Pink Elephant GmbH

Handout

Dokumentenempfehlung

Vorbereitung eines Disaster-Recovery-Konzepts (DR-Konzept)

Inhaltsverzeichnis

1 Einführung

ÜBER PINK DATAMANAGEMENT

Wir, die Pink DataManagement sind Spezialisten für Datenmanagement. Unser Fokus liegt auf Speicherlösungen, Backup- und Archivierungssoftware. Mit lokalen Standorten in Deutschland, den Niederlanden, Belgien, Spanien und Dänemark, betreuen wir Kunden weltweit.

We store, protect and manage your data

Providing our customers with a reliable and cost effective data management solution

Store

Wir analysieren Ihre Situation individuell. Basierend auf Ihren zukünftigen Anforderungen und unter Berücksichtigung Ihrer derzeitigen Speicherumgebung und aktueller Entwicklungen, bieten wir Ihnen die Lösung, die Ihrem Bedarf entspricht. Alle von uns empfohlenen Produkte sind sicher und schnell. Zusätzlich bieten sie unseren Kunden die benötigte Flexibilität für die Storage-Umgebung der Zukunft. Je nach Anforderungsprofil bieten wir zentrale Datenspeicherung als hybrid- oder all-flash, als hyper-converged oder auch als Software-Defined-Storage an. Unsere detaillierte, technische Analyse und unser Fachwissen ermöglichen es uns Sie optimal zu beraten.

Protect

Mit unserer langjährigen Erfahrung und unserem Know-how in allen Aspekten des Datenmanagements entwickeln wir mit Ihnen zusammen Ihr individuelles Datensicherungskonzept – sicher und schnell. Dazu kosteneffizient und unkompliziert durch unseren standardisierten Service Pakete. Die DMP Appliance ist unsere zuverlässige On-Premise Backup Lösung im Gesamtpaket. Eine Kombination der weltweit führenden Datensicherungssoftware – Commvault, mit bewährter Hardware zu einer feinabgestimmten Backup-Lösung. Sie lässt sich in alle bestehenden Umgebungen integrieren, ist gut zu dimensionieren und schnell einsetzbar. Außerdem sind die Datamanagement Professionals gern Ihr zentraler Ansprechpartner für alle dazugehörigen Belange. Mit der DMP Cloud unterstützen wir Sie bei der Auslagerung der Datensicherungen und bieten Ihnen eine sichere Disaster Recovery Site attraktiven Pay-per-Use. Wir bieten Ihnen genau die Flexibilität und Sicherheit die Sie benötigen.

Manage

Wir bieten unseren Kunden erstklassige Dienstleistungen mit umfänglicher Beratung und schnellen Support im Falle von akuten Herausforderungen, bis hin zum kompletten Management der Datensicherungen. Wir finden, das für Sie optimale und zuverlässige Speicher-, Backup- und Archivierungskonzept.

Damit Ihre Daten sicher sind, übernehmen wir gerne die Verantwortung und unterstützen Sie per Remote Management durch unsere Experten. Datenmanagement als Service inklusive aller Lizenzen, Hardware und Dienstleistungen. Unsere Kompetenz und die flexible Kostenkontrolle in Kombination sind unschlagbare Gründe für DMP. Deshalb entwickeln und implementieren wir erfolgreich Datensicherungskonzepte für Kunden weltweit.

1.1 Begriffserläuterung

Generell

BCM (Business Continuity Management):
Prozess zur Sicherstellung der Geschäftskontinuität im Falle von Störungen oder Katastrophen. **Verweis:** Es basiert auf einem strukturierten **BCMS**, das wiederum den **BIA**-Prozess nutzt, um geschäftskritische Ressourcen zu identifizieren.

BCMS (Business Continuity Management System):
Ein Rahmenwerk zur Implementierung von **BCM**, das sicherstellt, dass Maßnahmen zur Minimierung von Risiken und zur Wiederherstellung kritischer Geschäftsprozesse etabliert werden. **Verweis:** BCMS beinhaltet die Erstellung eines **DR-Plans**, die Durchführung von **DR-Tests** und die kontinuierliche Verbesserung durch Audits (Kapitel 5).

BCM-Policy:
Eine Richtlinie, die die Strategie für das **BCM** festlegt und sicherstellt, dass alle Mitarbeitenden informiert und geschult sind. **Verweis:** Unterstützt die **BIA** und definiert Vorgaben für **DR-Pläne** (Kapitel 5).

BCMS-Leitlinie:
Eine dokumentierte Richtlinie, die den Rahmen für das Business Continuity Management in einer Organisation definiert. Sie legt Ziele, Verantwortlichkeiten und Anforderungen für das **BCMS** fest. **Verweis:** Die Leitlinie dient als Grundlage für die Umsetzung von BCM-Maßnahmen (Kapitel 2).

BCMS-Geltungsbereich:
Das Dokument, das den Anwendungsbereich und die Gültigkeit des **BCMS** innerhalb einer Organisation definiert. Es beschreibt die geschützten Prozesse, Standorte und Ressourcen (Kapitel 3).

BIA (Business Impact Analysis):
Ein Prozess zur Bewertung der Auswirkungen von Betriebsstörungen auf die Geschäftsprozesse. **Verweis:** Wird verwendet, um **kritische Ressourcen** zu identifizieren und die Prioritäten im **DR-Plan** festzulegen, basierend auf **RTO** und **RPO** (Kapitel 3).

BIA-Fragebogen:
Eine Methode zur Erhebung von Informationen über Geschäftsprozesse, deren Kritikalität und Abhängigkeiten. **Verweis:** Der Fragebogen dient als Grundlage für die **BIA** und fließt in den **DR-Plan** ein (Kapitel 5).

BCB (Business Continuity Beauftragter):
Die Person, die für die Koordination des **BCM**-Programms verantwortlich ist. **Verweis:** Der BCB ist verantwortlich für die Entwicklung, Überwachung und Umsetzung der BCM-Maßnahmen in einer Organisation (Kapitel 4).

BPM (Business Process Management):
Ein Ansatz zur Analyse und Optimierung von Geschäftsprozessen, um Effizienz und Effektivität zu steigern. **Verweis:** BPM unterstützt die Entwicklung und Pflege von **DR-Plänen**, indem Prozesse analysiert und optimiert werden (Kapitel 5).

BPMN (Business Process Model and Notation):
Ein Standard zur grafischen Darstellung von Geschäftsprozessen in Form von Flussdiagrammen. **Verweis:** **BPMN** wird verwendet, um die Abläufe im **DR-Plan** und **Wiederanlaufplänen** zu visualisieren, um die Nachvollziehbarkeit und Klarheit der Prozesse zu gewährleisten (Kapitel 5).

Disaster Recovery (DR):
Ein Plan zur Wiederherstellung von IT-Systemen und kritischen Prozessen nach einem Vorfall. **Verweis:** DR ist ein Bestandteil des **BCM** und hängt eng mit den definierten **RTO** und **RPO** zusammen. Die Effektivität des **DR-Plans** wird durch regelmäßige **DR-Tests** überprüft (Kapitel 4).

DR-Plan:
Ein detaillierter Plan, der beschreibt, wie kritische Geschäftsprozesse und IT-Systeme nach einem Vorfall wiederhergestellt werden. **Verweis:** Der Plan wird basierend auf der **BIA** erstellt und berücksichtigt **Wiederanlaufpläne** und **Kommunikationspläne** (Kapitel 4).

DR-Planvorlagen:
Vorgefertigte Vorlagen zur Erstellung eines **DR-Plans**, um Standardisierungen zu gewährleisten. **Verweis:** Diese Vorlagen werden basierend auf den **BIA**-Ergebnissen und Best Practices erstellt (Kapitel 6.7).

DR-Konzept:
Das umfassende Konzept zur Wiederherstellung der Geschäftskontinuität nach einem Katastrophenfall. **Verweis:** Es beinhaltet den **DR-Plan**, die **BIA** und die regelmäßigen **DR-Tests** (Kapitel 6.2).

DR-Tests:
Regelmäßige Tests, um die Wirksamkeit des **DR-Plans** zu überprüfen. **Verweis:** Diese Tests stellen sicher, dass die festgelegten **RTO** und **RPO** erreicht werden können (Kapitel 4.1).

DR-Workbook:
Ein Handbuch, das als Leitfaden zur Erstellung und Verwaltung eines **DR-Plans** dient. **Verweis:** Es enthält auch Vorlagen für **Wiederanlaufpläne** und **DR-Tests** (Kapitel 6.7).

GFP (Geschäftsfortführungsplan):
Ein Plan zur Sicherstellung der Fortführung der Geschäftstätigkeiten während oder nach einem Notfall. **Verweis:** Wird als Teil der BCM-Dokumentation erstellt und basiert auf den Ergebnissen der **BIA** (Kapitel 4).

WAP (Wiederanlaufplan):
Ein Plan zur Wiederherstellung der kritischen IT-Systeme und Infrastruktur nach einem Ausfall oder Vorfall. **Verweis:** Der WAP ist ein Bestandteil des **DR-Plans** und wird durch regelmäßige **DR-Tests** validiert (Kapitel 4.3).

