Hochschule Niederrhein
University of Applied Sciences

Wirtschaftswissenschaften
Faculty of Business Administration
and Economics

BCSM 402 Business Continuity Management

Kapitel 09: IT-Service Continuity Management (ITSCM)

Prof. Dr. Gael Pentang
Gael.Pentang@hs-niederrhein.de

Sommersemester

2. Gliederung

- Kapitel 00: Organisatorisches
- Kapitel 01: Grundlagen des Business Continuity Management (BCM)
- Kapitel 02: Standards und Rahmenbedingungen für BCM
- Kapitel 03: Rollen und Verantwortlichkeiten im BCM-Prozess
- Kapitel 04: Business Impact Analyse: Methoden und Techniken
- Kapitel 05: BCM Risikomanagement: Strategien und Umsetzung
- Kapitel 06: Betrieb & Leistungsüberprüfung und Verbesserung
- Kapitel 07: Krisenmanagement - Krisenübung
- Kapitel 08: Zertifizierung und Auditierung des BCMS
- Kapitel 09: IT-Service Continuity Management (ITSCM)

Lernziele

Am Ende sind Sie in der Lage, …

- ✓ Die Unterschiede zwischen ITSCM und BCM (Business Continuity Management) zu erkennen
- ✓ Die Rolle von Managementsystemen und Standards im ITSCM zu erklären
- ✓ ITSCM in der Organisationsstruktur vom BCM zu integrieren, den ITSCM Life Cycle zu beschreiben und zu implementieren
- ✓ Die Kernbestandteile der IT-Notfallvorsorge zu definieren und IT-Notfallbewältigungsstrategien zu entwickeln

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.1. ITSCM-Beispiele aus der Praxis

Fall 1: Telekom, 2016

- **Angriff**: Botnet-Attacke auf DSL-Router
- **Schaden**: 1 Mio. Router zeitgleich offline
- Notfallpläne begrenzen den Schaden

Fall 2: Maersk, 2017

- **Angriff**: NotPetya Ransomware
- **Schaden**: $300 Mio. Ausfall der globalen Logistik
- keine vollständige ITSCM-Strategie
- Ein einziger überlebender Domain Controller in Ghana rettete das Netzwerk

Fall 3: Norsk Hydro, 2019

- **Angriff**: Ransomware
- **Schaden**: IT Systeme weltweit lahmgelegt
- starkes ITSCM und Business Continuity Management
- Betrieb manuell weitergeführt und transparent kommuniziert

Angriff war kein rein technisches Problem. Er wurde sofort zu einem Business-Problem. Denn wenn IT-Systeme ausfallen, stehen Geschäftsprozesse still.

Quellen: (Maersk) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Hydro) https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/ (Deutsche Telekom) https://de.wikipedia.org/wiki/Cyberattacke_auf_DSL-Router_am_27._November_2016

9.2. Abgrenzung ITSCM und BCM

- Ein Geschäftsprozess ist nur so resilient wie seine schwächste Abhängigkeit

Geschäftsprozess

z.B. Zahlungsverkehr, Handel – fordert Verfügbarkeit.

Fachlicher IT-Service

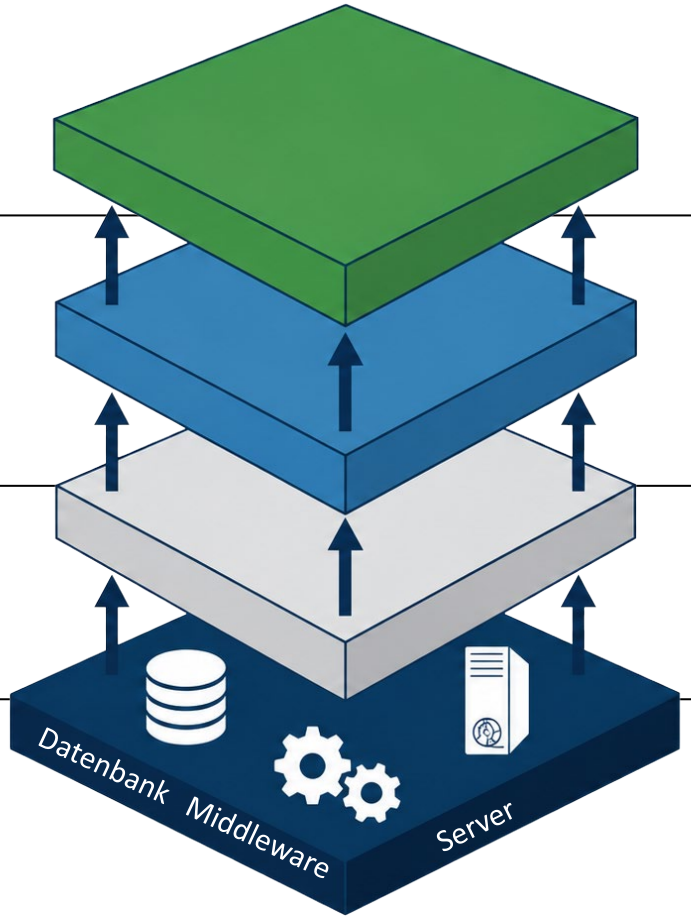
Die Anwendung, die der Nutzer direkt bedient.

Unterstützende IT-Services

z.B. Windows/Linux Services, Netzwerk Service.

Hardware & Software

Server, Switches, Betriebssysteme, Datenbanken.



Hochschule Niederrhein
University of Applied Sciences

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.2. Abgrenzung ITSCM und BCM

- **BCM rettet das Business, ITSCM rettet die Technik**

Business Continuity Management (BCM)

- **Fokus**: Prozesse & Menschen
- Widerstandsfähigkeit der Prozesse
- Organisatorische und personelle Maßnahmen zur Fortführung der Kerngeschäfte nach Eintritt von Notfällen
- **Ziel**: Das Unternehmen überlebt

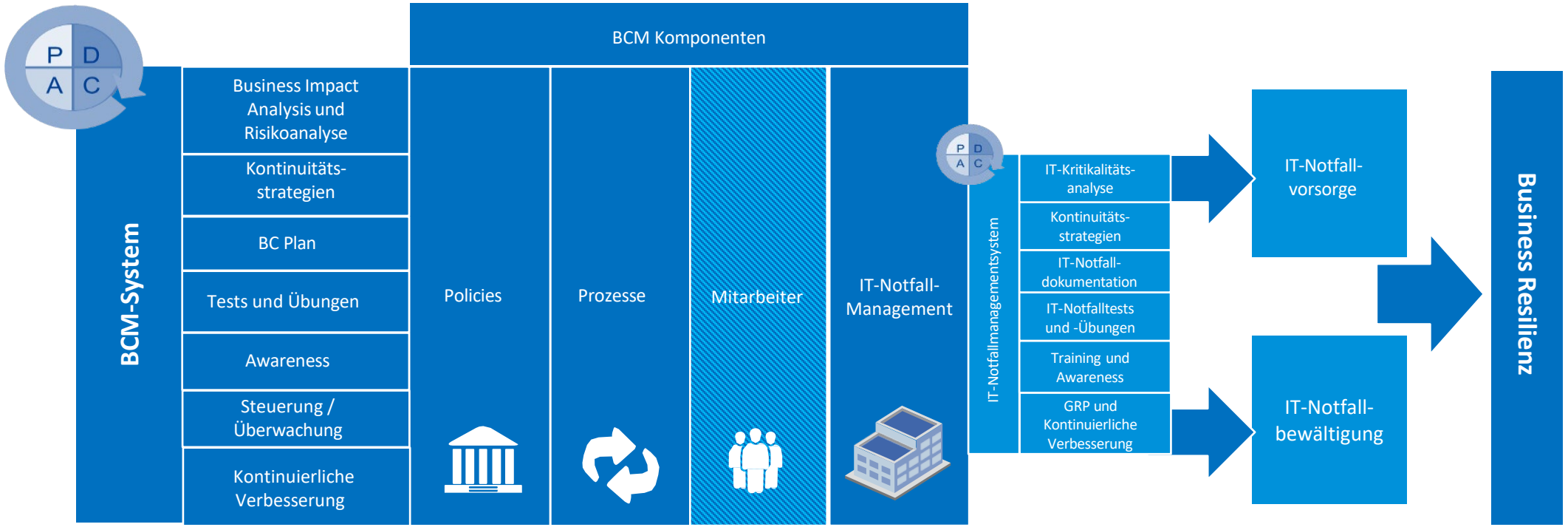
IT Service Continuity Management (ITSCM)

- **Fokus:** Technologie & Infrastruktur
- Widerstandsfähigkeit der IT-Ressourcen
- Technische Maßnahmen zum Schutz und zur Wiederherstellung kritischer IT-Komponenten
- **Ziel**: Server und Daten sind rechtzeitig wieder da

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.3. Aufbau des IT-Notfallmanagementsystems nach Standardrichtlinien



Mögliches Zielbild in Anlehnung an das Referenzmodell aus dem BSI 100-4 und der ISO 27031

Legende: BCM | BCM + IT-Notfall Organisation | IT-Notfallmanagement

- Das IT-Notfallmanagement / ITSCM ist integraler Bestandteil des Business Continuity Management Systems (BCMS).
- Das IT-Notfallmanagement untergliedert sich in die Teilprozesse der präventiven IT-Notfallvorsorge und der reaktiven IT-Notfallbewältigung.

Hochschule Niederrhein
University of Applied Sciences

9.3. ITSCM Standards

ISO 27031

- Der ISO 27031 enthält Best-Practice-Ansätze für **Informations- und Kommunikationstechnologie (IKT), um die Geschäftskontinuität sicherzustellen**.
- Da die meisten Prozesse in einer Organisation von IKT abhängen, können Störungen bzw. Ausfälle dieser Systeme zu großen Risiken führen und das Ansehen des Unternehmens schädigen. Sicherheitsereignisse, wie beispielsweise Systemangriffe oder Malware-Infektionen, führen bei schlecht geschützter IKT zu schwerwiegenden Auswirkungen auf unternehmenskritische Prozesse.
- Durch die Implementierung der Best-Practice-Ansätze können Organisationen ihre Verwaltungsvorgänge, Planungsprozesse, Datenverarbeitung und Datenübertragung verbessern und gleichzeitig kritische Informationen/Daten sicher aufbewahren.

Weitere gängige Standards im Umfeld von ITSCM			
ISO 22301:2020	BSI-Standard 200-4	BCI Good Practice	…

Hochschule Niederrhein
University of Applied Sciences

9.3. Themenblöcke im ITSCM

IT Service Continuity Management

I. IT-Notfallvorsorge

- Managementsystem PDCA
- Kritikalitätsanalyse/ Kontinuitätsstrategie
- Schadensszenarien/ IT-Notfalldokumente
- Gap Remediation Prozess (GRP)
- Kommunikation, Awareness und Training (KAT)
- Funktionen in der IT-Notfallvorsorge
- IT-Notfalltests und -Übungen (inkl. IT-Notfallstabs-übungen)
- Kontinuierlicher Verbesserungs-prozess (KVP)

II. IT-Notfallbewältigung

- Erkennung, Alarmierung und Ablaufbeschreibung
- Funktionen in der Notfallbewältigung
- Lessons Learned

Schnittstellen BCM

- Business Impact Analyse
- Risiko Impact Analyse
- Krisenstab

Wesentliche Schnittstellen und Informationsquellen

- Incident- / Change-/ Configuration-/ Capacity-/ Availabilitymanagement
- Infrastrukturanalyse
- Softwareentwicklungsprozess

Hochschule Niederrhein
University of Applied Sciences

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.4. ITSCM Organisation (Beispiel einer Umsetzung)

Notfallmanagement IT (als Teil des BCM)

Aufgaben von Notfallmanagement IT

- Legt den Standard fest (bspw. ISO 27031)
- Vorgabe von Schadensszenarien
- Vorgabe des IT-Kontinuitätsstandards
- Vorgaben an die ITSCM-Prozesse

Wer trägt die Verantwortung?

