Wenn alles kompliziert wird, mach es einfach! – Lean BCM

Know-how to go

HiSolutions Berlin, 25.09.2024

NIS-2

Herausforderungen und Lösungen für das Business Continuity Management

Übersetzung von NIS-2 auf BCM

Registrierungspflicht
- **Betreiber kritischer Anlagen**: sofort nach Umsetzung der Richtlinie in nationales Recht
- **Besonders wichtige & wichtige Einrichtungen**: innerhalb von 3 Monaten;
- **Anbieter Digitale Dienste**: 25.01.2025

Risikomanagement - verhältnismäßige und wirksame TOM*:
Risikoanalyse, Behandlung von Sicherheitsvorfällen, Business Continuity, Auslagerungsmanagement, Life Cycle Management, PDCA, Security Awareness, Kryptografie, Physische Sicherheit, Sichere Kommunikation

Nachweispflicht der Erfüllung der Anforderungen

Billigungs-, Überwachungs- und Schulungspflicht der GL

Meldepflicht bei Sicherheitsvorfällen

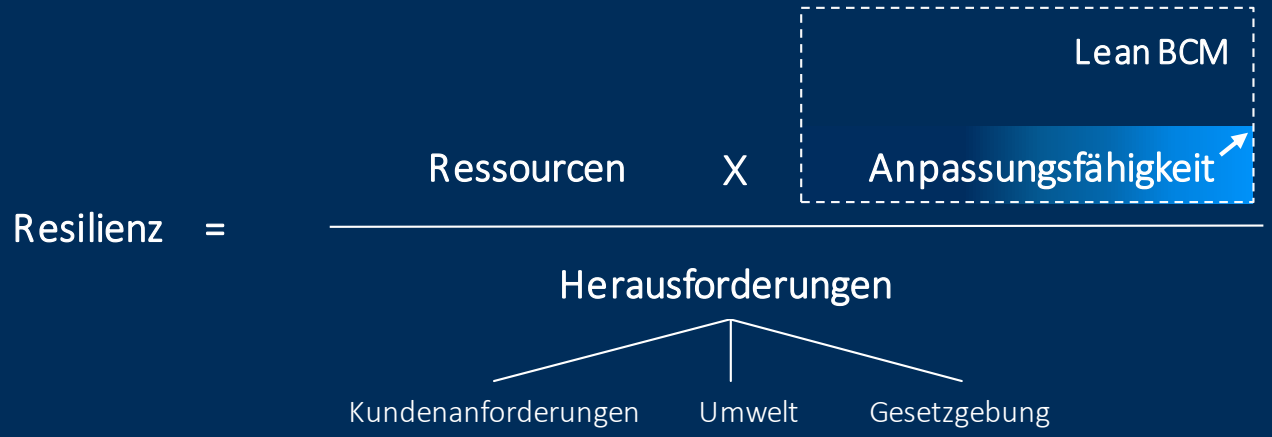
Unterrichtungspflicht gegenüber Kunden

- Aufrechterhaltung des Betriebs, z. B. Backup-Management und Wiederherstellung nach einem Notfall, Krisenmanagement, gesicherte Notfallkommunikation
- Maßnahmen sollten geeignet, verhältnismäßig, wirksam, nach Stand der Technik und auf Standards bzw. Normen basierend sein

Sind umfassende BCM-Projekte aufgrund von NIS-2 wirklich notwendig?

