

IT-Sicherheitsmanagement

als Basis für Security und Safety im Unternehmen

Univ.-Doz.DI Dr. Ingrid Schaumüller
ingrid.schaumueller@liwest.at

Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozesses
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität

Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozesses
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität

OCG-Arbeitskreis IT-Sicherheit

- Gegründet Juli 1993
- derzeit ca 110 Mitglieder
Experten aus Wissenschaft, Forschung,
öffentlicher Verwaltung, Wirtschaft
- Leitung: Dr. Ingrid Schaumüller, Linz
Dr. Heike Paschinger, Wien

www.ocg.at
(Arbeitskreise / IT-Sicherheit)

OCG-Arbeitskreis IT-Sicherheit

- Themen:
 - Sicherheitsmanagement, Sicherheitspolitik
 - Risikomanagement, Risiko- und Schwachstellenanalyse
 - Sicherheitsanforderungen
 - Sicherheitsmechanismen und -dienste
 - Methoden und Tools zur Entwicklung verlässlicher Systeme
 - Kryptographie und Kryptoanalyse
 - Sicherheit in bereichsspezifischen Applikationen (Bankwesen, Verwaltung, ...)
 - Evaluationskriterien
 - Rechtliche Aspekte, Datenschutz
 - Wirtschaftlichkeit von Sicherheitsmaßnahmen
 - Verantwortbarkeit des Technik-Einsatzes zwischen Verlässlichkeit, Risiko und Wirtschaftlichkeit
 - Sicherheit als Kriterium für die gesellschaftliche Akzeptanz von Informationssystemen

Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozesses
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität

Kennen Sie diese Situation ?



Ziel:
Richtlinien zur Unterstützung
und Vereinheitlichung der
erforderlichen Aktivitäten



Etablierung eines umfassenden und
kontinuierlichen
IT-Sicherheitsmanagementprozesses

Österreichisches IT-Sicherheitshandbuch

Teil 1: IT-Sicherheitsmanagement

Leitlinien zur Etablierung eines umfassenden, kontinuierlichen IT-Sicherheitsprozesses innerhalb einer Organisation

Teil 2: IT-Sicherheitsmaßnahmen

Sammlung organisatorischer, personeller, IT-technischer und infrastruktureller Maßnahmen zur IT-Sicherheit

Basis und Zielsetzung

- auf Basis internationaler Standards
- österreichische gesetzliche Vorgaben, Regelungen und Normen
- Kompatibilität
- umfassende Sammlung von IT-Sicherheitsmaßnahmen, jedoch keine systemspezifischen Details,
- Vermeidung von Redundanzen
- Einbeziehung des gesamten System-Lifecycles

