KPMG

Advisory

2. Deutschsprachiger BCI Kongress „Die Prüfung des Business Continuity Managements“

Matthias Hämmerle MBCI

Frankfurt

19. September 2007

Business Continuity Institute

AUDIT ▪ TAX ▪ ADVISORY

Würden Sie mit diesem Flieger fliegen?

Durchsage des Piloten:
„Sehr geehrte Passagiere, ich freue mich Ihnen mitteilen zu können, daß wir heute etwas früher abfliegen können und Sie kostenlose Verpflegung an Bord erhalten, denn unsere Fluggesellschaft verzichtet ab sofort auf alle Prüfungen der Notsysteme. Wir hatten in letzter Zeit keinen Unfall.“

… oder doch nicht?

be prepared!

AGENDA

Inhalt

- **Compliance des Business Continuity Managements**
- **Das Audit im Rahmen des BCM Lifecycle**
- **Der BCM Prüfungs Prozess**
- **Reviews von Notfallereignissen**

Verletzungen der Compliance Anforderungen ist ein Kündigungsgrund für Vorstände und Geschäftsführer

Nicht immer endet eine fehlende oder mangelhafte Prüfung tödlich, aber immer öfter mit dem Verlust des (Vorstands-)Jobs:

Das Landgericht Berlin sowie das Kammergericht Berlin hatten sich mit der fristlosen Kündigung eines Mitglieds des Bankvorstandes der Bankgesellschaft Berlin zu beschäftigen[1)]:

Die **fristlose Kündigung eines Mitglieds des Bankvorstands** war gerechtfertigt: Das Risikomanagement der Bankgesellschaft erfüllte die gesetzlichen Anforderungen nicht.
Auf einer ersten Stufe habe dabei der Vorstand die **Früherkennung bestandsgefährdender Entwicklungen** durch geeignete Maßnahmen **zu gewährleisten** und auf einer zweiten Stufe die eingeleiteten Maßnahmen **zu überwachen**.

[1)] Landgericht Berlin: Urteil vom 3. Juli 2002, Az: 2 O 358/01; Kammergericht Berlin: Urteil vom 27.09.2004, Az 2 U 191/02

Vorstände haften persönlich für die Schäden aus Pflichtverletzungen

Das Landgericht München entschied, daß der Hauptversammlungsbeschluss zur Entlastung des Vorstands für nichtig erklärt wurde[1)]:

Bei einem Münchner Großhändler für Mikroelektronik **mangelte es u.a. an der schriftlichen Dokumentation des Risikomanagements und der dahinter liegenden IT-Struktur**.
Nach Auffassung des LG München stellte die **fehlende Dokumentation des Risiko-Früherkennungssystems einen schwerwiegenden Rechtsverstoß des Vorstandes** dar.
Diese Versäumnisse stellen einen wichtigen Grund zur **außerordentlichen fristlosen Kündigung des Dienstvertrags und der Abberufung** dar.
Entstehen dem Unternehmen Schäden, können die Vorstände persönlich in die Haftung genommen werden.
Bei gravierenden Pflichtverletzungen und schwerwiegenden Schäden (wie z. Bsp. Durch Systemausfälle, Datenverluste oder Sicherheitslücken) kann die Gesellschaft trotz Entlastungsbeschluss **Schadenersatz** von den Vorständen verlangen

[1)] Landgericht München: Urteil vom 5. April 2007, Az: 5 HKO 15964/06

Die rechtliche Grundlage für die Compliance Anforderungen bildet das KonTraG

- **Gesetz zur Kontrolle und Transparenz in Unternehmen (KonTraG)**
  - § 91 Abs. 2 AktG Organisation. Buchführung, [1]
    - Der Vorstand einer Aktiengesellschaft hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden können
    - Wurden Risiken erkannt, muss die Unternehmensleitung entsprechende Maßnahmen ergreifen, um eine Pflichtverletzung zu vermeiden, z.B. Verfahren einrichten und Zuständigkeiten bestimmen.
  - § 93 Abs. 2 AktG Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder, [2]
  - § 43 Abs. 1,2 GmbHG Haftung der Geschäftsführer
  - Kommt es zu einem Unternehmensschaden, muss der Vorstand den Beweis erbringen, dass er Maßnahmen zur Risikofrüherkennung und –überwachung getroffen hat.[3]

1 KonTraG, KapAEG, StückAG, EuroEG; Textausgabe mit Begründungen der Regierungsentwürfe, Stellungnahmen des Bundesrates mit Gegenäußerungen der Bundesregierung; Ernst, Christoph; IDW-Verlag;1998; Nr. 9, § 91 AktG.

2 Aktiengesetz; Beck´sche Kurz-Kommentare; Hüffer, Uwe; Beck; 2006; RN 16, S. 489f.

3 Rechnungslegung und Prüfung der Unternehmen, Kommentar zum HGB, AktG, GmbHG, PublG nach den Vorschriften des Bilanzrichtlinien-Gesetzes; Adler, Düring, Schmaltz; 6. Auflage; Schäffer-Pöschel; 2001; S. 304ff., insb. RN 38.

Für Finanzdienstleister sind die Anforderungen an ein Notfallmanagement in den MaRisk konkretisiert

- **Mindestanforderungen für das Risikomanagement (MaRisk)***
  - AT 7.3 Abs. 1 Notfallkonzept

    „Für Notfälle in kritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen."

  - AT 7.3 Abs. 2 Notfallkonzept

    „Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen. Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind festzulegen.

    „Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen."

Die MARisk für Versicherungen liegen im Entwurf vor:
Analog zu den Banken forden die MaRisk für Versicherungen die Implementierung eines Notfallkonzepts.

