Richtlinie
IT Service Continuity Management

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

Fassung gemäß Vorstandsbeschluss vom 20.12.2021

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Richtlinie IT Service Continuity Management
Version	21.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft
Erstmalige Freigabe	03.12.2020
Verabschiedet durch (Datum)	Vorstand (20.12.2021)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz & Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
20.0	26.11.2020	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
21.0	01.12.2021	Redaktionelle Änderungen, Verallgemeinerungen des Managementreviews	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AFM	Anti-Fraud-Management
BC Manager	Business Continuity Manager
BCM	Business Continuity Management
bDSB	betrieblicher Datenschutzbeauftragter
BIA	Business Impact Analyse
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO 22301	Europäische Norm zur Sicherheit und Schutz des Gemeinwesens – Business Continuity Management
ISO 27031	Guidelines for information and communication technology readiness for business continuity - IRBC
IT	Informationstechnologie
ITSC Manager	IT Service Continuity Manager
ITSCM	IT Service Continuity Management
OpRisk	Operationelles Risiko
PDCA	Plan–Do–Check–Act
PER	Abteilung Personal
RL	Ressortleiter
RPO	Recovery Point Objective (Maximal zulässiger Datenverlust) Zeitpunkt, bezüglich dessen die Betriebsdaten einer Aktivität wiederhergestellt werden müssen, damit die Aktivität wieder aufgenommen werden kann (Quelle: ISO 22301).
RTO	Recovery Time Objective (Wiederanlaufzeit) Die geplante Wiederanlaufzeit (RTO) ist der Zeitraum nach einer Störung, innerhalb dessen ein Produkt bzw. Ressource wieder bereitgestellt werden müssen oder eine Aktivität wieder aufgenommen werden muss (Quelle: ISO 22031).
VAG	Versicherungsaufsichtsgesetz

1. ZIELSETZUNG UND GELTUNGSBEREICH

Für die VAV stellt die Fortführung des Geschäftsbetriebes nach einer Unterbrechung einen integralen Bestandteil der Geschäftspolitik dar. Die Verfügbarkeit und Verlässlichkeit der eingesetzten IT-Services, Verfahren sowie Daten und Informationen sind dabei essenziell. Um die Leistungsfähigkeit und Wettbewerbsposition der VAV und damit das Vertrauen der Mitarbeiter, Kunden, Geschäftspartner und das Ansehen in der Öffentlichkeit zu sichern, wird ein IT Service Continuity Management (ITSCM) betrieben. Die Leistungsfähigkeit des ITSCM stellt einen wesentlichen Faktor zur Unterstützung des Business Continuity Management (BCM) dar und trägt damit wesentlich zur Steigerung der Widerstandsfähigkeit der VAV gegen unvorhersehbare, schadhafte Ereignisse bei.

Das ITSCM steht dabei im Kontext der Unternehmensstrategie und unterstützt in diesem Kontext die Konkretisierung der IT Strategie. Hierzu definiert die vorliegende Richtlinie den Rahmen für den Betrieb des ITSCM der VAV. Im Fokus steht dabei alle internen sowie externen Anforderungen an das ITSCM zu erfüllen und diese in den Kontext des BCM einzubetten.

1.1. Zielsetzung

Das Ziel dieser Richtlinie ist die Schaffung einer Basis für die Sicherung des IT-Betriebs. Dies wird durch die Etablierung von geeigneten Maßnahmen erreicht, wodurch die Anforderungen an die IT aus den Geschäftsprozessen der VAV erfüllt werden.

Zu diesem Zweck ist in der IT ein IT Service Continuity Management zu etablieren, in dessen Rahmen entsprechende Aufgaben, Kompetenzen und Verantwortlichkeiten in vorausschauender Weise festgelegt sind. Gegenstand der Umsetzung sind präventive und reaktive Methoden und Maßnahmen, die darauf abzielen, dass geschäftskritische Prozesse und Bereiche im Fall von Unterbrechungen der IT nur in einem zulässigen Rahmen beeinträchtigt werden. Im Falle einer solchen Beeinträchtigung soll sichergestellt werden, dass die beeinträchtigten IT-Services in einem festgelegten Zeitrahmen (gemäß den Forderungen aus den geschäftskritischen Prozessen) wieder zur Verfügung gestellt werden. Um einem Ausfall entgegen zu wirken, wird einerseits die Reduzierung durch Präventivmaßnahmen auf ein akzeptables Schadensausmaß und andererseits die strukturierte Wiederbereitstellung durch angemessene Pläne angestrebt.