Der Vorstand / das Management ist verantwortlich für die Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung des IT-Notfallmanagements als Management- Prozess in seinem gesamten Lebenszyklus. Er stellt die erforderlichen Ressourcen und finanziellen Mittel bereit.
→Management Commitment

Vorgaben

2. Line of Defense
1. Line of Defense

ITSCM als IT-Kernprozess

Zwei Kernkomponenten: präventive IT-Notfallvorsorge und reaktive IT-Notfallbewältigung

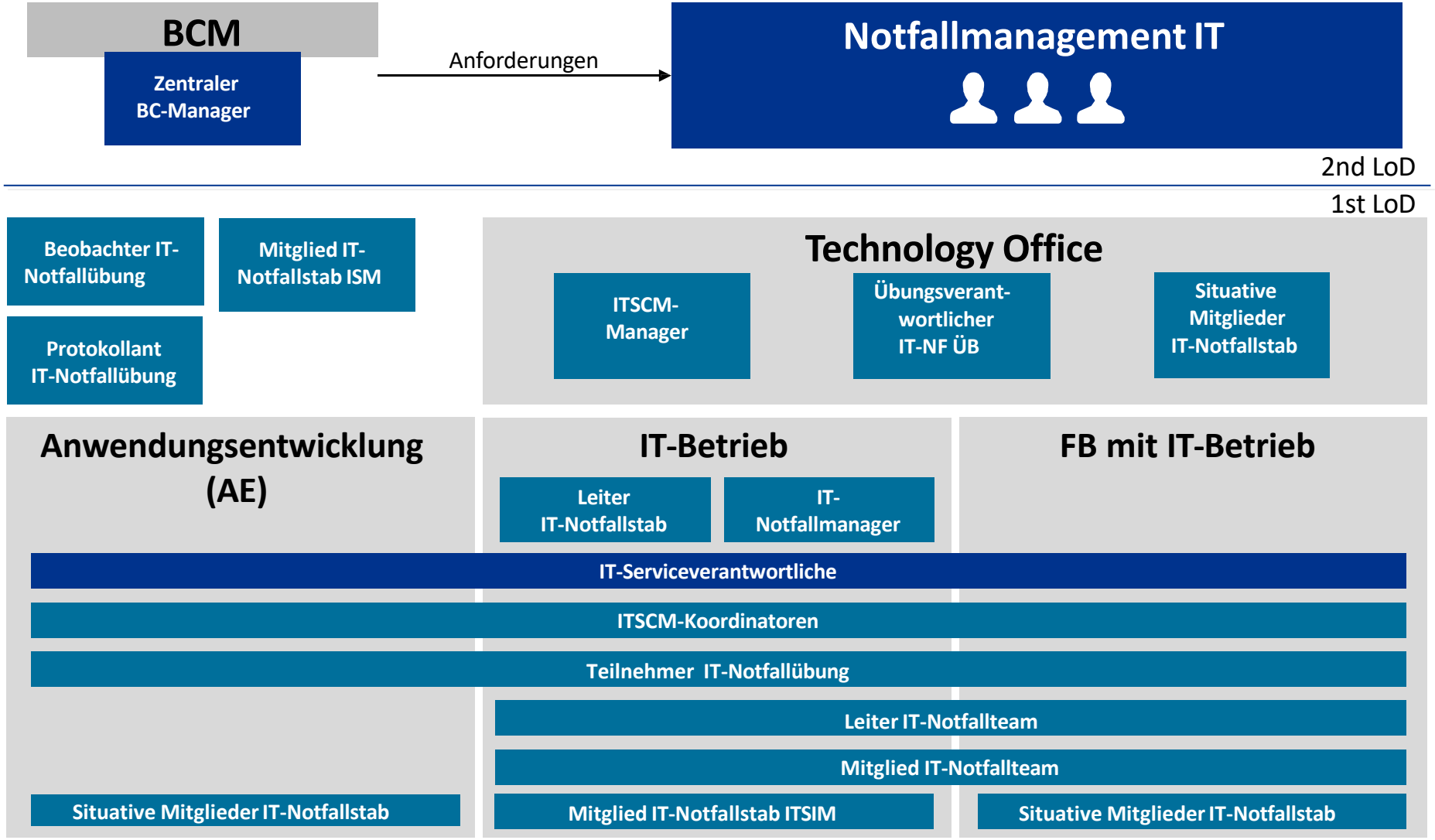
Ziele der IT-Notfallvorsorge

- Erstellung, Implementierung und regelmäßigen Überprüfung aller IT-Notfallvorsorgemaßnahmen
- Etablierung eines Notfallvorsorgeniveaus mit angemessenen Maßnahmen zur Minimierung von IT-Ausfallrisiken
- IT-Notfallorganisation ist in der Lage, (potentielle) IT-Notfälle zu erkennen

Ziele der IT-Notfallbewältigung

- die Schadensminderung, sowie die Sicherstellung der operativen Handlungsfähigkeit im IT-Notfall
- Steuerung der „IT-verantwortenden Einheiten“, um eine zielgerichtete effiziente Reaktion zu ermöglichen

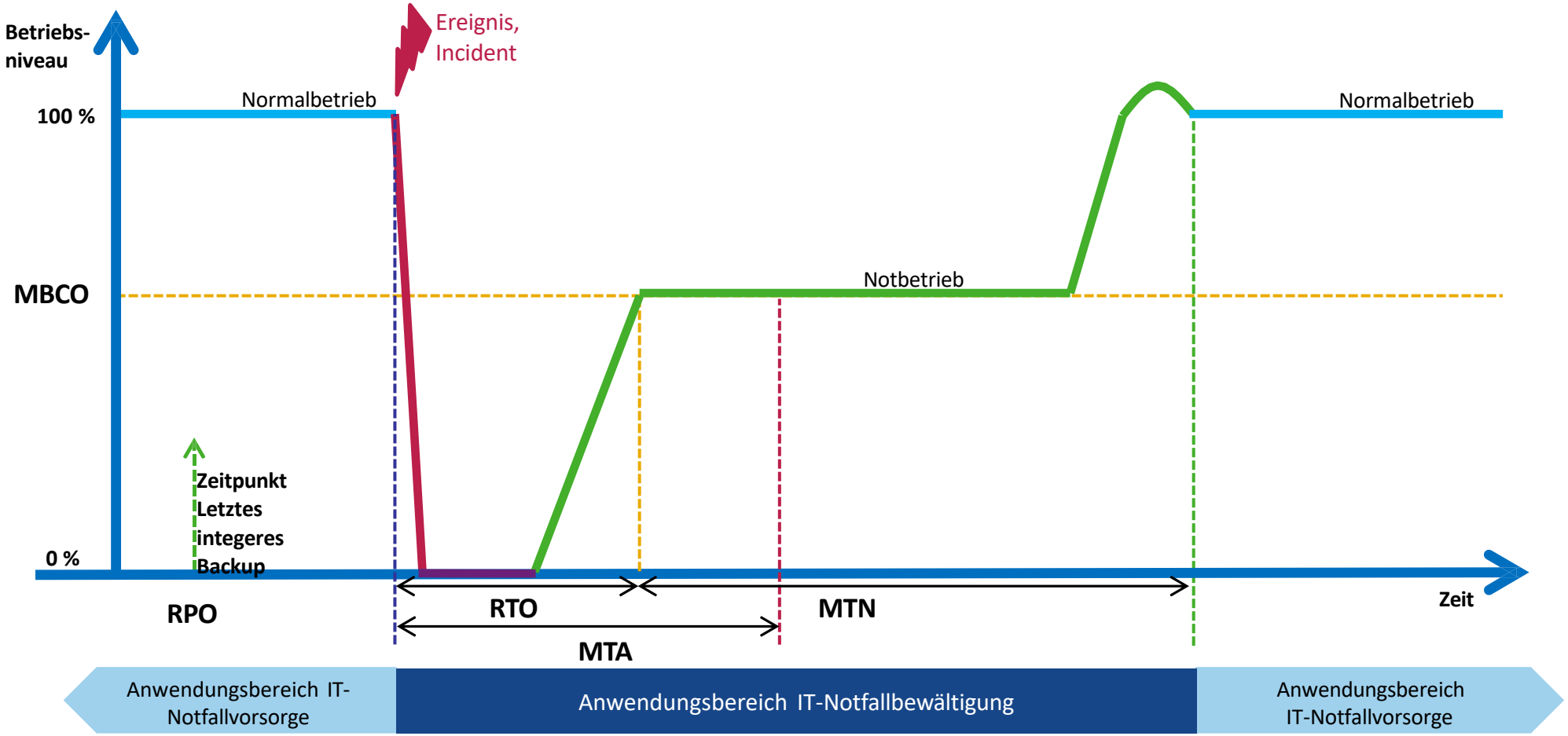
9.4. ITSCM Organisation (Kundenbeispiel)



Hochschule Niederrhein
University of Applied Sciences

9.4. Grundlegende Begriffe im ITSCM

Exkurs



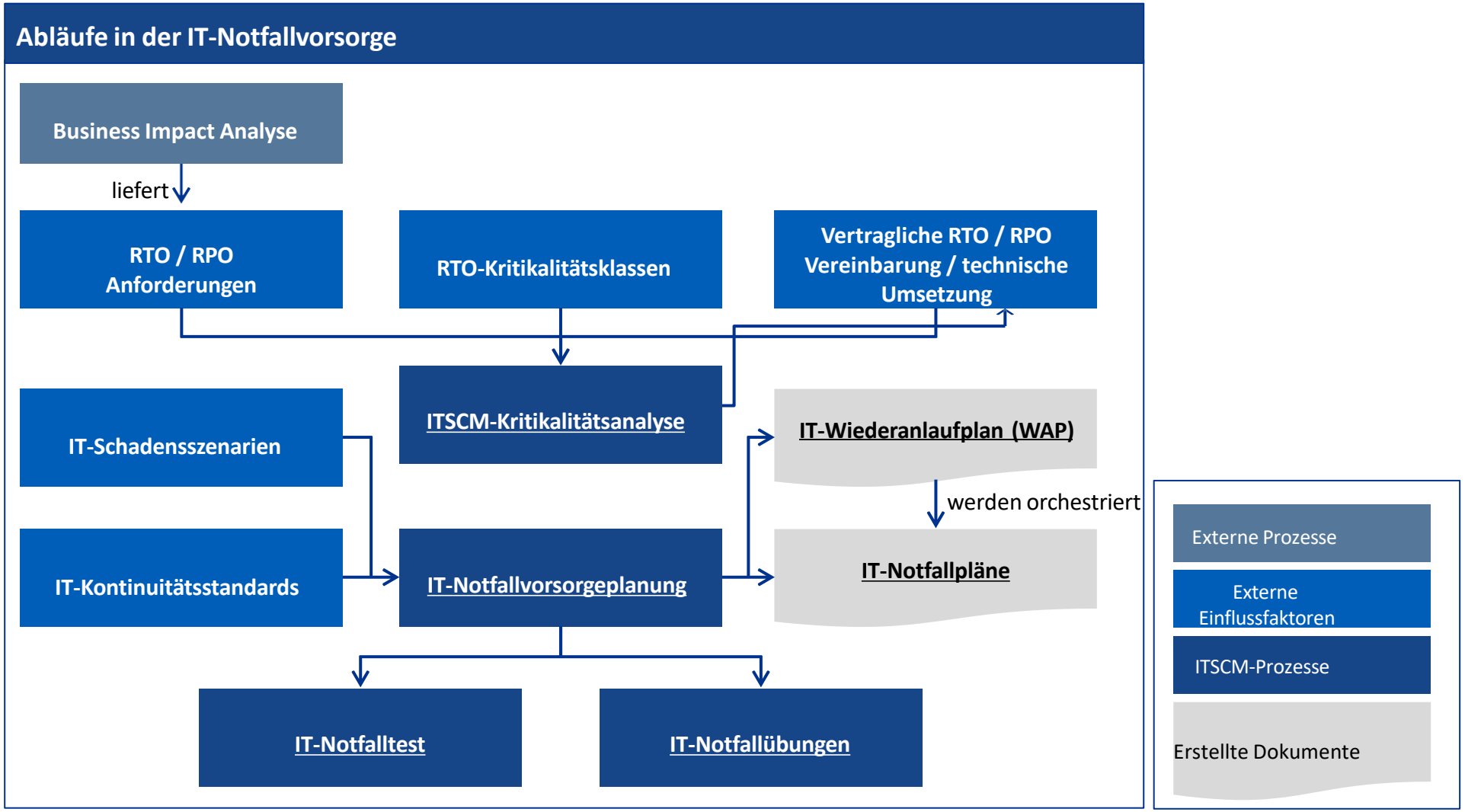
Hochschule Niederrhein
University of Applied Sciences

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.5. Zentrale Prozesse in der IT-Notfallvorsorge