*(Rundschreiben 18/2005 des BaFin auf der Grundlage des § 25a Abs. 1 (Besondere organisatorische Pflichten von Instituten) des Kreditwesengesetzes (KWG), Fassung vom 17.08.2006; gültig per 1.1.2007)

AGENDA

Inhalt

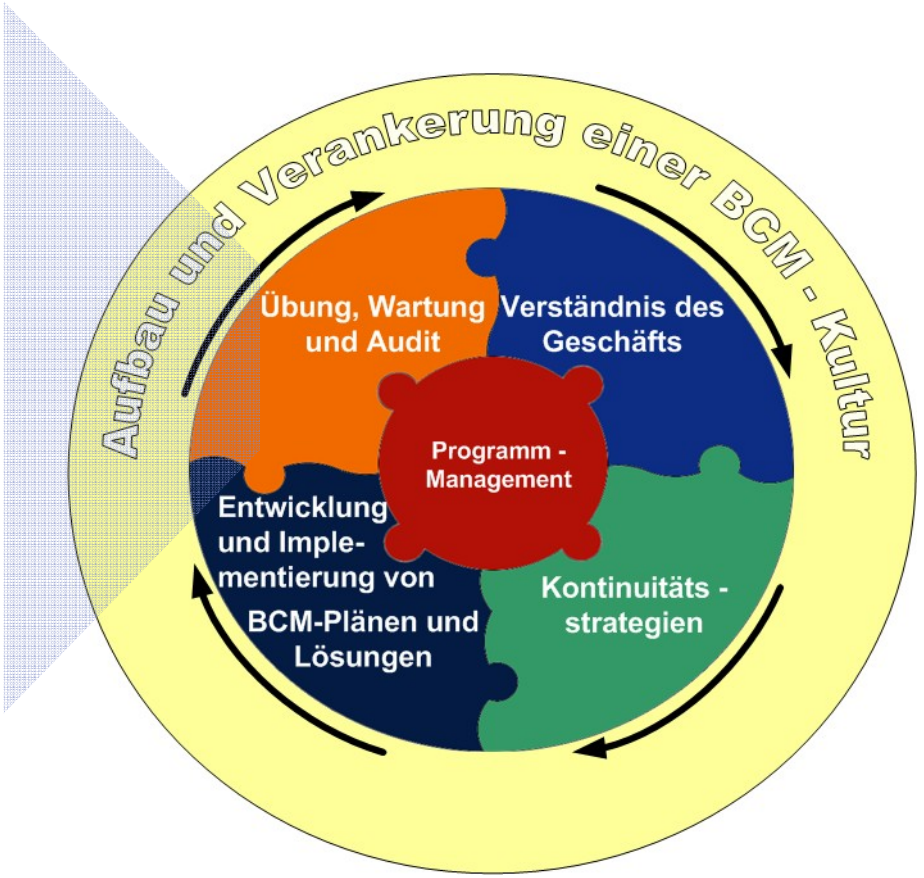
- **Compliance des Business Continuity Managements**
- **Das Audit im Rahmen des BCM Lifecycle**
- **Der BCM Prüfungs Prozess**
- **Reviews von Notfallereignissen**

BS 25999-1 sieht die Überwachung und Prüfung im Rahmen des BCM Lifecycle vor

Überwachung und Prüfung des BCM:

- **Audit (intern und extern):**
  Review der existierenden BCM (Kompetenzen und Fähigkeiten gegen zuvor festgelegte Standards und Kriterien)

- **Self-Assessment:**
  Prüfung des BCM gegen die Ziele des Unternehmens, Industrie-Standards und Best Practices



Es existieren gegenwärtig wenige Regelungen gegen die ein BCM geprüft werden kann (verglichen mit ITSCM)

IT Service Continuity Management:
- **ausführliche und weltweit akzeptierte Standards und Best Practices**

- ISO 20000:
  Availability Management und IT Service Continuity Management
- ISO 27001
  Information Security
- ITIL:
  Availability Management und IT Service Continuity Management
- PAS 77
  IT Service Continuity Management
- IDW[1] Prüfungsstandards
  IDW EPS 330

Business Continuity Management:
- **nationale Standards**
- **branchenspezifische Regelungen**

- KonTraG:
  Generalnorm, ohne inhaltliche Präzisierung der Umsetzung
- MaRisk
  lediglich für Banken, wenig präzise
  MaRisk für Versicherungen im Entwurf
- Nationale Standards:
  Bsp.: BS 25999-1, BS 25999-2
- Best Practices
  GPG des BCI

Standards, Normen und Best Practices konzentrieren sich auf das IT Service Continuity Management
Für das Business Continuity Management fehlen vergleichbare internationale (ISO-) Normen als Basis für Prüfungen und Zertifizierungen

1 IDW: Institut der Wirtschaftsprüfer

Der neue BSI Standard 100-4 Notfallmanagement – die Lösung?

