Arbeitsrichtlinie IT Service Continuity Management

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie IT Service Continuity Management
Version	21.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft; Abteilung XY
Erstmalige Freigabe	13.12.2021
Verabschiedet durch (Datum)	Daniel Fürdauer und Gerhard Steinwendter (ITSC Manager und RL IT/BO/FM; 13.12.2021)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz & Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	Oktober 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
21.0	13.12.2021	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 21.0.	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

Inhaltsverzeichnis ... 3

Abkürzungsverzeichnis ... 5

1. Zielsetzung und Geltungsbereich ... 6

1.1. Einleitung ... 6

1.2. Zielsetzung ... 6

1.3. Geltungsbereich ... 6

1.4. Änderungen ... 6

2. Grundlagen ... 7

3. IT Service Continuity Management in der VAV ... 8

3.1. Begriffe ... 8

3.1.1. BC (Business Continuity) ... 8
3.1.2. BCM (Business Continuity Management) ... 8
3.1.3. ITSCM / IRBC (ICT readiness for business continuity) ... 8
3.1.4. MBCO (minimum business continuity objective) (Wiederanlaufniveau) ... 8
3.1.5. MTPD (maximum tolerable period if disruption (maximal tolerierbare Ausfallzeit) ... 8
3.1.6. RTO (Recovery Time Objective) (Wiederanlaufzeit) ... 8
3.1.7. T-RTO (Technical - Recovery Time Objective) (technische Wiederanlaufzeit) ... 8
3.1.8. RPO (Recovery Point Objective) (Maximal zulässiger Datenverlust) ... 8

3.2. Grundsätze im IT Service Continuity Management ... 9

3.2.1. Aktiver Beitrag zur kontinuierlichen Verbesserung der IT Service Continuity ... 9
3.2.2. ITSCM Kultur ... 9
3.2.3. IT Service Continuity als Entscheidungsfaktor ... 9
3.2.4. Vorbildfunktion ... 9
3.2.5. Eigenverantwortung ... 9
3.2.6. Meldung von Beeinträchtigungen der IT Service Continuity ... 9
3.2.7. Ausbildung und Sensibilisierung ... 9

3.3. Der Regelprozess im IT Service Continuity Management (ITSCM) ... 10

4. Kontext der Organisation ... 11

4.1. Verstehen der Bedürfnisse und Erwartungen der Interessengruppen ... 11

4.2. Festlegung des Scope für das ITSCM ... 12

5. Führung im Kontext ITSCM ... 13

5.1. Führung und Selbstverpflichtung ... 13

5.2. Leitlinien ... 13

5.3. Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation ... 13

5.3.1. Projektleiter/Maßnahmenleiter ... 13
5.3.2. IT Patchmanager ... 13
5.3.3. Informationssicherheitsbeauftragter ... 13
5.3.4. Release Management ... 14
5.3.5. Change Management ... 14
5.3.6. IT Operations Management ... 14
5.3.7. IT Security Management ... 14
5.3.8. Facility Management ... 15
5.3.9. Outsourcing Risikocontroller ... 15

6. Planung ... 16

6.1. Maßnahmen zum Umgang mit Risiken und Möglichkeiten ... 16

6.2. Zielsetzung zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung ... 16

7. Unterstützung ... 17

7.1. Ressourcen ... 17

7.2. Kompetenzen ... 17

7.3. Awareness ... 17

7.4. Kommunikation ... 17

7.5. Dokumentierte Informationen ... 17

8. Leistungsüberprüfung des Notfallmanagements ... 18

8.1. Überwachung, Messung, Analyse und Bewertung ... 18

8.2. Interner Überprüfungsprozess ... 18

8.3. Managementreview ... 19

9. Weiterentwicklung des ITSCM ... 20

9.1. Abweichungen und Korrekturmaßnahmen ... 20

9.2. Ständige Verbesserung ... 20

ABKÜRZUNGSVERZEICHNIS

BC Manager	Business Continuity Manager
BCM	Business Continuity Management
BIA	Business Impact Analyse
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organisation for Standardization
ISO 22301	Norm zur Unternehmenssicherheit – Systeme für betriebliches Kontinuitätsmanagement
IT	Information Technologie
ITSCM	IT Service Continuity Management
PDCA	Plan – Do – Check – Act

1. ZIELSETZUNG UND GELTUNGSBEREICH

1.1. Einleitung

Die vorliegende Arbeitsrichtlinie ITSCM beschreibt den Aufbau und die Umsetzung des IT Service Continuity Managements (ITSCM) in der VAV, das gemäß international anerkannter Standards und nach Vorgaben der „Richtlinie IT Service Continuity Management (ITSCM) (im Folgenden „Richtlinie ITSCM“) etabliert wird.