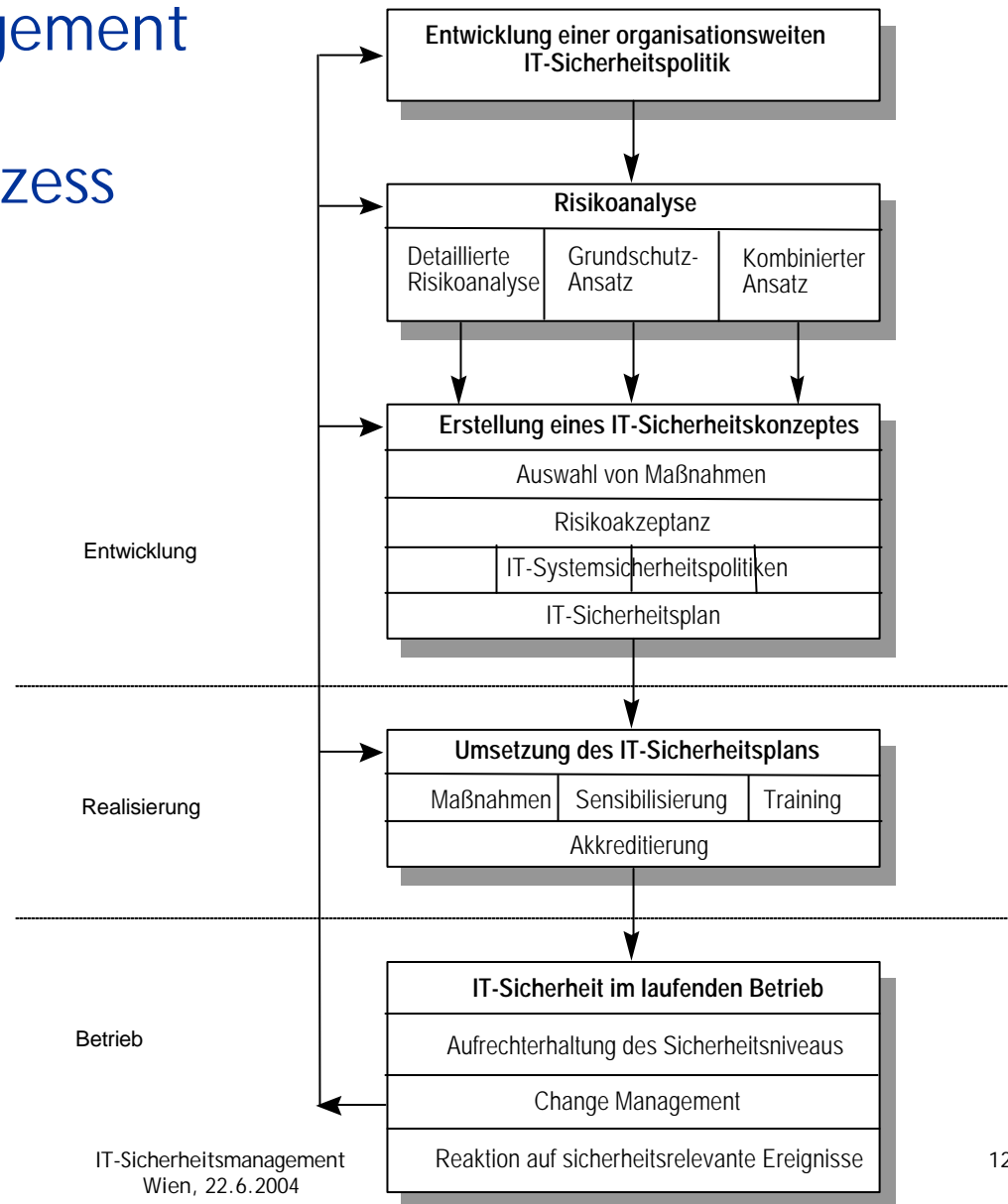
www.cio.gv.at

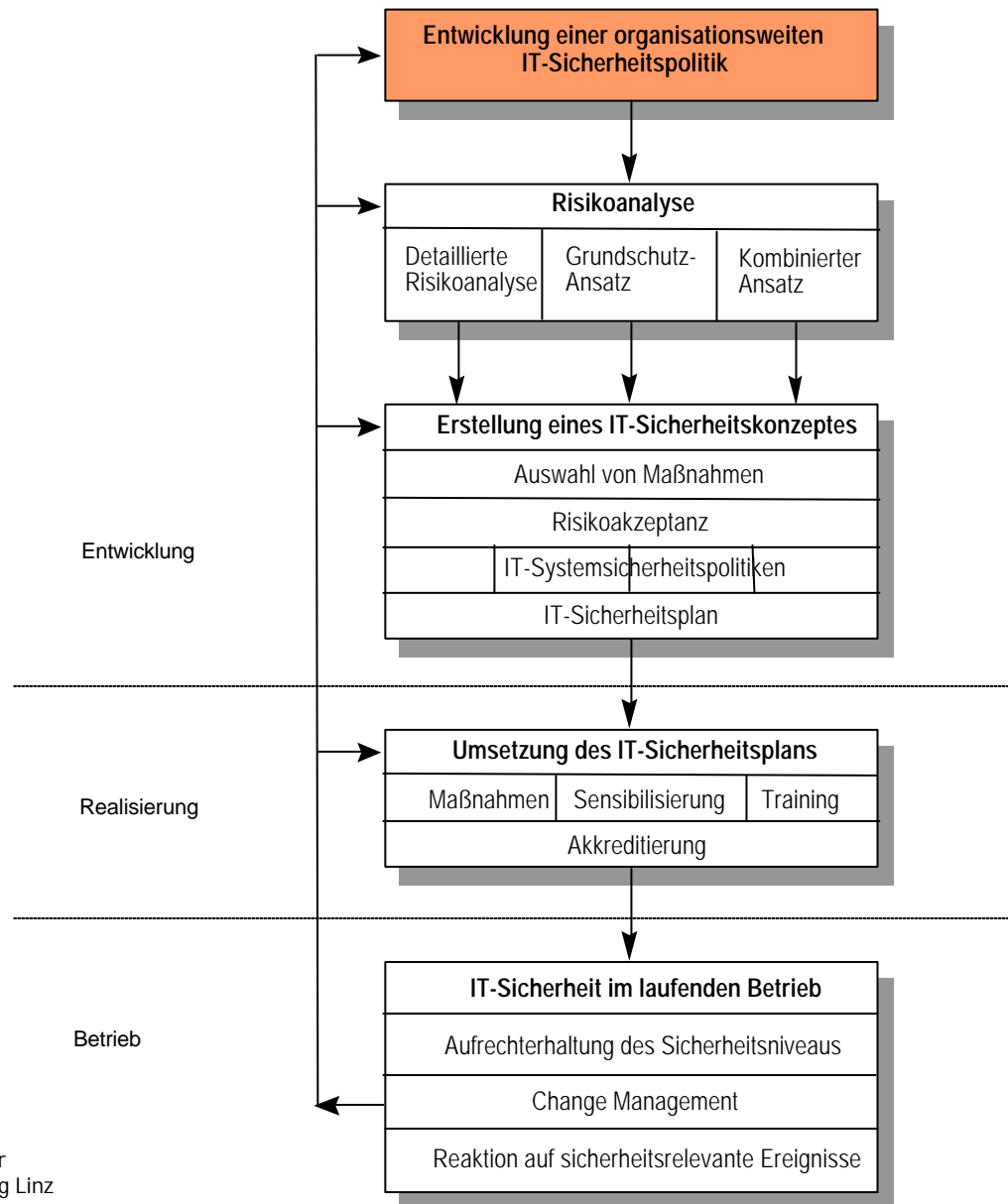
Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozesses
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität

IT-Sicherheitsmanagement als kontinuierlicher Prozess

**Aus:
Österreichisches
IT-Sicherheitshandbuch
Teil 1:
IT-Sicherheitsmanagement**





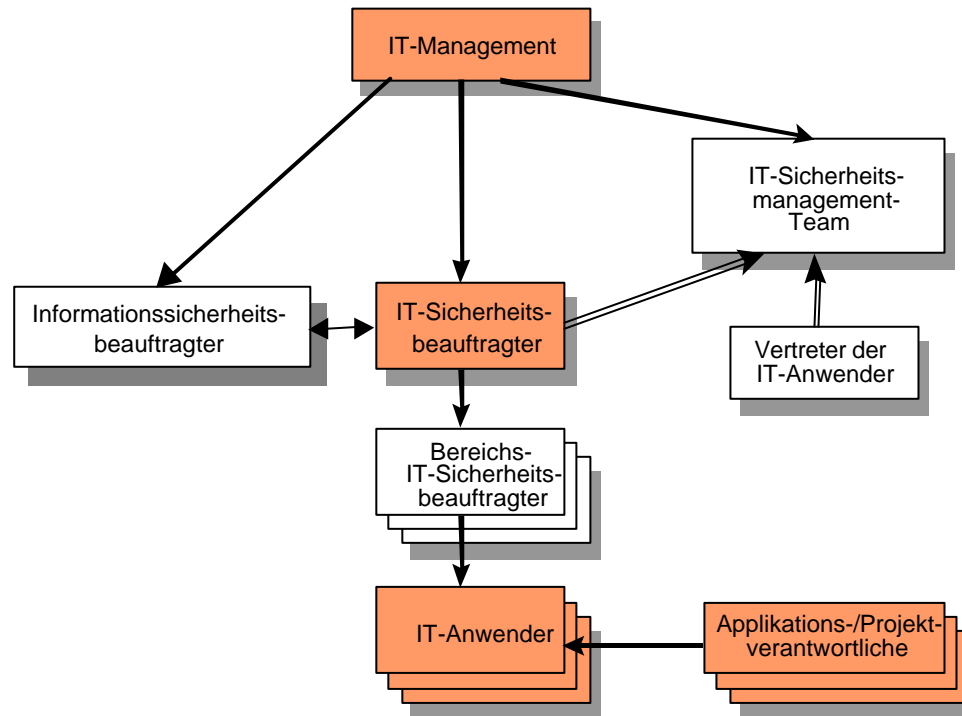
Inhalte einer IT-Sicherheitspolitik

- Grundsätzliche Ziele und Strategien
- Organisation und Verantwortlichkeiten für IT-Sicherheit
- Risikoanalyse-Strategien, Restrisiko und Risikoakzeptanz
- Klassifizierung von Daten
- Klassifizierung von IT-Anwendungen und IT-Systemen, BCP
- Organisationsweite Richtlinien
- Nachfolgeaktivitäten

Inhalte einer IT-Sicherheitspolitik

- Grundsätzliche Ziele und Strategien
- Organisation und Verantwortlichkeiten für IT-Sicherheit
- Risikoanalyse-Strategien, Restrisiko und Risikoakzeptanz
- Klassifizierung von Daten
- Klassifizierung von IT-Anwendungen und IT-Systemen, BCP
- Organisationsweite Richtlinien
- Nachfolgeaktivitäten

IT-Sicherheitsorganisation - Beispiel



Aufgabe:

➔ Definition der Rollen und Verantwortlichkeiten aller in den IT-Sicherheitsprozess involvierten Personen

Klassifizierung von Daten

Schritt 1: Festlegung von Sicherheitsklassen

Beispiel:

- **offen:**
Information, die ausdrücklich zur Veröffentlichung freigegeben wurde (z.B. Gesetze, Verordnungen, Pressemitteilungen)
- **vertraulich:**
Information, die für den internen dienstlichen Gebrauch bestimmt und grundsätzlich zur Veröffentlichung nicht vorgesehen ist (z.B. behördeninterner Schriftverkehr, interne Telefonverzeichnisse, Organisationspläne)
- **geheim:**
Information, deren Missbrauch der Organisation, der öffentlichen Verwaltung oder der Öffentlichkeit unter Umständen erheblichen Schaden zufügen könnte. Dazu zählen u.a. alle Daten, die unter eine Verschlusssachenverordnung fallen.

Klassifizierung von Daten

Schritt 2: Festlegung der Verantwortlichkeiten

Schritt 3: Regelungen zum Umgang mit klassifizierten Informationen

- Kennzeichnung klassifizierter Information (sowohl elektronischer als auch nicht-elektronischer)
- Speicherung klassifizierter Information (Zugriffsberechtigungen, etwaige Vorschriften zur Verschlüsselung)
- Übertragung klassifizierter Information (über welche Verbindungen, Vorschriften zur Verschlüsselung)
- Ausdruck klassifizierter Information (auf welchen Drucker, durch wen)
- Backup (Klartext, chiffriert, Schutz der Backup-Medien)
- Aufbewahrung / Wiederverwendung / Vernichtung von Datenträgern



**Empfehlung:
Erstellung einer Informationssicherheitspolitik**

Klassifizierung von IT-Anwendungen und IT-Systemen, BCP

Ziel:

- Gewährleistung der Verfügbarkeit der wichtigsten IT-Systeme und Applikationen innerhalb eines definierten Zeitraumes
- Schadensbegrenzung im Katastrophenfall

E) Klassifizierung von IT-Anwendungen und IT-Systemen, BCP

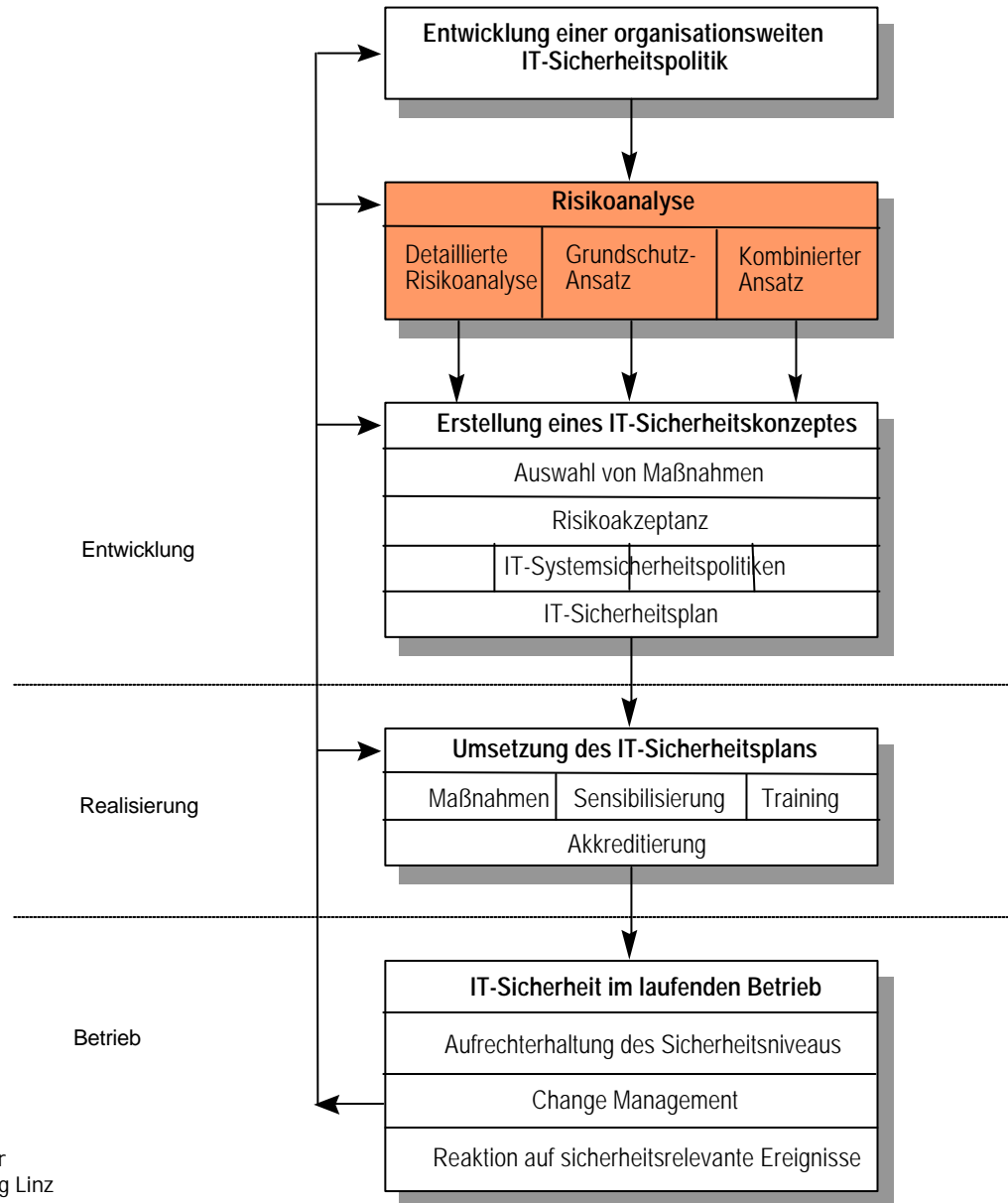
Klassifizierungsschema IT-SIHB 2003:

Betriebsverfügbarkeitskategorie 1: keine Vorsorge (unkritisch)
Ausfall für unbestimmte Dauer beeinträchtigt Aufgabenerfüllung nicht wesentlich

Betriebsverfügbarkeitskategorie 2: Offline-Sicherung
gängige Sicherungsmaßnahmen, externe Auslagerung, Wiederinbetriebnahme der Anwendung erst nach Behebung des Schadens an ursprünglichen System

Betriebsverfügbarkeitskategorie 3: redundante Infrastruktur
bei Ausfall einer Komponente: Fortsetzung des Betriebes ohne Unterbrechung

Betriebsverfügbarkeitskategorie 4: redundanter Standort
redundante Auslegung von Infrastruktur, Systemen und Anwendungen
bei Ausfall eines Standortes: Fortsetzung des Betriebes ohne Unterbrechung



Risikoanalyse-Strategien

A) Detaillierte Risikoanalyse:

- Analyse von Werten, Bedrohungen, Eintrittswahrscheinlichkeiten, Schwachstellen, ...
- Risikobewertung

B) Grundschutzansatz:

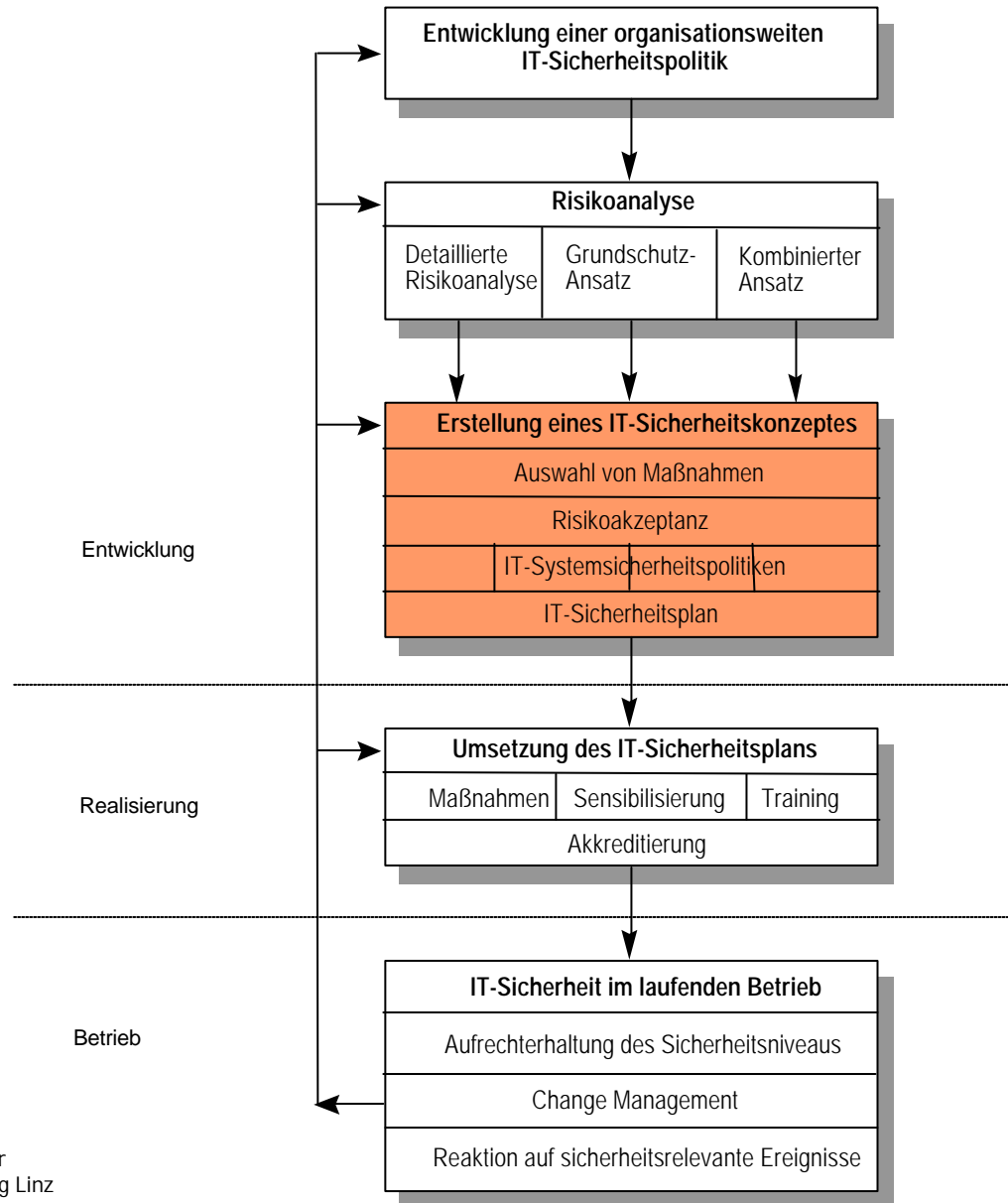
- ausgehend von pauschalisierter Gefährdungslage
- „Standardsicherheitsmaßnahmen“ für mittleren Schutzbedarf