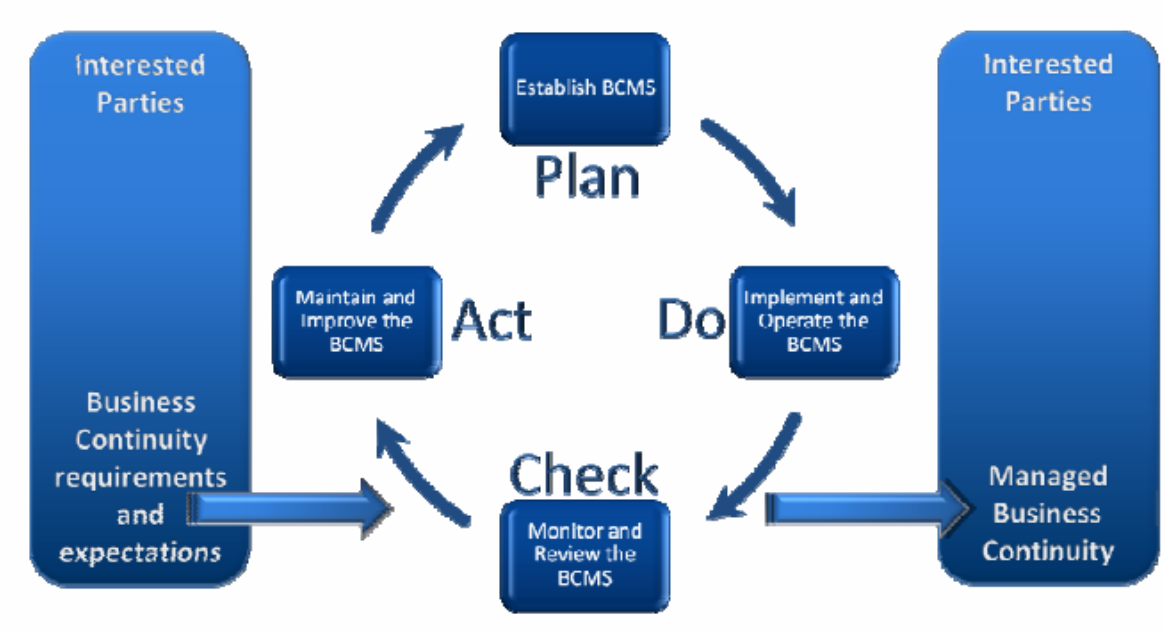
- Mit dem neuen BSI Standard 100-4 „Notfallmanagement“ wird es einen deutschen Standard geben, der eng an BS 25999-1 angelehnt ist
- Die Grundschutzkataloge haben hohe Akzeptanz innerhalb von Deutschland

- Die Grundschutzkataloge adressieren die IT
- BCM wird hierdurch automatisch (wieder) in der IT adressiert
- Die Grundschutzkataloge sind international nicht anerkannt
- International agierende Unternehmen benötigen einen international bekannten und anerkannten Standard für das BCM

Ein ISO Standard (auch) für das Business Continuity Management ist unabdingbar

BS 25999-2 als Grundlage für das Audit

- BS 25999-2 ist eine Spezifikation auf Basis von BS 25999-1 als Grundlage für das interne und externe Audit sowie Zertifizierungsbehörden
- Die Spezifikation definiert Anforderungen an ein effektives Business Continuity Management System (BCMS)
- Grundlage ist das auch in anderen Standards zugrundegelegte Plan-Do-Check-Act Modell (PDCA)



BS 25999-2: Monitoring und Review des BCM (aus dem Entwurf)

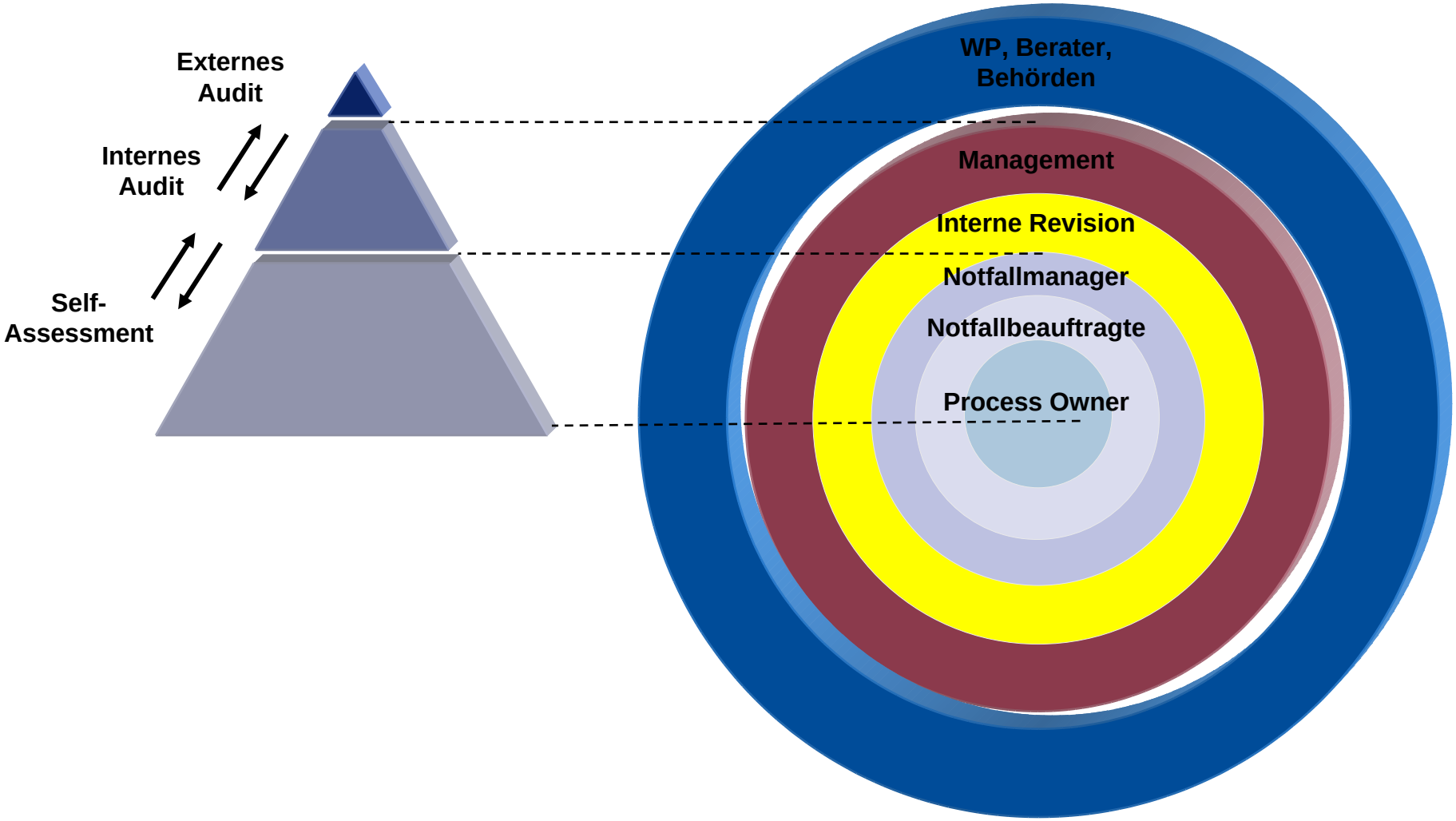
- Reviews können über Audits oder Self-Assessments erfolgen
- Das Management soll das BCM in geplanten Zeitabständen einem Review unterziehen
- Ziel der Reviews ist es, die Funktionsfähigkeit, Angemessenheit und Effektivität des BCM sicherzustellen
- Reviews sollen Verbesserungsmöglichkeiten für das BCM identifizieren
- Die Ergebnisse der Reviews sind zu dokumentieren und Maßnahmen nachzuhalten
- Ergebnisse eines Reviews
  - Entscheidungen und Maßnahmen
    - Um die Effektivität des BCM zu verbessern
    - Zur Anpassung von Prozeduren des BCM, um besser auf interne oder externe Ereignisse reagieren zu können
    - Zu Ressourcenbedarfen
    - Zu Budgeterfordernissen