Krisenmanagementplan:
Ein Plan, der die Maßnahmen und Abläufe während einer Krise festlegt. **Verweis:** Eng verknüpft mit dem **DR-Plan** und dem **Kommunikationsplan**, um eine schnelle Wiederherstellung sicherzustellen (Kapitel 4.4).

Kommunikationsplan:
Ein Plan, der die Kommunikationswege im Katastrophenfall festlegt. **Verweis:** Dieser Plan ist Bestandteil des **Krisenmanagementplans** und beschreibt interne und externe Kommunikationsmaßnahmen (Kapitel 4.2).

RTO (Recovery Time Objective):
Die maximale Zeitspanne, die nach einem Ausfall verstreichen darf, bevor ein System wieder betriebsbereit ist. **Verweis:** Wird in der **BIA** festgelegt und im **DR-Plan** umgesetzt (Kapitel 3.3).

RPO (Recovery Point Objective):
Das maximal tolerierbare Datenverlustfenster. **Verweis:** Im Rahmen der **BIA** und des **DR-Plans** wird die maximale Zeit für die Wiederherstellung von Daten festgelegt (Kapitel 3.3).

SLA (Service Level Agreement):
Vertragliche Vereinbarung über Serviceverfügbarkeiten und -leistungen zwischen Anbieter und Kunde. **Verweis:** Relevant für die Implementierung und Kontrolle der im **DR-Plan** definierten **RTO** und **RPO** (Kapitel 3.4).

Pink Elephant-spezifisch

(Data Management as a Service):
Eine Cloud-basierte Datenmanagementlösung von Pink Elephant, die Backup, Archivierung und Disaster-Recovery-Dienste umfasst. Verweis: -Dienste werden in Verbindung mit DR-Plänen verwendet, um eine flexible Datenwiederherstellung zu gewährleisten (Kapitel 8.1).

DR:
Der Disaster-Recovery-Dienst von Pink Elephant innerhalb der -Plattform. Verweis: Unterstützt die Umsetzung von DR-Plänen durch die Bereitstellung von Wiederherstellungsoptionen (Kapitel 8.2).

CloudDrive:
Ein Cloud-Speicher innerhalb der -Plattform zur Speicherung von Backups. Verweis: Kann als Teil des DR-Konzepts verwendet werden, um Offsite-Backups zu speichern und eine schnelle Wiederherstellung zu ermöglichen (Kapitel 8.3).

HybridCloud:
Eine hybride Lösung von Pink Elephant, die lokale und Cloud-Ressourcen für Backup und Disaster-Recovery kombiniert. Verweis: Bietet flexible Optionen im DR-Konzept, insbesondere für die Nutzung lokaler und Cloud-basierter Infrastrukturen (Kapitel 8.4).

DR Platinum:
Das höchste Servicepaket im DR-Portfolio, das maximale Sicherheit und minimale Wiederherstellungszeiten bietet. Verweis: Dieses Paket unterstützt kritische Systeme mit den kürzesten RTO und RPO (Kapitel 8.5).

DR Gold:
Ein erweitertes Servicepaket im DR-Angebot. Verweis: Bietet eine höhere Leistung als DR Silver, mit kürzeren RTO und besseren RPO (Kapitel 8.6).

Silver:
Das Basispaket im DR-Portfolio, das grundlegende Wiederherstellungsdienste für weniger kritische Systeme bietet. Verweis: Höhere RTO und RPO als bei den höheren Servicepaketen (Kapitel 8.7).

2 Pink Elephant - Vorbereitung eines Disaster-Wiederherstellungskonzepts

Projektangebot: Vorbereitung eines Disaster-Wiederherstellungskonzepts

1. Anforderungsanalyse

Erfassung von Anlagendaten (kostenlose Pre-Sales-Beratung)

- Erfassung vorläufiger Anlagendaten aus den vorhandenen Dateien.
  Verwendete Dateien:
  - xKundeAssetInfoFile{1..x}
  - Die Anlagendaten umfassen Hardware, Speicher und Anwendungsdetails, die für die Bewertung der DR-Anforderungen erforderlich sind.
    Erwartetes Ergebnis:
  - Gesammeltes Datenset der aktuellen Anlagen für die Einbeziehung in die DR-Planung.
    --> Weitere Anlagendaten erforderlich.

Erfassung von Prozessdokumentationen (kostenlose Pre-Sales-Beratung)

- Überprüfung der aktuellen Dokumentation zur Disaster-Wiederherstellung des Kunden, um das bestehende Setup zu verstehen. **Verwendete Dateien:**
  - xKundeProzessInfoFile{1..x}
- Erfassung aller fehlenden und unvollständigen Abschnitte, die zur Einhaltung der DR-Protokolle erforderlich sind.
  Erwartetes Ergebnis:
  - Erstes Verständnis der Sicherungs- und Wiederherstellungs-SLAs sowie der fehlenden Dokumentationslücken.
    --> Einige Dokumentationen sind noch unzureichend.

2. Entwicklung des Disaster-Wiederherstellungskonzepts (kostenpflichtige Beratung)

Dokumentations- und Anforderungslücken

- **Beratungskosten: 10 Stunden**
- Zusammenarbeit mit dem Kunden, um die Lücken im DR-Konzept zu schließen, durch Erstellung fehlender Dokumente.
  - Verwendung der Richtlinien aus dem [DR Workbook-DE_de.pdf] zur Sammlung von Personal- und Anlagedaten.
  - Bewertung der benötigten Ressourcen im DHC (Hybrid-Cloud) und DCD (CloudDrive).
  - Strukturierung des Konzepts anhand der besten Praktiken aus [CON_3_Datensicherungskonzept_Edition_2021.pdf].

Verwendete Dateien:

- [Standard_200-4_Vorlage_Wiederanlaufplan.docx] für DR-Planvorlagen.

Ergebnisse:

- Vorläufiger DR-Planentwurf (BPMN für Prozesse).
- Identifizierung und Dokumentation von Bedrohungen und erforderlichen Ressourcen.

3. Implementierung des Backup-Kopientransports und Schulung des Personals (kostenpflichtige Beratung)

Entwurf & Implementierung des Backup-Kopientransportsystems

- **Beratungskosten: 15 Stunden**
- Implementierung eines Transportsystems für eine zusätzliche Sicherungskopie mithilfe von:
    - Cloud Repository (S3-Bucket mit Pink Elephant CloudDrive).
    - Hybridlösung für die Speicherung, teilweise unveränderlich für DR-kritische Daten.
    - Bewertung von Tools wie
        - Rubrik Secure Vault
        - Zerto
        - NetApp SnapMirror
        - Veeam Cloud Connect

Ergebnisse:

- DR-relevante Sicherungsdaten werden durch zusätzliche Kopien außerhalb des Standorts gesichert.
- Schulung des Personals zur Verwaltung von Sicherungssystemen und Durchführung von DR-Protokollen.

4. Implementierung der Disaster-Wiederherstellungsumgebung

Entwurf und Einrichtung der Infrastruktur

- **Beratungskosten: 20 Stunden**
- Definition der notwendigen Infrastruktur für die DR:
    - Bewertung der Anforderungen an CPU, RAM und Compute-Ressourcen anhand der gesammelten Anlagendaten.
    - Implementierung der Wiederherstellungsinfrastruktur basierend auf den Pink Elephant DataCenter Services (DCS) und Recovery Infrastructure (DPS).

Pre-Sales (kostenlose Beratung)

- Schätzung der Infrastrukturbedarfe basierend auf den Berechnungen der DR-Last, Kunden-Workloads und Cloud-Speicheranforderungen.

Ergebnisse:

Vollständige Disaster-Wiederherstellungsumgebung entworfen, einschließlich Integration von Pink Elephant Cloud-Services (DR Silver/Gold/Platinum)

5. Testen und Support (optional – nicht im Preis enthalten. Wird im Nachgang im Rahmen eines POC`s berechnet)

Disaster-Wiederherstellungstest

- **Beratungskosten: 10 Stunden**
- Durchführung eines vollständigen DR-Tests basierend auf der entworfenen Umgebung.
    - Implementierung von Empfehlungen aus dem DR Workbook für die Durchführung des DR-Tests.
    - Dokumentation aller Ergebnisse und Anpassung der DR-Verfahren.

Remote Managed Services (optional)

- Laufender Support für die DR-Lösung, um sicherzustellen, dass das System kontinuierlich aktualisiert und getestet wird.

