Erfolg des Risk- und Notfall-Managements in Ihrem Unternehmen

Inhalt

- *Das Zusammenspiel zwischen externem Partner und internen Funktionen*
- *Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung*
- *Ansätze zur Erstellung von Notfallhandbüchern im engeren Sinn*

Das Zusammenspiel zwischen Berater und internen Funktionen (Beispiel Notfallhandbuch)

Projektunterstützung in Bezug auf ...

- **Notfallstrategie**
- **Risiko- und Bedrohungsanalysen (RIA)**
- **Geschäftsprozessaufnahme und -analyse**
- **Business Impact Analyse (BIA)**
- **BIA-GAP-Analyse**
- **Notfallplanung (operative Umsetzung = Handbuch)**
- **Szenarioorientierte Testkonzeption (IT / TK und Fachbereiche)**

Das Zusammenspiel zwischen Berater und internen Funktionen (Beispiel Notfallhandbuch)

... durch „Moderation“ und „Support“ mittels ...

- **Workshops zur Methodik, Datensammlung und -verarbeitung**
- **Projektleitung / - management**
- **Unterstützung bei der Anfertigung der notwendigen Dokumentation**
- **Kontinuierliche Einbindung der internen Funktionen zur Vorbereitung auf die künftigen Linienfunktion(en)**

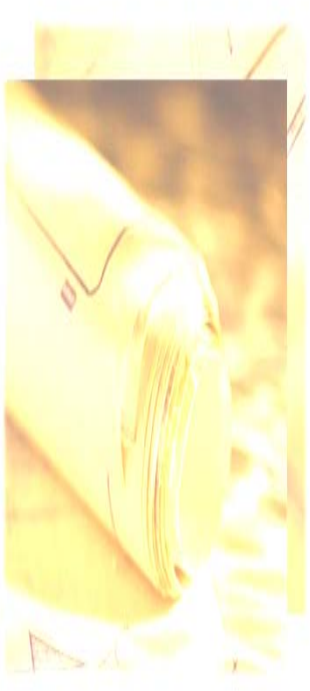
Inhalt

- Das Zusammenspiel zwischen externem Partner und internen Funktionen
- **Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung**
- Ansätze zur Erstellung von Notfallhandbüchern im engeren Sinn

Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung

Gibt es Notfallhandbücher von der Stange?

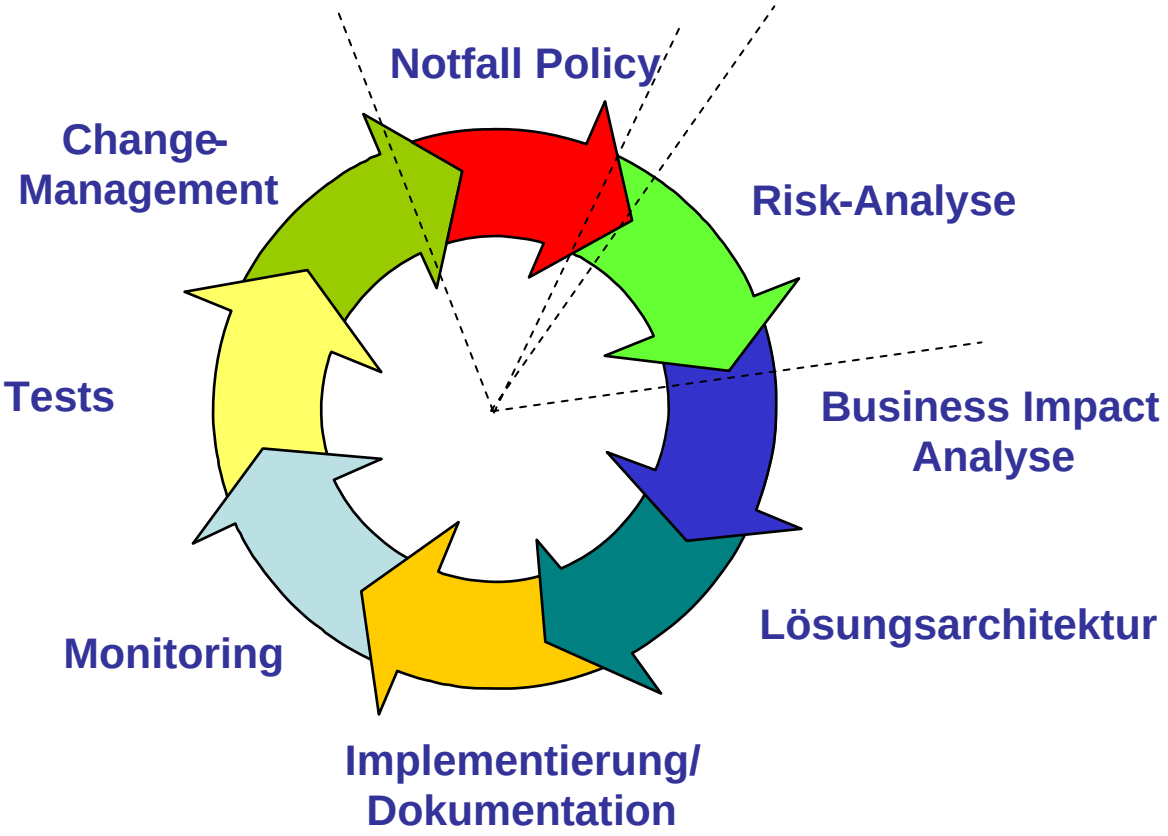
Nein!