AGENDA

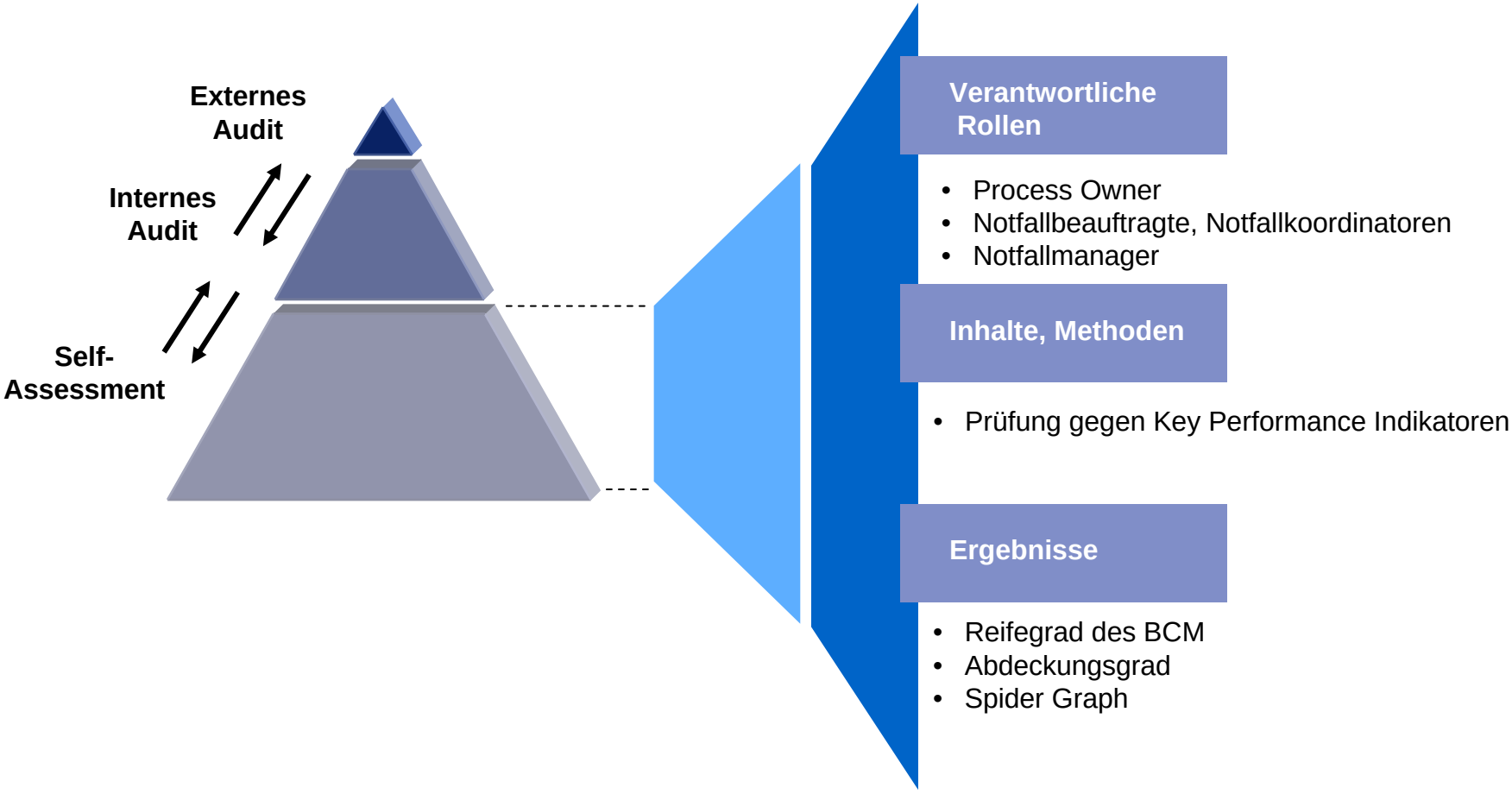
Inhalt

- **Compliance des Business Continuity Managements**
- **Das Audit im Rahmen des BCM Lifecycle**
- **Der BCM Prüfungs Prozess**
- **Reviews von Notfallereignissen**