1.2. Zielsetzung

Das Ziel der ITSCM Arbeitsrichtlinie ist die umfängliche Dokumentation des ITSCM der VAV mit besonderem Augenmerk auf Methoden, die darauf abzielen, dass geschäftskritische Prozesse und Bereiche im Fall von Geschäftsunterbrechungen nicht bzw. nur in einem definierten Rahmen beeinträchtigt und strukturiert wieder zu Verfügung gestellt werden.

Hierzu werden entsprechende Aufgaben, Kompetenzen und Verantwortlichkeiten festgelegt. 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.

Die vorliegende Arbeitsrichtlinie beschreibt, wie die Anforderungen aus den Normen zu IT-Service Continuity Management umgesetzt werden.

Die Anforderungen an das ITSCM orientieren sich an der Arbeitsrichtlinie der VHV, die sich an der folgenden Norm orientiert:

- ISO/IEC 27031
  Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

1.3. Geltungsbereich

Diese Arbeitsrichtlinie 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.

1.4. Änderungen

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

Diese Arbeitsrichtlinie wird grundsätzlich einmal jährlich in schriftlich dokumentierter Form überprüft.

2. GRUNDLAGEN

Das IT Service Continuity Management wird gemäß ISO 27031 als Regelprozess definiert.

Unter dem Oberbegriff des ITSCM versteht man somit die Entwicklung von Strategien, Planungen und Handlungsanweisungen um einen festgelegten und vereinbarten IT Service Level zu erhalten bzw. nach einer Unterbrechung wieder zur Verfügung zu stellen und die minimalen Anforderungen der kritischen Geschäftsprozesse zu unterstützen.

Als Grundlage für die Definition und Ausgestaltung des ITSCM der VAV wurde von der Geschäftsleitung die Richtlinie ITSCM verabschiedet.

3. IT SERVICE CONTINUITY MANAGEMENT IN DER VAV

Die Rahmenbedingungen des ITSCM in der VAV aus der Richtlinie ITSCM, einschließlich grundlegender Methoden und Maßnahmen, werden in der vorliegenden Arbeitsrichtlinie weiterführend detailliert und ausgestaltet.

3.1. Begriffe

Gemäß ISO27001 sind nachfolgende Begriffe, zur Sicherstellung eines einheitlichen Sprachgebrauchs und Verständnis, definiert.

3.1.1. BC (Business Continuity)

Fähigkeit einer Organisation, die Belieferung mit Produkten oder Dienstleistungen nach einem Zwischenfall mit Betriebsunterbrechung auf akzeptablen, zuvor festgelegten Niveaustufen fortzusetzen.

3.1.2. BCM (Business Continuity Management)

Unter Business Continuity Management wird ein ganzheitlicher Managementprozess verstanden, mit welchem potenzielle Bedrohungen für die Organisation identifiziert und entsprechende Vorsorgemaßnahmen und Notfallplanungen umgesetzt werden. Es schafft angemessene Strukturen mit denen die VAV, auf Notfallereignisse wirksam reagieren kann, um die Interessen der Hauptinteressengruppen, die Reputation, das Markenimage und die Wertschöpfungsketten zu schützen.

3.1.3. ITSCM / IRBC (ICT readiness for business continuity)

Management Prozess zur Sicherstellung der Fähigkeit einer Organisation, trotz eines Notfalls die IT Services auf einem akzeptablen, vom BCM vordefinierten Level (MBCO) liefern zu können.

3.1.4. MBCO (minimum business continuity objective) (Wiederanlaufniveau)

Mindestniveau von Dienstleistungen und / oder Produkten, dass für die Organisation akzeptabel ist, um ihre Geschäftsziele während einer Störung zu erreichen.

3.1.5. MTPD (maximum tolerable period if disruption (maximal tolerierbare Ausfallzeit)

Die Zeitdauer, bis negative Auswirkungen durch Nichtbereitstellung eines Produkts/Service bzw. Nichtdurchführung einer Aktivität inakzeptabel würden (ISO 22031) bzw. der Zeitpunkt an dem die Auswirkungen (Schadenausmaß) für das Unternehmen nicht mehr akzeptabel wäre.

3.1.6. 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 22031:2012).

3.1.7. T-RTO (Technical - Recovery Time Objective) (technische Wiederanlaufzeit)

Zeitraum, innerhalb dessen nach einer Störung Mindestleistungen und / oder -Services und die unterstützenden Systeme, Anwendungen oder Funktionen wiederhergestellt werden müssen.