*TOM = technisch organisatorische Maßnahmen

Maximierung der Resilienz durch Anpassungsfähigkeit



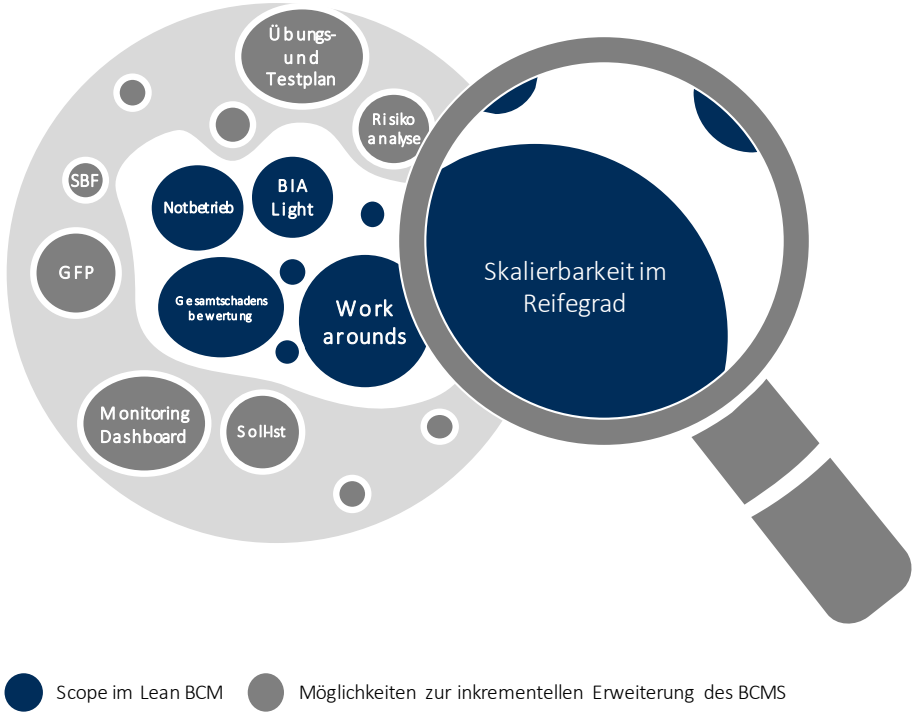
Lean BCM ermöglicht skalierbare und flexible Resilienz-Steigerung

Die Vorteile des Lean BCM…

- Schnelle Implementierung ausgewählter Maßnahmen
- Individueller Fokus
- Skalierbarkeit
- Geringer Steuerungs- und Implementierungsaufwand
- Zentrale Dokumentation
- Option zur Normkonformität

… für spezifische Zielgruppen.

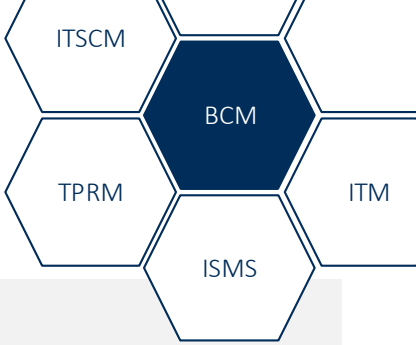
- BCM-Neulinge, KMU, KRITIS



DORA

Herausforderungen und Lösungen für das Business Continuity Management

DORA stellt neue Anforderungen an das BCM



- Größere Anzahl verpflichtender Szenarien für GFP, WAP/WHP
- Neues BIA-Schadensszenario „Markteffizienz“
- Neue, spezifischere Definitionen von kritischen und wichtigen Funktionen
- Aufbrechen von Notfallplan-Silos
- Expliziter erwähnt:
  Freigabe, Überwachung und Überprüfung des BCM und seiner Pläne durch ein Leitungsorgan
- Meldung geschätzter Kosten und Verluste durch schwerwiegende IKT-Vorfälle
  (übergeordneter Meldekopf für alle Behörden einschließlich Standardformulare)
- Notfallpläne für den Wiederanlauf bleiben abzuwarten
- Stärkere Gewichtung von Krisenkommunikation

Sorge: Die Szenarien-Vielfalt unter DORA

Der Großteil der definierten Szenarien kann den klassischen Ressourcenkategorien zugeordnet werden.

Gebäude und Infrastrukturen

- **Ausfall von Räumlichkeiten**, insbesondere von Büros, Geschäftsräumen und Rechenzentren.