Die Prüfung des BCM ist ein abgestuftes und abgestimmtes Verfahren



Self-Assessment



Verantwortliche Rollen

- Process Owner
- Notfallbeauftragte, Notfallkoordinatoren
- Notfallmanager

Inhalte, Methoden

- Prüfung gegen Key Performance Indikatoren

Ergebnisse

- Reifegrad des BCM
- Abdeckungsgrad
- Spider Graph

BCM Key Performance Indicators (KPI) – Beispiele (1)

Notfallpolicy	• Existiert eine Dokumentation des BCM, die vom Vorstand / Geschäftsleitung freigegeben ist? • Existiert eine Dokumentation des BCM, die vom Vorstand / Geschäftsleitung freigegeben ist?
Notfallorganisation	• Existiert eine Notfallorganisation für den Normalbetrieb, das Krisenmanagement und den Notbetrieb? • Ist die Notfallorganisation aktuell?
Business Impact Analyse	• Wann wurde die letzte Business Impact Analyse durchgeführt / aktualisiert? • Abdeckungsgrad der Geschäftsprozesse: sind die unternehmenskritischen Geschäftsprozesse abgedeckt?
Planung	• Ist die Notfallplanung vollständig? (Krisenmgt., Geschäftsfortführung, Wiederanlauf, Kommunikation) • Ist die Notfallplanung aktuell? • Sind ITSCM- und BCM-Notfallplanungen aufeinander abgestimmt?

BCM Key Performance Indicators (KPI) – Beispiele (2)

Wartung

- Existiert ein Wartungsprozess für das BCM?
- Wird der Wartungsprozess gelebt?

Tests, Übungen

- Wann wurden die letzten Tests, Übungen durchgeführt?
- Sind Testdurchführung und Ergebnisse dokumentiert?

Audit

- Existiert ein Audit Plan für das BCM?
- Ist die interne Revision eingebunden?
- Ist das BCM Inhalt der regulären Revisionsplanung?

Maßnahmen

- Wird die Umsetzung von BCM-Maßnahmen überwacht?
- Wie ist der Stand der Umsetzung?
- Gibt es regelmäßiges BCM Reporting an den Vorstand, Geschäftsführung?

BCM Key Performance Indicators (KPI) – Beispiele (3)

Awareness

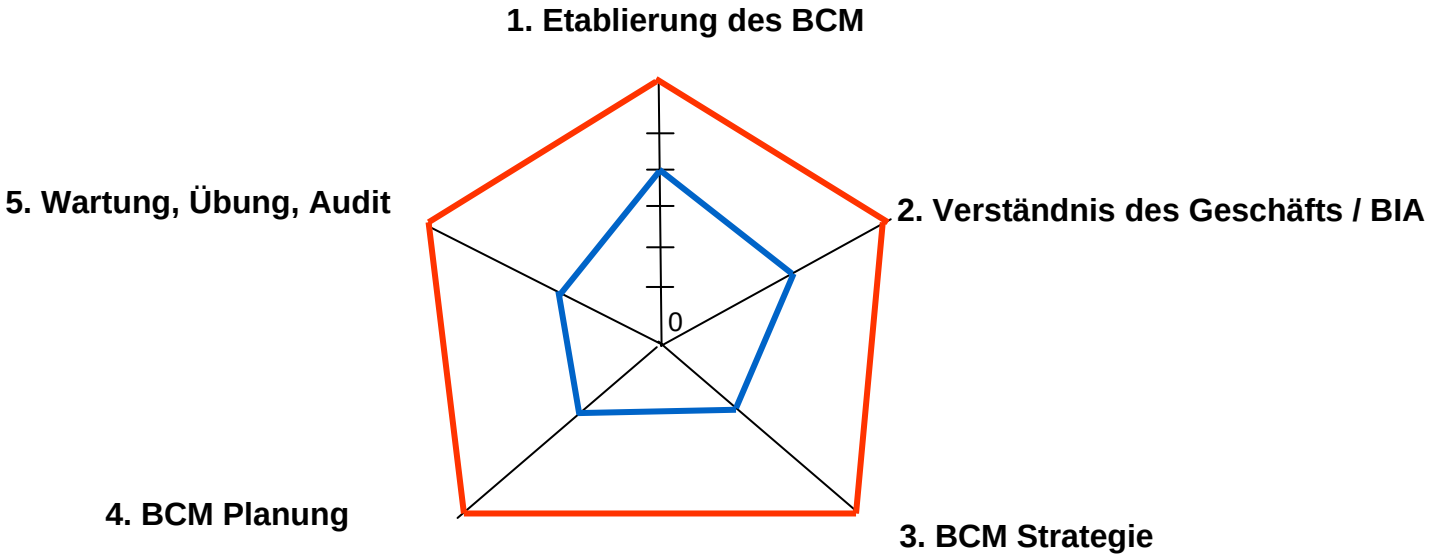
...

...

