Parameter für eine „entspannte“ Schnittstelle zwischen BCM und ITSCM

Frank Fischer, FCMS GmbH

Wien, 29.06.2021

FCMS

Driving Business Resilience

Kurzvorstellung
Frank Fischer

CV

- BWL 'er by Heart: Schnittstellenstudium an der TU Berlin
- BCM ‘er by Heart: ISO22301 LI, MBCI, CBCM, BS25999LA
- Seit 2006 in den Themen BCM, ITSCM und Krisenmanagement
- Seit 07.2013 selbstständig, seit 03.2019 GF der FCMS GmbH
- Seit 12.2020 Mitglied des Vorstandes des Instituts für Business Continuity & Resilience Management e.V.

Projektkompetenzen

Planung, Implementierung, Schulung, Prüfung und Optimierung von ganzheitlichen, zertifizierungsfähigen, aufsichtskonformen Business Continuity Management Systemen nach ISO 22301 und IT Service Continuity Managements nach ISO 27031.

Spezialgebiet

GAP-Analysen durchführen, Handlungsempfehlungen aufzeigen, Maßnahmen mit Hands-on-Mentalität umsetzen.

FCMS Driving Business Resilience

Business Continuity Management Standards

ISO 22301 und ISO 22313

- Zertifizierungsfähige **Requirements** auf 20 Seiten (davon 5 mit Begriffsdefinitionen, ersetzen Definition aus ISO 22300:2018), plus 3 zur Einleitung (z.E.); 10.2019.
- **Guidance** mit 54 Seiten plus 7 z.E.; 02.2020.

BCI Good Practice Guidelines

- Umsetzungsorientierte „best practices“ für Personen.
- 92 Seiten plus 6 z.E.; 2018.

Nationale Normen

- ÖNORM D 4902-3 Risikomanagement für Organisationen und Systeme - Leitfaden - Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement - Anleitung zur Umsetzung der ISO 31000, 19 Seiten; 01.2021
- BSI 100-4 des Bundesamtes für Sicherheit in der Informationstechnik, 112 Seiten plus 3 z.E.; 2008
- BSI 200-4 **CD**, 285 Seiten plus 4 z.E.; **01.2021**

Europäische Normen

- EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, EBA/GL/2019/04 , Kapitel 1.7 Geschäftsfortführungsmanagement, 4 Seiten, 28.11.2019.
- DORA - Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, 24.9.2020.
- ENISA, NIST, BCBS 239, SREP, …

IT Service Continuity Management
Standards

ISO 27031

- Guidelines for information and communication technology readiness for business continuity, 27 Seiten plus 3 z.E.; 03.2011.
- Working Draft; Stage 20.60 – study initiated (26.02.2021).

ITIL

- Framework of best-practice guidance for IT service management, V4 seit 02.2019
- Service Management practice wurde umbenannt zu „Service Continuity Management".

