UNIVERSITÄT LEIPZIG

Anwenderbericht OCTAVE-Methode

DFN-Nutzertagung, Mannheim, 07.05.2013

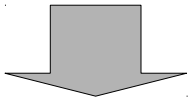
Martin Ullrich
Universität Leipzig

Agenda

- Ausgangslage
- Lösungsansatz: Risikoanalyse
- Umsetzung: Kurze Projektbeschreibung
- Ergebnisse: Empfehlungen und Maßnahmen

Ausgangslage

- Untersuchungsgegenstand: Personaldezernat
- Motivation:
  - Einführung Neues Verwaltungsnetz
  - Einführung Neue Hochschulsteuerung mit HISInOne-BI

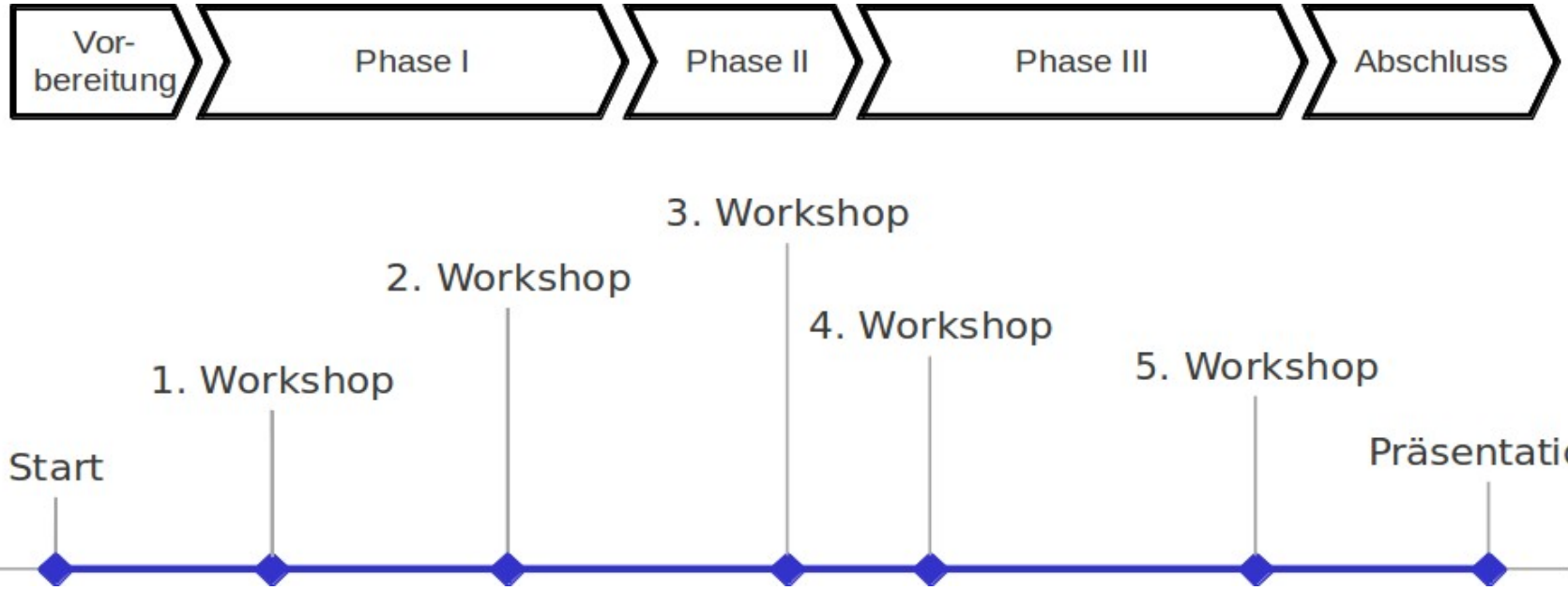


  - Datenschutzbetrachtung erforderlich
  - Anwendung der IT-Grundschutz-Methode nicht ziel führend

Lösungsansatz

- Einschätzung wo man steht
- Eingeschränkter Untersuchungsgegenstand
- Identifizierung von Defiziten
- Priorisierung von geeigneten Sicherheitsmaßnahmen
- Ziel: akzeptables Sicherheitsniveau