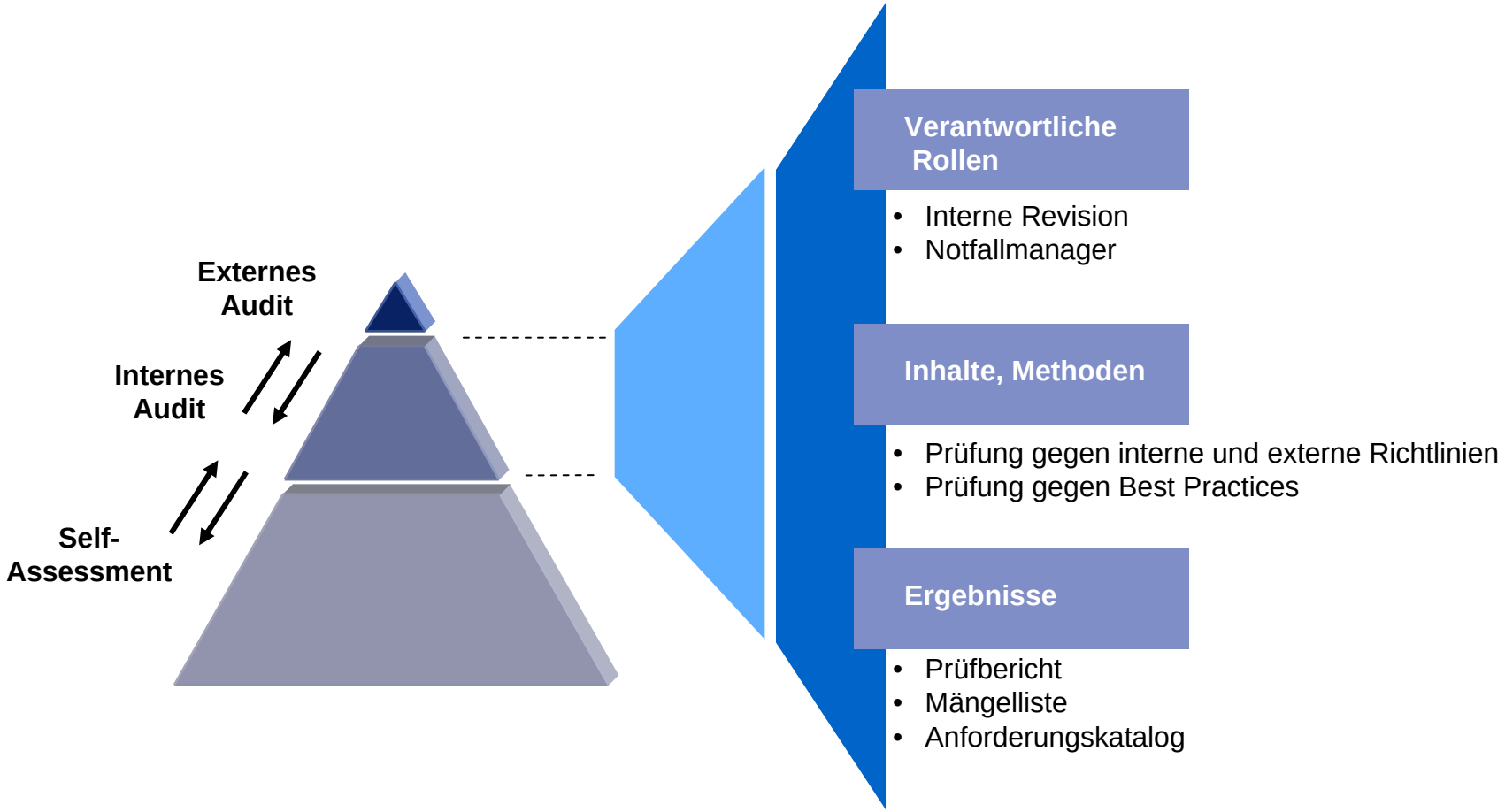
...

- Ist das BCM im Unternehmen bekannt?
- Steht ausreichend Budget für eine angemessene Realisierung zur Verfügung?
- Gibt es einen Verantwortlichen im Vorstand, in der Geschäftsleitung?