- BIA liefert RTO/RPO. ITSCM macht daraus Kritikalität, Pläne und Tests

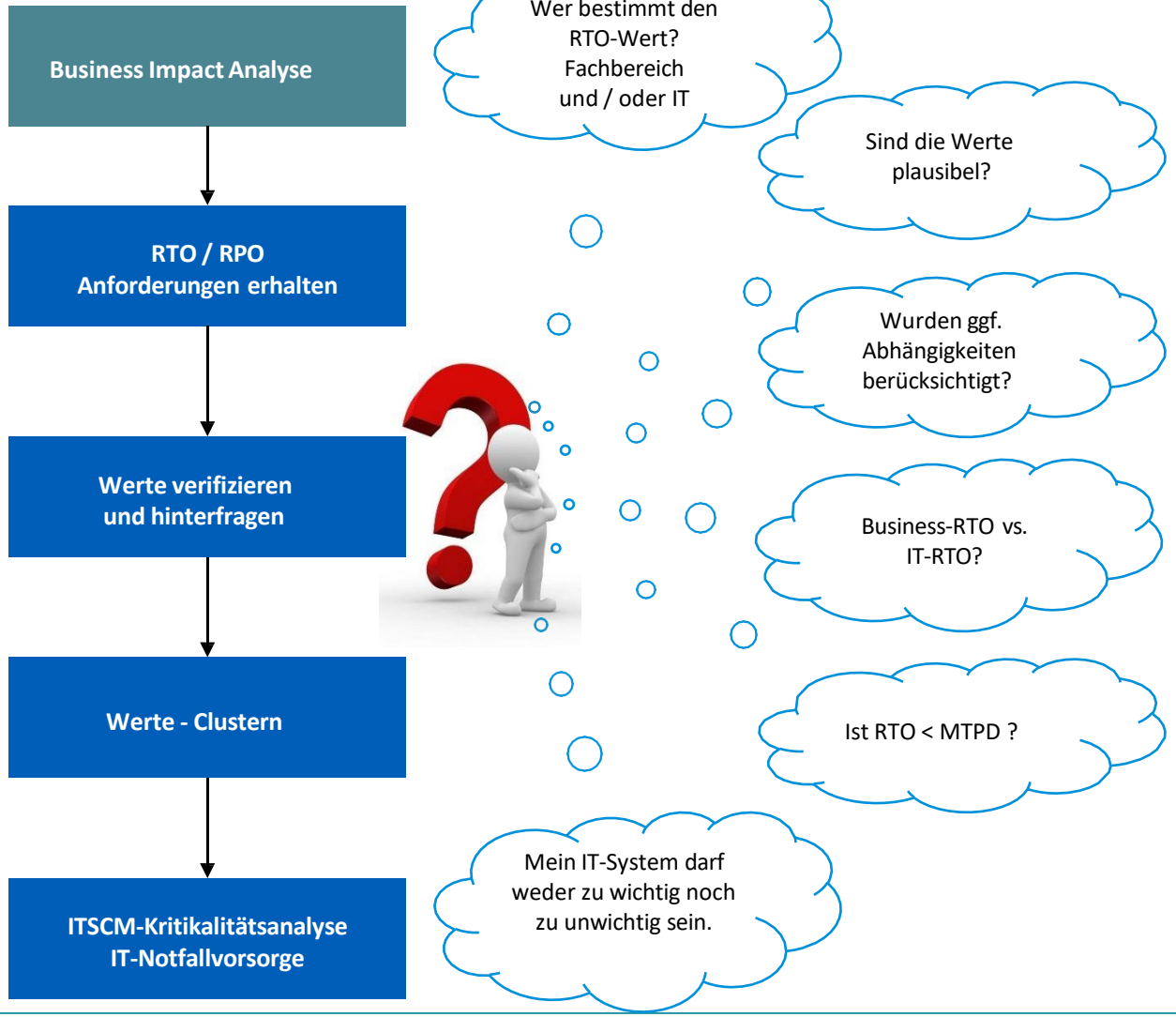


9.5. RTO / RPO Anforderungen aus der BIA

- RTO/RPO-Werte müssen hinterfragt und geclustert werden

IT-Service	Kürzest Angeforderte RTO	Zeiteinheit
ABAKUS	240	Std.
AbgMuGe	240	Std.
ABR	24	Std.
Abrechnung Berichtsjahr (B	240	Std.
Abstimmung ANL Derivate	240	Std.
Abstimmung Related Partie	240	Std.
Abwicklung Treasury	240	Std.
AccPay	72	Std.
Acctability	240	Std.
ACL	240	Std.
Administration & Reconcili	72	Std.
Admission	4	Std.
ADP	120	Std.
ADR Bestandsauswertung	240	Std.
ADR_KoLi	240	Std.

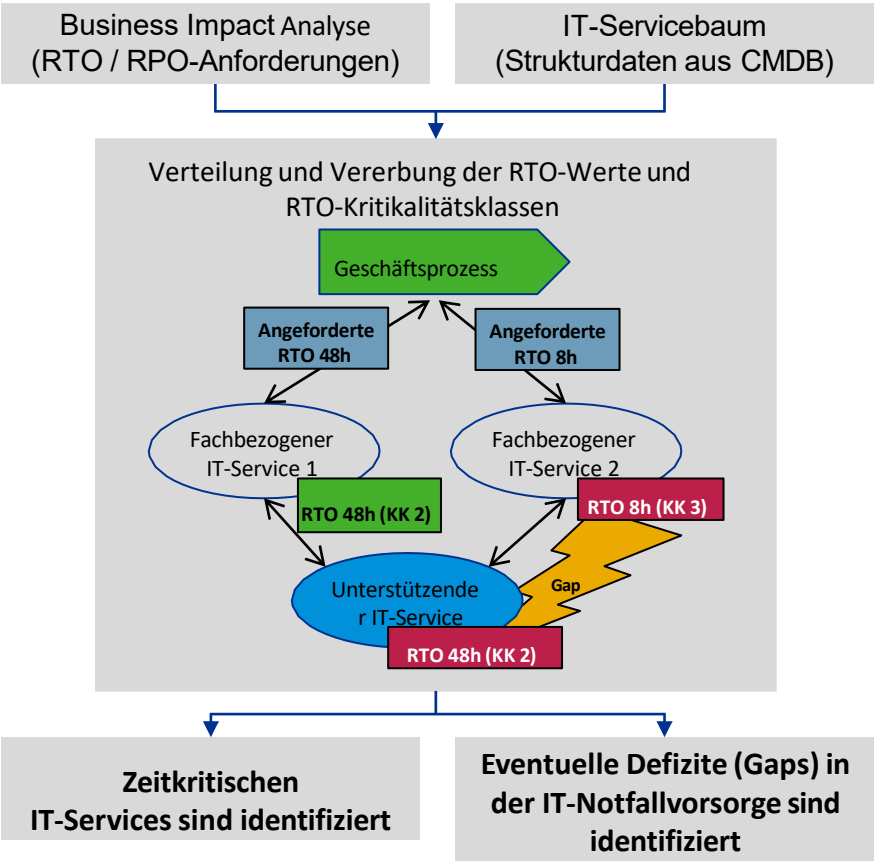
RTO-Werte	RTO-Kritikalitätsklasse
>0–4 h	4
>4–24 h	3
>24–120 h	2
>120–240 h	1



9.5. ITSCM-Kritikalitätsanalyse

- Ziel der ITSCM-Kritikalitätsanalyse ist die Identifikation aller (zeitkritischen) fachbezogenen sowie unterstützenden IT-Services

Ablauf der ITSCM-Kritikalitätsanalyse

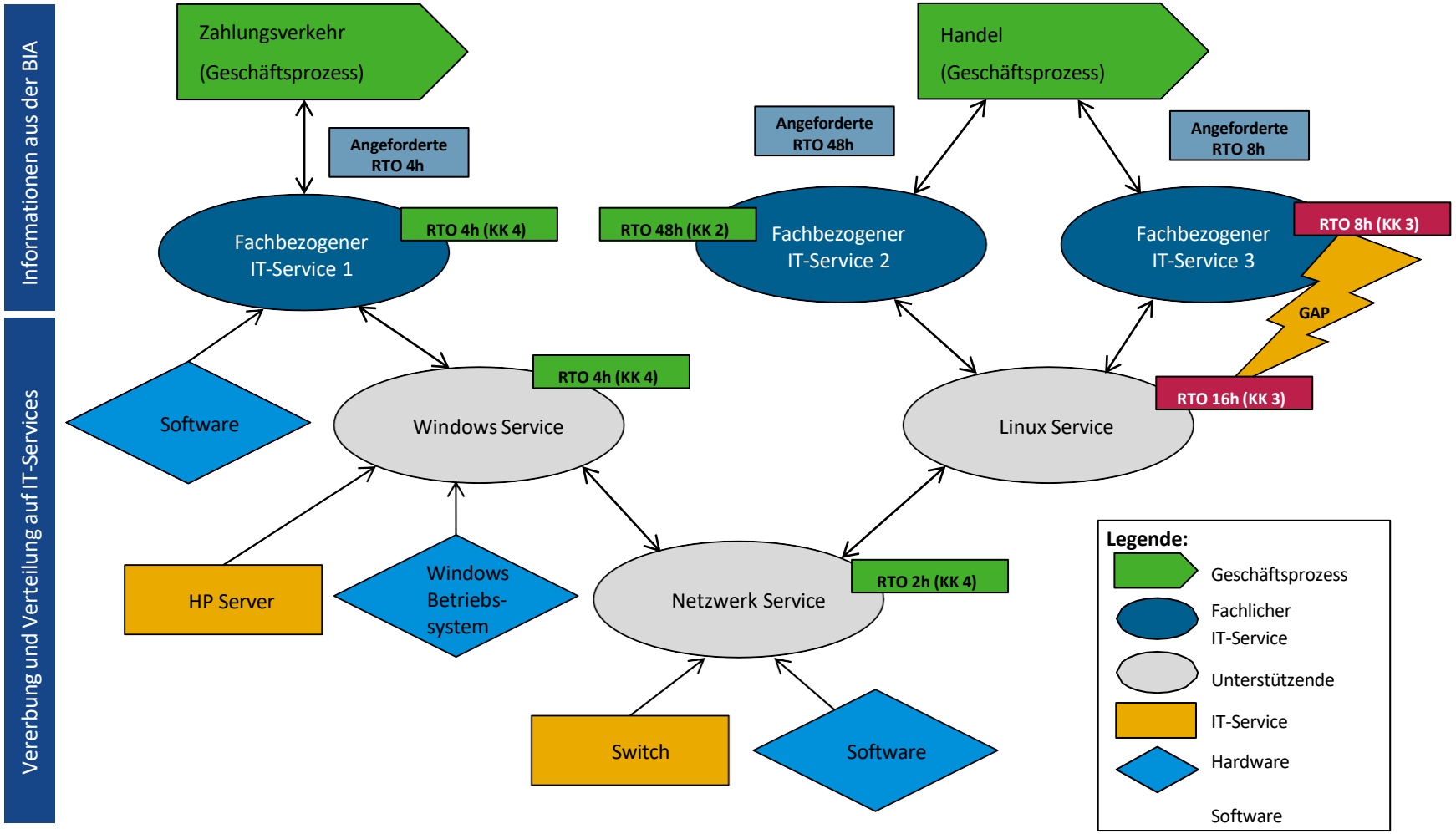


Erläuterungen zur ITSCM-Kritikalitätsanalyse

- Durchführung der ITSCM-Kritikalitätsanalyse bei:
  - Beantragung eines neuen IT-Services
  - Änderung der RTO-Anforderung eines fachbezogenen IT-Services
  - Rückbau eines fachbezogenen IT-Services
  - Ersetzen eines unterstützenden IT-Services
- Zuordnung und Dokumentation der RTO-Werte und RTO-Kritikalitätsklassen mittels Verteilung und Vererbung auf die unterstützenden IT-Services
- Kennzeichnung intern / extern verantworteter IT-Services
- End-to-End-Betrachtung berücksichtigen
- Sequenzielle Abhängigkeiten aufzeigen
- Parallele Abhängigkeiten aufzeigen
- Incident Bearbeitungszeit abziehen
- Eventuell identifizierte Abweichungen (Gaps) werden dokumentiert und gemeldet

9.5. ITSCM-Kritikalitätsanalyse

- RTO-Anforderungen werden auf IT-Services vererbt und verteilt



Hochschule Niederrhein
University of Applied Sciences

Übersicht

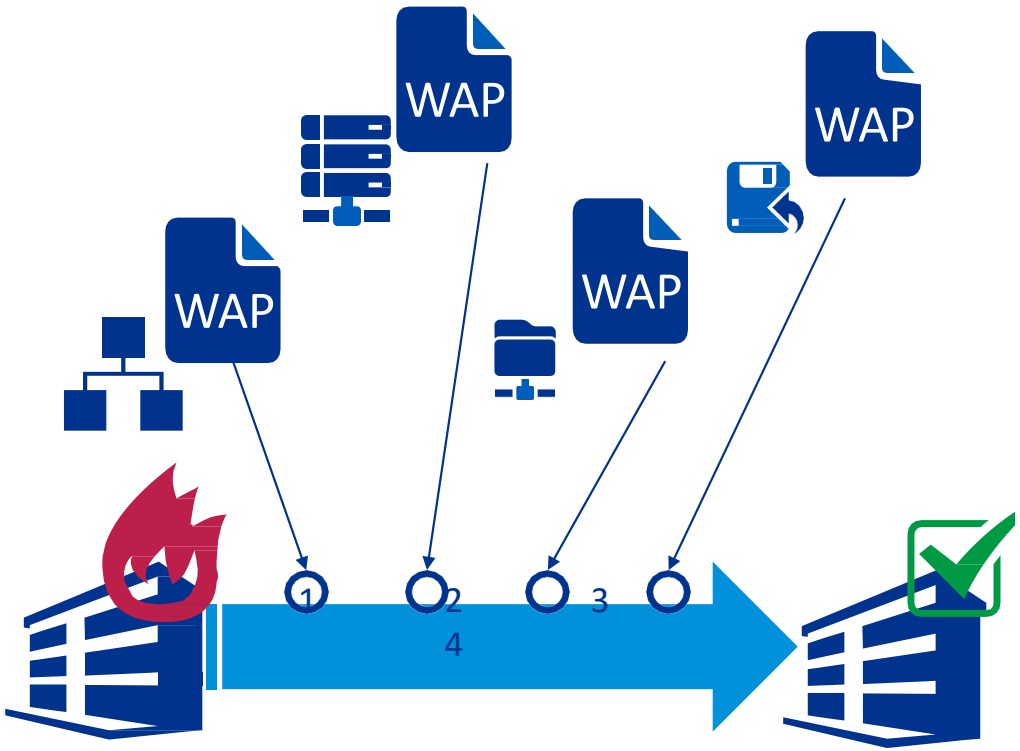
1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.6. IT-Notfallpläne und IT-Wiederanlaufpläne (WAP)