Insbesondere sind die folgenden Ziele zu berücksichtigen:

- Sicherung eines effektiven ITSCM durch eine zielgerichtete Planung für die, vom BCM gemeldeten, geschäftskritischen Prozesse.
- Einhaltung von gesetzlichen und regulatorischen Anforderungen an die Geschäftsfortführung, die im Wesentlichen aus der dem VAG sowie Solvency II bestehen.

Die in dieser Richtlinie dargestellten Methoden orientieren sich an der Konzernrichtlinie, die sich an den international anerkannten Standards ISO 27031 und ISO 22301 orientieren.

1.2. Geltungsbereich

Diese Richtlinie gilt für die VAV Versicherungs-Aktiengesellschaft.

Die Regelungen dieser Richtlinie richten sich an die gesetzlichen Vertreter, Führungskräfte und Mitarbeiter.

Die in der Richtlinie beschriebenen Rollen und Aufgaben gelten sofort. Die in der Richtlinie geforderte Dokumentation bzw. Unterlagen sind bis 31.12.2022 abzuschließen.

1.3. Änderungen

Redaktionelle Änderungen sowie Änderungen, die aufgrund veränderter rechtlicher Regelungen und Rahmenbedingungen notwendig geworden sind, können durch den ITSC Manager in Abstimmung mit dem RL IT/BO/FM beschlossen werden. Änderungen im Glossar oder in den Anlagen können durch den IT Service Continuity Manager beschlossen werden. Die Geschäftsleitung ist über erfolgte Änderungen zu informieren.

Diese Richtlinie wird zumindest einmal jährlich in schriftlich dokumentierter Form überprüft.

Wesentliche inhaltliche Änderungen an der/den konkretisierenden Arbeitsrichtlinie(n), die auf Basis dieser Richtlinie erstellt werden, können durch den ITSC Manager in Abstimmung mit dem RL IT/BO/FM beschlossen werden.

2. GRUNDLAGEN

Im Folgenden wird das Verständnis von Begrifflichkeiten im Kontext des ITSCM der VAV beschrieben, um einen einheitlichen Sprachgebrauch und somit ein gemeinsames Verständnis dieses Themas zu erlangen. In diesem Rahmen werden weitere Grundsätze des ITSCM und Anforderungen an das ITSCM festgelegt und Schnittstellen zu anderen Bereichen definiert.

2.1. Begriffe

Als IT Service Continuity versteht man die Fähigkeit einer Organisation, ihren Betrieb durch Prävention, Erkennung und Reaktion auf Störungen größeren Ausmaßes und Wiederherstellung von IT-Services zu unterstützen.

Das ITSCM managt Risiken, die gravierende Auswirkungen auf die IT-Services haben können. Dieser Prozess stellt sicher, dass die IT auch im Falle außergewöhnlicher Ereignisse die vereinbarten Minimalanforderungen bereitstellen kann. Hierbei stehen Störungen größeren Ausmaßes und Notfälle im Fokus, die über eine reguläre Incident Management Störungsbearbeitung hinausgehen. Dies geschieht durch risikomindernde Maßnahmen und durch eine gezielte Wiederherstellungsplanung für die IT-Services. ITSCM wird in einer Weise gestaltet, dass es das BCM zielgerichtet unterstützt.

Die Begriffe Störung, Notfall und Krise werden in der Richtlinie BCM definiert und daher hier nicht gesondert aufgezeigt.

2.2. Grundsätze im ITSCM

Das Thema ITSCM wird als kontinuierlicher Prozess verstanden und ist als solcher in der IT eingerichtet. Alle Aktivitäten des ITSCM werden zentral gesteuert und sind regelmäßig bzw. anlassbezogen durchzuführen und zu dokumentieren.

Das ITSCM besteht aus einer geeigneten Organisation und den zugehörigen Prozessen, die dahingehend ausgerichtet sind,

- die erforderliche IT Widerstandsfähigkeit zu erreichen,
- die angestrebte Betriebskontinuität der IT sicher zu stellen,
- IT Services nach Störungen größeren Ausmaßes oder Notfällen im Rahmen von vereinbarten Service Levels wiederherzustellen und
- laufend auskunftsfähig über den aktuellen Status des ITSCM zu sein.