Ergebnis: Reifegradbestimmung



Internes Audit

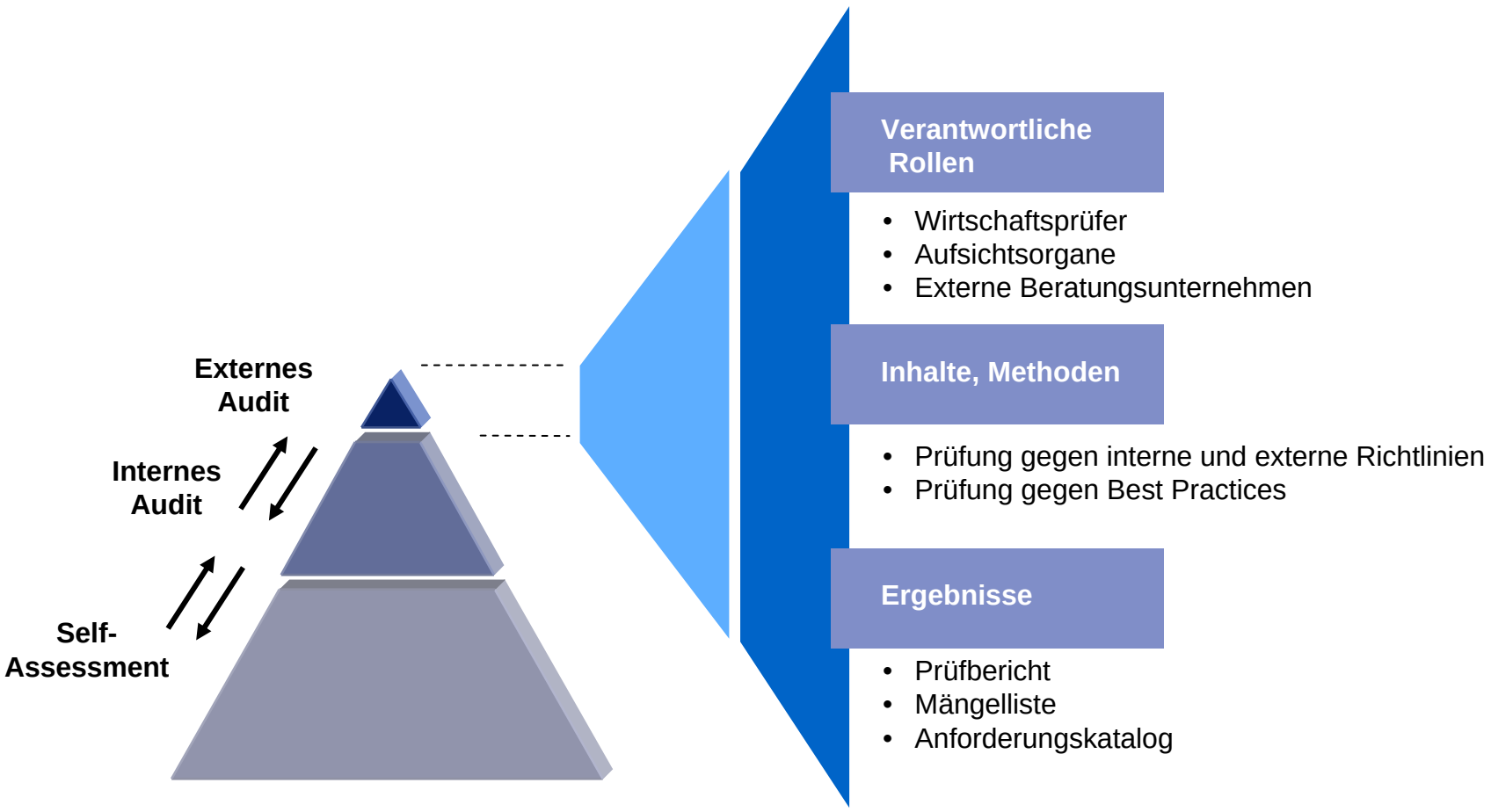


Die Rolle der internen Revision im BCM

Die interne Revision sollte eine zentrale Rolle bei der Implementierung des BCM einnehmen

- Abstimmung der Standards als Grundlage für die Prüfung
- Aufnahme der Prüfung des BCM in das Prüfungsprogramm der internen Revision
- Beteiligung bei Tests und Übungen (z. Bsp. Als unabhängige Beobachter)
- Durchführung interner Audits zum BCM durch die interne Revision
- Überwachung der Maßnahmen
- Unterstützung der Awareness im Unternehmen und bei Vorstand / Geschäftsleitung

Externes Audit



Ziel des Review-Prozesses ist es, die Angemessenheit, Effektivität, und Compliance sicherzustellen (1)

Angemessenheit

- Das BCM ist auf die Art, Komplexität und Kritikalität des Unternehmens anzupassen:
  es gibt kein „BCM out of the box“
- Innerhalb eines Unternehmens ist das BCM in Abhängigkeit der Kritikalität der Prozesse zu differenzieren:
  Handelsgeschäfte erfordern eine andere Notfallvorsorge als Marketingaktionen
- Die Differenzierung im Notfallvorsorgebedarf ist nachvollziehbar zu dokumentieren. Dies erfolgt im Rahmen einer „Business Impact Analyse“

Ziel des Review-Prozesses ist es, die Angemessenheit, Effektivität, und Compliance sicherzustellen (2)

Effektivität / Funktionsfähigkeit

- Das BCM muß angemessen geregelt und dokumentiert sein (BCM-Policy, Notfallpläne, BIA-Dokumentation, BCM-Organisation)
- Für das BCM sind Verantwortlichkeiten festzulegen sowohl für den Normal-, als auch für den Notbetrieb
- Die Aktualität der BCM-Dokumentationen und der BCM Organisation muß sichergestellt sein
- Die laufende Aktualisierung der BCM Dokumentationen muß sichergestellt sein
- Die BCM Verfahren müssen den Mitarbeitern im Unternehmen bekannt sein
- Die Funktionsfähigkeit eines BCM kann letztendlich nur über Test sichergestellt werden und nachweisbar gemacht werden

Ziel des Review-Prozesses ist es, die Angemessenheit, Effektivität, und Compliance sicherzustellen (3)