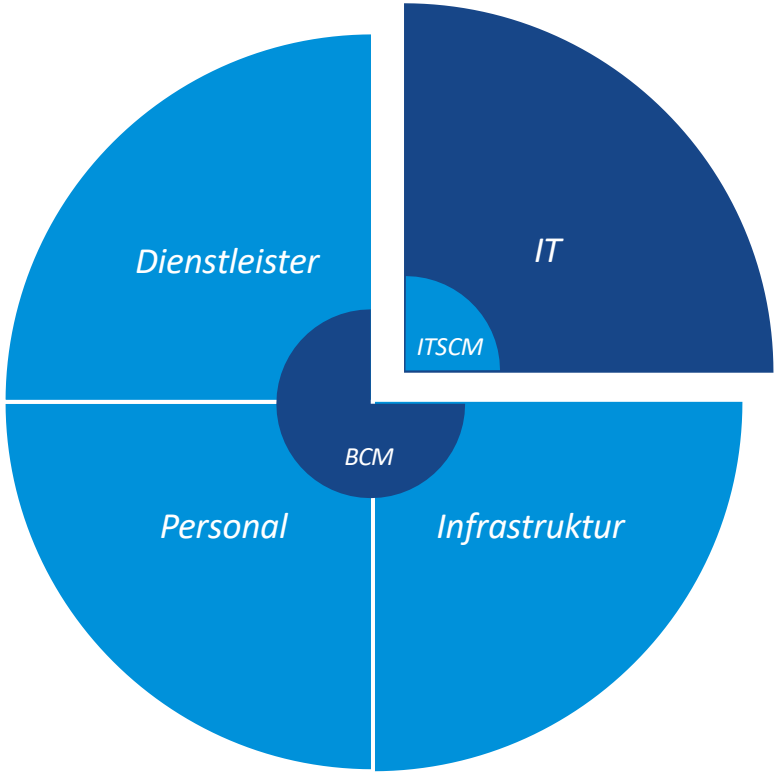
Ein **Wiederanlaufplan (WAP)** regelt

IT-Service-spezifische Aufgaben und Abläufe der IT-Notfallvorsorge und -bewältigung. Hier werden alle relevanten Inhalte, z.B. die spezifischen Verfügbarkeitsanforderungen, Zuständigkeiten, Kommunikations- und Eskalationslisten, IT-Architekturen, Art und Weise der Erreichung der Verfügbarkeits-ziele, Testkonzepte zum Notfallmanagement IT, beauftragte Dienstleister oder Abhängigkeiten dokumentiert.

Je nach IT-Schadensszenario wird der zugehörige IT-Notfallplan aktiviert. Im jeweiligen **IT-Notfallplan** werden die **Wiederanlaufpläne** der betroffenen IT- Services in der **vorgesehenen Reihenfolge orchestriert**. Hierdurch soll sichergestellt werden, dass Maßnahmen und Aktivitäten im Rahmen einer Wiederanlaufsequenz situationsgerecht abgewickelt werden.



9.6. Schadensszenarien im BCM und ITSCM

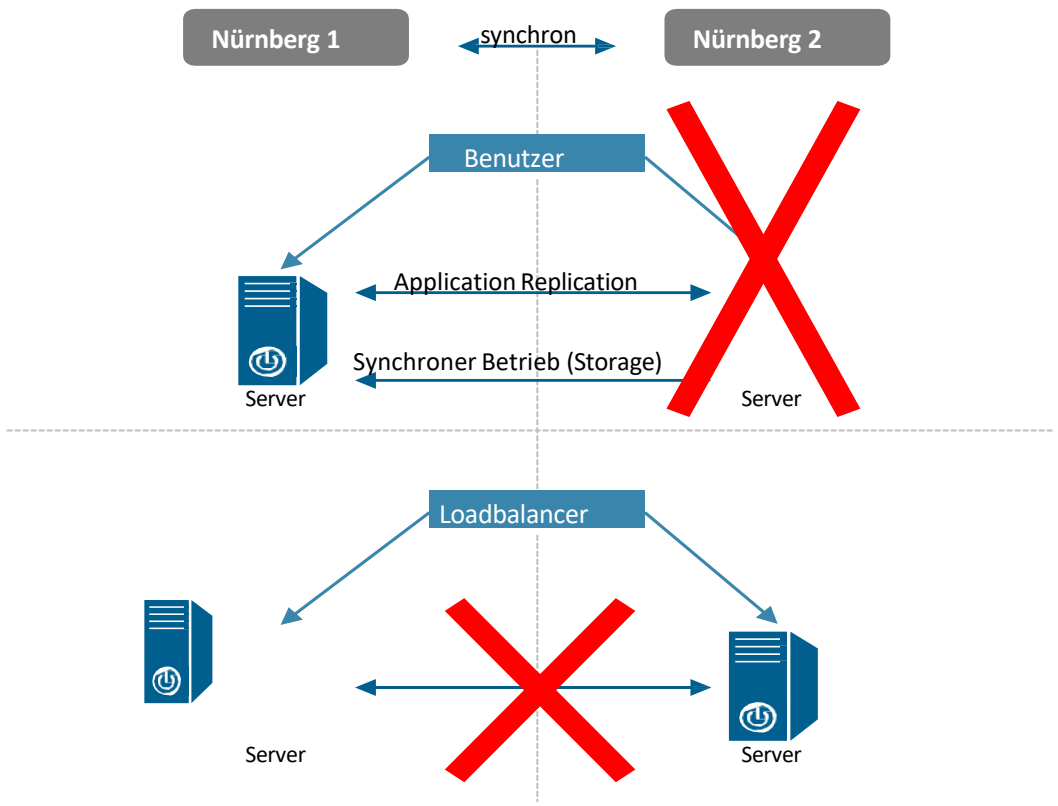


Schadensszenarien für die IT-Notfallvorsorge	
Nr.	**Schadensszenario ***
1	**Rechenzentrumsausfall**. Bei einem Rechenzentrumsausfall steht eine Site nicht mehr zur Verfügung. Ein Schwenk oder eine Wiederherstellung der ausgefallenen IT-Services muss auf ein Backup Rechenzentrum durchgeführt werden.
2	**Datenkorruption**. Bei einer Datenkorruption kann ein Schaden an der Verfügbarkeit der Geschäftsdaten entstehen, sodass der Geschäftsprozess die Geschäftsdaten als verloren deklarieren muss.
3	**Ausfall eines IT-Services**. Ein IT-Service steht nicht zur Verfügung (z.B. Storage fällt aus, Datenbankcluster nicht funktionsfähig oder Mailservice nicht verfügbar). Ersatzgeräte oder eine Wiederherstellung ist erforderlich.
4	**Konsistenzverlust/ Logische Fehler**. Die Konsistenz der Software oder Konfiguration eines AWS oder einer IT- Infrastrukturkomponente ist kompromittiert (z.B. nach dem Patching stürzt ein Server ab oder der Administrator hat eine fehlerhafte Konfiguration eingespielt).
5	**Sicherheitsvorfälle**. Bei Sicherheitsvorfällen kann ein Schaden an der Hardware oder Software von IT-Services entstehen.

* Basierend auf ISO 27031

Schadensszenario 1: Rechenzentrumsausfall

Übersicht



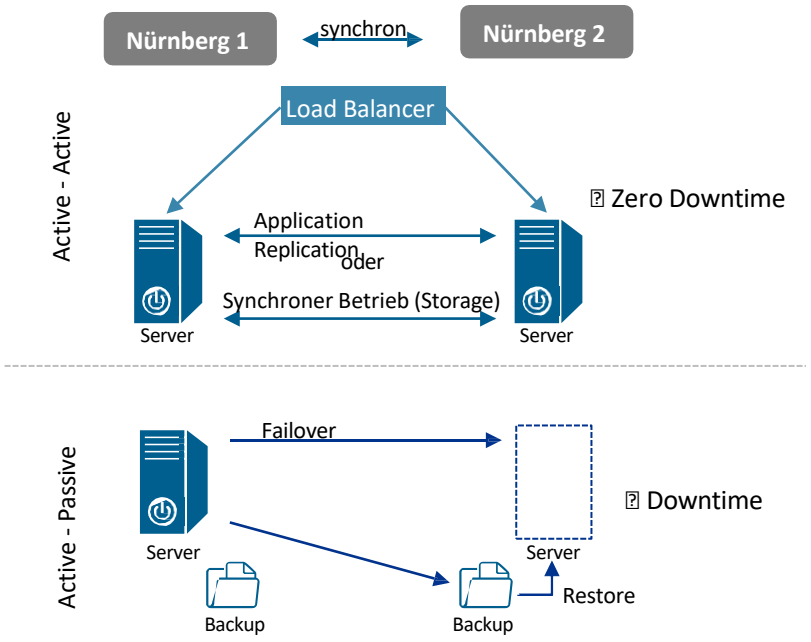
Beispiel

Erläuterung des Szenarios

- Eine **Rechenzentrumslokation fällt** bspw. durch physische Schäden oder eine getrennte Zuleitung **aus**
- **Alle Services** dieser Lokation und die **gespeicherten Daten stehen nicht zur Verfügung**
- Der **Betrieb muss auf** in **einem oder mehrere Backup Rechenzentren** verlagert werden
- **Split Brain** stellt eine Sub-Form dieses Szenarios dar:
  - **Beide Rechenzentren eines Clusters sind aktiv**, aber alle **Zwischenverbindungen** zwischen den Clusterteilen werden **gleichzeitig unterbrochen**
  - Somit können beide weiter Daten erhalten, die aber nicht synchronisiert werden – die Folge sind **inkonsistente Datenbestände**
  - Es ist nicht klar, welches Rechenzentrum den führenden Datenbestand hält

Schadensszenario 2: Rechenzentrumsausfall

Übersicht



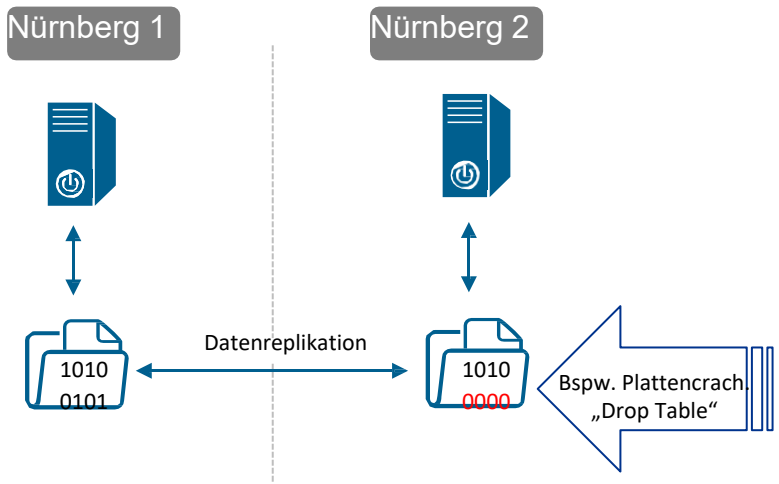
Beispiel

Erläuterung des Szenarios

- Welche **DR-Strategie** wird verfolgt (z.B. Failover oder Restore)?
- In welchen Rechenzentren werden die IT-Architekturkomponenten betrieben und in welcher Konfiguration (bspw. Active/Active oder Active/Passive)?
- Sind die Entfernungen zwischen den Rechenzentren ausreichend?
- Welche Redundanzen/Kapazitäten müssen während des IT-(Not-)betriebs verfügbar sein?
    - Sind im zweiten Rechenzentrum alle abhängigen IT-Directory, Netzwerkanbindungen, Datenbanken etc.)
    - Wird ausreichend Kapazität in dem zweiten Rechenzentrum für den Restore vorgehalten
    - Decken die Beauftragungen die benötigten Kapazitäten und Redundanzen ab?
- Sind relevante Daten für den Wiederanlauf in den Ausweichrechenzentren gespeichert (z B Konfigurationen)?
- Ist ein Betrieb im Backup Rechenzentrum mit allen abhängigen Services End to End sichergestellt?
- Sind manuelle Schritte für einen RZ Schwenk notwendig? (Konfiguration von IP Adressen)
- Werden die vorgegebenen RTO und RPO Werte bei Anwendung der Strategie eingehalten?