C) Kombiniertes Ansatz:

- Schutzbedarfsfeststellung
- detaillierte RA in ausgewählten Teilen, sonst Grundschutz

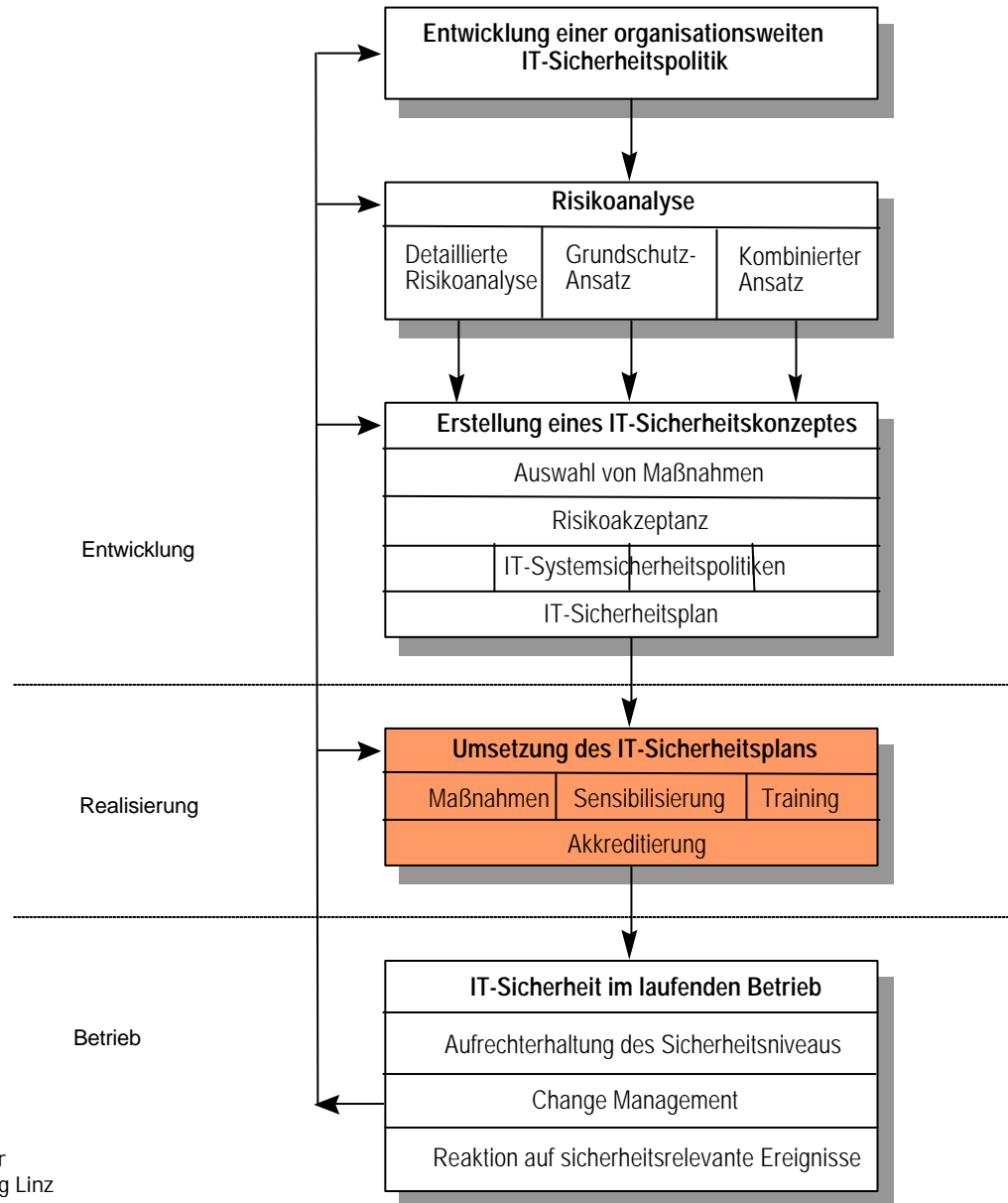
Be sure to
consider all risks ... !