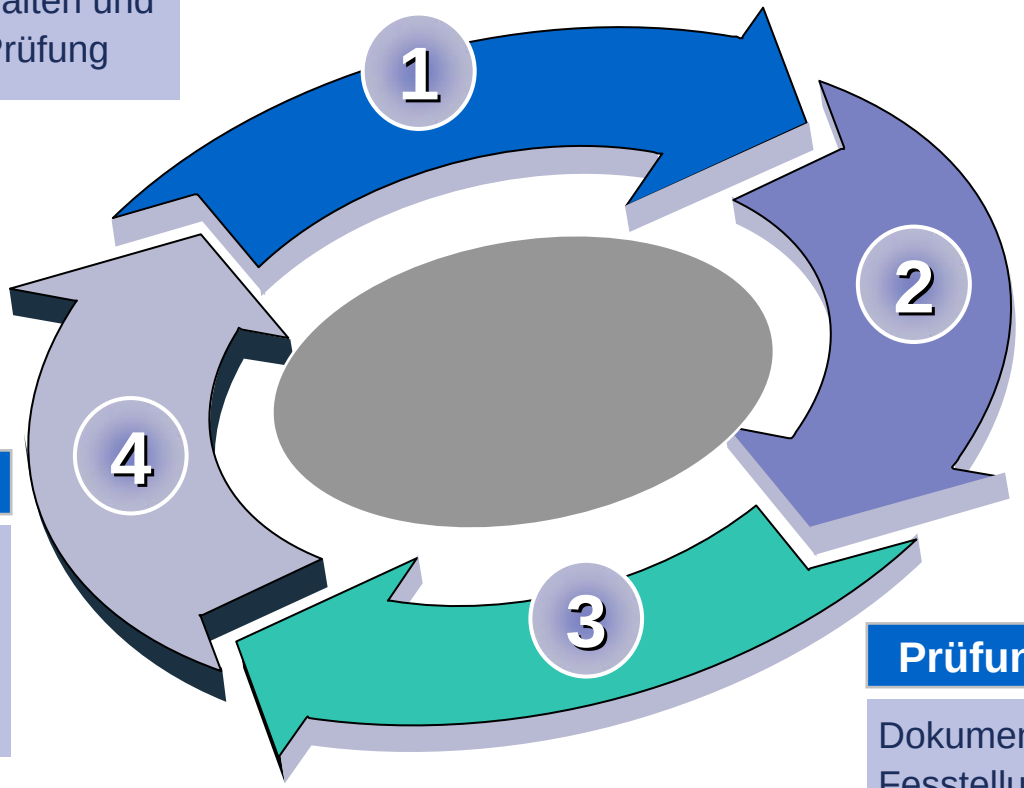
Compliance

- Identifikation der gesetzlichen und aufsichtlichen Regelungen, die für das Unternehmen relevant sind
- Festlegung zu verwendender Standards, Best Practices
- Einbindung der internen Revision
- Abstimmung mit den Wirtschaftsprüfern
- Compliance-gerechte Dokumentation des BCM

Der BCM Prüfungs-Prozess (1)

BCM Prüfungsplan

Festlegung von Zielen, Umfang, Inhalten und Rollen der Prüfung



BCM Prüfung

Prüfung des BCM gegen definierte Standards und Performance Indikatoren

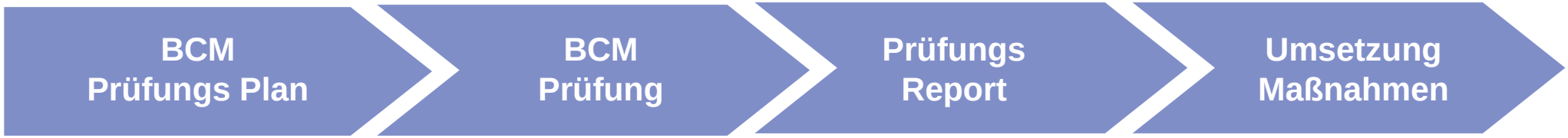
Maßnahmen

Monitoring der Umsetzung der Maßnahmen, Dokumentation

Prüfungsbericht

Dokumentation der Fesstellungen und des Handlungsbedarfs

Der BCM Prüfungs-Prozess (2)



Festlegung

- Der Art der Prüfung:
  - •Compliance
  - •Effektivität
  - •Angemessenheit
- Der Prüfungsziele und –ergebnisse
- Der Normen und Standards gegen die geprüft wird
  - •Prüfungs-Framework
- Des Prüfvorgehens
  - •Dokumentenanalyse
  - •Interviews, Befragungen
  - •Reviews von Ergebnissen und Maßnahmen
- Interne / externe Prüfung

Durchführung

- Dokumentenanalyse
  - •Policy
  - •Pläne
  - •Testdokumentationen
- Interviews
- Begehungen
  - •Rechenzentren
  - •Ausweichstandorte
  - •Command Centre

Analyse und Report

- Abweichungen gegen Gesetze, Standards und Best Practices
- Abgleich gegen Key Performance Indicators
- Stand der Awareness im Unternehmen
- Reifegrad des BCM
- Maßnahmenempfehlungen

Analyse und Report

- Monitoring des Umsetzungsstandes der Maßnahmen
- Zeitplanung
- Budgetplanung
- Messung des Erfolgs der Maßnahmen

AGENDA

Inhalt

- **Compliance des Business Continuity Managements**
- **Das Audit im Rahmen des BCM Lifecycle**
- **Der BCM Prüfungs Prozess**
- **Reviews von Notfallereignissen**

Das Review von Notfallereignissen und deren Ablauf

Ziele

- Aus den gemachten Erfahrungen möglichst viel lernen
- Ablauf für Behörden, Versicherungen, Anwälte etc. möglichst vollständig (nach-) dokumentieren
- Die erforderlichen Maßnahmen festlegen und deren Umsetzung überwachen

Verfahren

- Sammlung von relevanten Dokumenten und Daten
- Daten- und Systemanalysen
- Fehleranalysen, Fehlerprotokolle
- Interviews mit Beteiligten, Protokollierung

Ergebnisse

- Dokumentation des Vorfalls und der Abläufe
- Schwachstellenbericht
- Notwendige Verbesserungsmaßnahmen, Verantwortlichkeiten

Wärend des Notfalls muss der Ablauf mitdokumentiert werden!

- Entscheidungsprotokolle
- Getroffene Maßnahmen
- Fehler

Vielen Dank für Ihre Aufmerksamkeit

Fragen ? / Diskussion

Matthias Hämmerle MBCI

Senior Manager
KPMG DTAG
Marie-Curie-Strasse 30
60439 Frankfurt / Main
49 (69) 9587-4960
49 (173) 5764211
mhaemmerle@kpmg.com