3.1.8. RPO (Recovery Point Objective) (Maximal zulässiger Datenverlust)

Zeitpunkt, bezüglich dessen die Betriebsdaten einer Aktivität wiederhergestellt werden müssen, damit die Aktivität wieder aufgenommen werden kann.

3.2. Grundsätze im IT Service Continuity Management

In der Planung und Durchführung von Maßnahmen zur Aufrechterhaltung der Verfügbarkeit von IT-Services wird auf eine ausgewogene und angemessene Service Continuity, in der das Dreieck „Strategien vs. Service Continuity vs. Wirtschaftlichkeit“ in einem sinnvollen Gleichgewicht steht, geachtet.

3.2.1. Aktiver Beitrag zur kontinuierlichen Verbesserung der IT Service Continuity

Das Management stellt zum Zweck des Betriebs eines ITSCM die nötigen Ressourcen zur Verfügung, sorgt für einen angemessenen Ausbildungsstand der Mitarbeiter und sichert die Einhaltung definierter Prozesse und Abläufe.

3.2.2. ITSCM Kultur

Die Vorgesetzten fördern und fordern in ihrem Einflussbereich eine positive Einstellung zum ITSCM und vermitteln die dazu nötigen Werte.

3.2.3. IT Service Continuity als Entscheidungsfaktor

Die VAV wird den rechtlichen, wirtschaftlichen und betrieblichen Anforderungen an das ITSCM gerecht. Dies wird bei Entscheidungen, Auftragserteilung, Überprüfung, Abnahmen und anderen Führungstätigkeiten berücksichtigt.

3.2.4. Vorbildfunktion

Die Führungskräfte der VAV sind auch Vorbilder bezüglich IT Service Continuity. Sie leben die dazu nötigen Grundsätze konsequent vor und gehen mit gutem Beispiel voran.

3.2.5. Eigenverantwortung

Bei der VAV gilt in Bezug auf IT Service Continuity das Prinzip der Eigenverantwortung. Jeder Mitarbeiter hat sich in seinem Einflussbereich über die gültigen Regelungen zu informieren und diese zu beachten.

3.2.6. Meldung von Beeinträchtigungen der IT Service Continuity

Die Mitarbeiter melden festgestellte Probleme, die den IT Betrieb beeinträchtigen können, zeitnah den zuständigen Stellen. Aus diesen Meldungen darf den meldenden Mitarbeitern kein Schaden entstehen.

3.2.7. Ausbildung und Sensibilisierung

Der Ausbildungsstand und gezielte Sensibilisierung sind wesentliche Einflussfaktoren für die IT Service Continuity. Die verantwortlichen Mitarbeiter aus dem ITSCM nehmen an Schulungen und Weiterbildungsmaßnahmen teil, sie geben Informationen weiter und führen im Bedarfsfall (z.B. bei Prozessänderungen) Schulungen durch.

Ein weiterer Baustein sind die IT-internen Notfallübung sowie Notfallübung, die IT zusammen mit dem Fachbereich durchführt.

3.3. Der Regelprozess im IT Service Continuity Management (ITSCM)

ITSCM ist als Regelprozesse eingeführt, die einer kontinuierlichen Durchführung unterliegt. Die folgende Grafik stellt die Prozesse dar und zeigt welche Tätigkeiten in den einzelnen Phasen durchgeführt werden, um das ITSCM aufrechtzuerhalten und ständig zu verbessern.