Projektablauf und Analysepfad



Workshop

- Jeweils 4-8 Stunden
- In 3-wöchigem Abstand
- Gesamtzeit 5 Monate

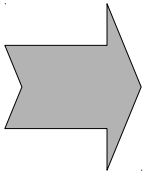
Vorbereitung:
Bildung des Analyseteams

- Bereichsübergreifendes Team
- Überschaubare Größe

- Personaldezernat
- URZ / Verwaltungs-IT, Netzwerk-ADM
- DSB
- DFN-CERT

Phase 1:
Festlegung der kritischen Werte

Identifizierung der organisationsspezifischen Informationen



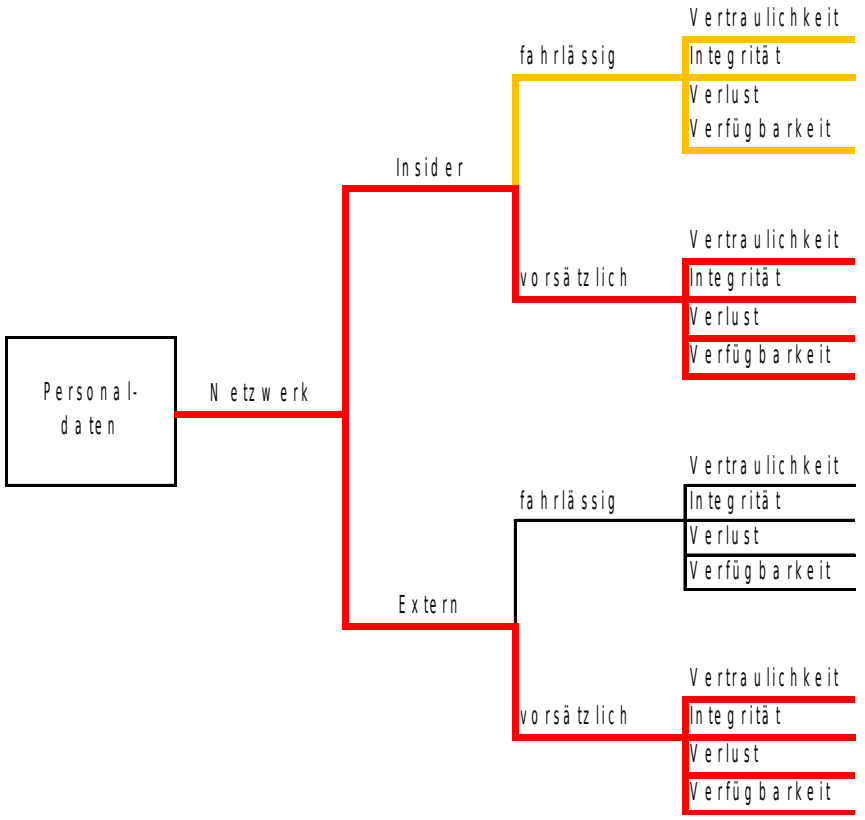
Personaldaten	Elektronisches Schriftgut
personenbezogene Daten zur Verwaltung der Arbeits- und Dienstverhältnisse	schützenswerte elektronische Informationen, sensible Reports, Übersichten