Gesamtberatungsstunden: ~45 Stunden
Pre-Sales (kostenlos): 5 Stunden für erste Beratung und Bewertung.
Gesamtstunden: ca. 30h ohne Testen und Support

3 Zwei-Stunden-Meeting zur DR-Plan-Erstellung

1. **Begrüßung und Zielsetzung des Meetings** (15 Minuten)
   - Vorstellung der Teilnehmer
   - Ziel des Meetings: Klärung der nächsten Schritte zur Umsetzung des Disaster Recovery (DR)-Plans und zur Erstellung des Wiederanlaufplans auf Basis des DR-Workbooks und relevanter Dokumente.
2. **Überblick über das DR Workbook und relevante Dokumente** (30 Minuten)
   - **Einführung in das DR-Workbook** (5 Minuten)
     - Erläuterung des Workbooks als Grundlage für den DR-Prozess und die Wiederherstellung
     - Schlüsselkomponenten des DR-Plans aus dem Workbook (Geschäftsanforderungen, DR-Test, RTO/RPO)
   - **Vorstellung der allgemeinen Dokumentation** (15 Minuten)
     - Überblick über die beigefügten Dokumente wie den Anforderungskatalog und das Wiederanlaufplan-Dokument
     - Bedeutung der technischen und organisatorischen Voraussetzungen im Wiederanlaufplan
   - **Klärung der Verantwortlichkeiten des Kunden** (10 Minuten)
     - Welche Informationen und Dokumente müssen vom Kunden bereitgestellt werden?
     - Klärung des Aktivierungsprozesses und der beteiligten Ansprechpartner (Technik und Organisation)
3. **Anforderungsanalyse für den Wiederanlaufplan** (40 Minuten)
   - **Technische Voraussetzungen** (20 Minuten)
     - Prüfung der aktuellen IT-Umgebung des Kunden und Klärung, welche Ressourcen gesichert und wiederhergestellt werden müssen (basierend auf dem Anforderungskatalog)
     - Bestimmung der Kernressourcen und deren Anforderungen (Server, Datenbanken, Netzwerkinfrastruktur)
   - **Organisatorische Voraussetzungen** (10 Minuten)
     - Definition der organisatorischen Ansprechpartner und Eskalationsprozesse
     - Klärung der notwendigen internen und externen Kontakte sowie der relevanten Dokumentationen
   - **Risikoanalyse und Planungsdetails** (10 Minuten)
     - Einschätzung potenzieller Risiken und Klärung der Prioritäten im Katastrophenfall (Platinum, Gold, Silber Anwendungen)
     - Priorisierung von Maßnahmen basierend auf den RTO/RPO-Vorgaben des Kunden

4. Klärung der nächsten Schritte und Aufgabenverteilung (20 Minuten)

- Zusammenfassung der besprochenen Punkte
    - Festlegung der nächsten Schritte zur Erstellung und Implementierung des Wiederanlaufplans
    - Aufgaben des Kunden zur Bereitstellung von Informationen und Ressourcen
- Zeitplan und weitere Kommunikation
    - Klärung des Zeitplans für die Implementierung
    - Vereinbarung regelmäßiger Checkpoints und Kommunikation

5. Offene Fragen und Abschluss (15 Minuten)

- Beantwortung offener Fragen des Kunden
- Vereinbarung der nächsten Meetings oder Follow-up-Kommunikation

4 Projektphasen

1. Initialisierung des Projekts

- **Ziele**:
  - Klärung der Anforderungen gemäß BSI.
  - Erstellung eines detaillierten Umsetzungsplans.
  - Sicherstellung der Leitungseinbindung und Festlegung der Verantwortlichkeiten.
- **Aktivitäten**:
  - Projektteam aufstellen (inklusive BCB, Führungskräfte, IT, externe Berater).
  - Projektziele und Rahmenbedingungen definieren.
  - Erstellung der BCMS-Leitlinie und deren Freigabe durch die Institutionsleitung.
- **Deliverables**:
  - Projektauftrag und Projektteam.
  - Initiale BCMS-Leitlinie.
- **Zeitplan**: 2 Wochen.

2. Anforderungen identifizieren und analysieren

- **Ziele**:
  - Ermittlung der relevanten Interessengruppen und deren Anforderungen.
  - Erfassung der internen und externen Einflussfaktoren auf das BCMS.
- **Aktivitäten**:
  - Stakeholderanalyse durchführen.
  - BIA (Business Impact Analysis) durchführen.
  - Dokumentation der Anforderungen von Stakeholdern.
- **Deliverables**:
  - Stakeholderanalyse und Anforderungen.
  - BIA-Bericht.
- **Zeitplan**: 4 Wochen.

3. BCMS-Geltungsbereich festlegen

- Ziele:
    - Festlegung des Geltungsbereichs und der zu schützenden Prozesse.
- Aktivitäten:
    - Festlegung des BCMS-Geltungsbereichs unter Berücksichtigung der BSI-Anforderungen.
    - Abstimmung der BCMS-Ziele mit den strategischen Zielen der Institution.
- Deliverables:
    - Dokumentation des BCMS-Geltungsbereichs.
- Zeitplan: 2 Wochen.

4. Erstellung der BCMS-Dokumentation

- Ziele:
    - Erstellung der vollständigen BCMS-Dokumentation, inklusive Leitlinien, Handbüchern, Plänen und Kommunikationsstrategien.
- Aktivitäten:
    - Erstellung der BCMS-Leitlinie.
    - Ausarbeitung des Notfallhandbuchs und der Wiederanlaufpläne.
    - Erstellung der Geschäftsfortführungspläne (GFP) und Wiederanlaufplanung (WAP).
    - Definition der Eskalationsstufen und Alarmierungsprozesse.
- Deliverables:
    - BCMS-Leitlinie.
    - Notfallhandbuch.
    - GFP und WAP.
    - Eskalations- und Alarmierungspläne.
- Zeitplan: 6 Wochen.

5. Umsetzung der BC-Strategien

- **Ziele**:
    - Implementierung der dokumentierten Strategien und Maßnahmen zur Sicherstellung der Geschäftsfortführung.
- **Aktivitäten**:
    - Ressourcenplanung für Notfall- und Wiederanlaufprozesse.
    - Technische und organisatorische Maßnahmen umsetzen.
    - Einrichtung von Notfallkommunikation und Eskalationsverfahren.
- **Deliverables**:
    - Umsetzungspläne für BC-Strategien.
    - Einrichtung der Kommunikationsinfrastruktur.
- **Zeitplan**: 8 Wochen.

6. Training und Sensibilisierung

- **Ziele**:
    - Sicherstellung, dass alle Mitarbeitenden über das BCMS informiert sind und im Notfall adäquat reagieren können.
- **Aktivitäten**:
    - Durchführung von Schulungen und Sensibilisierungsmaßnahmen für alle Mitarbeitenden.
    - Übungen und Notfalltests planen und durchführen.
- **Deliverables**:
    - Schulungsunterlagen.
    - Übungsberichte.
- **Zeitplan**: 4 Wochen.

7. Kontinuierliche Überwachung und Verbesserung

- Ziele:
    - Sicherstellung der fortlaufenden Eignung, Angemessenheit und Wirksamkeit des BCMS.
- Aktivitäten:
    - Implementierung des PDCA-Zyklus (Plan, Do, Check, Act).
    - Regelmäßige Audits, interne Revisionen und Überprüfungen durchführen.
    - Managementbewertung und Anpassung der Leitlinie bei Bedarf.
- Deliverables:
    - Auditberichte und Revisionsberichte.
    - Aktualisierte BCMS-Leitlinie.
- Zeitplan: Fortlaufend (jährlich und nach Bedarf).

Ressourcen und Verantwortlichkeiten:

- **Projektleitung**: BCB (Business Continuity Beauftragte/r).
- **Institutionsleitung**: Überwachung und Freigabe aller Maßnahmen.
- **IT-Teams**: Unterstützung bei technischen Implementierungen.
- **HR und Kommunikation**: Schulungen und Sensibilisierungsmaßnahmen.
- **Externe Berater**: Unterstützung bei Audits und spezifischen Anforderungen.

Meilensteine (grobe Wochenangaben):

1. Projektinitialisierung abgeschlossen (Woche 2).
2. Geltungsbereich des BCMS festgelegt (Woche 6).
3. BCMS-Dokumentation fertiggestellt (Woche 12).
4. BC-Strategien umgesetzt (Woche 20).
5. Erste Übung und Schulungen durchgeführt (Woche 24).
6. Erste Managementbewertung abgeschlossen (nach 12 Monaten).

Risiken und Maßnahmen:

- **Mangelnde Mitarbeiterschulung**: Regelmäßige Schulungen einplanen.
- **Unzureichende technische Ressourcen**: Frühzeitige Bedarfsanalyse und Budgetierung.
- **Kommunikationsprobleme im Krisenfall**: Redundante Kommunikationskanäle einrichten.

5 Dokumentenstruktur für das BCMS

Hiermit erhalten Sie eine Empfehlung welche und in welcher Art strukturiert Sie Dokumentation in Ihrem Business Continuity Managemen System (BCMS) – das kann ein Filesystem sein oder ein dediziertes System – vorhalten sollten.