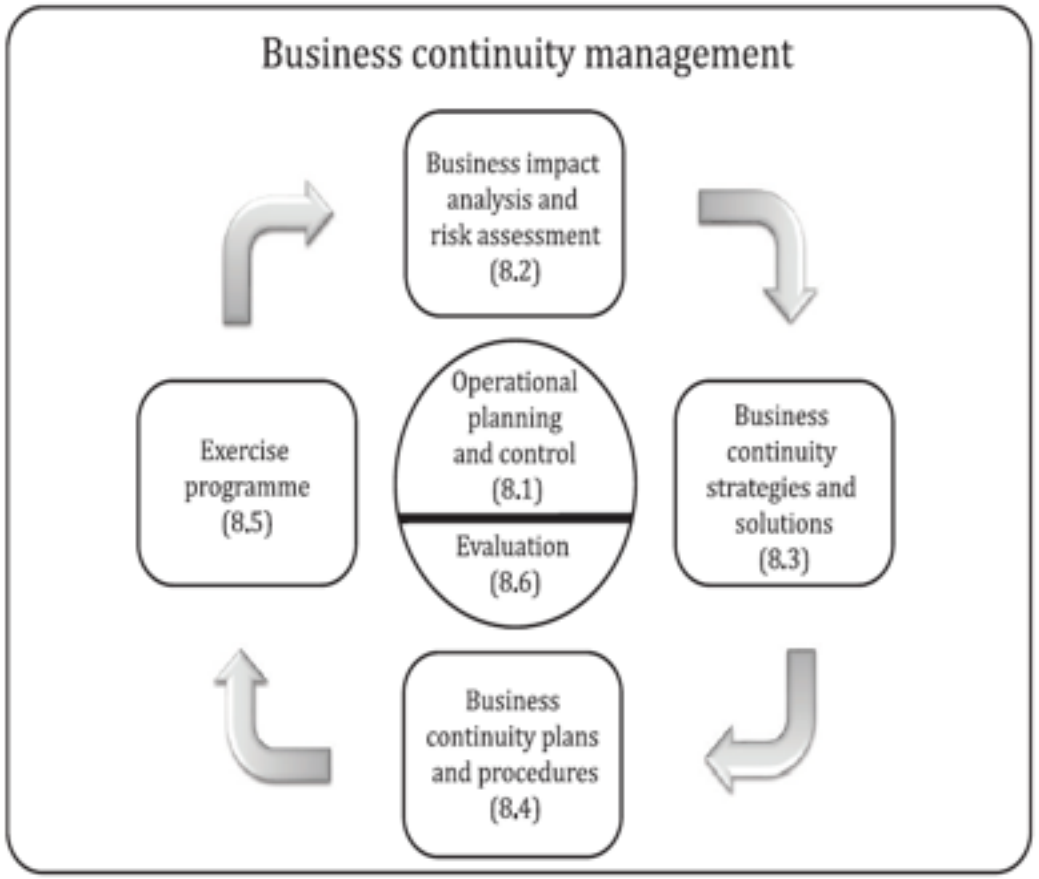
Europäische Normen

- EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, EBA/GL/2019/04 , Kapitel 1.7 Geschäftsfortführungsmanagement,4 Seiten, 28.11.2019
- DORA - Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector, 24.9.2020
- ENISA, NIST, BCBS 239, SREP, …

Nationale Normen

- Österreichisches Informationssicherheitshandbuch, Version 4.2.3, Kapitel 17: Disaster Recovery und Business Continuity, 14 Seiten (von 735); 31.05.2021
- Bankaufsichtliche Anforderungen an die IT (BAIT), Rundschreiben 10/2017 der Bundesanstalt für Finanzdienstleistungsaufsicht als „Interpretation der gesetzlichen Anforderungen des § 25a Absatz 1 Satz 3 Nummern 4 und 5 KWG", ergänzt am 14.09.2018 um ein optional anwendbares Modul „Kritische Infrastrukturen", ggw. 29 Seiten.

Definitionen und Ziele: BCM



Elements of BCM; Quelle: ISO 22313:2020

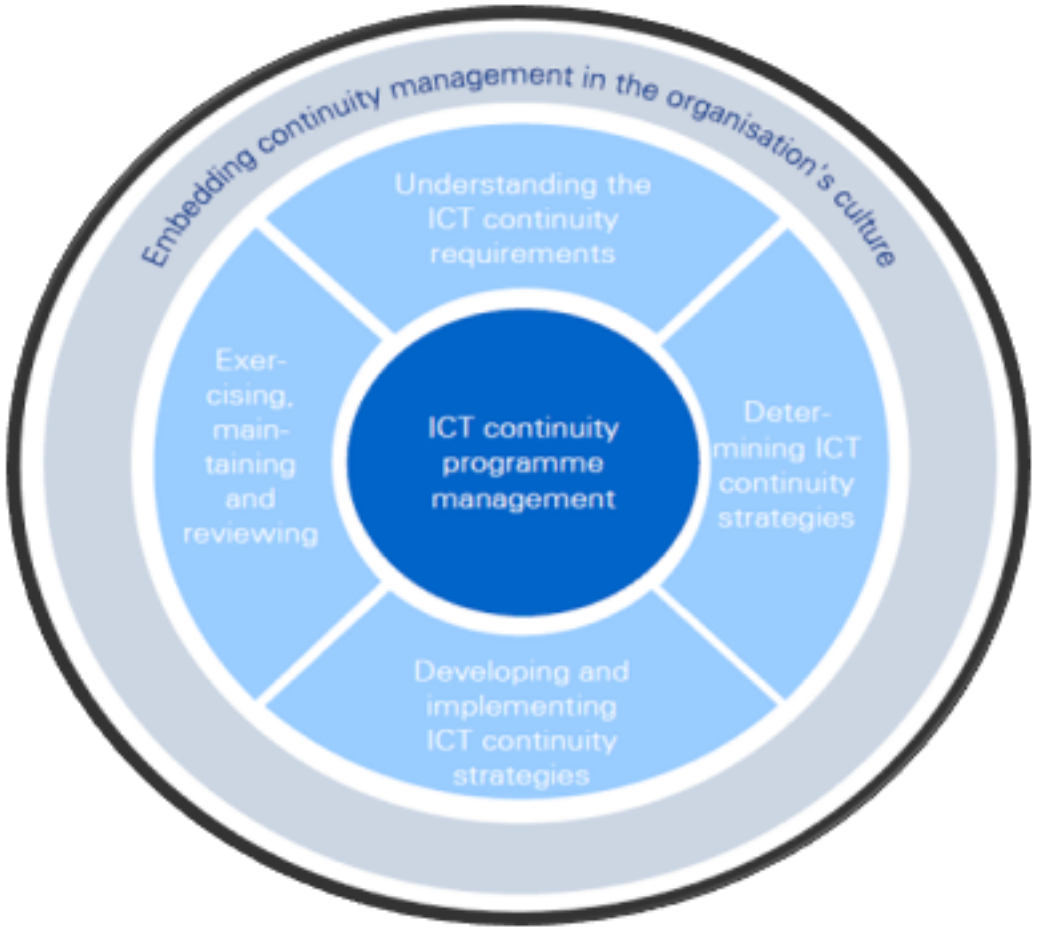
BCM nach ISO22300:2021 (02.2021)