Die Durchsetzung und Aufrechterhaltung einer angemessenen Service Continuity wird nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet. Im Rahmen des Managementreviews wird dem Vorstand der Umsetzungsstand des ITSCM dargestellt. Diese Managementreviews zeigen Abweichungen des ITSCM auf und schlagen korrigierende Maßnahmen vor, die dem Vorstand ermöglichen das ITSCM zu kontrollieren und angemessen zu steuern.

2.3. Gesetzliche und regulatorische Anforderungen

In der VAV wird nachweisbar die Einhaltung der geltenden internen und externen Anforderungen an das ITSCM sichergestellt. Zu diesen Anforderungen zählen gesetzliche und regulatorische Pflichten, insbesondere jene des VAG sowie unternehmensinterne Vorgaben und Vorschriften.

Das ITSCM und die darin enthaltenen Prozesse und Maßnahmen sind dahingehend ausgelegt eine regelkonforme Corporate Governance sicherzustellen und dadurch die gesetzten Ziele (Kapitel 1.1 Zielsetzung) zu erreichen.

2.4. Schnittstellen des ITSCM

Im Rahmen des ITSCM werden die Aspekte betrachtet die notwendig sind um die Verfügbarkeit von IT Business Services, unter Berücksichtigung von IT Anwendungen und IT Systemen mit Relevanz für geschäftskritische Prozesse, sicherzustellen.

Dies umfasst über die IT hinaus wichtige Ressourcen und Themenbereiche wie Gebäude, Personal sowie Dienstleister der IT.

2.4.1. Business Continuity Management

Das ITSCM wird ergänzend zum BCM betrieben und setzt seinen Fokus auf Kontinuitätsmaßnahmen für die IT. Um das BCM optimal zu unterstützen erfolgt eine starke Interaktion zwischen den beiden Bereichen. Dies umfasst unter anderem die Abstimmung der Ergebnisse der durch das BCM durchgeführten Business Impact Analyse (BIA), u.a. fließen die Werte für geplante Wiederanlaufzeit (Recovery Time Object – RTO) und maximal zulässiger Datenverlust (Recovery Point Objective – RPO) als Anforderung an den Wiederanlauf in die entsprechenden technologischen und geschäftsspezifischen Wiederanlaufpläne mit ein. Darüber hinaus findet eine gegenseitige Berücksichtigung bei Notfalltests und Notfallübungen.

Im Rahmen von Störungen der IT, bei einer Priorität 1, ist eine enge Abstimmung und ein ausreichender Informationsfluss zwischen dem BCM und der IT sichergestellt. Diese wird durch eine frühzeitige Information an das BCM und bei Bedarf, im Rahmen von länger andauernden Störungen, durch Statusmeetings erreicht.

Der ITSC Manager oder ein Vertreter kann bei Bedarf in den Krisenstab der VAV einberufen werden.

2.4.2. Informationssicherheitsmanagementsystem

Die VAV betreibt ein Informationssicherheitsmanagementsystem (ISMS) mit dem Ziel eine angemessene Authentizität, Verfügbarkeit, Vertraulichkeit und Integrität der Informationswerte der VAV zu gewährleisten. Kann aufgrund eines Ereignisses die Verfügbarkeit durch die etablierten Maßnahmen des ISMS nicht gewährleistet werden, beginnt das ITSCM die Verfügbarkeit wiederherzustellen.

Über die Abstimmung zwischen ITSCM und ISMS ist sicherzustellen, dass die Bereitstellung von IT Anwendungen und IT Systemen in Notfällen für die Schutzziele Authentizität, Vertraulichkeit und Integrität auf dem gleichen Sicherheitsniveau erfolgt, wie dies im Normalbetrieb gefordert ist.

2.4.3. Anforderungs-, Test-, Change- und Release Management

Um einen robusten IT Betrieb zu gewährleisten, ist es essenziell notwendig die Anforderungen des ITSCM in das Anforderungs-, Test-, Change- und Release Management einzubinden. Dies umfasst konkret bei Bedarf die Einbeziehung des ITSCM durch das Change und Release Management in den IT-Service Lebenszyklus im Rahmen der Einführung von neuen Lösungen (Projekte) und bei Changes. Hierbei sind jeweils die Anforderungen des ITSCM an präventive und Wiederanlaufmaßnahmen zu berücksichtigen.