Einschätzung aktueller Informations-Sicherheitsmaßnahmen

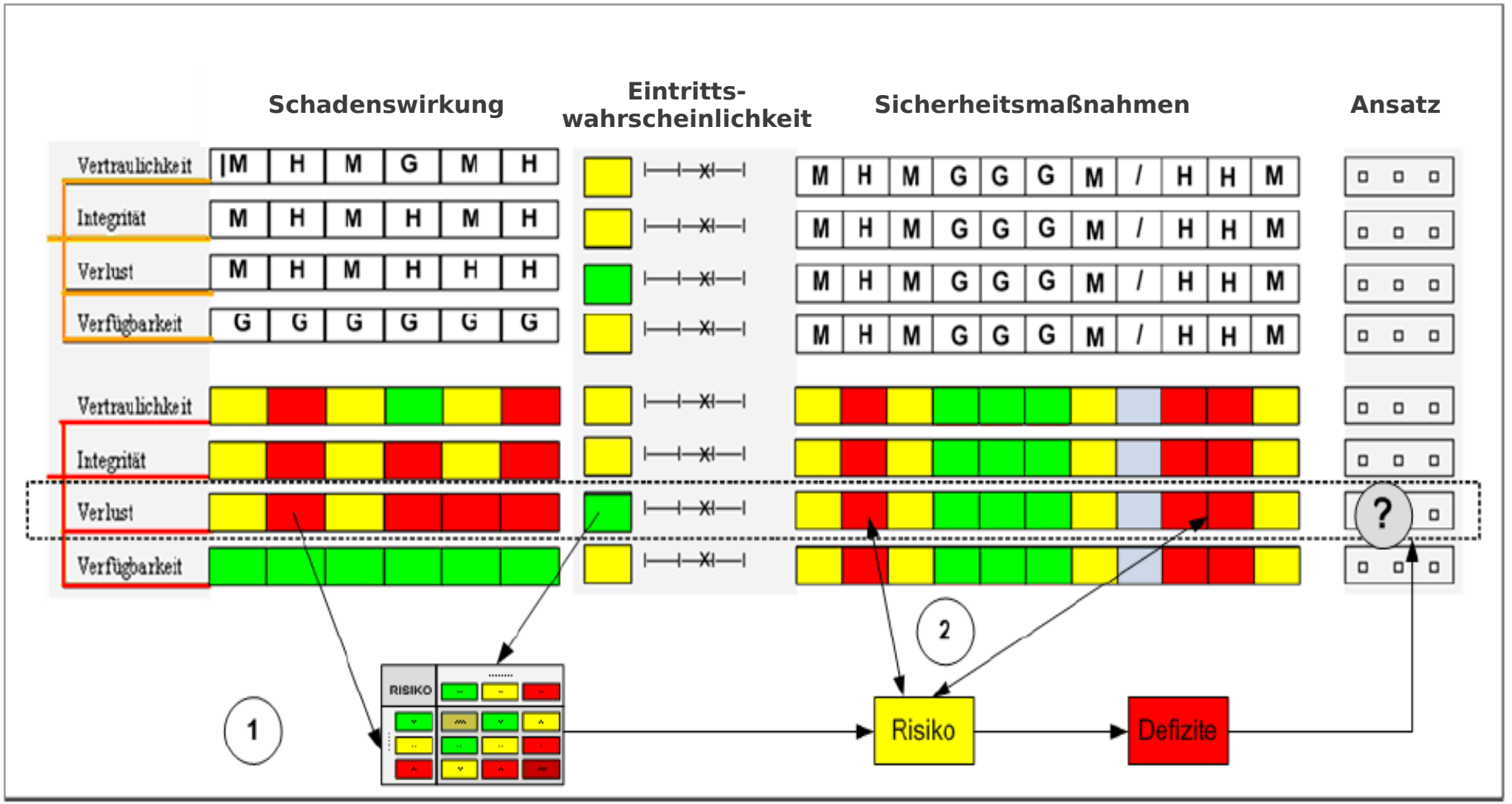
Themengebiet	Ampelstatus
Informationssicherheitsmanagement und Informationssicherheitspolitik	
Organisation	
Klassifizierung und Kontrolle von Werten	
Personal	
Physische Sicherheit	
Kommunikation und Betrieb	
Zugangs- und Zugriffskontrolle	
Entwicklung und Wartung	
Behandlung von Sicherheitsvorfällen	
Notfallplanung - Business Continuity	
Einhaltung von Verpflichtungen	