- Def.: process of implementing and maintaining business continuity.
- BC: capability of an organization to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption.
- BCMS: part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

BCM nach BCI GPG 2018

- Def. basierend auf ISO22301:2012: A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Definitionen und Ziele: ITSCM



Quelle: BS25777: IT Continuity (Nachfolger von PAS77 und Vorgänger von ISO 27031)

ITSCM nach ISO27031

- Def.: provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.
- **Ziele:** Aufrechterhaltung der IT Services für die kritischen Prozesse bei allen Störungen (inkl. Informationssicherheits-relevanten).

ITSCM nach ITIL

- Def.: ITSM ist das Management der optimalen Verfügbarkeit von IT Services.
- **Ziele:** Sicherstellung der Verfügbarkeit der Services innerhalb der vereinbarten Zeiten, unter Berücksichtigung der Wirtschaftlichkeit.

Gemeinsamkeiten und Unterschiede

LifeCycle-Approach

- ISO-Normen sind „aligned“ an den PDCA.
- Erstellung von Leitlinie (Policy), Richtlinie (Guideline) und Prozessbeschreibungen.
- Analyse, Design, Implementierung, Verifizierung.

Unterstützung der Fachbereiche

- BCM und ITSCM werden nicht zum Selbstzweck dieser Abteilungen durchgeführt, sondern im Interesse des Unternehmens/der Organisation. Dafür benötigen beide Management-Awareness.

Im Fokus des BCM:

- Im Rahmen der Business Impact Analyse (BIA) wird zur Ermittlung der zeitlichen Dringlichkeit (Kritikalität) eine Bewertung ALLER Prozesse bzw. Aktivitäten durchgeführt (und die dafür erforderlichen Ressourcen erhoben).
- Dies beinhaltet also auch die Prozesse der IT und die dafür erforderlichen Ressourcen!

Im Fokus des ITSCM:

- Das ITSCM nutzt die Im Rahmen der BIA ermittelten Daten und richtet die Verfügbarkeiten der Services und Ressourcen (IT Landschaft) daran aus.

FCMS

Input durch BCM

Zusammengefasste Daten der mindestens jährlich durchzuführenden BIA:

- Kritische IT-Services der Fachbereiche.
- RTO/RPO-Werte der IT-Services.
- Tolerierbare Einschränkungen im Notbetrieb (Kapazitätslevel).
- Ressourcenbedarf der Notfall-Arbeitsplätze für die kritischen Prozesse (IT- und Telekommunikations-Ausstattung).

Im Rahmen der Governance:

- Review der ITSCM-Framework-Dokumente
- Aufforderung zur Planung und Erstellung des Test- und Übungskonzeptes
- Aufforderung zur Übermittlung des ITSCM-Statusberichtes

und durch ITSCM

Im Vorfeld der BIA:

- Zusammenstellung der IT-Services bzw. der Anwendungen.
- Übersicht der dahinter aufgebauten IT-Landschaft, wie Datenbanken, Servern (inkl. Virtuelle), Netzwerken, Betriebssystemen etc. (CMDB).

Im Nachgang zur BIA:

- Überprüfung der Anforderungen aus den Fachbereichen und den tatsächlichen Möglichkeiten.

Für die Compliance:

- Ausrichtung der ITSCM-Framework-Dokumente an den BCM-Vorgaben (und den Unternehmenszielen bzw. der IT-Strategie).
- Erstellung des Test- und Übungskonzeptes.
- SLA-Abgleich mit Dienstleistern.
- Erstellung des ITSCM-Statusberichtes.

Parameter zur Abstimmung der Schnittstellen

Rollen und Verantwortlichkeiten

Definieren und etablieren der Rollen und Festlegen der Verantwortlichkeiten:
- BCM Verantwortliche/r
- ITSCM Verantwortliche/r

Jour Fixe vereinbaren

Empfehlung: min. 1 Mal pro Monat
Realität: Intensiverer Austausch, gerade vor und nach der BIA

Begriffe eindeutig definieren

BCM Glossary,
ITSCM Glossary

Unterstützung durch Software

- Ein Tool für beide
- Schnittstelle zur CMDB vs. manuellen Import

Kontinuierliche Verbesserung

- Methoden zur Messung,
- zum Reporting und Internen Kontrollsystem implementieren
- Ergebnisse von Audits untereinander teilen/besprechen

Gegenseitige Prozesskenntnisse

Die Themen sind teilweise sehr nach aufbauorganisatorischer Verankerung und methodischer Ausrichtung geprägt. ITSCM nach ITIL? BCM nach ISO oder nationaler Norm?
Break down the silo!