IT

- **Cyberangriffe und Umstellung** auf **redundante IKT-Infrastruktur, Backups und Systeme**
- **Erheblicher Ausfall von IKT-Assets** oder der **Infrastruktur**

Dienstleistungen

- **Inakzeptabler Qualitätsverlust** oder **Ausfall einer kritischen Funktion**, einschließlich der potenziellen Auswirkungen der Insolvenz oder des Ausfalls eines IKT-Drittdienstleisters.

Personal

- **Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern** oder von Mitarbeitern, die für die Betriebskontinuität verantwortlich sind.
- Pandemien

Sorge: Die Szenarien-Vielfalt unter DORA

Vereinzelte speziellere Szenarien lassen sich argumentativ behandeln.

Auswirkungen des Klimawandels, […] und physische Angriffe

Betreffen die klassischen Ressourcen und können entsprechend behandelt werden.

Insiderangriffe

Maßnahmen der allgemeinen Sicherheitsstrategie tragen Außen- wie Innentätern Rechnung.

Politische & soziale Instabilität, auch im Land des Dienstleisters und am Standort der Datenspeicherung:

Bestehende Pläne zur Absicherung gegen Lieferkettenausfälle und IT-Drittdienstleister könnten entsprechend erweitert werden, ohne tiefgreifende Anpassungen.

Weitverbreitete Stromausfälle

Bereits eingeplante Backup- und Notstromlösungen lassen sich argumentativ auf großflächige Stromausfälle anwenden.

Sorge: Neues BIA-Schadensszenario „Markteffizienz“

DORA fordert, die Auswirkungen auf die Markteffizienz zu berücksichtigen.

Ergänzung eines Schadensszenarios im BIA- oder GRC-Tool

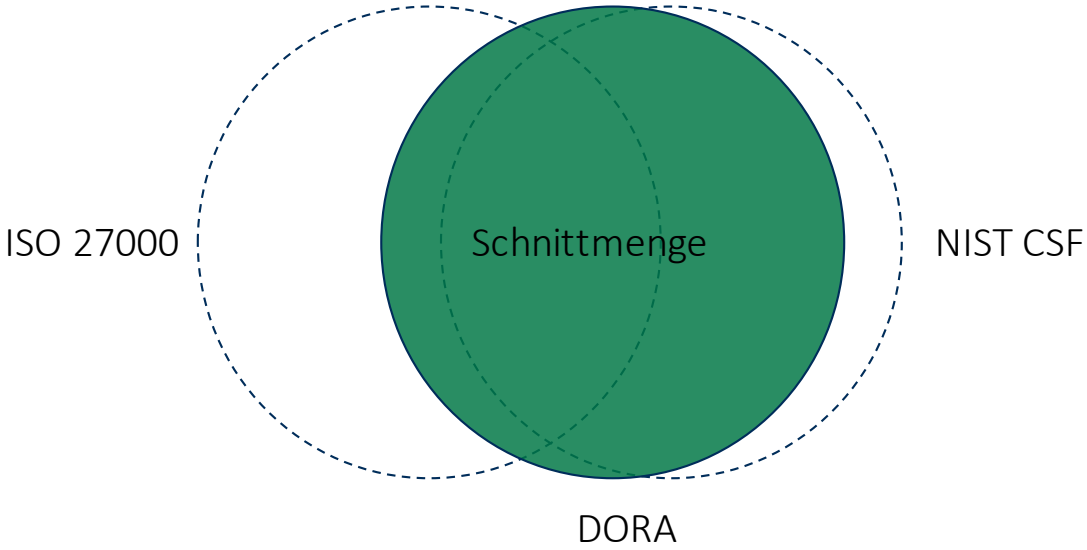
- „Finanzmarktstabilität/Markteffizienz gewährleistet? Ja/Nein“

Anpassung der Legende

Integration in ein bestehendes Schadensszenario wie „Verstoß gegen Verträge/Gesetze/Compliance“