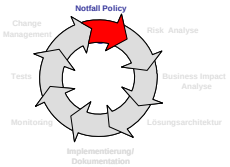
- **Es gibt jedoch „Schablonen“, die zu einer individuellen Maßanfertigung veredelt werden müssen.**
- **Tools können zur Unterstützung eingesetzt werden, müssen aber auch mit individuellen Daten und Prozessabläufen versehen werden und können in keinem Falle die „Beratungsleistung“ ersetzen.**
- **Die folgenden Ausführungen zeigen am Beispiel eines Life-Cycles die entsprechenden Ausprägungen.**

Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung

Ein „Life-Cycle“ als roter Faden für die konkrete Vorgehensweise



Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung

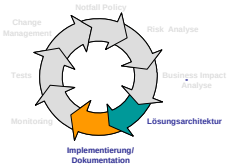


Notfall Policy

- Nutzung von internationalen Standards (z.B. BSI GSHB, BS 25999, BS 27999, ISO 27001, BS7799, COBIT, COSO)
  - Anpassung an die unternehmensspezifischen Bedürfnisse notwendig

Risk- und Business Impact- Analyse

- Erstellung auf Basis von Risikokatalogen und/oder entsprechenden Tools in Bezug auf das Unternehmen
- Detaillierung auf Basis der Risikobereitschaft und der individuellen Anforderungen aller Organisations-einheiten im Unternehmen

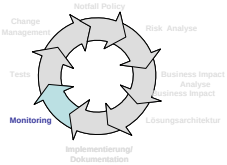


Lösungsarchitektur und -implementierung

- Evaluierung bereits vorhandener Konzepte (ggf. von externen Providern unterstützt)
- „Customizing“ unter Einbeziehung der Analysedaten

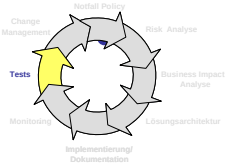
Erläuterung zu den Unterpunkten: 1.Punkt = „von der Stange“ (Standard), 2. Punkt = Maßanfertigung

Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung



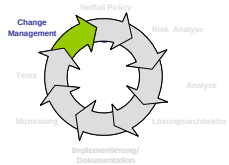
Monitoring

- **Evaluierung von am Markt existenten Verfahren (z.B. Surveys)**
- **Konsolidierung mit anderen Bereichen (z.B, Security, Compliance, OpRisk)**



Tests

- **Nutzung standardisierter Testkonzepte / -methoden**
  - **Ausrichtung auf BCM - Anforderungen und - Besonderheiten**



Change-Management

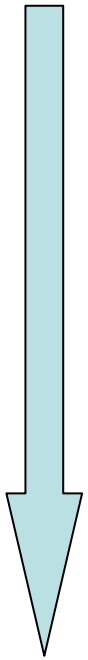
- **Durchführung mittels standardisiertem Workflow - Management**
  - **Einbettung in die internen Rollenkonzepte und Prozesse**

Erläuterung zu den Unterpunkten: 1.Punkt = „von der Stange“ (Standard), 2. Punkt = Maßanfertigung

Inhalt

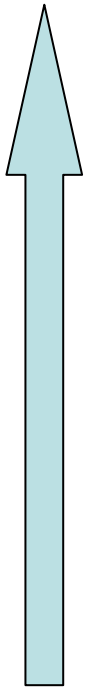
- Das Zusammenspiel zwischen externem Partner und internen Funktionen
- Notfallhandbuch „von der Stange“ oder doch als Maßanfertigung
- **Ansätze zur Erstellung von Notfallhandbüchern im engeren Sinn**