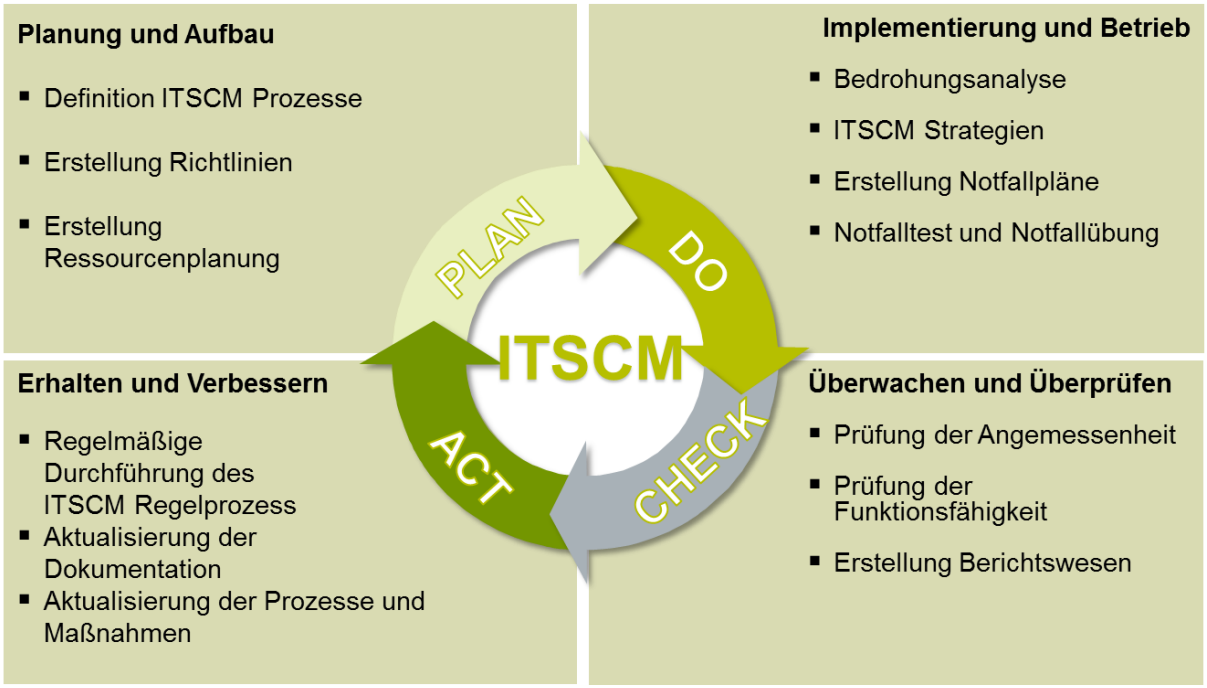

Abbildung 1: ITSCM Regelprozess

4. KONTEXT DER ORGANISATION

Für den Aufbau des ITSCM wurde der Unternehmenskontext der VAV berücksichtigt und wird im Rahmen der kontinuierlichen Verbesserung regelmäßig auf Änderungen untersucht. Im Zuge der Analyse werden die relevanten Personen und Organisationen mit Bezug zum ITSCM durch den ITSC Manager eingesetzt.

4.1. Verstehen der Bedürfnisse und Erwartungen der Interessengruppen

Unter Interessensgruppen im ITSCM der VAV werden Personen und Organisationen verstanden, die Anforderungen an die Geschäftsfortführung der VAV haben und somit an die fortwährende Bereitstellung von IT Services.

Bei den Interessensgruppen wird nicht unterschieden, ob es sich um explizite (z.B. Gesetze, Verträge) oder implizite Anforderungen (z.B. Erwartungshaltung) an das ITSCM bzw. an die Geschäftsfortführung handelt.

Die identifizierten Interessensgruppen sind in der folgenden Tabelle beschrieben:

Interessengruppe		Anforderungen
Interne Interessengruppen	Vorstand und weitere Managementsystemverantwortliche (z.B. BCMS, ISMS, Risikomanagement)	• Sicherung des Geschäftsbetriebs • Wahrung der Verfügbarkeit der Geschäftsprozesse und damit verbundenen Ressourcen • Wahrung der Reputation der VAV • Fortlaufende Kenntnis des bestehenden Risiko- bzw. Sicherheitsniveaus • Angemessene Kooperation mit dem BCM • Erfüllung der regulativen und vertraglichen Anforderungen • Transparenz • Rechtskonformität • Planungssicherheit
	Mitarbeiter	• Wahrung der Verfügbarkeit von Ressourcen und des Fortbestands der VAV • Wahrung des Arbeitsplatzes (Einkommen) • Soziale Sicherheit
	Kunden	• Wahrung der Verfügbarkeit der Services (funktionsfähiges ITSCM) • Qualitativ und quantitativ angemessene Marktleistungen

Interessengruppe		Anforderungen
Externe Interessengruppen	Dienstleister	• Transparente Einbindung in das ITSCM der VAV • Klare Definitionen von Anforderungen an das ITSCM der Dienstleister inkl. Reporting • Stabile Liefermöglichkeiten • Günstige Konditionen • Zahlungsfähigkeit der VAV
	Kooperationspartner	• Transparente Einbindung in das ITSCM der VAV • Wahrung der Verfügbarkeit der Services und des Fortbestandes der VAV
	Datenschutzbeauftragter	• Technische und organisatorische Maßnahmen gem. EU-DSGVO und ggf. weiteren internationalen Gesetzen
	Regulierer und Behörden	• Einhaltung von regulatorischen Anforderungen • Durchsetzen von Anforderungen anderer Interessengruppen (Gesellschaft, Staat, usw.)
	Staat und Gesellschaft	• Steuern • Sicherung der Arbeitsplätze • Sozialleistungen • Einhalten von Rechtsvorschriften und Normen • Erhalten einer lebenswerten Umwelt
	Mitbewerber	• Einhaltung fairer Grundsätze der Marktkonkurrenz • Kooperation auf branchenpolitischer Ebene