Phase 2:
Risikoprofile und Bedrohungen

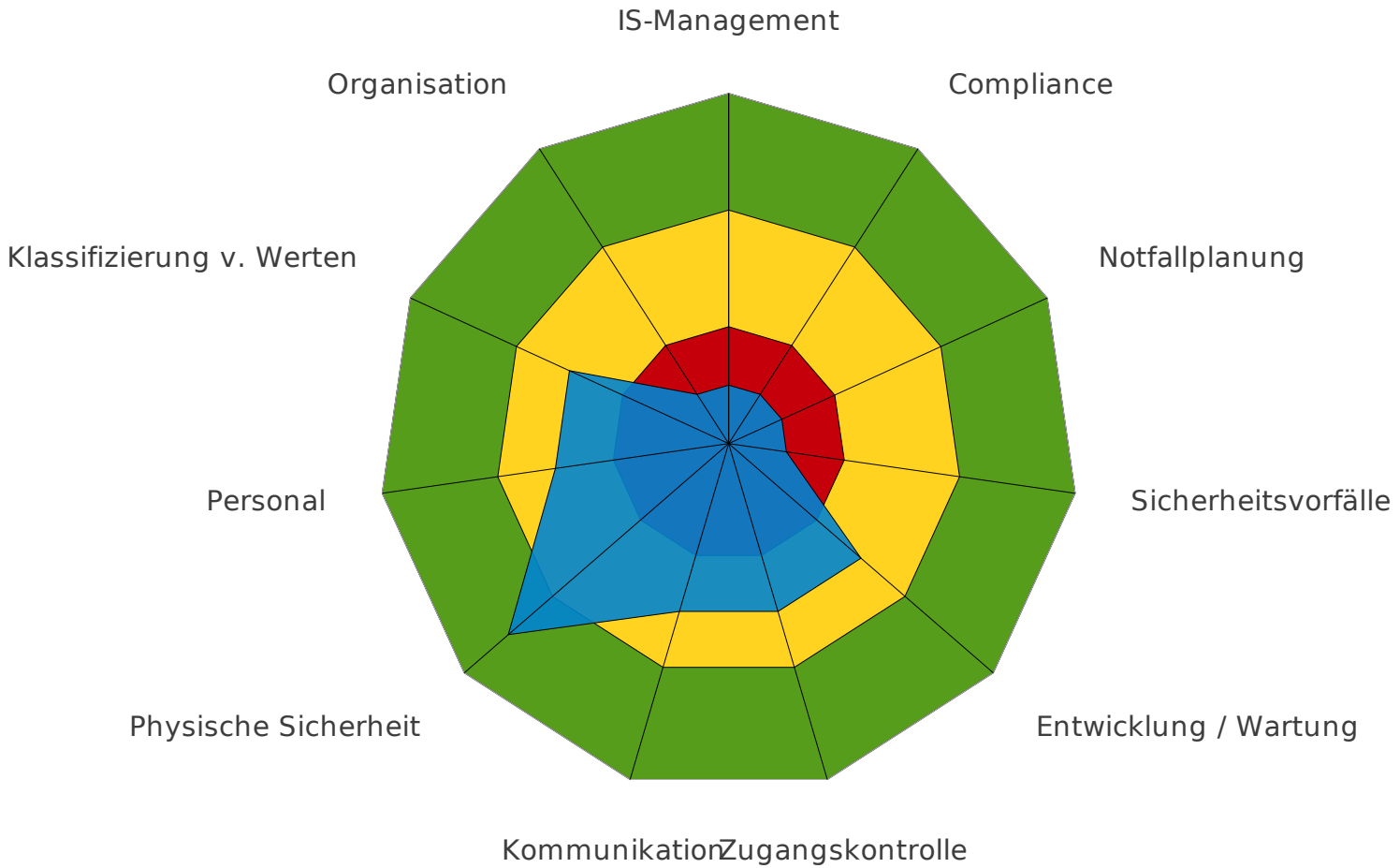
- Bedrohungsprofile:
  - Personen mit Netzzugang
  - Personen mit physischem Zugang
  - Technische Probleme
  - Weitere Problemfelder
- Identifizierung relevanter Zugriffspfade



Ansatz zur Risikominimierung



Phase 3
Analyseergebnis / aktueller Stand



Zu verbessernde Themenbereiche

Übergeordnete Bereiche

- Informationssicherheitsmanagement
- Organisation
- Behandlung von Sicherheitsvorfällen

Verwaltungsbezogene Bereiche

- Personelle Sicherheit
- Kommunikation und Betrieb
- Entwicklung und Wartung

Maßnahmen und Verantwortlichkeiten

Maßnahmen	Verantwortlichkeiten	Bemerkungen
Übergeordnete Aspekte	Leitungsebene und ISB	ISB benannt mit voller Stelle oder Support von Extern
Verwaltungsbezogene Aspekte	ISB, DSB, Personaldezernat, URZ	ISB benannt Zuarbeit aller Beteiligten (~80 PT) zzgl. Support von Extern für Audit, Beratung (>20 PT)

Nächste Schritte

Zu verbessernde Themenbereiche

Übergeordnete Bereiche

- Informationssicherheitsmanagement
- Organisation
- Behandlung von Sicherheitsvorfällen

