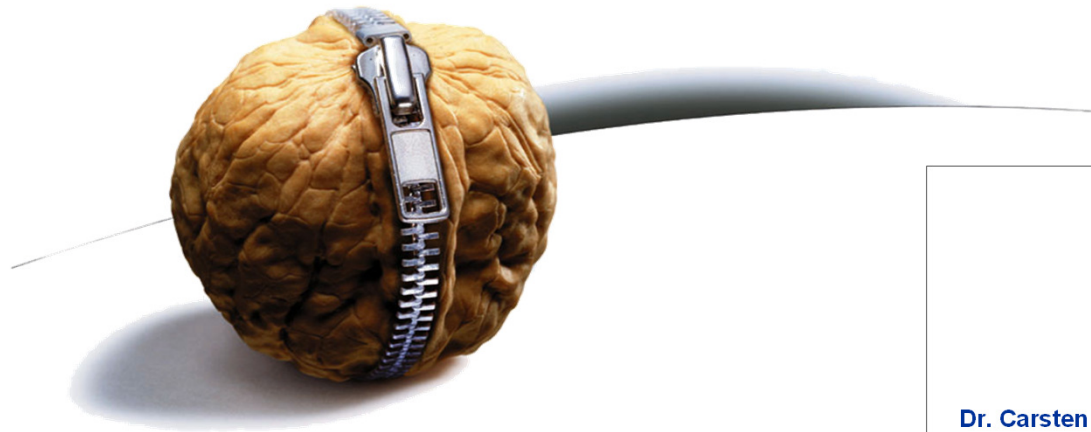
## Herausforderungen

- Risikokultur als einen entscheidenden Wettbewerbsfaktor nutzen
- Balance zwischen Risiko und Business finden
- Verantwortung übernehmen und positionieren
- Vergangenheitswerte nicht überschätzen
- Schwache Signale wahrnehmen
- Akzeptanz vs. Awareness



## Quellen

- Deloitte Consulting (2013): Cultivating a Risk Intelligent Culture.  
<http://www.deloitte.com/assets/Dcom-Bermuda/Local%20Content/Articles/Cultivating%20a%20Risk%20Intelligent%20Culture.pdf>
- Institute of Operational Risk (2013): Operational Risk Sound Practice Guidance, Risk Culture.  
<https://www.ior-institute.org/sound-practice-guidance/risk-culture>
- McConnell, P. (2013): A Risk Culture Framework for Systemically Important Banks.  
*Journal of Risk and Governance*, Vol. 3, No. 1, 2013. <http://ssrn.com/abstract=2345542>
- Power, M.; Ashby, S.; Palermo, T. (2012): Risk Culture in Financial Organisations.  
<http://www.lse.ac.uk/researchAndExpertise/units/CARR/pdf/Final-Risk-Culture-Report.pdf>
- Racz, N., Weippl, E. & Seufert, A. (2010): *A frame of reference for research of integrated GRC*.  
In: De Decker, B., Schaumüller-Bichl, I. (Hrsg.): *Communications and Multimedia Security, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings*. Berlin, S. 106-117.
- Steinhoff, C., Sprengel, R. (2014): Governance as the Starting Point for a Reputational Risk-Management Process. In: Kaiser, Thomas, Merl, Petra (Hrsg.): *Reputational Risk Management in Financial Institutions*. London (Erscheint im IV. Quartal 2014).



**NORD / LB**

**Dr. Carsten Steinhoff**

Finanz- und Risikocontrolling  
Leiter OpRisk Controlling

**Norddeutsche Landesbank Girozentrale**  
Friedrichswall 10  
30159 Hannover  
GERMANY

Phone +49 511 361-6436  
Mobil +49 173 2 454 035  
Fax +49 511 361-98 6436  
carsten.steinhoff@nordlb.de

 **Finanzgruppe**