1. **Einführung und Richtlinien**
    - **BCMS-Leitlinie** (z.B. BCM-Policy)
    - **Scope-Dokument** (Festlegung des Geltungsbereichs und der Ziele des BCMS)
    - **Governance-Struktur** (Zuständigkeiten und Verantwortlichkeiten)
    - **Regelwerk zur kontinuierlichen Verbesserung** (Dokumentation der regelmäßigen Überprüfung und Anpassung)
2. **Risikomanagement**
    - **Risikobewertung und -analyse** (Dokumentation aller identifizierten Risiken)
    - **Risk Treatment Plan** (Maßnahmen zur Risikobewältigung und Minimierung)
3. **Business Impact Analysis (BIA)**
    - **BIA-Bericht** (Dokumentation der Auswirkungen von Störungen auf die Geschäftsprozesse)
    - **Kritikalität von Prozessen und Ressourcen** (Priorisierung von Prozessen und Systemen, Definition von RTO und RPO)
4. **Krisenmanagement**
    - **Krisenmanagementplan** (Prozesse und Eskalationsstufen im Krisenfall)
    - **Kommunikationsplan** (Interne und externe Kommunikationswege)
5. **Disaster-Recovery (DR)**
    - **DR-Workbook** (Leitfaden zur Erstellung und Verwaltung des DR-Plans)
    - **Wiederanlaufplan** (Detaillierte Pläne zur Wiederherstellung von IT-Systemen und -Ressourcen)
    - **Technische Handbücher** (Betriebshandbücher für Server, Netzwerkinfrastruktur, Virtualisierungsumgebungen)
    - **Testpläne für DR-Tests** (Testplan für die regelmäßige Durchführung von DR-Tests)
6. **Notfallhandbuch**
    - **Notfallkontaktdaten** (Kontakte interner und externer Stakeholder)
    - **Verfahren zur Notfallbenachrichtigung** (Alarmierungskette)
    - **Notfallmaßnahmen** (Checklisten für Erstmaßnahmen bei verschiedenen Szenarien, z.B. Stromausfall, Cyberangriff)

7. **Dokumentation und Nachbereitung**
    - **Übersicht der durchgeführten Tests und Ergebnisse** (Testprotokolle)
    - **Dokumentation der Lessons Learned** (Erkenntnisse aus Vorfällen und Übungen)
    - **Wartungs- und Aktualisierungspläne** (Zeitpläne für die Aktualisierung der BCMS-Dokumente)
8. **Externe Dokumente**
    - **Vertragliche Vereinbarungen** (SLA mit IT-Dienstleistern, Backup- und Recovery-Vereinbarungen)
    - **Behördliche Anforderungen und gesetzliche Bestimmungen** (ISO 22301, BSI-Standards)

Zu externen Dokumenten geben wir Ihnen Beispiele an die Hand

- BSI-Standard 200-4
    - Anforderungskatalog
    - Vorlage Wiederanlaufplan

6 Dokumentations-Empfehlungen zu Beginn

Bei Start des Projektes sollen nachfolgende Dokumente vorhanden sein – zu diesem Zwecke unterbreiten wir Ihnen ein Angebot, so dass die nicht vorhandenen gemeinsam mit uns im Professional Services Consulting erstellt oder aufbereitet werden können. Dies dient dem Consultant zum Kennenlernen und schafft die Voraussetzungen für die Erstellung eines DR-Konzeptes.

Zu Beginn des Projekts notwendige Dateien

1. Anschreiben an Verantwortliche
2. BCMS-Leitlinie
3. Scope-Dokument und Geltungsbereichsdefinition
4. Risikobewertung (Erste Version der Risikomatrix)
5. BIA-Fragebogen (Zur Erhebung der notwendigen Informationen zu kritischen Prozessen)
6. DR-Workbook (Bereitstellung der Rahmenbedingungen für das DR-Konzept)
7. Anforderungskatalog (Für Ressourcen, Applikationen, Netzwerke)
8. Wiederanlaufplan-Dokument (Erste Version, z.B. *Wiederanlaufplan XYZ*)
9. Organisatorische und technische Anforderungen (Dokument mit klaren Vorgaben zur Infrastruktur)

6.1 Anschreiben an Verantwortliche (Beispiele)

Betreff: Notwendige Schritte zur Implementierung des Disaster-Recovery-Plans (DR-Plan) gemäß DR-Workbook

An:

- IT-Leitung
- Ressourcenzuständige
- Geschäftsleitung (Geschäftsführung)

Sehr geehrte Damen und Herren,

im Rahmen unseres kürzlich durchgeführten Meetings zur Einführung des Disaster-Recovery-Plans (DR-Plan) gemäß dem DR-Workbook, möchten wir Ihnen eine detaillierte Übersicht der MUSS-Anforderungen und die nächsten Schritte im Projektverlauf mitteilen. Ziel ist es, eine robuste und einsatzbereite Disaster-Recovery-Strategie zu entwickeln, die sicherstellt, dass die im Fall einer Katastrophe ihre Kernprozesse schnellstmöglich wieder aufnehmen kann.

Anschreiben an die Geschäftsleitung

Sehr geehrte Geschäftsführung,

wie besprochen, ist die Einrichtung eines Disaster-Recovery-Plans von zentraler Bedeutung, um die Geschäftskontinuität im Falle eines Systemausfalls oder anderer unvorhersehbarer Ereignisse zu gewährleisten. Der DR-Plan basiert auf den im DR-Workbook und in Workshop mit unserem Partner Pink Elephant festgelegten Standards und beinhaltet alle notwendigen Maßnahmen zur Wiederherstellung kritischer Ressourcen.

Die Umsetzung dieses Projekts erfordert die enge Zusammenarbeit der IT-Abteilung sowie klar definierte Verantwortlichkeiten. Die Geschäftsführung wird gebeten, die nötige Unterstützung und Ressourcen bereitzustellen, um das Projekt in den nächsten Wochen/Monaten erfolgreich umzusetzen.

Technischer Teil für die IT-Leitung

Betreff: Nächste Schritte zur Implementierung des DR-Plans gemäß DR-Workbook

Sehr geehrte IT-Leitung,

nach unserem letzten Meeting sind die folgenden MUSS-Anforderungen für die Implementierung des Disaster-Recovery-Plans festgelegt worden. Diese Maßnahmen müssen ergriffen werden, um sicherzustellen, dass der DR-Plan erfolgreich und zeitnah eingeführt wird.

MUSS-Anforderungen für die Umsetzung des DR-Plans

1. **Definition der Geschäftsanforderungen und Prioritäten**
    - Identifizieren Sie die kritischsten Geschäftsprozesse, Anwendungen und Daten, die für die Aufrechterhaltung des Betriebs im Katastrophenfall erforderlich sind.
    - Bestimmen Sie die Reihenfolge, in der die Wiederherstellung der Ressourcen erfolgen soll, basierend auf den RTO- und RPO-Vorgaben.
2. **Umweltbewertung und Analyse**

- Führen Sie eine detaillierte Analyse der aktuellen IT-Umgebung durch, einschließlich Server, Netzwerkinfrastruktur und Speicher.
- Bestimmen Sie die physische und virtuelle Infrastruktur, die für die Wiederherstellung erforderlich ist, und klären Sie, ob Cloud- oder lokale Lösungen bevorzugt werden.

3. Erstellung eines detaillierten Wiederanlaufplans
   - Basierend auf dem Anforderungskatalog und den Ergebnissen des Meetings, muss ein spezifischer Wiederanlaufplan für jede kritische Ressource erstellt werden (siehe beigefügtes Dokument *Wiederanlaufplan XYZ*).
   - Der Plan muss klare Verantwortlichkeiten und Anweisungen für das IT-Team enthalten, um im Katastrophenfall sofort handeln zu können.
4. Technische und organisatorische Voraussetzungen
   - Sicherstellen, dass alle organisatorischen und technischen Voraussetzungen erfüllt sind, um einen reibungslosen Wiederanlauf zu ermöglichen. Dazu gehören:
     - Verfügbarkeit der Stromversorgung und Netzwerkinfrastruktur
     - Bereitstellung von Notfallhandbüchern und entsprechenden Zugriffsrechten für die relevanten IT-Verantwortlichen
     - Sicherstellung der Kommunikationswege zwischen internen und externen Ansprechpartnern
     - Bereitstellung eines Offsite-Backups, das regelmäßig getestet und aktualisiert wird.
5. Planung und Durchführung eines DR-Tests
   - Planen Sie den ersten DR-Test, um sicherzustellen, dass die Wiederanlaufpläne und die Wiederherstellungsprozesse wie erwartet funktionieren.
   - Führen Sie den DR-Test durch und dokumentieren Sie alle Abweichungen oder Verbesserungsmöglichkeiten.
   - Falls erforderlich, passen Sie den Wiederanlaufplan auf Basis der Testergebnisse an und planen Sie einen zweiten Test, um Optimierungen zu bestätigen.

Nächste Schritte

1. Datenbereitstellung durch die XKundeFirmaName
   - Wir wurden gebeten, alle notwendigen Informationen zur Priorisierung der Geschäftsprozesse, Anwendungen und Ressourcen an Pink Elephant zu liefern.
2. Koordinierung der IT-Abteilung
   - Die IT-Abteilung wird mit der Durchführung der Umweltbewertung beginnen und die notwendigen Schritte zur Erstellung des Wiederanlaufplans einleiten.
   - Ein interner Ansprechpartner wird benannt, um die Kommunikation zwischen den Ressourcenzuständigen und externen Dienstleistern zu koordinieren.
3. Zeitplan für die Umsetzung

- Ein detaillierter Zeitplan für die schrittweise Implementierung und den DR-Test wird in der nächsten Woche festgelegt.
- Regelmäßige Fortschrittsberichte werden alle zwei Wochen an die Geschäftsführung und die IT-Leitung übermittelt.

6.2 BCMS-Leitlinie

1. Zweck der Leitlinie

Diese Leitlinie beschreibt den Ansatz der XKundeFirmaName zur Sicherstellung der Geschäftskontinuität im Falle von schwerwiegenden Störungen oder Katastrophen. Ziel ist es, sicherzustellen, dass kritische Geschäftsprozesse auch unter extremen Bedingungen fortgeführt oder schnellstmöglich wiederhergestellt werden können. Das Business Continuity Management System (BCMS) bildet das Rahmenwerk, um Risiken zu minimieren und die Verfügbarkeit von Ressourcen und Dienstleistungen sicherzustellen.