Schadensszenario 2: Datenkorruption

Übersicht

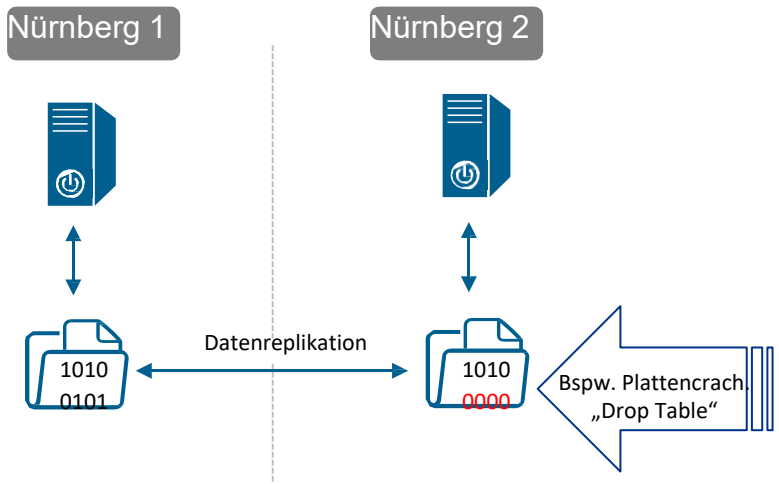


Erläuterung des Szenarios

- Durch **technisches** (bspw. Fehler oder Ausfall von Software oder Hardware) **oder menschliches Versagen** werden **Geschäftsdaten** soweit **beschädigt oder gelöscht**, sodass diese als verloren deklariert werden.
- Eine **Rekonstruktion der Live-Daten ist nicht möglich.**
- Geschäftsprozesse können erst nach einer Wiederherstellung der Geschäftsdaten fortgesetzt werden.
- Die **Datenverfügbarkeit** umfasst primär die Integrität und Vollständigkeit von Geschäftsdaten. Alle hierauf zu entwickelnden Verfahren müssen den Nachweis erbringen, ihre Eignung zur Wiederherstellung von Geschäftsdaten gewährleisten zu können.
- SAN (Storage Area Network) Storage Datenspeicher definieren sich als Blockdaten Medien. Diese eignen sich nicht, um die Integrität und Verfügbarkeit von Geschäftsdaten zu gewährleisten. Der Ausfall eines Blockdaten Mediums kann ohne weitere Sicherungsverfahren zu einem Totalverlust führen. Sofern SAN Speicher eine tragende Funktion besitzen, ist ein Nachweis zur Sicherstellung der Integrität und Vollständigkeit von Geschäftsdaten zu erbringen.

Schadensszenario 2: Datenkorruption

Übersicht



Überlegungen in Bezug auf das Szenario

- Werden geeignete **Backup- und Recovery-Strategien** und -Technologien eingesetzt, um den geforderten RPO einzuhalten?
- Wie häufig werden Datensicherungen durchgeführt?
- Wurden Backup Intervalle (Tages-, Wochen-, Montatssicherungen) ordnungsgemäß festgelegt und beauftragt?
- Werden „Medienbrüche“ in den Backup- und Recovery-Strategien eingesetzt? (z.B. Disk-to-Tape)
- Ist das Datensicherungsverfahren auf die Datenintegrität von Geschäftsdaten geeignet? Sichert der Betreiber eine „application aware“ Sicherung zu? (Achtung bei der Angabe von SAN Speicher als Datensicherungsmedium)
- Kann die zu sichernde Datenmenge in der vorgegebenen Zeit (RTO) wiederhergestellt werden?
- Wurde festgelegt, wie die Integrität und Vollständigkeit der wiederhergestellten Geschäftsdaten ermittelt werden kann?
- Ist der Fachbereich zur Bestätigung der Integrität und Vollständigkeit der Geschäftsdaten eingebunden? Ist eine Fortführung der ausgefallenen Geschäftsprozesse sichergestellt?

Schadensszenario 3: Komponentenausfall

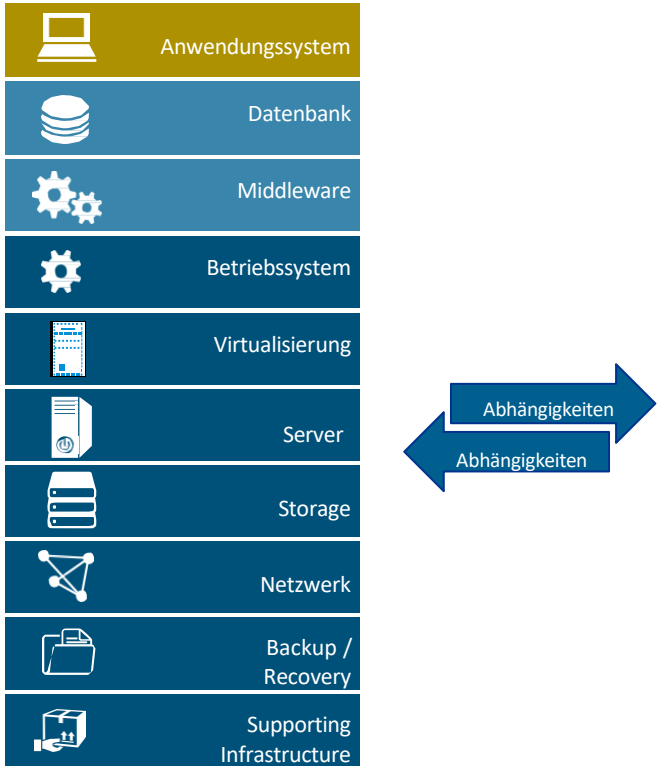
Übersicht	
Anwendungssystem	
Datenbank	Defekter Datenbankcluster
Middleware	MQ Services leiten keine Nachrichten weiter
Betriebssystem	Windows Bluescreen OS bootet nicht mehr
Virtualisierung	Hypervisor korrupt
Server	HW Defekt
Storage	Defekte Festplatte Spiegelung unklar
Netzwerk	Ausfall Load Balancer Defekter Switch
Backup / Recovery	Ausfall Backup-Mechanismus Defekter Tape-Roboter
Supporting Infrastructure	Ausfall Active Directory

Erläuterung des Szenarios

- Die für eine Plattform und ein Anwendungssystem eingesetzten IT-Architekturkomponenten funktionieren nicht wie vorgesehen. Der Betrieb der vorhandenen Hardware kann erst nach Instandsetzung oder durch ein Ersatzgerät wieder aufgenommen werden.
- Der Ausfall von abhängigen Komponenten (bspw. Active Directory) führt ebenfalls dazu, dass IT-Architekturkomponenten nicht genutzt werden können.
- Einschränkungen der Leistungsfähigkeit (z.B. durch hohe Antwortzeiten), die eine Fortführung des Geschäftsbetriebs unterbinden bzw. erheblich einschränken, sind als nicht funktionsfähig einzustufen. Der Grad der Einschränkung ist in Zusammenarbeit mit dem Availability Management festzulegen. Wegen AWS- oder Infrastrukturspezifischen Anforderungen können abweichende Indikatoren vereinbart werden.
- Genutzte dritte Dienste (Abhängigkeiten), die eine Auswirkung auf die eigene Anwendungsverfügbarkeit besitzen, sind zu betrachten. Dies kann technische Dienste (z.B. Active Directory) und/oder fachliche Dienste (z.B. Vertragsdatenbank) umfassen.
- Ein Komponentenausfall bewertet den Ausfall von Ressourcen, die im Rahmen einer IT-Notfallbewältigung ersetzt oder vollständig wiederhergestellt werden müssen

Schadensszenario 3: Komponentenausfall

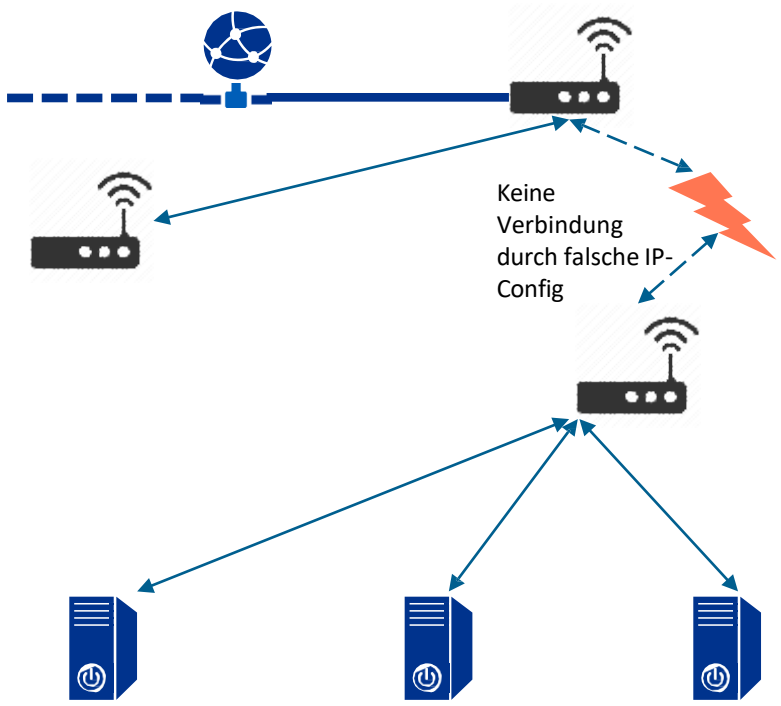
Übersicht



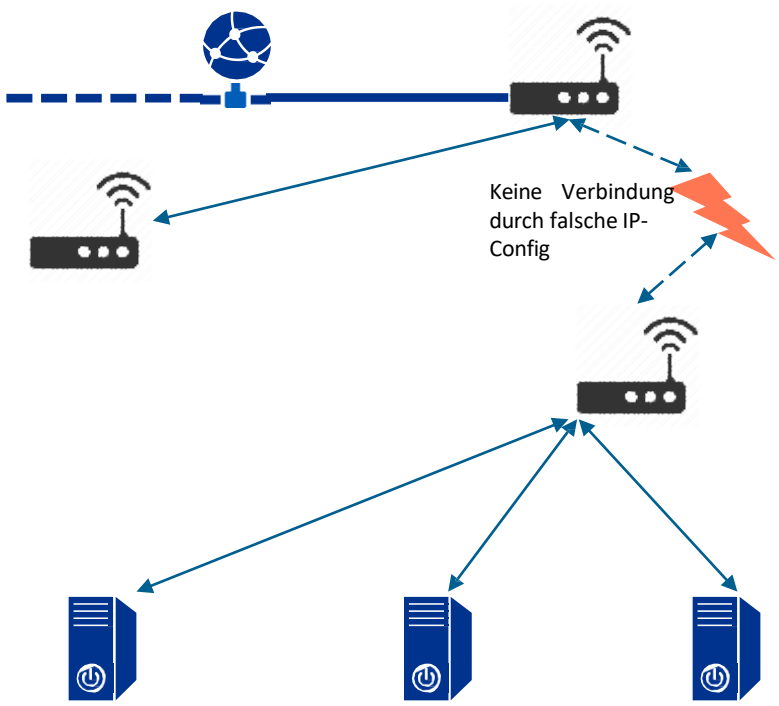
Überlegungen in Bezug auf das Szenario

- Sind Abhängigkeiten von und zu anderen IT-Architekturkomponenten analysiert? (bspw. kann der Ausfall des AD weitreichende Auswirkungen mit sich führen)
- Erfüllen genutzte IT-Services die Anforderungen an die geforderten Verfügbarkeiten?
- Existiert für jede Hardwarekomponente eines AWS eine Ersatzkomponente?
- Kann der Betrieb (vorübergehend) auf anderer Hardware fortgesetzt werden (bspw. in einem anderen Rechenzentrum)?
- Wurden erforderliche Beauftragungen im Hinblick auf die erforderlichen Redundanzen und Kapazitäten getätigt?
- Defekte Komponente:
    - Werden entsprechende Ersatzkomponenten gelagert oder können innerhalb der geforderten RTO-Zeiten beschafft werden?
    - Ist mit Providern vertraglich eine Strategie vereinbart, wie diese bei Ausfall einer Komponente zu reagieren sollen?
- Sind alle Ebenen der IT-Architekturen betrachtet worden?