2.4.4. Outsourcing-Risikocontroller

Der Outsourcing-Risikocontroller ist verantwortlich für die Begleitung und Betreuung aller Auslagerungen von Funktionen, Prozessen, Dienstleistungen oder Tätigkeiten der VAV. Hierbei wird eine Liste aller BCM relevanten Dienstleister geführt. Das Auslagerungsmanagement setzt den ITSC Manager über Auslagerungen in Kenntnis, die für die IT relevant sind.

Jährlich wird die Liste aller Auslagerungen zwischen Outsourcing-Risikocontroller, ITSC und BC Manager abgestimmt, um mögliche Änderungen oder Abweichungen der BCM Relevanz festzustellen.

Der ITSC Manager ermittelt die zuständige IT Gruppe des BCM-relevanten Dienstleisters und veranlasst durch diese die Erstellung einer IT Notfallplanung.

2.5. ITSCM Strategie

Die Ausrichtung der ITSCM Strategie richtet sich stets an der Unternehmensstrategie und der damit einhergehenden IT Strategie aus und unterstützt diese angemessen.

Das ITSCM wird daher so ausgerichtet, dass ein angemessenes Sicherheitsniveau nach dem Stand der Technik für das Schutzziel Verfügbarkeit mit Blick auf das jeweilige Risikoprofil der IT-Services erreicht wird.

3. ROLLEN UND VERANTWORTLICHKEITEN

Zum regelgerechten Betrieb des ITSCM sind die im Folgenden beschriebenen Rollen essenziell und bilden den Kern zum Betrieb eines angemessenen ITSCM. Darüberhinausgehende und unterstützende Rollen und Funktionen sind in der ITSCM Arbeitsrichtlinie beschrieben.

3.1. ITSC Manager

Der Aufbau, die Weiterentwicklung und die Durchsetzung des ITSCM werden durch den IT Service Continuity Manager (ITSC Manager) wahrgenommen. Er trägt die Verantwortung für das Erreichen der definierten Prozessziele. Des Weiteren stellt er die Schnittstelle von IT zu BCM und ISMS dar.

Zu den Aufgaben des ITSC Managers zählt es das ITSCM gemäß den Anforderungen der VAV zu betreiben und mit vertretbarem Aufwand kontinuierlich zu verbessern. Zur Erreichung eines effektiven ITSCM wird der ITSC Manager befähigt alle notwendigen Aktivitäten zur operativen Umsetzung des ITSCM durchzusetzen. Dies beinhaltet insbesondere die Erstellung und fortlaufende Pflege der Wiederanlaufplanungen.

Die wesentlichen Aufgaben sind:

- Information der Mitarbeiter über präventive Maßnahmen des ITSCM.
- Koordination und Steuerung in Planung und Umsetzung ITSCM inkl. dessen Dokumentation in der VAV
- Fortlaufende Aktualisierung und Weiterentwicklung des ITSCM und dessen Arbeitsunterlagen
- Koordination und Ausführung des ITSCM Regelprozesses mit dem Ziel der kontinuierlichen Verbesserung
- Definition/Abstimmung und Dokumentation der IT Service Continuity Strategien/Notfalloptionen
- Abstimmung von Eskalationsstrategien und –prozesse im Rahmen von Notfällen
- Beschreibung der Schnittstellen zu anderen Prozessen
- Analyse und Bewertung IT Service Continuity relevanter Changes
- Kommunikation zu den anderen Prozessen
- Koordination der Erstellung und Pflege der technischen Wiederanlaufpläne
- Erstellung und Pflege der geschäftsprozessspezifischen Wiederanlaufplanungen
- Zusammenarbeit mit den IT Service Continuity Performern
- Planung, Organisation und Durchführung von Notfalltests und Notfallübungen
- Abstimmung und Zusammenarbeit mit dem Business Continuity Prozess
- Regelmäßige Reviews des IT Service Continuity Management Prozesses
- Regelmäßiges Reporting an das BCM
- Durchführung von Bedrohungsanalysen im Kontext der IT
- Begleitung und Unterstützung der Business Impact Analysen des BCM
- Regelmäßiges Review der Business Continuity Pläne der IT
- Der ITSC Manager oder ein Vertreter kann bei Bedarf in den Krisenstab der VAV einberufen werden.