2. Anwendungsbereich

Diese Leitlinie gilt für alle Abteilungen und Bereiche der XKundeFirmaName. Sie umfasst alle kritischen Geschäftsprozesse, IT-Systeme, physische Einrichtungen und personellen Ressourcen, die für den Betrieb notwendig sind. Die Leitlinie deckt die Vorfallsvorsorge, Notfallplanung und Wiederherstellungsmaßnahmen ab.

3. Ziele des BCMS

- Sicherstellung der Geschäftskontinuität und Minimierung von Unterbrechungen im Betrieb.
- Schutz von Mitarbeitern, Kunden, Vermögenswerten und dem Ruf der XKundeFirmaName.
- Wiederherstellung kritischer Geschäftsprozesse und IT-Systeme innerhalb akzeptabler Wiederanlaufzeiten (RTO) und Datenverluste (RPO).
- Sicherstellung der Einhaltung gesetzlicher und regulatorischer Anforderungen, z.B. ISO 22301 oder BSI-Standards.
- Kontinuierliche Verbesserung und Anpassung des BCMS auf Basis von Tests und geänderten Rahmenbedingungen.

4. Grundsätze des BCMS

4.1 Risikomanagement

Ein zentrales Element des BCMS ist das Risikomanagement. Alle potenziellen Risiken, die den Betrieb beeinträchtigen könnten, werden systematisch identifiziert, bewertet und behandelt. Die XKundeFirmaName verpflichtet sich, regelmäßig Risikobewertungen durchzuführen und Maßnahmen zu ergreifen, um die Auswirkungen potenzieller Katastrophen zu mindern.

4.2 Business Impact Analysis (BIA)

Zur Identifizierung der kritischen Geschäftsprozesse wird regelmäßig eine Business Impact Analysis (BIA) durchgeführt. Die BIA hilft, die Auswirkungen von Betriebsstörungen auf die Organisation zu verstehen und priorisiert die Wiederanlauf- und Wiederherstellungsmaßnahmen.

4.3 Kontinuierliche Verbesserung

Das BCMS wird regelmäßig überprüft, getestet und verbessert, um sicherzustellen, dass es den aktuellen Bedürfnissen der Organisation entspricht. Nach jeder Simulation, Test oder tatsächlichen Notfallsituation werden Verbesserungsmöglichkeiten identifiziert und umgesetzt.

4.4 Schulung und Sensibilisierung

Alle Mitarbeiter werden regelmäßig über das BCMS informiert und in ihre Rolle innerhalb des Notfallmanagements eingeführt. Schulungen werden durchgeführt, um sicherzustellen, dass alle Beteiligten ihre Aufgaben im Krisenfall kennen.

5. Verantwortlichkeiten

- **Geschäftsleitung**: Die oberste Verantwortung für das BCMS liegt bei der Geschäftsleitung. Sie stellt sicher, dass die notwendigen Ressourcen zur Verfügung stehen, um das BCMS zu implementieren und aufrechtzuerhalten.
- **BCM-Beauftragter**: Der BCM-Beauftragte ist für die Entwicklung, Implementierung und kontinuierliche Überwachung des BCMS verantwortlich. Er ist der Ansprechpartner für alle Fragen rund um die Geschäftskontinuität.
- **Abteilungsleiter**: Jede Abteilung ist dafür verantwortlich, die für ihren Bereich relevanten Prozesse und Ressourcen zu identifizieren und mit dem BCM-Beauftragten an der Entwicklung und Umsetzung geeigneter Maßnahmen zur Aufrechterhaltung der Geschäftskontinuität zu arbeiten.
- **Mitarbeiter**: Jeder Mitarbeiter trägt die Verantwortung, sich mit den BCMS-Prozessen vertraut zu machen und im Notfall die Anweisungen gemäß den vorliegenden Notfallplänen umzusetzen.

6. Prozesse des BCMS

Das BCMS der XKundeFirmaName umfasst die folgenden Hauptprozesse:

1. **Risikobewertung**: Regelmäßige Bewertung der Risiken, die die Geschäftskontinuität beeinträchtigen könnten.
2. **Business Impact Analysis (BIA)**: Feststellung der geschäftskritischen Prozesse und deren Abhängigkeiten.
3. **Notfallplanung und Prävention**: Entwicklung und Pflege von Notfallplänen, einschließlich Wiederanlauf- und Wiederherstellungsplänen für kritische IT- und Geschäftssysteme.
4. **Durchführung von Tests und Übungen**: Regelmäßige Simulation von Notfallszenarien und Tests der Wiederanlauf- und Wiederherstellungspläne.
5. **Überprüfung und Anpassung**: Regelmäßige Überprüfung der BCMS-Dokumentation und Anpassung an geänderte Bedingungen oder nach Tests und Übungen.

7. Überwachung und Verbesserung

Das BCMS unterliegt einem kontinuierlichen Verbesserungsprozess, der durch regelmäßige interne Audits und Bewertungen sichergestellt wird. Die Ergebnisse der Audits sowie Erkenntnisse aus Tests und realen Notfällen werden genutzt, um das BCMS kontinuierlich anzupassen und zu verbessern.

8. Dokumentation und Berichterstattung

Alle Maßnahmen und Prozesse des BCMS sind in entsprechender Dokumentation festgehalten. Dazu gehören:

- BCMS-Richtlinien und -Leitlinien
- Notfallpläne (einschließlich Wiederanlauf- und Wiederherstellungspläne)
- Ergebnisse der BIA und Risikobewertung
- Testberichte und Lessons Learned

Berichte über die Implementierung und Überwachung des BCMS werden regelmäßig der Geschäftsleitung vorgelegt.

9. Gültigkeit und Überprüfung

Diese Leitlinie tritt ab dem [Datum] in Kraft und wird jährlich sowie nach bedeutenden Änderungen überprüft und bei Bedarf angepasst.

6.3 RASCI-Matrix für die Verantwortlichkeiten

In Anlehnung an die verbreitete Methode Verantwortlichkeiten in einer Matrix darzustellen verwenden wir eine Erweiterung der RACI-Matrix mit Pink Elephant als externem Dienstleister:

RASCI-Matrix für Disaster Recovery Planning

Task	BCB (Business Continuity Beauf-tragter)	BCM-Team	Geschäftsleitung	Fachabteilungen	DMP (Serviceprovider)
BCMS-Leitlinie entwickeln	R	C	A	I	S
BIA durchführen	A	R	C	C	S
DR-Plan erstellen	A	C	I	R	S
Wiederanlaufplan erstellen	C	A	I	R	S
Kommunikations-plan erstellen	C	A	I	R	S
DR-Tests durchführen	C	R	I	C	S
Krisenmanagement-plan erstellen	A	C	R	I	S
Kontinuierlicher Verbesserungspro-zess (KVP)	A	R	A	C	S
RTO und RPO festlegen	C	R	A	C	S
DR-Tests auswerten	C	R	I	I	S
Krise bewältigen	I	A	C	R	S
Rollen und Verant-wortlichkeiten klä-ren	R	C	A	C	S

Hier bedeutet:

- R = Responsible (Verantwortlich)
- A = Accountable (Rechenschaftspflichtig)
- C = Consulted (Beraten)
- I = Informed (Informiert)
- S = Serviceprovider (Dienstleister, in diesem Fall Pink Elephant)

Scope-Dokument und Geltungsbereichsdefinition für das BCMS

1. Zweck des Dokuments

Dieses Dokument definiert den Anwendungsbereich und Geltungsbereich des Business Continuity Management Systems (BCMS) der XKundeFirmaName. Ziel ist es, den Umfang der Aktivitäten, Geschäftsprozesse und Ressourcen festzulegen, die im Rahmen des BCMS geschützt und aufrechterhalten werden sollen.

2. Geltungsbereich des BCMS

Das BCMS der XKundeFirmaName umfasst alle wesentlichen Geschäftsprozesse, IT-Systeme, physischen Standorte sowie personellen und technologischen Ressourcen, die für den Fortbestand der Organisation und die Sicherstellung der Geschäftskontinuität notwendig sind.