Tabelle 1: Interessengruppen des ITSCM

4.2. Festlegung des Scope für das ITSCM

Für die Festlegung des Scope und des Umfangs des ITSCM werden die folgenden Aspekte geprüft und in den Entscheidungsprozess zur Festlegung einbezogen:

- Strategie der VAV
- Zielsetzung der VAV
- Rechtliche und behördliche Vorgaben
- Anforderungen der Interessengruppen
- Bedürfnisse und Interessen von Kunden
- Größe, Beschaffenheit und Komplexität der VAV
- Ergebnisse von Risikoanalysen

5. FÜHRUNG IM KONTEXT ITSCM

Um die Bedeutung des ITSCM für die VAV zu verdeutlichen und die Vorgaben für alle Mitarbeiter zugänglich zu machen wurde die Richtlinie ITSCM im Intranet der VAV veröffentlicht und bekannt gemacht.

Als Verantwortlicher für das ITSCM wurde ein ITSC Manager benannt, der über die entsprechenden Befugnisse und Kompetenzen zur Umsetzung und Instandhaltung des ITSCM verfügt.

5.1. Führung und Selbstverpflichtung

Die Führung und Selbstverpflichtung für das Thema ITSCM kann dargestellt werden, indem Personen mit einer Rolle im ITSCM ermutigt und befähigt werden, einen Beitrag zur Effektivität des ITSCM zu leisten. Der ITSC Manager trägt stets dafür Sorge, dass dieses Selbstverständnis erhalten bleibt.

5.2. Leitlinien

Die Geschäftsleitung der VAV hat eine „Richtlinie IT Service Continuity Management (ITSCM)“ verabschiedet, in der die Ziele und die strategische Ausrichtung des ITSCM der VAV festgelegt wurden.

5.3. Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation

Zur Etablierung und Umsetzung eines angemessenen ITSCM müssen die einzelnen Funktionsbereiche, die für das ITSCM relevant sind in die Arbeit des ITSCM eingebunden werden, die nachfolgend beschrieben sind. Die wesentlichen Rollen und Funktionen sind in der ITSCM Richtlinie beschrieben und werden hier nicht mehr gesondert aufgeführt.

5.3.1. Projektleiter/Maßnahmenleiter

Projektleiter/Maßnahmenleiter sind umsetzungsverantwortlich für Anforderungen des ITSCM in Projekten/Maßnahmen. Dazu zählt:

- Berücksichtigt IT Service Continuity Aspekte bei der Projektplanung und Projektumsetzung
- Bezieht bei Unklarheiten zu Kontinuitätsaspekten den ITSC Manager mit ein
- Bereitstellung von Detailinformationen zu ITSCM relevanten Produktionsfreigaben an den ITSC Performer

5.3.2. IT Patchmanager

Der IT Patchmanager koordiniert innerhalb des IT-Betriebs Veränderungen an der IT Infrastruktur und bezieht dabei Überlegungen zum ITSCM ein.

Der IT Patchmanager trägt die Verantwortung das ITSCM insofern einzubinden, wenn durch seine Tätigkeit ein Ausmaß erreicht wird, dessen Auswirkungen auf die Verfügbarkeit schwer einzuschätzen sind

5.3.3. Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte (ISB) ist für die Aufrechterhaltung der Informationssicherheit verantwortlich und stellt die Berücksichtigung im ITSCM sicher.

Wesentliche Aufgaben im ITSCM Kontext:

- Kontinuierliche Abstimmung mit dem ITSC Manager

- Definiert Anforderungen an das Informationssicherheitsniveau bei Wiederanlauf und Notbetrieb
- Genehmigt Ausnahmen bei Abweichung
- Berät das ITSCM in Fragen der Informationssicherheit

5.3.4. Release Management

Das Release Management ist dafür verantwortlich den Release und Deployment Prozess zu erstellen und zu verwalten. Der Prozess hat einen ganzheitlichen Blick auf Änderungen an produktiven Services und stellt sicher, dass durch den Einsatz standardisierter Methoden und Verfahren das Risiko minimiert und negative Auswirkungen auf die produktiven Services vermieden werden. Hierzu zählt insbesondere aus ITSCM-Sicht:

- Risikoabschätzung in Bezug auf mögliche Beeinträchtigung auf die Service Continuity
- Einbeziehung der ITSC in Releases
    - generell, wenn durch das Release BCM-relevante Geschäftsprozesse verändert werden und
    - speziell, wenn durch die Risikobetrachtung ein großes Risiko für das Release identifiziert wurde.
- Bereitstellung von Detailinformationen zu ITSCM relevanten Produktionsfreigaben an den ITSC Performer

5.3.5. Change Management

Das Change Management ist dafür verantwortlich, den Change-Prozess zu erstellen und zu verwalten. Der Prozess stellt sicher, dass Änderungen geplant, effizient, kostengünstig und aus ITSCM Gesichtspunkten:

- mit minimalem Risiko ausgeführt und dokumentiert sowie
- mit minimalen Unterbrechungen der IT-Services durchgeführt werden.