3.2. IT Service Continuity Performer (IT Mitarbeiter)

Die Rolle des IT Service Continuity Performers ist in der Regel durch Mitarbeiter in der IT-Abteilung besetzt. Er ist für die operative Umsetzung des IT Service Continuity Management Prozesses verantwortlich. Der IT Service Continuity Performer ist für den Betrieb von IT Systeme und Anwendungen zuständig. Bei BCM Relevanz ist er der zuständige operative Ansprechpartner des

ITSC Managers. Er ist verantwortlich für die Erstellung der erforderlichen Notfalldokumentation und unterstützt darüber hinaus den ITSC Manager im Rahmen von Notfallübungen sowie bei realen Notfällen.

Die wesentlichen Aufgaben des ITSC Performers sind folgende:

- Unterstützt den ITSC Manager bei der Umsetzung des ITSCM und berichtet an diesen.
- Erstellung und Aktualisierung von Wiederanlaufplänen.
- Pflege der Dokumentation im IT-Notfallhandbuch und mitgeltenden Dokumenten unter Berücksichtigung der Nutzbarkeit.
- Unterstützung des ITSC Managers bei der Planung, Durchführung und Nachbereitung von Notfalltests und Notfallübungen.
- Melden von Vorfällen oder Aktivitäten, die die IT Service Continuity beeinträchtigen.
- Analyse und Bewertung IT Service Continuity relevanter Changes.
- Einbindung des ITSCM in Tätigkeiten, deren Auswirkungen auf die Verfügbarkeit schwer einzuschätzen sind.
- Wiederherstellen von IT-Services gemäß Wiederanlaufplanung.
- Erstellung von Notfallplänen für die IT.
- Es wird sichergestellt, dass für von der IT beauftragte und BCM relevante Dienstleister, die in direkter oder indirekter Abhängigkeit zur IT stehen, Notfallpläne erstellt werden. Diese sind stets aktuell zu halten und Änderungen sind mit dem ITSC Manager abzustimmen.
- Operative Umsetzung der in den Notfallplänen der IT und Wiederanlaufplänen definierten Maßnahmen.
- Mitteilung von Änderungen an bestehenden Planungen, die eine Auswirkung auf Wiederanlaufparameter haben, an den ITSC Manager.

3.3. Business Continuity Management

Neben dem ITSCM, das den Fokus auf IT-bezogene Kontinuitätsmechanismen legt, betreibt die VAV ein Business Continuity Managementsystem mit dem Fokus auf Kontinuitätsmechanismen für Geschäftsprozesse. Zur zielgerichteten Steuerung des ITSCM gemäß den Anforderungen der Geschäftsprozesse führt das BCM regelmäßig eine Business Impact Analyse (BIA) durch. Die Ergebnisse, insbesondere RTO und RPO, werden dem ITSCM durch das BCM mitgeteilt und fließen als Anforderung an den Wiederanlauf in die entsprechenden technologischen und geschäftsspezifischen Wiederanlaufpläne ein.

3.4. BC Manager

Der BC Manager verantwortet das Business Continuity Management der VAV.

Die wesentlichen Aufgaben sind:

- Fortlaufende Aktualisierung und Weiterentwicklung der Business Continuity Richtlinie
- Stellt die Bedrohungsanalyse zur Verfügung und holt Feedback dazu ein
- Führt Business Impact Analyse durch und liefert damit die Grundlage zu einer zielgerichteten IT Service Continuity Planung und Umsetzung
- Koordination für geplante Arbeitsplatzverdrängung der IT zusammen mit Facility Management
- Involviert den ITSC Manager frühzeitig in ITSCM relevante Anforderungen des Business
- Stimmt sich regelmäßig mit dem ITSC Manager ab

3.5. IT-Abteilung

Die IT-Abteilung ist für den laufenden IT-Betrieb verantwortlich.

Wesentliche Aufgaben sind:

- Analyse und Bewertung IT Service Continuity relevanter Changes.
- Meldung von möglichen Ereignissen mit Einfluss auf Wiederanlaufparameter an den ITSC Manager.
- Einhaltung der Vorgaben des Incident Management Prozesses, um eine schnellstmögliche Störungsbearbeitung sicherzustellen.
- Gesamte Koordination und Steuerung der Störungsbehebung bei “Prio1/2/3” Störungen
- Der ITSC Manager wird bei Prio 1 –Störungen einbezogen.
- Störungs-Meldungen verfassen und bei Bedarf veröffentlichen.
- Im Bedarfsfall durchgängige Störungsdokumentation erstellen (im Nachgang).
- Fachliche und hierarchische Eskalation und Kommunikation im Störungsfall (Störung größeren Ausmaßes).