2.1 Geschäftsprozesse

Die folgenden Geschäftsprozesse sind als kritisch für den Betrieb der XKundeFirmaName identifiziert und werden im Rahmen des BCMS priorisiert:

1. Finanzwesen und Rechnungswesen
    - Verarbeitung und Schutz sensibler Finanzdaten
    - Sicherstellung der Zahlungsströme und der Liquidität der XKundeFirmaName
    - Schutz und Wiederherstellung der Buchhaltungssoftware und Datenbanken
2. Kunden- und Servicemanagement
    - Sicherstellung der Kundendaten und der Servicetools
    - Aufrechterhaltung der Kommunikation mit Kunden, insbesondere bei Störungen
    - Schutz der CRM-Systeme und Wiederherstellung der Kundenkontaktprozesse
3. IT-Betrieb und Infrastruktur
    - Schutz und Wiederherstellung von Servern, Datenbanken, Netzwerken und Anwendungen
    - Sicherstellung der Verfügbarkeit von Schlüsselanwendungen und IT-Diensten
    - Wiederherstellung des E-Mail- und Kommunikationssystems
4. Human Resources
    - Sicherstellung der Gehaltsabrechnungen und Personaldaten
    - Verfügbarkeit der HR-Management-Systeme und relevanter Datenbanken

2.2 Standorte

Das BCMS deckt alle Standorte der XKundeFirmaName ab, die für den Betrieb und die Unterstützung der kritischen Geschäftsprozesse notwendig sind. Dazu gehören:

1. Hauptsitz (Standortbeschreibung, Adresse)
    - Standort des Managements und der zentralen IT-Infrastruktur
    - Wichtiger Standort für Entscheidungsfindung und Krisenkommunikation
2. Rechenzentrum (Standortbeschreibung, Adresse)
    - Hosting von geschäftskritischen IT-Systemen und Datenbanken
    - Sicherstellung der kontinuierlichen Datenverfügbarkeit und -sicherheit

3. **Zweigstellen/Büros** (Standortbeschreibung, Adressen)
    - Sicherstellung der operativen Kontinuität und Kundenkommunikation
    - Zugriff auf kritische Anwendungen und Kommunikationssysteme

2.3 Ressourcen

Die folgenden Ressourcen werden im Rahmen des BCMS geschützt und aufrechterhalten:

1. **IT-Systeme und Anwendungen**
    - Server, Netzwerke, Datenbanken und Anwendungen, die für den täglichen Betrieb notwendig sind
    - Cloud-Dienste und Remote-Arbeitsplätze, die zur Aufrechterhaltung des Betriebs in Notfallsituationen benötigt werden
2. **Daten und Datensicherungen**
    - Schutz sensibler Daten (z.B. Finanz-, Kunden- und Mitarbeiterdaten)
    - Regelmäßige Backups und Notfallwiederherstellungsmechanismen
3. **Mitarbeiter und deren Rollen im Krisenfall**
    - Sicherstellung der Personalverfügbarkeit für die Fortführung der kritischen Geschäftsprozesse
    - Notfallrollen und Verantwortlichkeiten werden klar definiert und regelmäßig geschult

2.4 Verantwortlichkeiten

Das BCMS umfasst die Zuständigkeiten und Verantwortlichkeiten auf allen Ebenen der Organisation:

- **Geschäftsleitung**: Gesamtverantwortung für die Aufrechterhaltung und Überwachung des BCMS.
- **BCM-Beauftragter**: Verantwortlich für die Entwicklung, Implementierung und laufende Verbesserung des BCMS.
- **Abteilungsleiter**: Zuständig für die Identifizierung und Sicherstellung der geschäftskritischen Prozesse und Ressourcen in ihren Bereichen.
- **Mitarbeiter**: Sind in ihren spezifischen Rollen im Notfallmanagement verantwortlich, die entsprechenden Maßnahmen umzusetzen.

2.5 Externe Stakeholder

Das BCMS der XKundeFirmaName berücksichtigt auch externe Parteien und deren Einfluss auf die Geschäftskontinuität:

1. **Kunden und Geschäftspartner**
    - Sicherstellung der Kommunikation und Dienstleistungskontinuität für wichtige Kunden
    - Minimierung von Unterbrechungen in Lieferketten und Partnerbeziehungen
2. **IT-Dienstleister und externe Anbieter**
    - Absicherung der Service-Level-Vereinbarungen (SLA) für kritische IT-Dienstleistungen

- Einbindung externer Anbieter in die Wiederherstellungs- und Notfallpläne (z.B. Backup- und Replikationsdienste)

2.6 Eingeschränkter Geltungsbereich

Folgende Bereiche und Prozesse sind nicht Bestandteil des BCMS, da sie als nicht kritisch für die Aufrechterhaltung der Geschäftskontinuität identifiziert wurden:

1. Nicht-geschäftskritische Anwendungen
    - Systeme und Prozesse, die keinen wesentlichen Einfluss auf die Geschäftskontinuität haben (z.B. interner E-Mail-Verkehr für allgemeine Kommunikation)
2. Nicht-kritische Standorte
    - Standorte, die nicht unmittelbar für die Fortführung der wichtigsten Geschäftsprozesse notwendig sind (z.B. Archivierungsstandorte)

3. Ziele des BCMS-Geltungsbereichs

Das BCMS der XKundeFirmaName verfolgt die folgenden Ziele:

1. Sicherstellung der Fortführung der kritischen Geschäftsprozesse im Falle einer schwerwiegenden Störung oder Katastrophe.
2. Reduzierung der Auswirkungen von Betriebsunterbrechungen auf die XKundeFirmaName, ihre Mitarbeiter und ihre Kunden.
3. Einhaltung gesetzlicher und regulatorischer Anforderungen (z.B. ISO 22301, BSI-Standards) im Bereich Geschäftskontinuität und Notfallmanagement.
4. Ständige Verbesserung der Wiederherstellungsprozesse durch regelmäßige Tests, Übungen und Audits.

4. Überwachung und Anpassung des Geltungsbereichs

Der Geltungsbereich des BCMS wird regelmäßig überprüft und angepasst, um auf veränderte Rahmenbedingungen zu reagieren. Dies umfasst Änderungen an den Geschäftsprozessen, der IT-Infrastruktur, der Organisationsstruktur und externen Faktoren.

6.4 Risikomatrix für XKundeFirmaName

Hier bieten wir Ihnen eine beispielhafte Risikomatrix an, die wir mit Ihnen weiter ausarbeiten werden

Risiko	Beschreibung	Wahrscheinlichkeit	Auswirkung	Risikostufe	Maßnahmen	Verantwortlich	Frist
1. Stromausfall	Ausfall der Stromversorgung führt zur Unterbrechung des Betriebs	Mittel	Hoch	Hoch	- Notstromaggregat installieren	IT-Leitung	3 Monate
					- Regelmäßige Tests der Notstromversorgung	Facility Management	
					- Verträge mit alternativen Stromanbietern prüfen	Beschaffung	
2. Cyberangriff (Ransomware)	Hacker legen Systeme lahm und erpressen Lösegeld	Niedrig	Sehr hoch	Hoch	- Implementierung von Firewall und Antivirus	IT-Security	1 Monat
					- Schulung der Mitarbeiter zum Thema IT-Sicherheit	Personalabteilung	6 Monate
					- Regelmäßige Backups und deren externe Speicherung	IT-Leitung	
3. Naturkatastrophe (Überschwemmung)	Überflutung des Rechenzentrums führt zu Totalausfall der IT-Infrastruktur	Gering	Sehr hoch	Mittel	- Verlegung des Rechenzentrums in ein höhergelegenes Gebiet	IT-Leitung	12 Monate
					- Regelmäßige Test der DR-Pläne und Notfallübungen	BCM-Beauftragter	
					- Abschluss einer Versicherung gegen Elementarschäden	Finanzabteilung	
4. IT-Systemausfall	Totalausfall von Servern und kritischen Anwendungen	Mittel	Hoch	Hoch	- Redundante Server und Backup-Strategien	IT-Leitung	6 Monate
					- Implementierung eines Disaster-Recovery-Plans	IT-Leitung	
5. Mitarbeiterausfall (Pandemie)	Krankheitswelle führt zu erheblichem Personalausfall	Mittel	Mittel	Mittel	- Einführung flexibler Arbeitsmodelle (Homeoffice)	HR-Abteilung	3 Monate
					- Schulung der Mitarbeiter zur Einhaltung von Hygienemaßnahmen	HR-Abteilung	
					- Einrichtung eines Ersatzteams für kritische Bereiche	Abteilungsleiter	
6. Lieferantenprobleme	Ausfall eines kritischen Lieferanten beeinträchtigt die Produktion	Mittel	Mittel	Mittel	- Diversifizierung der Lieferketten	Einkauf	9 Monate
					- Abschluss langfristiger Verträge mit Alternativlieferanten	Einkauf	
7. Datenschutzverletzung (GDPR)	Verlust oder Missbrauch sensibler Daten führt zu hohen Geldstrafen	Niedrig	Sehr hoch	Hoch	- Einführung und Überwachung von Datenschutzrichtlinien	Datenschutzbeauftragter	2 Monate
					- Regelmäßige Schulungen zu Datenschutzanforderungen	HR-Abteilung	

Erläuterungen:

- Risiko: Kurzbeschreibung des identifizierten Risikos.
- Beschreibung: Ausführlichere Erklärung des potenziellen Szenarios und seiner Auswirkungen.
- Wahrscheinlichkeit: Wahrscheinlichkeit, dass dieses Risiko eintritt (z.B. gering, mittel, hoch).
- Auswirkung: Einschätzung der Auswirkungen auf die Organisation im Falle des Eintritts (z.B. gering, mittel, hoch).
- Risikostufe: Die Kombination von Wahrscheinlichkeit und Auswirkung ergibt eine Risikostufe, die die Dringlichkeit der Maßnahmen bestimmt (z.B. niedrig, mittel, hoch).
- Maßnahmen: Vorschläge zur Risikominderung oder -bewältigung.
- Verantwortlich: Die Person oder Abteilung, die für die Umsetzung der Maßnahmen verantwortlich ist.
- Frist: Zeitraum, bis wann die Maßnahme umgesetzt sein sollte.