Schadensszenario 4: Konsistenzverlust

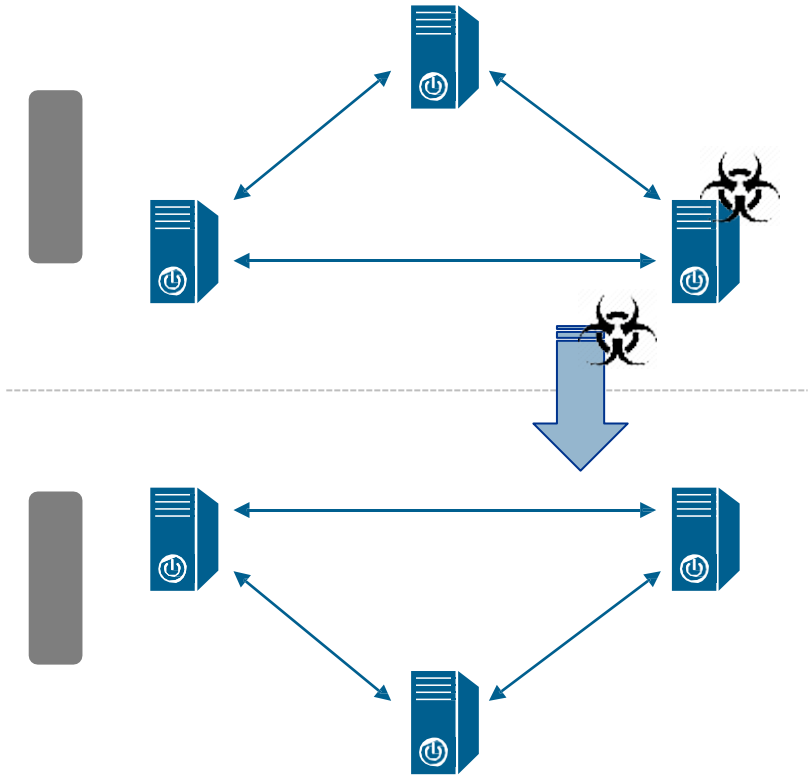
Übersicht	Erläuterung des Szenarios
	• Durch das Einspielen eines fehlerhaften Patches oder einer fehlerhaften Konfiguration funktioniert die bearbeitete IT- Architekturkomponente nicht wie gewünscht. Geschäftsprozesse können in der Zeit nicht über diese Komponenten abgewickelt werden. • Erst nach Behebung des Fehlers kann der Prozess wieder über diese Komponente bereitgestellt werden. • Beispiele hierfür sind u.a. fehlerhaft konfigurierte Netzwerkkomponenten, fehlerhafte Patches für Software- oder Hardwarekomponenten. • Die Hardware kann weiterhin genutzt werden, so dass eine Ersatzbeschaffung entfällt. Die Wiederherstellung der Servicefunktionalität ist durch administrative Maßnahmen möglich. • Der Betrieb sollte Maßnahmen ergreifen, eine Roll-Back Fähigkeit zu etablieren und neue Funktionen und Konfigurationen vor eine Inbetriebnahme zu testen. Siehe hierzu auch das neue Staging Konzept für IT-Anwendungen und IT-Infrastrukturen.

Schadensszenario 4: Konsistenzverlust

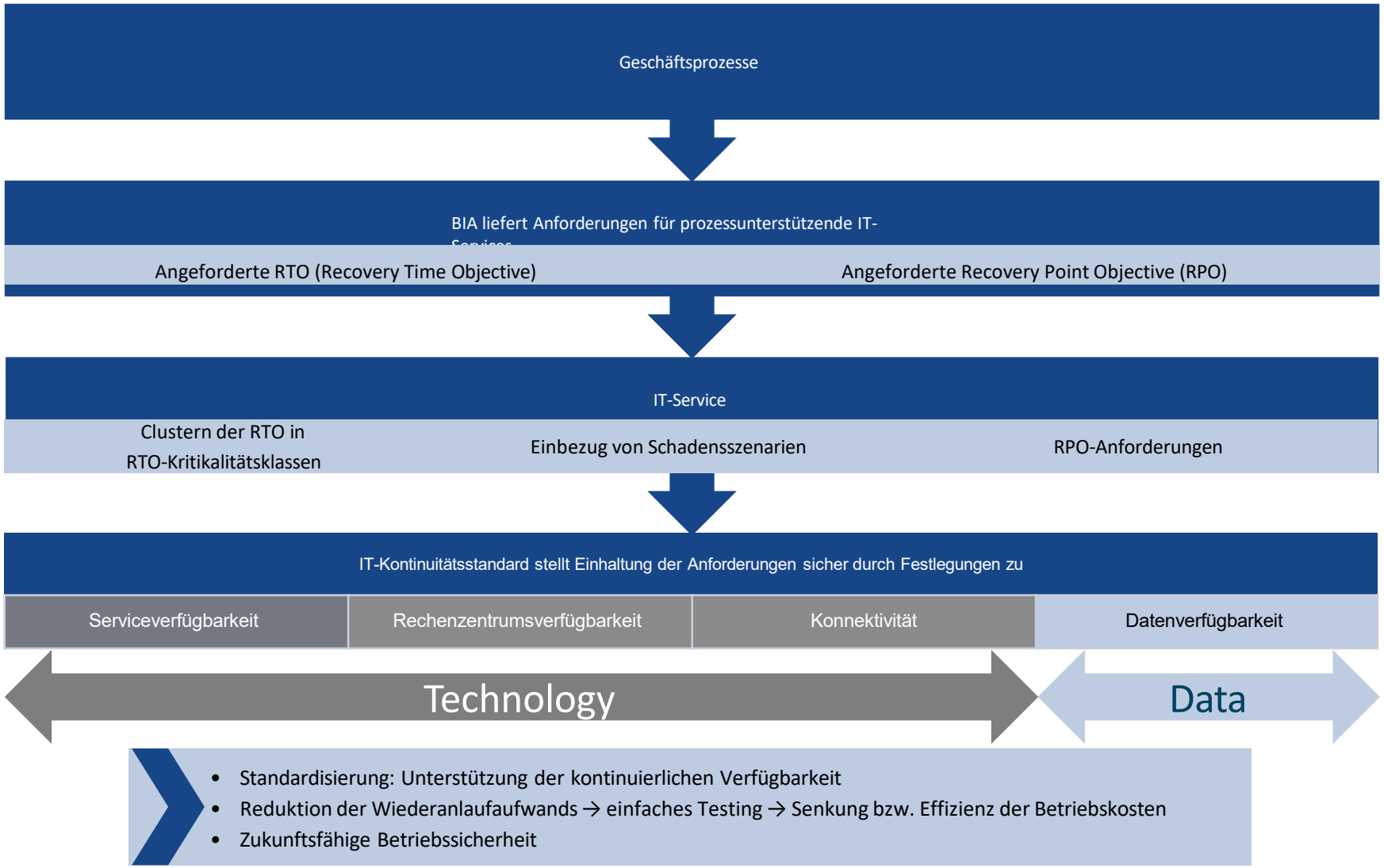
Übersicht	Überlegungen in Bezug auf das Szenario
	• Wird ein Staging-Konzept betrieben, welches Konfigurationsfehler durch das Testen auf gleicher Hardware minimieren kann? • Existieren Backup-Strategien, um vorherige Konfigurationen wiedereinzuspielen? • Liegt ein Roll-Back Konzept vor, um eine Wiederherstellung des zuletzt funktionierenden Versionsstandes zu ermöglichen? • Kann ein Funktionsversagen einer technischen Komponente (z.B. Storage) zu einem Totalausfall (sowohl im aktiven als auch im Backup Rechenzentrum) führen? Wurden hierfür Maßnahmen ergriffen? • Können Wiederherstellungsmaßnahmen auch ohne die Verfügbarkeit der ausgefallenen Komponente durchgeführt werden? (z.B. Konfigurationsdateien liegen außerhalb des ausgefallenen Storages) • Software und Konfigurationsdaten werden auf ihre Integrität (z.B. Hash Prüfsummen oder Code Signing) geprüft

Schadensszenario 5: Sicherheitsvorfälle

Übersicht	Überlegungen in Bezug auf das Szenario

	• IT-Sicherheitsvorfälle sind sehr vielseitig. Einige Beispiele, die das BSI nennt:
	  • Fehlkonfigurationen, die zur Offenlegung vertraulicher Daten oder zu Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen,
	  • Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten durch inhärente Fehler,
	  • Auftreten von Schadsoftware oder
	  • kriminelle Handlungen (etwa Hacking von Internet-Servern, Einbruch in IT-Systeme, Diebstahl von Daten, Sabotage oder Erpressung mit IT-Bezug).
	• Strategien mit dem Umgang von IT-Sicherheitsvorfällen sind bei der Erstellung der IT-Notfalldokumente mit dem Information Security Management (ISM) abzustimmen.
	• Bei der Nicht-Verfügbarkeit aufgrund eines IT-Sicherheitsvorfalls ist ISM immer sofort einzubinden
	• Sofortmaßnahmen, wie bspw. das Abschalten von Servern, sind mit ISM abzustimmen, da bspw. forensische Untersuchungen sonst nicht vorgenommen werden können.

9.6. IT-Kontinuitätsstandard /-strategie



- Standardisierung: Unterstützung der kontinuierlichen Verfügbarkeit
- Reduktion der Wiederanlaufaufwands → einfaches Testing → Senkung bzw. Effizienz der Betriebskosten
- Zukunftsfähige Betriebssicherheit

9.6. Details: IT-Kontinuitätsstandard /-strategie

Das Ziel von Notfallmanagement IT (2nd Line of Defense) und ITSCM (1st Line of Defense) ist die Sicherstellung eines angemessenen Notfallvorsorgeniveaus. Zur Sicherstellung eines angemessenen Notfallvorsorgeniveaus sollte eine Standardisierung der IT-Kontinuitätsoptionen für IT-Services sowie die Festlegung übergreifender Vorgaben zur Behandlung von Schadensszenarien und Abdeckung der Kontinuitätsanforderungen gemäß RTO (Recovery Time Objective) und RPO (Recovery Point Objective) erfolgen.

Technologie

Serviceverfügbarkeit

Wesentliche Bestandteile: Redundanzen in IT-Services, Aktive Komponenten, Einhaltung RTO-Anforderungen

Rechenzentrumsverfügbarkeit

Wesentliche Bestandteile: Einhaltung RTO- und RPO-Anforderungen, Standorte, Entfernungen, Anforderungen an Rechenzentren

Konnektivität von Rechenzentren und Niederlassungen

Wesentliche Bestandteile: Verbindungen zwischen den Rechenzentren sowie Niederlassungen und Rechenzentren, Vorgaben zur Ausgestaltung der Verbindungen

Daten

Datenverfügbarkeit

Einhaltung RPO-Anforderungen, Anzahl Datenkopien, Snapshots, Backups

Die IT-Kontinuitätsstandards setzt sich aus den Themen Technologie und Daten zusammen. Für jedes Themengebiet sind entsprechende Vorgaben zu definieren. Als wesentliche Grundlage dienen die angeforderten RTO- und RPO-Zeiten und die festgelegten Schadensszenarien.

Hochschule Niederrhein
University of Applied Sciences

9.6. Details: IT-Kontinuitätsstandard /-strategie

Technologie - Serviceverfügbarkeit

Wesentliche Bestandteile:

- Redundanzen in IT-Services,
- Aktive Komponenten,
- Einhaltung RTO-Anforderungen

Maßnahmen:

- Bedarfsgerechte Dimensionierung der IT- Architektur zur Einhaltung der Kontinuitätsanforderungen
- **Entkopplung der Serviceverfügbarkeit**

von Datenverfügbarkeit ermöglicht granulares IT-Service Design

- Festlegung der IT-Architekturvorgaben für die Serviceverfügbarkeit und eines
- Vorgaben zu Service Aufbau (Aktiv-Aktiv/Aktiv-Passiv) gemäß ITSCM-Kritikalitätsklasse

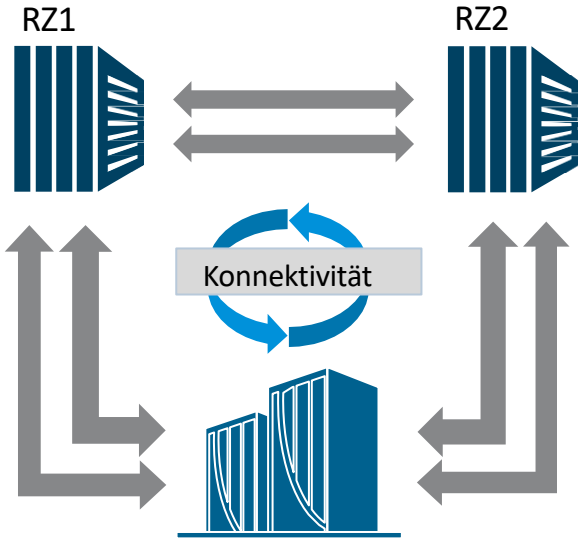
RTO-Kritikalitätsklasse	Umsetzungsoptionen
4 (>0–4h)	**AKTIV – AKTIV** **AKTIV – PASSIV** (HOT-Standby)
3 (>4–24h)	**AKTIV – PASSIV** (HOT-Standby) **AKTIV – PASSIV** (WARM-Standby)
2 (>24–120h)	**AKTIV – PASSIV** (COLD-Standby)
1 (>120–240h)	**SINGLE AKTIV** (Bereitstellung zusätzlicher Hardware durch Provider in garantierter Zeit)