5.3.6. IT Operations Management

Das IT-Operations Management bündelt die Teilprozesse, die die operativen, betrieblichen Aufgaben umfassen, die notwendig sind, IT Services gemäß den SLAs und Geschäftszielen zu erbringen. Das IT-Operations Management ist verantwortlich für die Ausführung der laufenden Routinetätigkeiten, die mit dem Betrieb von Infrastruktur-Komponenten und Anwendungen verbunden sind.

Hierbei stellen die folgenden Themenbereiche des IT-Operations Managements eine zentrale Aufgabe für das ITSCM dar:

- Backup- / Recovery Management
- Operation Control (z.B. Monitoring der IT-Systeme)
- Operation Security

5.3.7. IT Security Management

Das IT Security Management stimmt die IT Security auf die Anforderungen des Business ab und unterstützt das ITSCM dabei die IT Security in Notfällen aufrecht zu erhalten.

Wesentliche Aufgaben im ITSCM Kontext:

- Berät das ITSCM zu Fragen der IT Security
- Regelmäßige Information des ITSC Managers über die aktuelle IT Security Bedrohungslage, inklusive der Behebung von Schwachstellen mit Auswirkung auf die Verfügbarkeit von Services und Systemen

5.3.8. Facility Management

Das Facility Management ist Ansprechpartner für die gesamte Versorgungsinfrastruktur aller Gebäude und somit für alle Rechenzentren.

Wesentliche Aufgaben im ITSCM Kontext:

- Informiert den ITSC Manager und die IT über Maßnahmen an der infrastrukturellen Versorgung (Stromschaltung, Umbaumaßnahmen, usw.)

5.3.9. Outsourcing Risikocontroller

Der Outsourcing Risikocontroller ist der zentrale Ansprechpartner für den Auslagerungsprozess und erstellt Risikoanalysen für Auslagerungen.

Wesentliche Aufgaben im ITSCM Kontext:

- Stellt Anforderungen hinsichtlich Notfallkonzepten und Wiederherstellungsplänen
- Führt eine zentrale Liste mit Dienstleistern und einer Einschätzung bezüglich deren Relevanz für den Geschäftsbetrieb bzw. den IT Betrieb

6. PLANUNG

Die VAV hat zum angemessenen Umgang mit Bedrohungen und Möglichkeiten ein Kontrollsystem im BCM implementiert, in welches das ITSCM eingebettet ist.

6.1. Maßnahmen zum Umgang mit Risiken und Möglichkeiten

In einem jährlichen Turnus führt das BCM eine Bedrohungsanalyse durch. In diese Bedrohungsanalyse fließen relevante Bedrohungen der IT ein und werden dem BCM zurückgemeldet.

6.2. Zielsetzung zur Aufrechterhaltung der Betriebsfähigkeit und Pläne zur Zielerreichung

Die VAV hat es sich zum Ziel gesetzt die wirtschaftliche Existenz und den Fortbestand der VAV auch bei größeren Betriebsunterbrechungen zu sichern, was durch die starke Abhängigkeit des Geschäftsbetriebs von der IT besondere Anforderungen schafft, die durch das ITSCM gehandhabt werden müssen.

Um dieses Ziel zu erreichen, identifiziert das BCM fortlaufend die geschäftskritischen Bereiche, für die zusätzlich zur Notfallplanung eine Wiederanlaufplanung (geschäftsspezifische und systemspezifische Wiederanlaufpläne) der zugehörigen IT Ressourcen notwendig sind. Dies erlaubt es IT-Services, zielgerichtet für die im BCM identifizierten geschäftskritischen Bereiche, auf einem definierten Mindestniveau wieder zur Verfügung zu stellen.

Die Erstellung der Wiederanlaufpläne bei der VAV wird als fortschreitender Regelprozess verstanden. Somit ist es das Ziel bei der ersten Erstellung und jeder weiteren Bearbeitung der Wiederanlaufpläne grundlegende Ideen für den Wiederanlauf zu entwickeln und den jeweiligen Detaillierungsgrad zu verfeinern.