Ansätze zur Erstellung von Notfallhand-büchern im engeren Sinn



- **Top down**
  - **Auswertung/Aufnahme der Geschäftsprozesse**
  - **Relevanz der Geschäftsprozesse führt zu den „lebens-wichtigen“ Systemmodulen und ihren Abhängigkeiten zueinander**
  - **Auswertung der RIA[1)] / BIA[2)] in Bezug auf die relevanten Geschäftsprozesse**
  - **Analyse der Systemabhängigkeiten zueinander**
  - **RTO[3)] / RPO[4)] für die Systeme leiten sich aus den Geschäftsprozessangaben ab**
  - **Maßnahmen leiten sich aus RTO / RPO Angaben sowie den Systemabhängigkeiten ab**
  - **…**

Ansätze zur Erstellung von Notfallhand-büchern im engeren Sinn



- **Bottom up**
  - **Maßnahmen leiten sich aus RTO / RPO Angaben und den Abhängigkeiten der Systeme zueinander ab**
  - **RTO / RPO für die Systeme festlegen**
  - **Beschreibung der Abhängigkeiten der Syteme zueinander analysieren**
  - **Geschäftsprozessrelevanz der System ermitteln**
  - **Relevanz der Geschäftsprozess ermitteln**
  - **Ableitung der Relevanz für jedes System**
  - **RIA, BIA für jedes System**
  - **Aufnahme jeden Systems**
  - **…**

Ansätze zur Erstellung von Notfallhand-büchern im engeren Sinn

Top down

Vorteile:

- Zusammenhang zwischen den Geschäfts-prozessen und Systemen i.d.R. einfacher ableitbar
- Konzentriert sich direkt auf die überlebens-wichtigen Systeme
- Leitet Rangreihenfolge zur Wiederher-stellung der Systeme gemäß Kritikalitäts-einstufung der Geschäftsprozesse ab
- Test kann schneller modular aufgebaut werden, da bekannt ist, welche Systeme welche Geschäftsprozesse unterstützen
- Konzentration nur auf die wesentlichen Systeme und Systemkomponenten
- …

Nachteile:

- Kritikalitätseinstufung der Geschäftsprozesse muss bereits vorliegen
- Zusammenhänge zwischen Geschäftsprossen und Systemen müssen vorliegen
- CMDB Informationen dienen als Ergänzungsbasis
- …

Bottom up

Vorteile:

- Erfassung aller Systeme – keines wird „vergesessen“
- Zusammenhänge der Systeme werden eindeutig dargestellt
- Kritikalitätseinstufung der Geschäftsprozesse muss nicht von Anfang an vorliegen
- Alle Systeme gleichwichtig – Wiederanlauf-reihenfolge durch technische Notwendigkeit bestimmt
- …

Nachteile:

- Alle Systeme müssen aufgenommen werden – sehr Zeitaufwendig
- Geschäftsprozessbewertung muss vorgenommen werden
- Zusammenhänge zwischen Geschäftsprossen und Systemen werden aus Systemsicht erarbeitet
- CMDB Informationen müssen sehr gut gepflegt sein, da Ausgangsbasis für das handeln
- …

Fazit

Die Entscheidung des Ansatzes obliegt ausschließlich der Geschäftsführung bzw. dem Vorstand.

Unter anderem aus dem § 43 Abs 1 GmbHG bzw. dem § 93 Abs 1 Satz 1 AktG abzuleiten sowie u. a. aus dem KonTraG, dem BDSG, der GDPdU als auch dem BDSG. Die hierin beschriebene Verantwortlichkeiten lassen sich nicht delegieren – analog zur Verantwortlichkeit des Unternehmens für die Ordnungsmäßigkeit der Geschäftsprozesse, welche im Outsourcing durchgeführt werden.

Erfahrungsgemäß ist der „Top down“ Ansatz zu empfehlen, da dieser sich direkt auf die wesentlichen Geschäftsprozesse des Unternehmens konzentriert und somit auch die daraus abgeleiteten Arbeiten zu Notfallhandbüchern für die entsprechenden Systeme.

Wir freuen uns auf Ihr Feedback sowie auf eine mögliche Zusammenarbeit.

Danke für Ihre Aufmerksamkeit!

Klaus-Dieter Krause

Dipl.-Inform. - FR Wirtschaftsinformatik
CMC, MBCI, CISA, CISM, ITILFZ, DSB, QAR-IT

KK Management Consulting

Unternehmensberatung BDU

Spatzenweg 11 - 53844 Troisdorf
Tel.: +49 (0) 2241 945 470
Mobil: +49 (0) 172 65 17 99 5
E-Mail: klaus.d.krause@kkmc.de
www: www.kkmc.de

Fazit

Ein Berater *hilft*

***Ressourcen* zu *schonen* und**

unabhängig* ggf. vorhandene *Lücken

zu *schließen*.

Backup sheets