Verwaltungsbezogene Bereiche

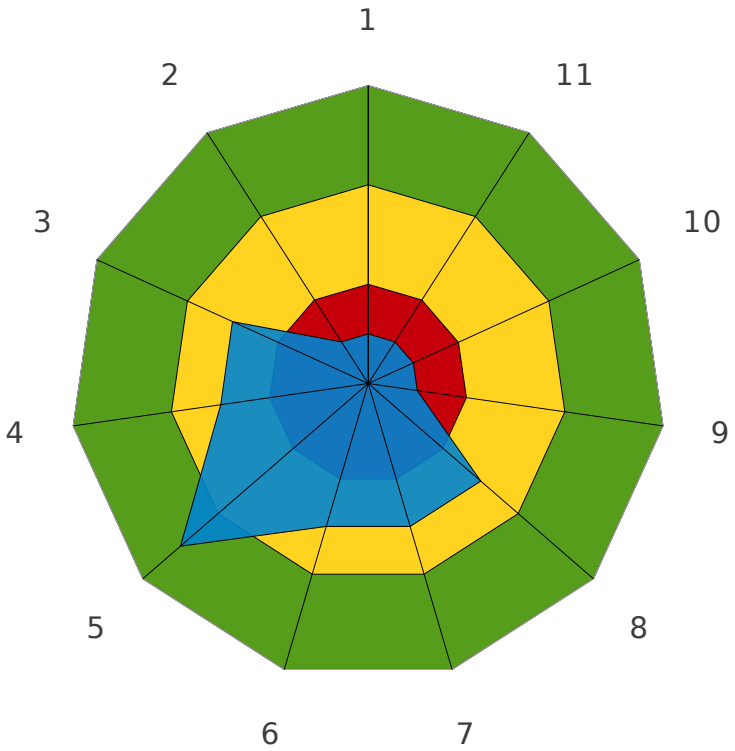
- Personelle Sicherheit
- Kommunikation und Betrieb
- Entwicklung und Wartung

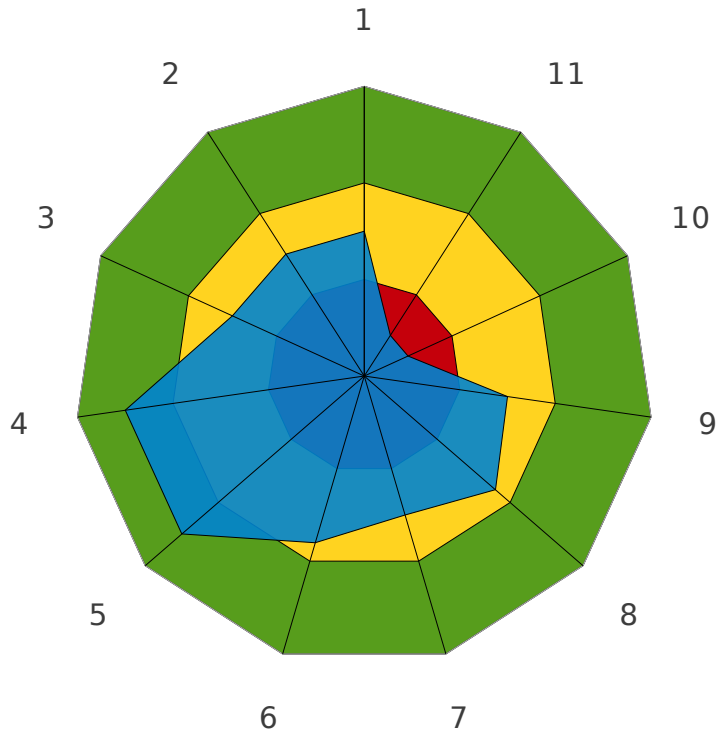
Rektoratsbeschluss

ISB als gemeinsam finanzierter „Shared Service“ der Leipziger Hochschulen
sowie ggf. außeruniversitärer Forschungseinrichtungen in den Varianten eigenes Personal/Shared Service

Veröffentlichung einer Leitlinie für Informationssicherheit

Sicherheitsstatus-Vergleich
Nach erfolgreicher Maßnahmenumsetzung





1	Management	7	Zugangskontrolle
2	Organisation	8	Entwicklung / Wartung
3	Klassifizierung	9	Sicherheitsvorfälle
4	Personal	10	Notfallplanung
5	Physische Sicherheit	11	Compliance
6	Kommunikation		

Vielen Dank
für Ihre Aufmerksamkeit!

Martin Ullrich
www.urz.uni-leipzig.de
martin.ullrich@uni-leipzig.de