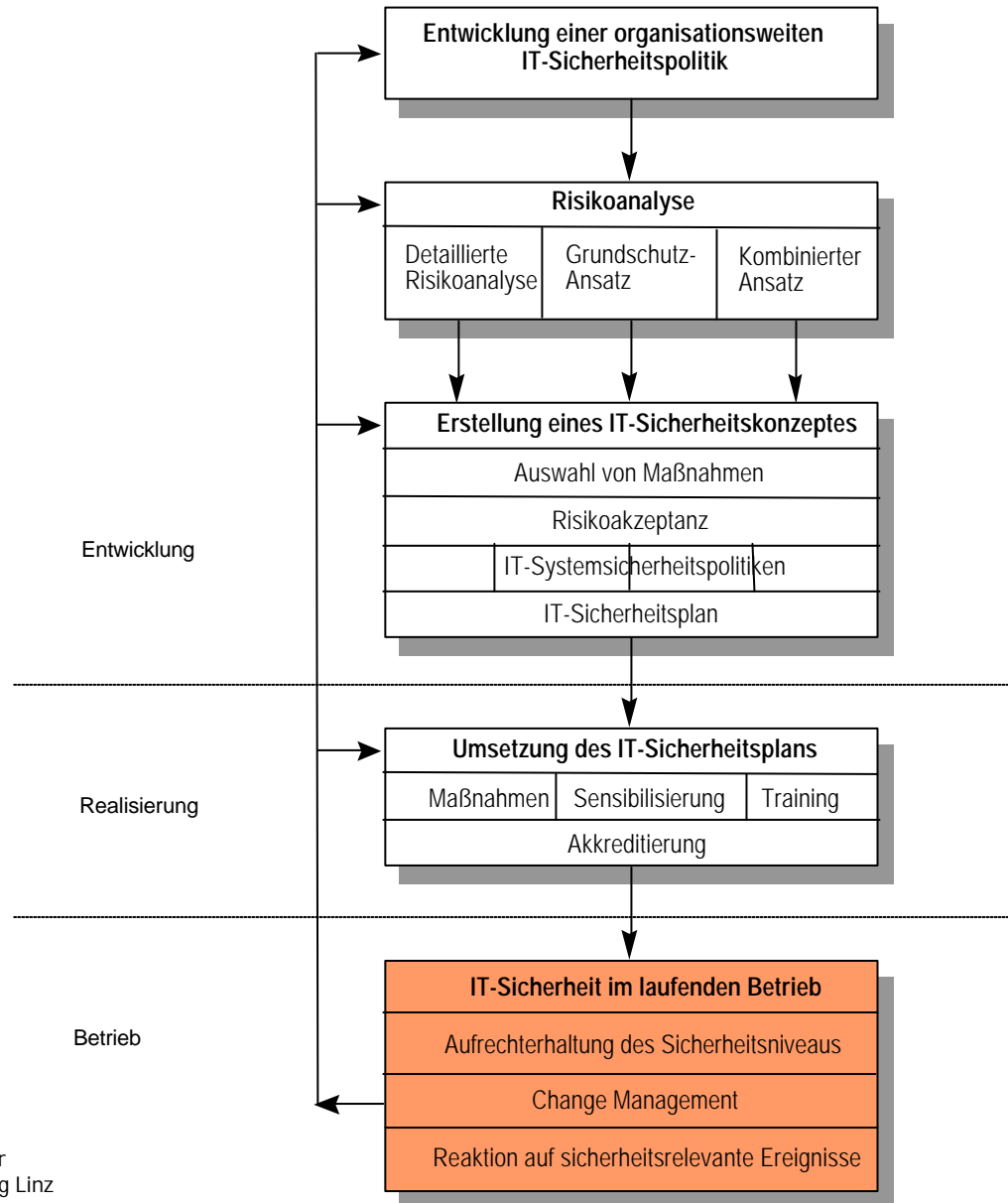
Erstellung eines IT-Sicherheitskonzeptes

- Auswahl von Maßnahmen
 - (informations-)technische, bauliche, organisatorische, personelle
 - organisationsweite - systemspezifische
- Ausgangsbasis
 - existierende Maßnahmen
 - Ergebnis der Risikobewertung
 - Rahmenbedingung
- Risikoakzeptanz
 - Quantifizierung und Bewertung der Restrisiken
 - Entscheidung über nicht-akzeptable Restrisiken
 - Akzeptanz von außergewöhnlichen Restrisiken



Umsetzung von IT-Sicherheitskonzepten in die betriebliche Praxis

- Implementierung von Maßnahmen
 - Implementierung
 - Test
 - Security Compliance Checking
- Akkreditierung:
 - Freigabe des IT-Systems zum Betrieb in einer speziellen Umgebung
- Sensibilisierung und Schulung
 - regelmäßige Veranstaltungen und Publikationen
 - Schulung bei einschneidenden Änderungen
 - Schulung für Mitarbeiter mit speziellen Sicherheitsaufgaben