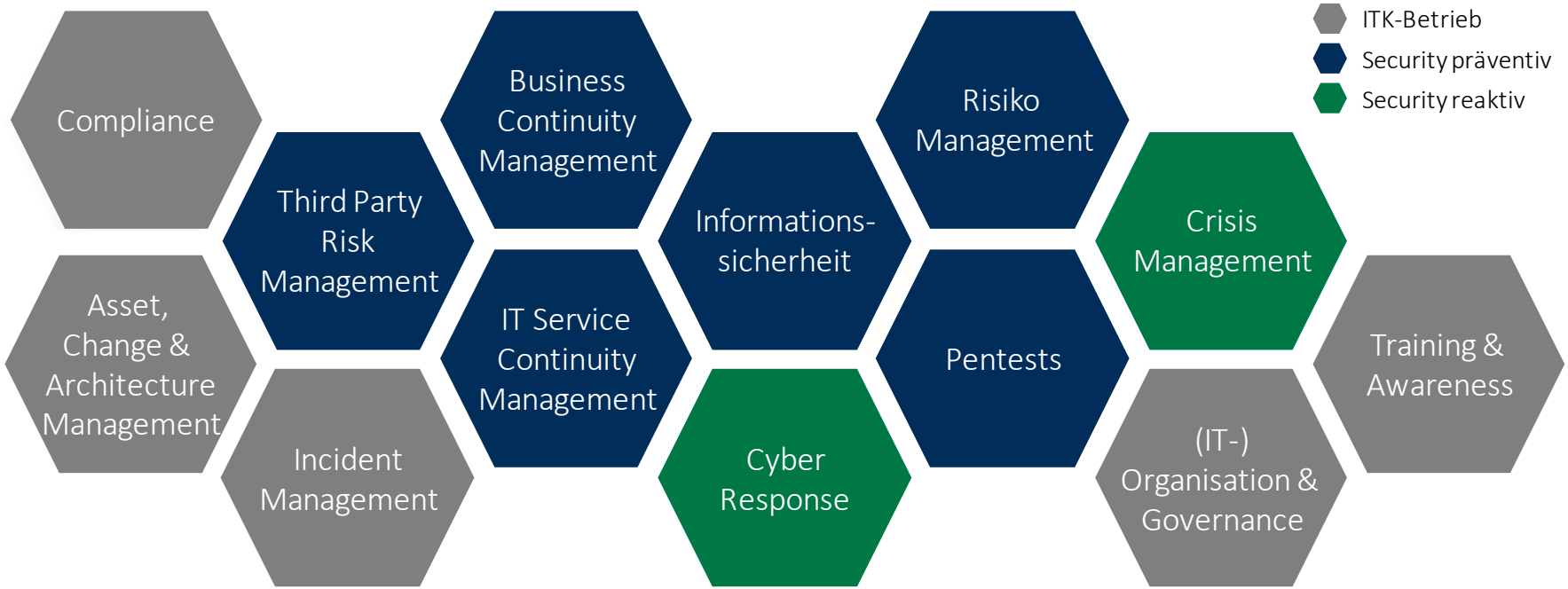
- Modifizierung der Stufen-Definitionen:
  Mit der DORA werden neben den Auswirkungen auf die Institution auch Auswirkungen auf die Finanzmarktstabilität berücksichtigt.
- Für Bankkunden kann „Auswirkung auf die Finanzmarktstabilität“ vorerst als Auslöser für die Kategorie „sehr hoch“ in der Schadenskategorie „Aufgabenerfüllung“ integriert werden.

Sorge: Erhöhte Aufwände durch Reorganisation der Sicherheitsorganisation



Übergang von ISO 27000 (BAIT, etc.) zu NIST CSF im Rahmen von DORA

Aber: Optimierung statt Neuschaffung



Schnittstellenklarheit und Aufgabenbündelung bei der Reorganisation

Ist Ihr Unternehmen für DORA gerüstet?