- Maßnahmen gelten für alle IT-Services: Host, Cloud, Server, Netzwerk, …
- Es sind abgestufte Maßnahmen zur Abbildung der einheitlichen Service Levels reduziert die Serviceverfügbarkeiten möglich um die Spannbreite der Diversifizierung in der Umsetzung geforderten RTO-Zeiten abbilden zu können
  - Je höher die RTO-Kritikalitätsklasse, desto umfangreicher die Maßnahmen

Hochschule Niederrhein
University of Applied Sciences

9.6. Details: IT-Kontinuitätsstandard /-strategie

Technologie - Konnektivität



- Die Konnektivität der Rechenzentren und Niederlassungen ist in Abgrenzung zum Netzwerk in Gebäuden und Rechenzentren gesondert zu betrachten
- Die volle Funktionsfähigkeit von Geschäftsprozessen kann nur durch verfügbare Konnektivität gewährleistet werden

  - Hieraus leitet sich eine kontinuierliche Verfügbarkeitsanforderung für die Konnektivität ab
  - Alle IT-Services für die Bereitstellung der Konnektivität gelten als sehr kritisch (RTO ~0h): LAN, WAN, VPN, Firewalls, DNS, NTP
  - Für diese IT-Services ist eine ausführliche Behandlung im Schadensszenario 3 (Ausfall von IT-Services) im Wiederanlaufplan zu definieren um die Verfügbarkeit der Konnektivität im IT-Notfall sicherzustellen

Maßnahmen für die Konnektivität

Rechenzentrumskonnektivität	Konnektivität von Niederlassungen
Redundante Leitungen und getrennte Trassen	Redundante Anbindung und Fallback/Ausweichleitung (bspw. LTE)
WAN Verbindungen sind verschlüsselt	Ausweichmöglichkeiten über Public Internet (z.B. VPN) sind zu etablieren
aktive Nutzung von max. 50% der Kapazität pro Leitung, Standortübergreifend um Ausfall einer Leitung kompensieren zu können	Remote Einwahl (Terminalserver) funktional äquivalent zu normaler Anbindung inklusive ausreichend Kapazitäten für Aufrechterhalten des Notbetrieb

9.6. Details: IT-Kontinuitätsstandard /-strategie

Datenverfügbarkeit

- Die Datenverfügbarkeit zielt auf die technische Verfügbarkeit von Geschäftsdaten ab. Eine fachliche Bewertung der Daten findet nicht im Rahmen von ITSCM statt.
- **Der RTO und RPO sind unabhängig voneinander zu betrachten**
- Die Laufzeit von Datenwiederherstellungsverfahren (Backup & Restore) kann den angeforderten RTO beeinflussen und ist entsprechend auszuwählen und zu gestalten
- Datensicherheit durch **mindestens zwei Kopien** (+Quorum) oder mindestens drei Kopien
- Verschlüsselung und Integritätsschutz von ausgelagerten Datensicherungen
- **Storage und Backup sind organisatorisch voneinander zu trennen** (regulatorische Anforderung; Einzelperson darf nicht in der Lage sein Daten vollständig vernichten zu können)
- **Backups sind bei zwei Rechenzentren kreuzweise zu speichern**.

Angeforderter RPO	Umsetzungsoptionen	Erläuterung / Hinweise	Technologie Beispiele
>0–4h	• Synchrone Replikation • Fast Restore (Hot-Standby)	• Transaktionssicherheit durch mindestens „zwei Commits“ • SAN Spiegelung fokussiert auf Blockstorage, stellt jedoch keine Transaktionssicherheit	• Oracle Dataguard • MS Always On • Oracle ZDLRA (Zero Data Loss Recovery Appliance)
>4–24h	• Snapshot Sicherungen • Asynchrone Datenhaltung (Mitigation Schadens-szenario 3 & 5)	• Inkrementelle Sicherung; Snapshot • Vollständige Sicherung mindestens Wöchentlich • Asynchrones Backup an dritter Lokation	• Cloud Backup • NFS-Ablage (z.B. SAP Redologs) • Storagesicherungen
>24h	• Backup oder Neu-Installation	• Backup Zeitpläne sind entsprechend der Datenmenge und damit verbundenen Wiederherstellungszeiten zu spezifizieren	• TSM • Cloud Backup • „Backup to Disk“ • „Backup to Tape“

9.6. Details: IT-Kontinuitätsstandard /-strategie

Business Impact Analyse

IT-Schadens-szenarien

RTO-Kritikalitätsklasse	Umsetzungsoptionen
4 (>0–4h)	**AKTIV – AKTIV** **AKTIV – PASSIV** (HOT-Standby)
3 (>4–24h)	**AKTIV – PASSIV** (HOT-Standby) **AKTIV – PASSIV** (WARM-Standby)
2 (>24–120h)	**AKTIV – PASSIV** (COLD-Standby)
1 (>120–240h)	**SINGLE AKTIV** (Bereitstellung zusätzlicher Hardware durch Provider in garantierter Zeit)

Angeforderter RPO	Umsetzungsoptionen
>0–4h	• Synchrone Replikation • Fast Restore (HOT-Standby)
>4–24h	• Snapshot Sicherungen • Asynchrone Datenhaltung
>24h	• Backup oder Neu-Installation

SLA Provider

exemplarisch

Platin

Gold

Silber

Bronze

Backup-Optionen

Der IT-Kontinuitätsstandard muss beim Design neuer oder der Anpassung bestehender IT-Services durch die IT-Service Verantwortlichen, Solution Designer und IT-Dienstleister berücksichtigt werden!

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.7. IT-Notfalltests

IT-Notfalltestsstufen und Abdeckung für Schadensszenarien

IT-Notfalltestsstufe	Rechenzentrums-ausfall	Datenkorruption	Ausfall kritischer IT-Service	Logische Fehler	Sicherheitsvorfall
Schreibtischtest	Schreibtischtest – „Was passiert wenn…“				
Einzeltest	Schwenktest	Backup & Restore	Schwenk / Restore	Backup & Restore	Isolation / Forensik
Blocktest	Rechenzentrum Schwenktest		Simulation Komponentenausfall		Security Incident Response Testing
Umfassender Test	Black Building Test				

Zentral koordiniert

Dezentral koordiniert

Erläuterungen zu den IT-Notfalltests

- *IT-Notfalltestsstufen unterscheiden sich in Komplexität, Aufwand und notwendigem Budget*
- *IT-Notfalltests werden **zentral** durch ITSCM oder **dezentral** durch die jeweiligen IT-Service Verantwortlichen gesteuert*
  - *Ermöglicht flexible Anpassung an Release-Pläne von IT-Services*
- *IT-Dienstleister beteiligen sich an den IT-Notfalltests und testen eigenverantwortete IT-Services selbstständig*
- *Test Periode für IT-Services in Abhängigkeit zur ITSCM-Kritikalitätsklasse (KK) festgelegt:*
  - *KK 3&4: Jährlich,*
  - *KK 1&2: Zwei-Jährlich.*
- *Sowohl zentrale als auch dezentrale Tests werden zentral dokumentiert*

Alle IT-Notfalltests werden in einem Mehrjahrestestplan konsolidiert und deren Wirksamkeit sollte durch eine zentrale Dokumentation der IT-Notfalltestergebnisse sichergestellt werden.

Hochschule Niederrhein
University of Applied Sciences

9.7. IT-Notfallübungen

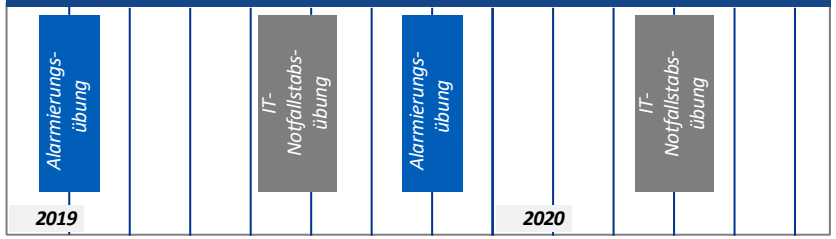
Verschiedene Übungsarten

- ***Alarmierungsübung:*** *Die Alarmierungskette wird entlang der beteiligten Organisationsbereiche für einen IT-Notfall geübt.*
- ***IT-Notfallstabsübung:*** *Der IT-Notfallstab und IT-Notfallteams trainieren an einem fiktiven IT-Notfall (verschiedene Schadensszenarien) ihre Reaktionen und die vorgegebenen Abläufe der IT-Notfallbewältigung.*

Übungszyklen

- *Alarmierungs- und IT-Notfallstabsübungen sollten jährlich stattfinden*
- *Unangekündigte Alarmierungsübungen sollten in unregelmäßigen Abständen stattfinden*

Konsolidierung in mehrjährigem IT-Notfallübungsplan



IT-Notfallübungen nach Plan durchführen

Durch die IT-Notfallübungen wird die Eignung und Funktionsfähigkeit der IT-Notfallorganisation (u.a. unter Einbindung von IT-Dienstleistern) in den existierenden Schadensszenarien überprüft und demonstriert.

9.7. Kommunikation, Awareness und Training (KAT)

Was ist KAT?

- Kommunikation:
  - Bekanntgabe und Auftritt des ITSCM: W-Fragen
- Awareness:
  - Vergleich IT-Sicherheit: Change your Password Day
- Training:
  - Schulung der Mitarbeitern in ihren zugewiesenen Rollen und somit Befähigung

Warum ist KAT so wichtig?

- ITSCM kennenlernen - Bewusstsein schärfen
- Prozesse, Intention und Hintergründe verstehen: „Warum muss ich einen Wiederanlaufplan schreiben?“
- Sensibel auf pot. Ausfälle reagieren und nicht wegschauen
- Aktiv an der Verbesserung mitarbeiten

Inhalte KAT

- Was ist ITSCM und welche Ziele verfolgt es
- Inhalte der Policy und der Regelwerke
- Aufgaben und Pflichten in der 1st bzw. 2nd LoD
- Sensibilisierung für IT-Notfallvorsorge und -bewältigung
- Was ist eine IT-Störung, ein (potentieller) IT-Notfall?
- Tiefgehende Inhalte des ITSCM

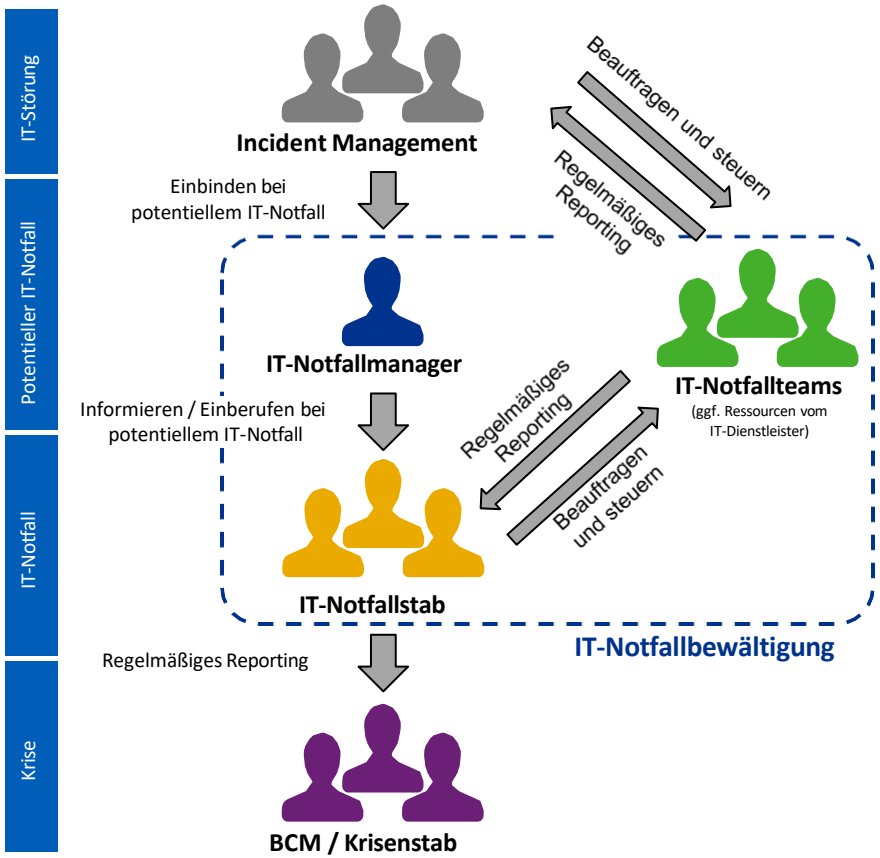
Erläuterungen

- Unternehmensweites Verständnis über das ITSCM schaffen
- Zielgruppenorientierte Befähigung der Rollen in der IT-Notfallvorsorge und IT-Notfallbewältigung
  - Zielgruppenorientierte Trainings
- Jährliches ITSCM-Awareness Programm, das zielgruppenrelevant für alle Mitarbeiter vermittelt wird
- Trainings für 2nd LoD (BCM), für IT-verantwortende Einheiten über IT-Notfallvorsorge und IT-Notfallbewältigung

Kommunikation, Awareness und Training unterstützen die Befähigung der Mitarbeiter zur Etablierung einer IT- Notfallvorsorge sowie Schaffung der notwendigen Sensibilisierung in Unternehmen.