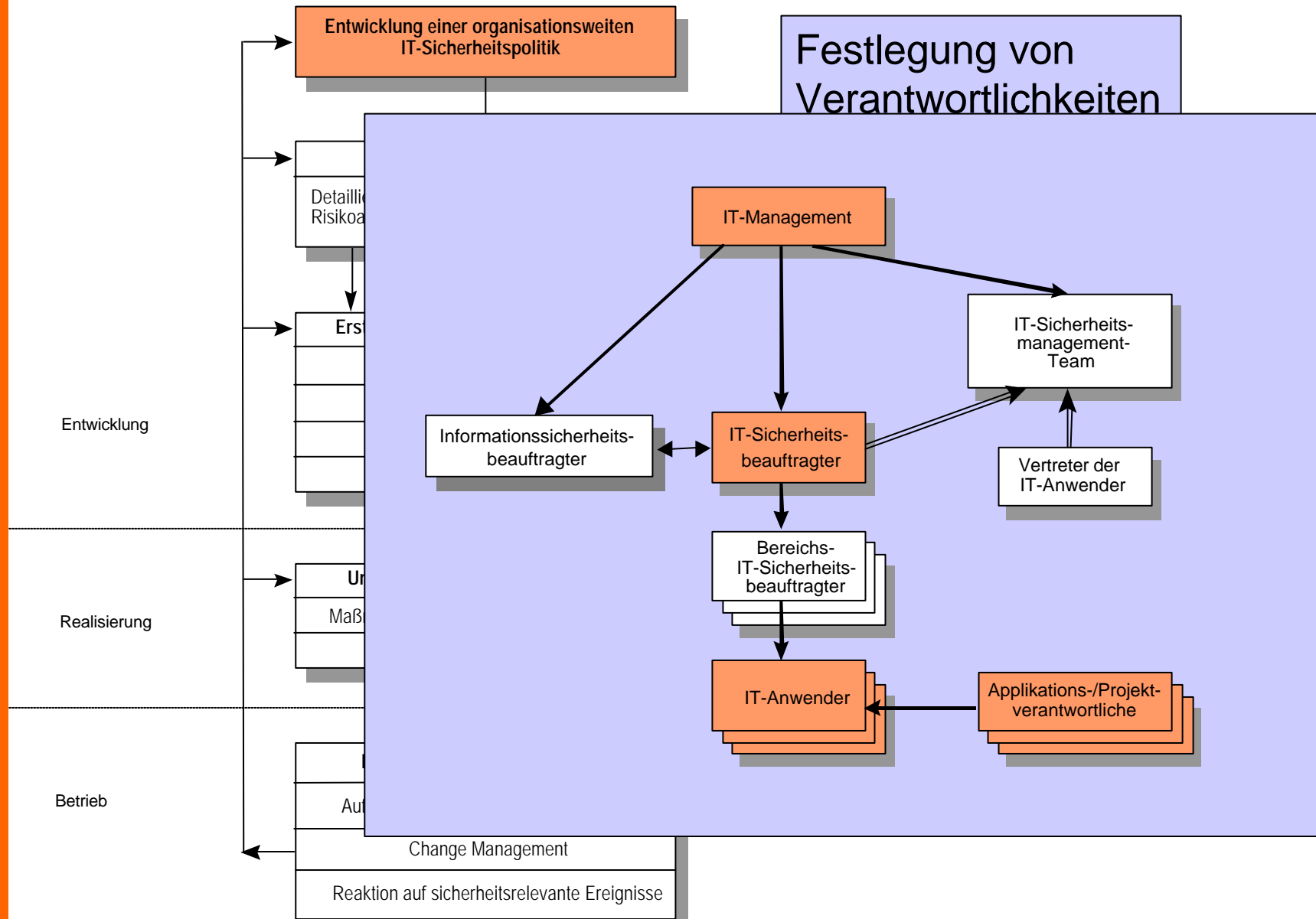


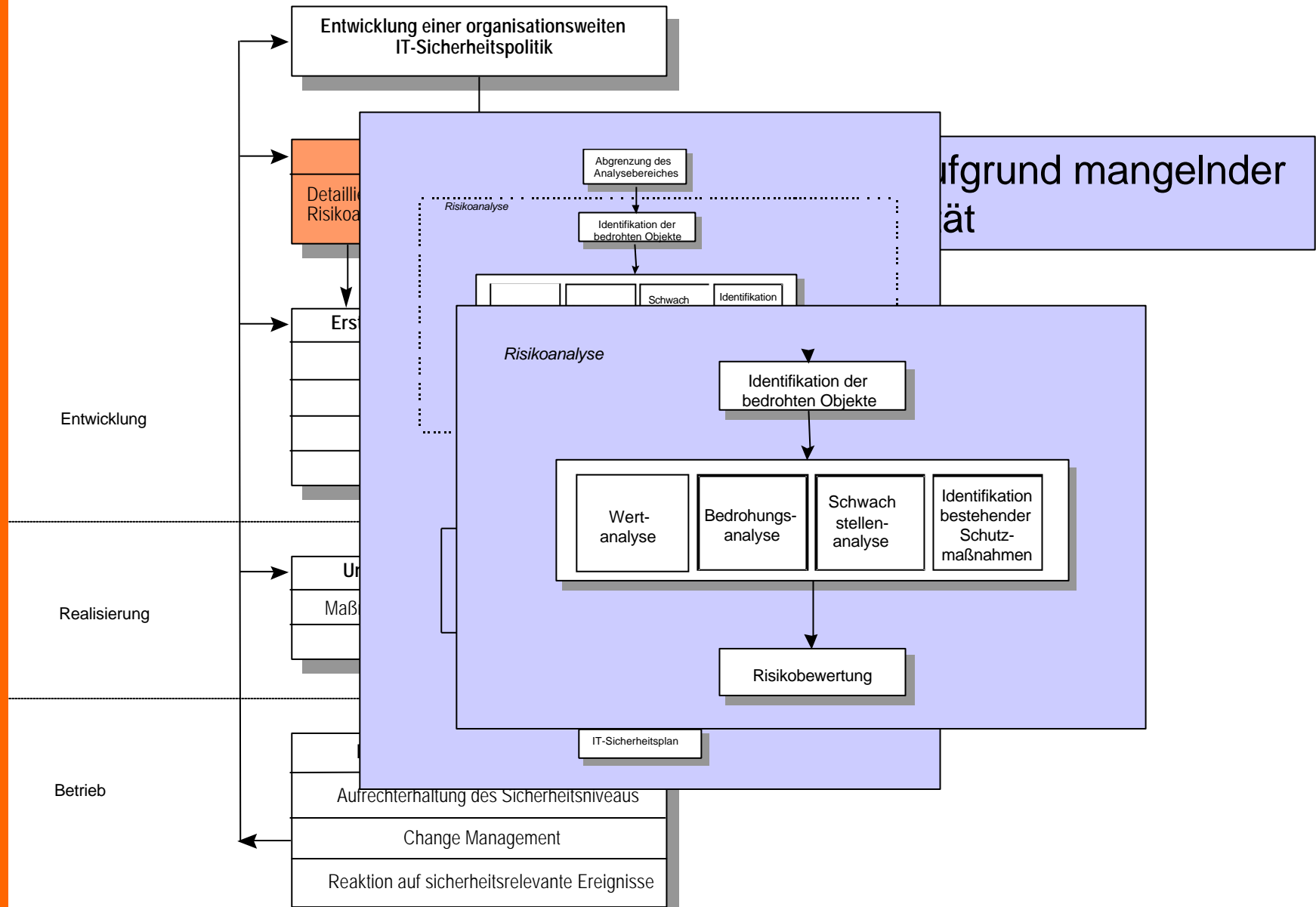
IT-Sicherheit im laufenden Betrieb

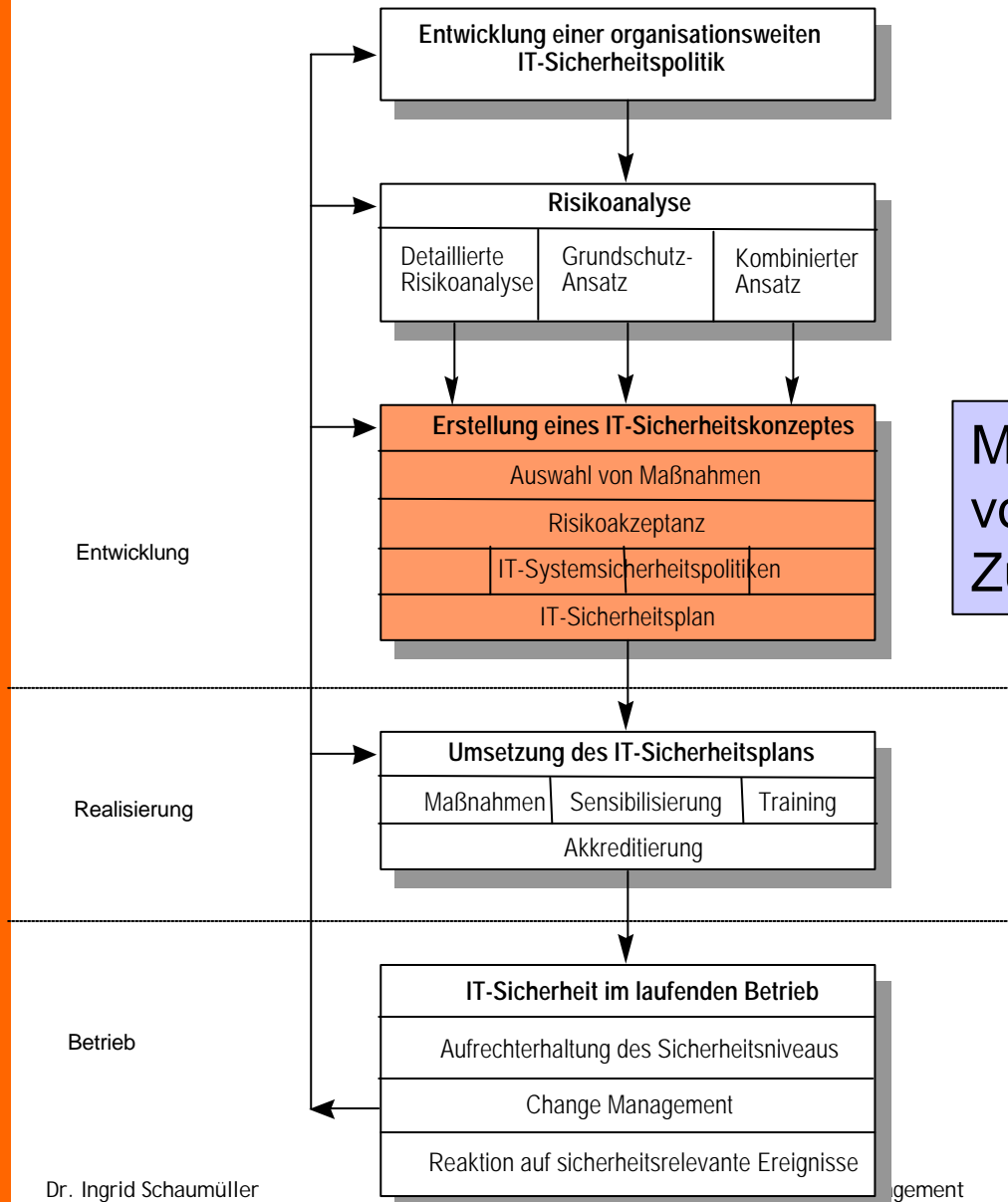
- Aufrechterhaltung des Sicherheitsniveaus
 - Wartung der Sicherheitseinrichtungen
 - fortlaufende Überwachung der IT-Systeme (Monitoring)
- Change Management
 - neue Sicherheitsanforderungen infolge von Systemänderungen
 - angemessene Reaktion auf alle sicherheitsrelevanten Änderungen
- Incident Handling
 - Verantwortlichkeiten und Meldewege
 - nach Möglichkeit in schriftlicher Form (IHP)
 - Protokollierung und Auswertung

Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozess
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität







Maßnahmen zur Sicherstellung von SW-Sicherheit und Zuverlässigkeit

Inhalte von Teil 2 des IT-SIHB

Kapitel 1: Bauliche und infrastrukturelle Maßnahmen

Kapitel 2: Personelle Maßnahmen

Kapitel 3: IT-Sicherheitsmanagement

Kapitel 4: Sicherheit in der Systementwicklung