4. ABLAUFORGANISATION DES ITSCM

ITSCM ist als Regelprozess definiert, der einer kontinuierlichen Verbesserung unterliegt. Dieser Regelprozess ist in der folgenden Grafik dargestellt und wird im Folgenden beschrieben.

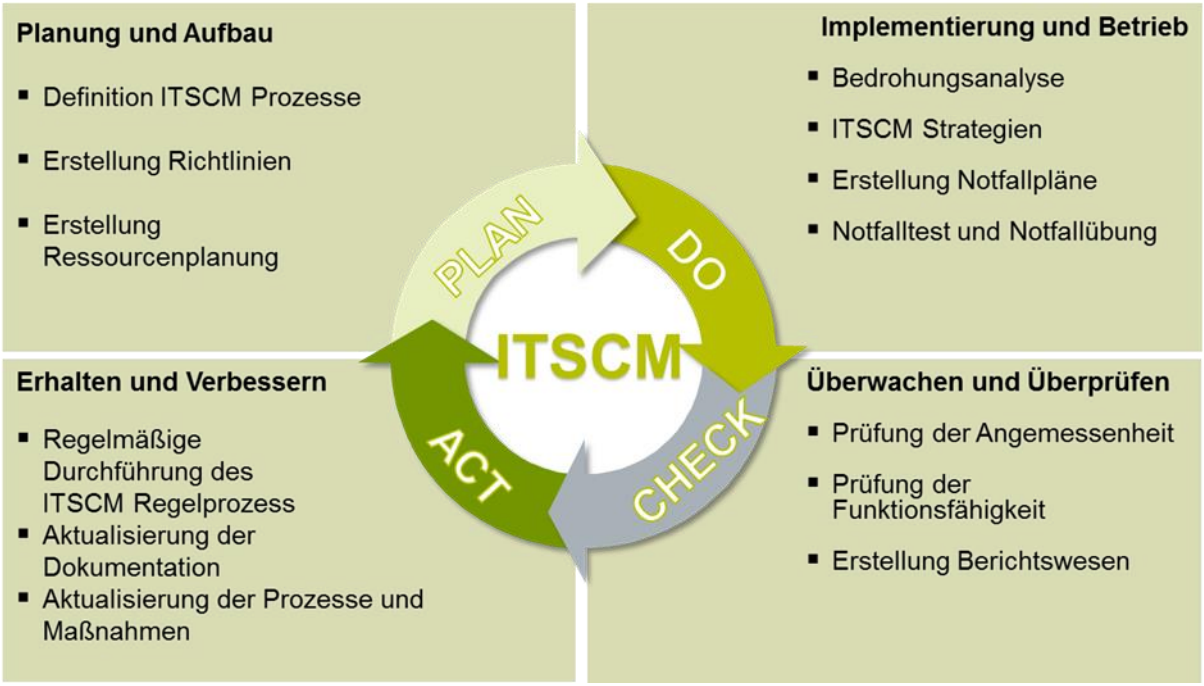

Abbildung 1: ITSCM Regelkreis

4.1. Planung und Aufbau des ITSCM

Es werden die Anforderungen an das ITSCM aus den strategischen IT-Zielen (abgeleitet aus der Unternehmensstrategie), den aufsichtsrechtlichen Anforderungen sowie internen und externen Erfordernissen analysiert. Aus den Ergebnissen dieser Analyse leiten sich die zukünftigen Ziele für das ITSCM ab, die sich in der vorliegenden Richtlinie widerspiegeln. Das ITSCM wird in Folge so ausgestaltet, dass die festgelegten Ziele erreicht werden.

4.2. Implementierung und Betrieb des ITSCM

In dieser Phase erfolgt die Umsetzung der geplanten Aktivitäten des ITSCM, wie Bedrohungsanalyse, festlegen der IT Service Continuity Strategien, Erstellen von Wiederanlaufplänen sowie Notfalltest und Notfallübungen.

4.3. Überwachen und Überprüfen des ITSCM

Es wird die Leistungsfähigkeit des ITSCM mit Blick auf die Ziele des ITSCM bewertet. Die Ergebnisse werden im Managementreview berichtet und Optimierungsmaßnahmen zu Verbesserung des ITSCM werden vorgestellt.

4.4. Erhalten und Verbessern des ITSCM

Basierend auf den Ergebnissen des Managementreviews werden Korrekturmaßnahmen zur Verbesserung des ITSCM ergriffen, was vornehmlich die Aktualisierung von Prozessen und Maßnahmen bedeutet.