Der Reifegrad der Wiederanlaufpläne ist durch regelmäßige Übungen zu bestätigen, wobei Erkenntnisse aus Notfalltests und Notfallübungen direkt zu einer Steigerung des Reifegrades der Wiederanlaufpläne beitragen. Damit liegt neben der Verbesserung des ITSCM stets auch die fortwährende Verbesserung der Wiederanlaufpläne im Fokus.

7. UNTERSTÜTZUNG

Die VAV hat sich durch die „Richtlinie IT Service Continuity Management (ITSCM)“ dazu verpflichtet die notwendigen personellen und materiellen Ressourcen zur Verfügung zu stellen, um ein ITSCM einzuführen, zu betreiben, instand zu halten und ständig zu verbessern.

7.1. Ressourcen

Die personellen Ressourcen in Form von Rollen und Verantwortlichkeiten im ITSCM sind in „Kapitel 5.3 Funktionen, Verantwortlichkeiten und Befugnisse innerhalb der Organisation“ definiert und festgelegt.

7.2. Kompetenzen

Der Aufbau und Erhalt von fachlichen Kompetenzen seiner Mitarbeiter und Führungskräfte ist Bestandteil des ITSCM der VAV. Zur Erreichung dieses Zieles dienen die folgenden Maßnahmen:

- Berücksichtigung notwendiger Qualifikationen bei der Personalauswahl bei Neueinstellungen (z.B. Einstellungsgesprächen, Qualifikationsnachweis)
- Interne Seminare
- Schulungen
- Bedarfsorientierte fachliche Weiterbildungen durch die Fachabteilungen

7.3. Awareness

Der Aufbau und ständige Erhalt eines Bewusstseins für IT Service Continuity bei den Mitarbeitern und Führungskräften der IT ist ein wichtiger Bestandteil des ITSCM der VAV und wird unter anderem durch folgende Maßnahmen unterstützt:

- Allen Mitarbeiter wird die „Richtlinie IT Service Continuity Management (ITSCM)“ im Intranet zur Verfügung gestellt
- Veröffentlichungen zu IT Störungen und Notfällen im Intranet bzw. per E-Mail
- „operationelle“ Bewusstseinsbildung, Beratung (z.B. in Business Impact Analysen, Notfallplanung, Notfalltests)
- Awareness Kampagnen

7.4. Kommunikation

Für das ITSCM der VAV sind Kommunikationskonzepte und Kommunikationspläne festgelegt.

Detaillierte Informationen zur Vorgehensweise bei Störungen sowie in Notfällen finden sich in:

- Richtlinie BCM (Kapitel 5.1.3).

7.5. Dokumentierte Informationen

Die dokumentierten Informationen des ITSCM beschreiben zum einen das ITSCM selbst, dessen Grundlagen, Methoden und Anwendung. Sie definieren andererseits Vorgaben in Form von anweisenden Dokumenten und dokumentieren letztendlich die Umsetzung und Ergebnisse.

Die „Richtlinie IT Service Continuity Management (ITSCM)“ und die vorliegende „Arbeitsrichtlinie IT Service Continuity Management (ITSCM)“ stellen die Kerndokumente des ITSCM dar.

Um die Dokumentenlenkung zu vereinheitlichen wurden die Vorgaben zu Erstellung, Aktualisierung und Steuerung dokumentierter Informationen im Bereich Datenschutz und Informationssicherheit gemäß der Richtlinie Informationssicherheit festgelegt.

8. LEISTUNGSÜBERPRÜFUNG DES NOTFALLMANAGEMENTS

Die Effektivität des ITSCM im operativen Betrieb erfolgt durch Notfalltests und Notfallübungen.

8.1. Überwachung, Messung, Analyse und Bewertung

Zur Leistungsüberprüfung des ITSCM werden KPI festgelegt, die im Rahmen der Überwachungsverpflichtung folgende Zielsetzungen verfolgen:

- Priorisierte IT-Incidents
  Ziel: Übersicht über alle priorisierten IT-Incidents (ohne Changes o.ä.)
- IT-Business Services
  Ziel: Abdeckung der IT-Business Services für alle geschäftskritischen Prozesse
- Wiederanlaufpläne
  Ziel: Sicherstellung von Wiederanlaufplanungen pro IT-Business Service
- Validierte Wiederanlaufzeiten
  Ziel: Validierte Wiederanlaufzeiten pro IT-Business Service
- Notfalltests/Notfallübungen
  Ziel: Sicherstellung der Durchführung von Notfalltests und Notfallübungen

8.2. Interner Überprüfungsprozess

In der VAV verantwortet der ITSC-Manager den internen Überprüfungsprozess für das IT Service Continuity Management. Die Prüfhandlungen für das ITSCM erfolgen unabhängig und nach eigener Planung.