Kapitel 5: Systemsicherheit

Kapitel 6: Aufrechterhaltung der Sicherheit im laufenden Betrieb

Kapitel 7: Disaster Recovery und Business Continuity Planung

Inhalte von Teil 2 des IT-SIHB

Anhänge:

- A: Wichtige Normen
 - Brandschutz
 - Sicherheitstüren und einbruchhemmende Türen
 - Wertbehältnisse
 - Vernichtung von Akten und Daten
 - IT-Sicherheit
- B: Referenzdokumente
- C: Muster für Verträge, Verpflichtungserklärungen und Inhaltsverzeichnisse
- D: Wichtige Adressen

Themen

- Der Arbeitskreis IT-Sicherheit
- Aufgaben des IT-Sicherheitsmanagements
- Etablierung eines IT-Sicherheitsmanagementprozess
- Aspekte der Software-Sicherheit und Zuverlässigkeit in ISMS
- IT-Sicherheit und SW-Qualität

IT-Sicherheitsmanagement und SW-Qualitätspolitik

Informationssicherheits-Managementsysteme (ISMS)

als Basis für

- sichere Systeme
- zuverlässige Systeme

Unterstützung des Entwicklungsprozesses

Danke für Ihre Aufmerksamkeit!

ingrid.schaumueller@lwest.at