6.5 Business Impact Analysis (BIA) Fragebogen für xKundeFirmaName

1. **Allgemeine Informationen**

1. **Abteilung:**
    - Name der Abteilung:
    - Name des Verantwortlichen:
    - Kontaktinformationen:
2. **Geschäftsprozess:**
    - Name des Prozesses:
    - Prozessbeschreibung:
    - Hauptziel des Prozesses:
3. **Wichtige Kennzahlen:**
    - Anzahl der Mitarbeiter im Prozess:
    - Wichtige Systeme, Anwendungen oder Datenbanken:
    - Externe Abhängigkeiten (Lieferanten, Dienstleister etc.):

---

2. **Kritikalität des Prozesses**

1. **Wie wichtig ist dieser Prozess für den Betrieb der xKundeFirmaName?**
    - Kritisch (bei Ausfall drohen große Gefahren für die öffentliche Sicherheit)
    - Hoch (wichtiger Prozess, der aber bei einem kurzfristigen Ausfall keine unmittelbaren Gefahren birgt)
    - Mittel (Ausfall beeinträchtigt den Betrieb, aber keine unmittelbare Gefahr)
    - Niedrig (nicht kritischer Prozess, Ausfall hat kaum Einfluss)
2. **Welche Services sind von diesem Prozess abhängig?**
    - Gasversorgung
    - Wasserversorgung
    - Elektrizitätsversorgung
    - Kundendienst
    - Abrechnung/Billing
    - IT-Services
    - Andere: _____
3. **Welche Kunden oder Bereiche sind direkt betroffen, wenn dieser Prozess ausfällt?**
    - Haushaltskunden

- Gewerbliche Kunden
- Öffentliche Einrichtungen
- Kritische Infrastrukturen (z.B. Krankenhäuser, Feuerwehren)

---

3. Auswirkungen eines Ausfalls

1. **Wie schnell muss der Prozess nach einem Ausfall wiederhergestellt werden?**
   - Sofort (RTO ≤ 1 Stunde)
   - Innerhalb von 4 Stunden (RTO ≤ 4 Stunden)
   - Innerhalb von 24 Stunden (RTO ≤ 24 Stunden)
   - Innerhalb von 72 Stunden (RTO ≤ 72 Stunden)
2. **Welche Auswirkungen hat der Ausfall auf die öffentliche Sicherheit und Gesundheit?**
   - Hohe Gefahr (Gefahr für Leib und Leben)
   - Mittlere Gefahr (Beeinträchtigung der Versorgung, z.B. Gas oder Wasser)
   - Geringe Gefahr (keine unmittelbaren Auswirkungen)
3. **Finanzielle Auswirkungen eines Ausfalls dieses Prozesses:**
   - Sehr hoch (> 500.000 € Verlust pro Tag)
   - Hoch (100.000 € – 500.000 € Verlust pro Tag)
   - Mittel (10.000 € – 100.000 € Verlust pro Tag)
   - Gering (< 10.000 € Verlust pro Tag)
4. **Verlust an Kundenzufriedenheit bei Ausfall des Prozesses:**
   - Hoch (sofortige Beschwerden und Imageverlust)
   - Mittel (Beschwerden nach längerem Ausfall)
   - Gering (kaum Auswirkungen)

---

4. Abhängigkeiten

1. **Von welchen internen IT-Systemen ist dieser Prozess abhängig?**
   - SCADA-System (Steuerung und Überwachung)
   - Abrechnungssysteme
   - Netzüberwachung und -management
   - Kundensysteme (z.B. CRM)
   - Andere: _____
2. **Von welchen externen Diensten ist dieser Prozess abhängig?**

- Lieferanten für Gas, Wasser oder Strom
- Netzbetreiber
- Externe Dienstleister für IT-Services
- Andere: _____

3. **Welche physischen Ressourcen sind für den Betrieb des Prozesses notwendig?**
   - Kraftwerke / Anlagen
   - Rohrleitungen und Leitungsnetze
   - Fahrzeuge und Techniker vor Ort
   - Lagerbestände (z.B. Ersatzteile, Materialien)
   - Andere: _____

---

5. **Notfallpläne und Wiederherstellung**
6. **Gibt es einen Notfallplan für diesen Prozess?**
   - Ja
   - Nein
   - Wenn ja, wo ist der Plan dokumentiert?
7. **Wie wird dieser Prozess im Katastrophenfall aufrechterhalten oder wiederhergestellt?**
   - Manuelle Arbeitsweise möglich (wenn ja, wie lange?)
   - Backup-Systeme vorhanden (welche?)
   - Alternative Standorte nutzbar
   - Andere: _____
8. **Gibt es regelmäßige Tests und Übungen für die Wiederherstellung dieses Prozesses?**
   - Ja, wie oft? _____
   - Nein

---

9. **Verbesserungspotential**

1. **Welche Maßnahmen würden Ihrer Meinung nach die Resilienz dieses Prozesses verbessern?**
   - Bessere IT-Redundanz
   - Zusätzliche Schulungen für Mitarbeiter
   - Externe Dienstleister verstärken
   - Erweiterung der Notfallpläne
   - Andere: _____

2. Welche weiteren Risiken sehen Sie in diesem Prozess?
    -
3. Weitere Kommentare oder Anmerkungen:
    -

---

10. Abschließende Informationen

1. Datum der Erhebung:
    -
2. Name des Ausfüllenden:
    -

6.6 Disaster Recovery Workbook

XKundeFirmaName

Datum: [TT/MM/JJJJ]
Version: 1.0

---

1. Inhaltsverzeichnis

Einführung

1. Geschäftsanforderungen

Für die XKundeFirmaName ist die Sicherstellung der kontinuierlichen Versorgung mit Gas, Wasser und Elektrizität von entscheidender Bedeutung. Ein DR-Plan muss garantieren, dass alle kritischen Geschäftsprozesse auch im Fall von Naturkatastrophen, IT-Ausfällen oder anderen schwerwiegenden Störungen schnellstmöglich wiederhergestellt werden können.

Zu den wichtigsten Geschäftsanforderungen zählen:

- Sicherstellung der ununterbrochenen Versorgung von Haushalts- und Gewerbekunden.
- Einhaltung der regulatorischen Vorgaben und gesetzlichen Anforderungen.
- Verfügbarkeit der Systeme zur Netzüberwachung und Steuerung (z.B. SCADA).
- Sicherstellung der Kundensysteme (CRM, Abrechnung).
- Wiederherstellung der Betriebsprozesse (Wasseraufbereitung, Stromerzeugung, Gasverteilung).

---

2. DR-Plan

Ein Disaster-Recovery-Plan beschreibt die Maßnahmen, die erforderlich sind, um den Betrieb nach einem Vorfall so schnell wie möglich wieder aufzunehmen. Er umfasst Prozesse für die Wiederherstellung der IT-Systeme, die Kommunikationswege sowie die physischen und technischen Voraussetzungen.

Der DR-Plan sollte bei folgenden Szenarien aktiviert werden:

- Naturkatastrophen wie Überschwemmungen oder Stürme.
- Stromausfälle, die mehrere Standorte betreffen.
- IT-Sicherheitsvorfälle (z.B. Cyberangriffe).
- Ausfall kritischer Infrastrukturen (z.B. Wasserwerke, Stromnetze).
- Ausfall wichtiger Dienstleister oder Lieferanten.

---

3. Nutzung dieses Workbooks

Dieses Workbook dient als Leitfaden zur Erstellung und Verwaltung eines Disaster-Recovery-Plans für die XKundeFirmaName. Es unterstützt die Verantwortlichen bei der Planung und Umsetzung von Maßnahmen zur Wiederherstellung des Betriebs und der IT-Infrastruktur nach einem Vorfall.

Ist-Aufnahme

1. Bewertung der kritischen Ressourcen

Die folgenden Ressourcen sind als kritisch für den Betrieb der xKundeFirmaName identifiziert:

Ressource	Kritikalität	RTO (Wiederanlaufzeit)	RPO (Wiederherstellungspunkt)	Verantwortlich
SCADA-System (Netzsteuerung)	Hoch	≤ 1 Stunde	Letzte Datensicherung	IT-Leitung
Wasserversorgungssysteme	Hoch	≤ 2 Stunden	Letzte Datensicherung	Abteilungsleiter Wasser
Stromverteilung	Hoch	≤ 1 Stunde	Letzte Datensicherung	Abteilungsleiter Strom
Gasverteilung	Hoch	≤ 2 Stunden	Letzte Datensicherung	Abteilungsleiter Gas
Kundensystem (CRM, Abrechnung)	Mittel	≤ 4 Stunden	Letzte Datensicherung	Kundenservice
Abrechnungssysteme	Mittel	≤ 24 Stunden	Letzte Datensicherung	IT-Abteilung

2. IT-Systeme und Anwendungen

Die IT-Systeme der xKundeFirmaName spielen eine zentrale Rolle bei der Aufrechterhaltung des Betriebs. Dazu gehören:

1. **SCADA-System**: Überwachung und Steuerung der Versorgungsnetze für Gas, Wasser und Strom.
2. **CRM-System**: Verwaltung von Kundendaten, Serviceanfragen und Rechnungen.
3. **ERP-System**: Abwicklung von Finanzprozessen, Materialwirtschaft und Personalverwaltung.
4. **Datenbanken**: Speicherung von Betriebsdaten, Kundendaten und Abrechnungsinformationen.