Die Grundlagen des internen Überprüfungsprozesses im ITSCM sind:

- Umsetzung der „Richtlinie IT Service Continuity Management (ITSCM)“
- Aktualität, Vollständigkeit und Rückmeldung der Bedrohungsanalyse
- Vollständige Abdeckung aller geschäftskritischen Prozesse durch IT-Business Services in Analogie zu geschäftskritischen Geschäftsprozessen
- Aktualität und Vollständigkeit der vorliegenden systemspezifischen Wiederanlaufpläne
- Aktualität und Vollständigkeit der vorliegenden Betriebsdokumentationen der Systeme, die für die systemspezifischen Wiederanlaufplänen notwendig sind
- Aktualität und Vollständigkeit der vorliegenden gruppenbezogenen Notfallpläne (BCP) der IT
- Aufzeichnungen zur Einbeziehung des ITSCM im Change Prozess
- Aktualität und Vollständigkeit der Aufzeichnungen zu durchgeführten Notfalltests und Notfallübungen
- Aktualität, Vollständigkeit und Rückmeldung der festgelegten KPIs des ITSCM
- Prüfberichte (z.B. der internen Revision, von Wirtschaftsprüfern, interne/externe Auditoren, ITSC Manager)

Im derzeitigen Aufbau des ITSCM beschränkt sich der interne Überprüfungsprozess auf sporadische Prüfung der oben genannten Punkte. Ein Auditprogramm für das ITSCM wird explizit nicht etabliert, kann jedoch bei Bedarf kurzfristig etabliert werden.

Unabhängig von der Etablierung eines Auditprogramms wird bei Entscheidungen, die das ITSCM betreffen stets darauf geachtet den Anforderungen der Norm zu entsprechen, was insbesondere bei der Implementierung des ITSCM berücksichtigt wurde.

8.3. Managementreview

Die Geschäftsleitung der VAV führt in regelmäßigen Abständen eine Managementüberprüfung des ITSCM durch, in dessen Rahmen der Stand des ITSCM dargestellt wird.

Dem Management werden dabei folgende Themen berichtet:

- die KPIs der IT und dadurch die des ITSCM,
- die relevanten Bedrohungen auf die IT im Rahmen der Bedrohungsanalyse dargestellt,
- Ergebnisse der IT Notfalltests und Notfallübungen
- Reifegrad des IT Service Continuity Managementsystems

9. WEITERENTWICKLUNG DES ITSCM

Zur stetigen Weiterentwicklung ist das ITSCM der VAV unter dem Aspekt der kontinuierlichen Verbesserung etabliert. Hierzu sind Maßnahmen in dieser Arbeitsrichtlinie verankert, die dazu beitragen das ITSCM und dessen Betriebsergebnisse ständig zu verbessern und deren Reifegrad kontinuierlich zu erhöhen.

9.1. Abweichungen und Korrekturmaßnahmen

Abweichungen zu normativen und Vorgaben der Richtlinien des ITSCM werden im Rahmen des internen Überprüfungsprozesses identifiziert und dokumentiert.

Zur Behandlung von Abweichungen werden geeignete Maßnahmen entwickelt. Können diese Maßnahmen durch den ITSC Manager veranlasst werden, sind Abweichungen schnellstmöglich zu beheben. Erfordern Korrekturmaßnahmen eine höhere Entscheidungskompetenz, so werden Korrekturmaßnahmen im Rahmen des internen Reviews zur Entscheidung vorgelegt.

9.2. Ständige Verbesserung

Zur Gewährleistung der kontinuierlichen Verbesserung, der fortlaufenden Aktualität des ITSCM der VAV und der Nutzbarkeit der Ergebnisse und Methoden im Schadensfall sind alle in dieser Richtlinie und den mitgeltenden Dokumenten aufgeführten Aktivitäten und Maßnahmenumsetzungen zeitnah durchzuführen.

Neben der Pflege der Dokumentationen sind auch die Methoden und Dokumentationen fortlaufend auf einem aktuellen Stand zu halten.

Die fortlaufende Pflege der Daten, Methoden und Dokumentationen im ITSCM wird durch den ITSC Manager sichergestellt und im Rahmen eines regelmäßigen Reviews auf Wirksamkeit, Aktualität und Angemessenheit geprüft und bewertet. Notwendige Anpassungen oder Änderungen werden im Rahmen des kontinuierlichen Verbesserungsprozesses eingeleitet, abgestimmt und implementiert.