Herausforderungen

Existenz weiterer Schnittstellen:
- Risikomanagement
- Informationssicherheitsmgmt
- Datenschutz
- HR, Legal, Compliance
- Vendor Management
- Real Estate & Workplace Mgmt
- Communication!

Datenaustausch abstimmen

- Lieferung der ITSCM-Daten
- Lieferung der BIA-Daten
- Soll-/Ist-Abgleich der Verfügbarkeits-anforderungen
- Review-Termine für Dokumente

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Kontaktmöglichkeiten:

contact@fcms.online

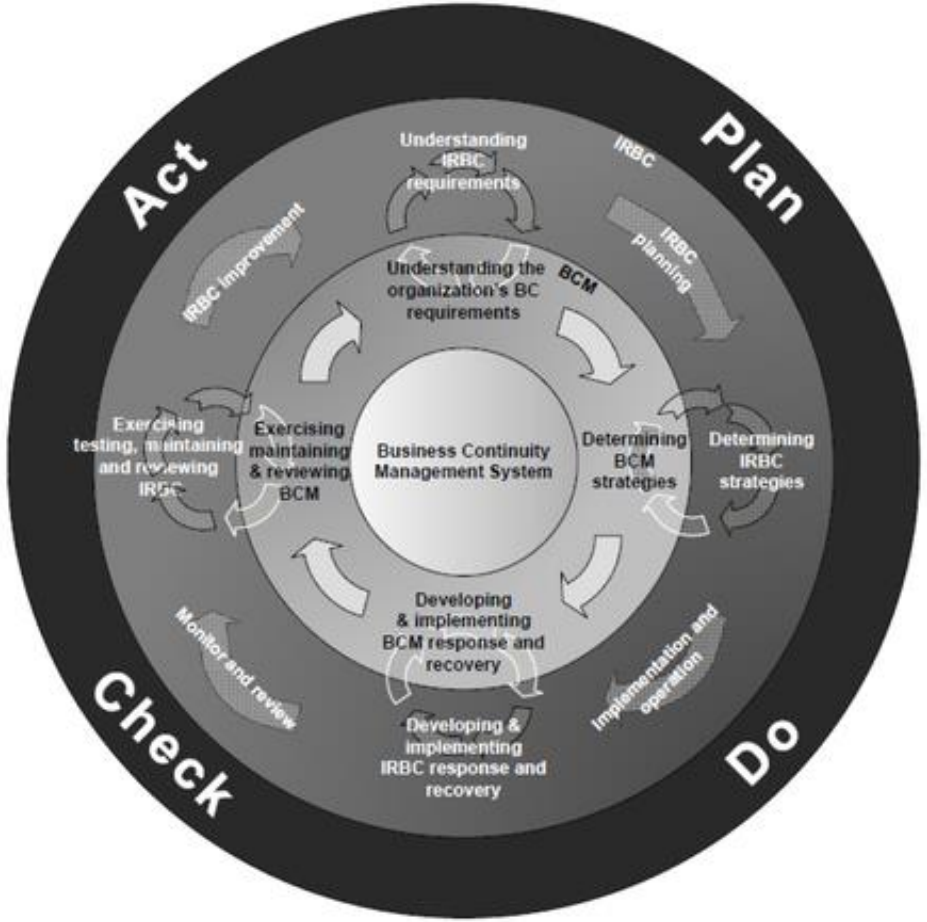
ITIL4 management practices

Table 6.1 The ITIL management practices

General management practices	Service management practices	Technical management practices
Architecture management	Availability management	Deployment management
Continual improvement	Business analysis	Infrastructure and platform management
Information security management	Capacity and performance management	Software development and management
Knowledge management	Change enablement	
Measurement and reporting	Incident management	
Organizational change management	IT asset management	
Portfolio management	Monitoring and event management	
Project management	Problem management	
Relationship management	Release management	
Risk management	Service catalogue management	
Service financial management	Service configuration management	
Strategy management	Service continuity management	
Supplier management	Service design	
Workforce and talent management	Service desk	
	Service level management	
	Service request management	
	Service validation and testing	

Quelle: Introductory Overview of ITIL® 4

Integration of IRBC and BCMS



Quelle: ISO/IEC 27031:2011 (en)

IT Service Continuity Management nach ITIL umfasst die folgenden Teil-Prozesse

1. Service-Design für Kontinuität
2. ITSCM-Training und –Test
3. ITSCM Review

Quelle: In Anlehnung an ITSCM process map