9.7. IT-Notfallbewältigung

Übersicht IT-Notfallbewältigung



Erläuterungen zur IT-Notfallbewältigung

Im Zentrum der IT-Notfallbewältigung steht das Ausführen der IT-Notfall- und IT-Wiederanlaufpläne durch die IT-Notfallteams. Der IT-Notfallstab koordiniert und steuert die IT-Notfallteams bei diesen Aktivitäten.

Kriterien für die Einbindung des IT-Notfallmanagers

- Gesonderte Notfallorganisation bringt Mehrwert
- Wiederanlauf innerhalb der vorgeschriebenen Störungsbearbeitungsfrist kann nicht zugesichert werden
- Ein Datenverlust liegt vor und ein früherer Datenstand muss wiederhergestellt werden
- Es ist absehbar, dass ein kritischer IT-Service nicht aufrecht erhalten werden kann

Mitglieder des IT-Notfallstabs

- Leiter IT-Notfallstab
- IT-Notfallmanager
- Vertreter aus dem Incident Management
- Vertreter von ISM
- Protokollant IT-Notfallstab
- ggf. Vertreter des IT-Dienstleister in beratender Funktion

Abläufe und Kommunikationswege für eine effiziente Bewältigung eines IT-Notfalls müssen definiert sein, sodass sie auch in einer Stresssituation einwandfrei funktionieren.

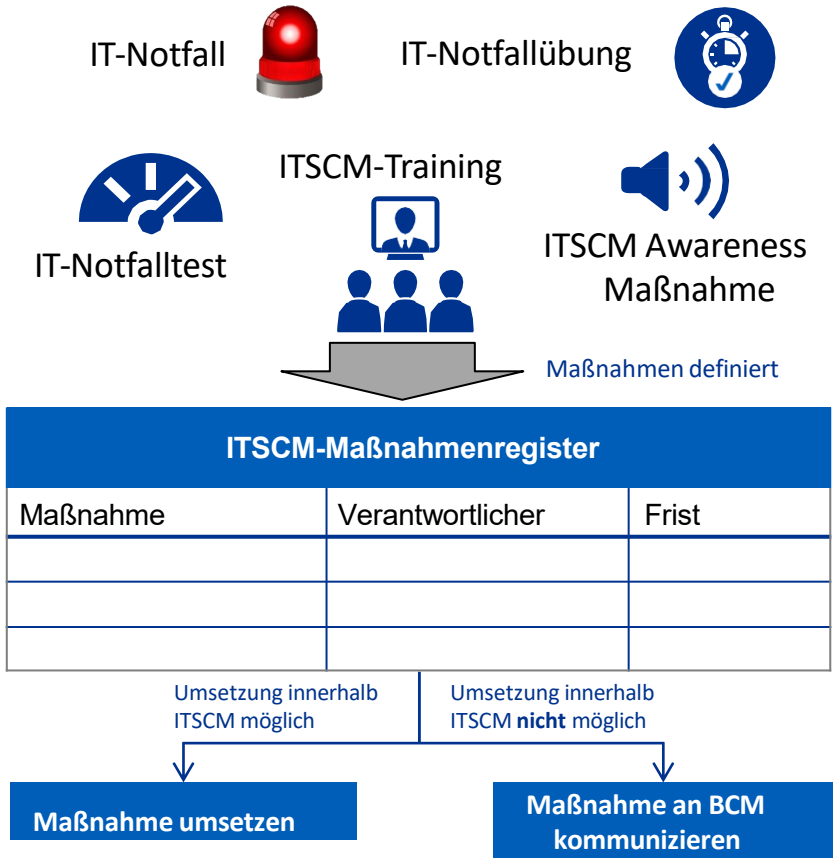
Hochschule Niederrhein
University of Applied Sciences

Übersicht

1. ITSCM-Beispiele aus der Praxis
2. Abgrenzung ITSCM und BCM
3. Managementsystem und ITSCM-Standards
4. ITSCM in der Organisation
5. ITSCM Life Cycle und Zentrale Prozesse
6. Bestandteile der IT-Notfallvorsorge
7. IT-Notfallbewältigung
8. Weitere Bestandteile

9.8. Lessons Learned

Übersicht Lessons Learned



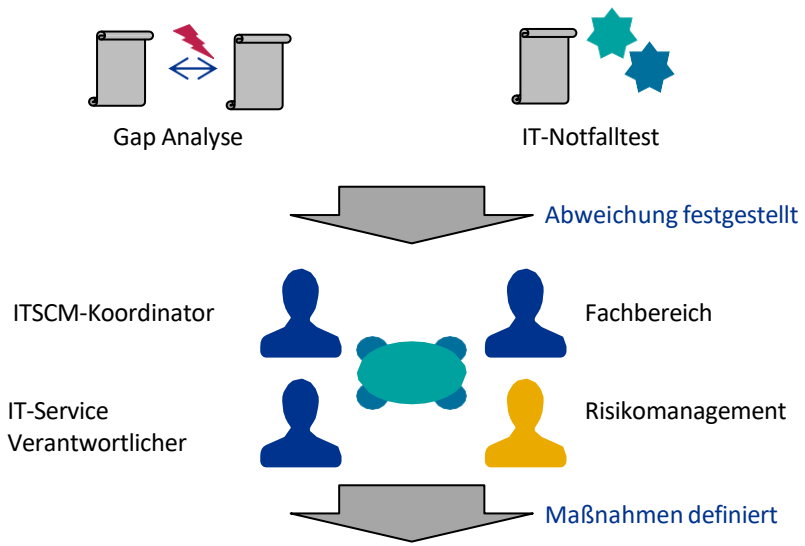
Erläuterungen zu Lessons Learned

- Positive und negative Beobachtungen werden von den an der Durchführung beteiligten Rollen dokumentiert.
- Der ITSCM-Manager pflegt und ergänzt die gesammelten Beiträge aus Lessons Learned in das Register "ITSCM- Lessons Learned".
- Der ITSCM-Manager schlägt mögliche Maßnahmen zur Verbesserung vor. Die vorgeschlagenen Maßnahmen werden in dem "ITSCM-Maßnahmenregister" erfasst.
- Der ITSCM-Manager entscheidet zusammen mit Notfallmanagement IT, ob die Maßnahme innerhalb von ITSCM umgesetzt werden kann. Dies ist nicht der Fall, falls:
  - Die Vorgaben von BCM dies nicht zulassen,
  - Die Maßnahme hat Auswirkungen außerhalb des Gültigkeitsbereichs von ITSCM,
  - Die Kompetenzen des ITSCM-Managers überschritten werden.
- Falls die Maßnahmen innerhalb von ITSCM umgesetzt werden, adressiert der ITSCM-Manager die notwendigen Maßnahmen (ggf. auch in Abstimmung mit dem IT- Dienstleister) und überwacht deren Umsetzung.

Beobachtungen aus vergangenen ITSCM-Aktivitäten werden dokumentiert und tragen zur kontinuierlichen Verbesserung des IT-Notfallmanagements bei.

9.8. Gap Remediation Process

Übersicht "Inhaltliche Abweichungen beheben"



ITSCM-Maßnahmenregister

Maßnahme	Verantwortlicher	Frist

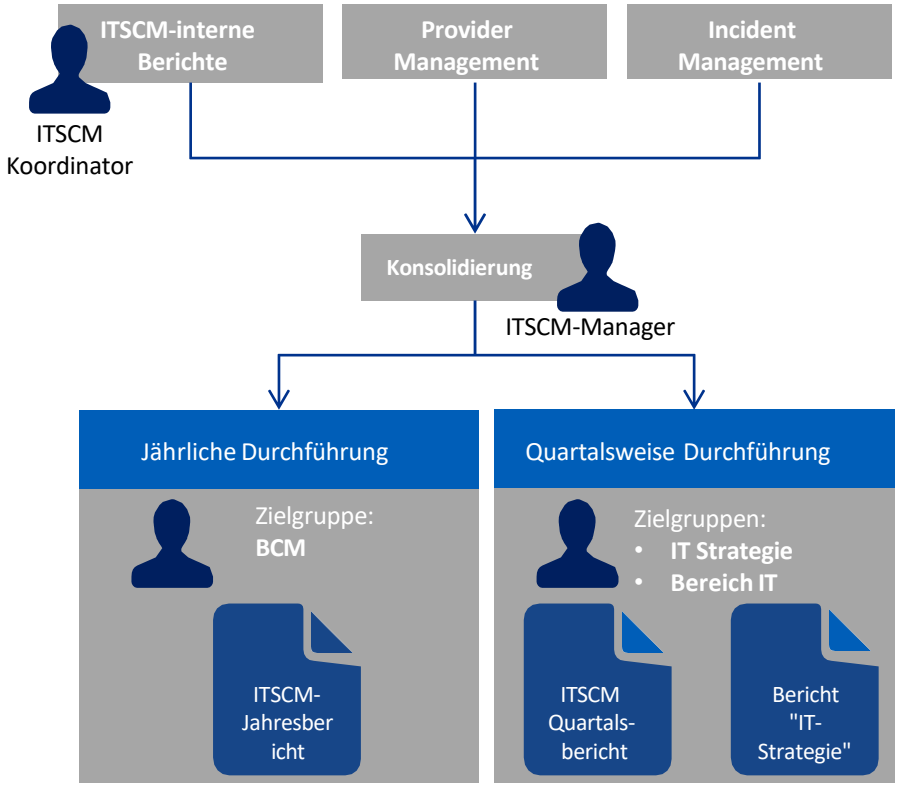
Erläuterungen zum Prozess

- Der ITSCM-Koordinator koordiniert die Abstimmung mit den Fachbereichen und dem betroffenen IT-Service Verantwortlichen. Ziel ist es, die Abweichungen zu diskutieren und eine Entscheidungsgrundlage herbeizuführen.
- Es gibt grundsätzlich drei Lösungsansätze:
  - **Option 1:** Der über die BIA angeforderte RTO/RPO- Wert wird vom Fachbereich nachträglich angepasst,
  - **Option 2:** Der über die IT-Notfallplanung zugesicherte RTO/RPO-Wert wird angepasst,
  - **Option 3:** Es wird entschieden, die Differenz zwischen den Anforderungen des Fachbereichs und der IT-Notfallplanung zu akzeptieren.
- Grundsätzlich sind bei der Entscheidungsfindung die Aspekte **'Risiko'**, **'Kosten'** und **'Machbarkeit'** zu beachten.
- Zur Risikobewertung und -akzeptanz wird die Methodik vom Risikomanagement verwendet. (**Schnittstelle zum Risikomanagement**)
- Maßnahmen zur Schließung der Abweichung werden ins **"ITSCM-Maßnahmenregister"** aufgenommen und deren Umsetzung wird überwacht.

Methoden und Verfahren zur Bearbeitung der über die Gap Analyse oder über IT-Notfalltests identifizierten Abweichungen für IT-Services werden dokumentiert und deren Umsetzung wird überwacht.

9.8. Reporting

Übersicht Reporting



Erläuterungen zum Reporting

- ITSCM sollte in Intervallen über den Status der IT-Notfallvorsorge berichten.
- Der ITSCM-Manager prüft und konsolidiert die monatlichen Berichte. Daraus entstehen Quartalsübersichten.
- ITSCM berichtet über folgende Inhalte:
  - ITSCM-relevante Ereignisse - Major Incidents und (potentielle) IT-Notfälle
  - IT-Notfalltests und IT-Notfallübungen
  - ITSCM-Trainings und Awareness-Programme
  - ITSCM-Kritikalitätsanalyse
  - Maßnahmen für die kontinuierliche Verbesserung und Behebung von Abweichungen
  - Status der extern beauftragten IT-Services
  - Status der IT-Notfallvorsorge
  - Offene Feststellungen, geplante Maßnahmen und Termine
  - Ausblick
  - Weitere definierte KPI`s

Das Reporting dokumentiert den Status des Notfallmanagement IT und ermöglicht verlässliche Aussagen über die Wirksamkeit. Zudem dienen Reports als Unterstützung der kontinuierlichen Verbesserung des Notfallmanagement IT.

Key Takeaways

1. **Rollen kennen:** BCM = Business, ITSCM = Technik
2. **Gaps ernst nehmen:** Business-Anforderung und IT-Fähigkeit müssen passen
3. **Security-Regel**: Bei Cyberangriffen ISMS sofort einbinden.
4. **ITSCM lebt**: Testen, üben, verbessern

Nächste Schritte

Bis zur nächsten Sitzung	
	✓ Fragestunde – Etherpad für Fragen
	✓ Typ-Aufgaben für die Klausur

Thema nächste Woche: Fragestunde

Fragen zur Veranstaltung

Impressum

Prof. Dr. Gael Pentang
Cybersecurity Management
Gael.Pentang@hs-niederrhein.de

BACKUP