3. Physische Infrastruktur

Die folgenden Standorte und physischen Ressourcen sind essenziell:

1. **Wasserwerke**: Wasseraufbereitung und -verteilung.

2. **Stromerzeugung und -verteilung**: Kraftwerke und Verteilernetze.
3. **Gasverteilungsanlagen**: Steuerung und Verteilung des Gasnetzes.
4. **IT-Rechenzentren**: Hosting der kritischen IT-Systeme und Daten.

DR-Planung und Maßnahmen

1. DR-Test und Evaluation

Regelmäßige Tests des DR-Plans sind unerlässlich, um sicherzustellen, dass er im Ernstfall funktioniert. Die folgenden Tests und Übungen werden mindestens einmal jährlich durchgeführt:

- **Test des SCADA-Systems**: Überprüfung der Wiederherstellbarkeit innerhalb der festgelegten RTO.
- **IT-Notfallübung**: Simulation eines Cyberangriffs auf die Kundensysteme und Bewertung der Reaktionsfähigkeit.
- **Netzüberwachung**: Test der physischen Infrastrukturen wie Strom- und Wasserversorgungssysteme.

Evaluation: Nach jedem Test werden die Ergebnisse dokumentiert und eventuelle Schwachstellen identifiziert. Der DR-Plan wird daraufhin angepasst.

2. Notfallkommunikation

Eine klare und schnelle Kommunikation ist im Katastrophenfall von zentraler Bedeutung. Folgende Kommunikationswege werden genutzt:

1. **Interne Kommunikation**: Aktivierung der Notfallteams und Eskalationspfade. Verwendung von Funkgeräten, Notfalltelefonen und alternativen Kommunikationswegen (z.B. Satellitentelefone) bei Ausfall regulärer Netzwerke.
2. **Externe Kommunikation**: Information von Behörden, Kunden und wichtigen Lieferanten. Veröffentlichung von Informationen über Medienkanäle (z.B. lokale Radiosender) zur Kommunikation mit der Bevölkerung.

3. Wiederanlaufpläne

Jede kritische Ressource und jedes System hat spezifische Wiederanlaufpläne:

1. **SCADA-System**:
    - Wiederanlauf des Netzüberwachungssystems in < 1 Stunde.
    - Datenwiederherstellung aus dem letzten Backup.
    - Prüfung der Verbindungen zu Netzsensoren und -steuerungen.
2. **Wasserversorgung**:
    - Sicherstellung der Stromversorgung der Wasseraufbereitungsanlagen.
    - Neustart der Pumpen und Überwachungssysteme.
3. **Stromverteilung**:
    - Überprüfung der Hauptverteilungsnetze und Sicherstellung der Verbindung zum Notstromnetz.

    - Neustart der Überwachungssysteme und Netzsteuerung.
4. **Gasverteilung**:
    - Sicherstellung der Drucksteuerung und Neustart der Gasverteilungsanlagen.
5. **Kundensysteme (CRM/Abrechnung)**:
    - Wiederherstellung der Kundendatenbank.
    - Prüfung der Verbindungen zu den Netzsystemen.

Schlussfolgerungen und Verbesserungen

Nach jeder DR-Übung und jedem tatsächlichen Vorfall wird eine detaillierte Analyse durchgeführt. Dabei werden folgende Punkte evaluiert:

- **Reaktionsfähigkeit**: Wie schnell konnten die Systeme wiederhergestellt werden?
- **Kommunikation**: Waren die Kommunikationswege effektiv?
- **Verbesserungspotenzial**: Welche zusätzlichen Maßnahmen sind erforderlich, um die Ausfallzeiten zu minimieren?

Empfehlungen für nächste Schritte:

- Regelmäßige Überarbeitung des DR-Plans basierend auf den neuesten Technologien und Bedrohungen.
- Investition in redundante IT-Systeme und physische Infrastrukturen zur Sicherstellung der Betriebskontinuität.

Verantwortliche Personen:

- **DR-Manager**: [Name]
- **IT-Leitung**: [Name]
- **Abteilungsleiter Wasser, Strom, Gas**: [Namen]
- **Kundenservice**: [Name]

Anforderungskatalog für die xKundeFirmaName

1. Allgemeine Informationen

- **Version**: 1.0
- **Erstellt am**: [Datum]
- **Erstellt von**: [Name]
- **Verantwortlich**: IT-Leitung, Abteilungsleiter Gas, Wasser, Elektrizität
- **Freigabe durch**: Geschäftsführung
- **Zielsetzung**: Definition der Anforderungen für die technische und organisatorische Umsetzung des Disaster Recovery (DR)-Plans für die xKundeFirmaName.

---

2. Technische Anforderungen

2.1 IT-Systeme und Anwendungen

Anwendung/System	Kritikalität	RTO (Wiederanlaufzeit)	RPO (Wiederherstellungspunkt)	Technische Anforderungen	Verantwortlich
SCADA-System (Netzsteuerung)	Hoch	≤ 1 Stunde	Letzte Datensicherung	- Redundante Serverstruktur - Backup- und Replikationslösungen - Zugang zu Fernsteuerungssystemen	IT-Leitung
CRM-System (Kundendaten)	Mittel	≤ 4 Stunden	Letzte Datensicherung	- Backup täglich - Verschlüsselung der Kundendaten - Integration von Cloud-basierten Speicherlösungen	IT-Leitung
ERP-System (Abrechnung und HR)	Mittel	≤ 24 Stunden	Letzte Datensicherung	- Sicherung aller Finanz- und HR-Datenbanken - Replikation auf ein Offsite-System	IT-Abteilung
E-Mail-System	Niedrig	≤ 24 Stunden	Letzte Datensicherung	- Regelmäßiges Backup - Sicherstellung des Zugriffs auf Mailsysteme von alternativen Standorten	IT-Abteilung
Telefonie (VoIP)	Mittel	≤ 2 Stunden	Letzte Datensicherung	- Redundante VoIP-Infrastruktur - Backup der Kontaktinformationen	IT-Leitung

2.2 Infrastruktur und Netzwerk

Infrastruktur/Netzwerkkomponenten	Kritikalität	RTO (Wiederanlaufzeit)	Technische Anforderungen	Verantwortlich
Netzwerkverbindungen (intern/extern)	Hoch	≤ 1 Stunde	- Redundante Netzwerkverbindungen - Notfall-Switchover-Mechanismen für Kernnetzwerke	Netzwerkadministrator
Server-Infrastruktur	Hoch	≤ 2 Stunden	- Virtualisierte Serverlandschaft - Redundanz und Datenreplikation auf Notfallstandorte	IT-Leitung
Backup-Server	Hoch	≤ 1 Stunde	- Sicherung aller Kernressourcen täglich - Offsite-Sicherung der wichtigsten Daten	IT-Abteilung
Notstromversorgung	Hoch	≤ 1 Stunde	- Notstromgeneratoren an kritischen Standorten - Regelmäßige Wartung und Testläufe	Facility Management
Kommunikationssysteme	Mittel	≤ 2 Stunden	- Redundante Kommunikationswege (VoIP, Mobilfunk, Satellitentelefone)	IT-Leitung

2.3 Physische Ressourcen

Ressource	Kritikalität	RTO (Wiederanlaufzeit)	Technische Anforderungen	Verantwortlich
Stromerzeugung	Hoch	≤ 1 Stunde	- Redundante Stromerzeugung - Verbindung zu Notstromquellen	Abteilungsleiter Strom
Wasserversorgung	Hoch	≤ 2 Stunden	- Sicherstellung der Versorgung durch Backup-Pumpen - Notfallreserven	Abteilungsleiter Wasser
Gasverteilungsanlagen	Hoch	≤ 2 Stunden	- Sicherstellung der Gasversorgung durch redundante Verteilungsanlagen	Abteilungsleiter Gas
Fahrzeuge und mobile Geräte	Mittel	≤ 4 Stunden	- Regelmäßige Wartung von Servicefahrzeugen - Vorhaltung von Ersatzteilen	Logistikabteilung

3. Organisatorische Anforderungen

3.1 Notfallteams und Eskalationswege

1. **DR-Notfallteam**
    - Das DR-Notfallteam wird aktiviert, wenn ein Vorfall die Versorgung oder die IT-Systeme der xKundeFirmaName gefährdet. Es besteht aus den Abteilungsleitern der kritischen Bereiche (IT, Strom, Wasser, Gas).
2. **Eskalationsprozess**
    - Die Eskalationsstufen im Falle eines Vorfalls sind klar definiert. Im Falle eines Ausfalls wird das Notfallteam innerhalb von 15 Minuten informiert. Falls innerhalb einer Stunde keine Lösung gefunden wird, erfolgt die Eskalation an die Geschäftsführung.
3. **Notfallkontakte**
    - Eine Liste mit internen und externen Kontakten wird regelmäßig aktualisiert, darunter Notrufnummern für Techniker, Lieferanten, Behörden und Stromnetzbetreiber.

3.2 Kommunikationsanforderungen

Kommunikationsebene	Kritikalität	Technische Anforderungen	Verantwortlich
Interne Kommunikation	Hoch	- Sicherstellung von Notfalltelefonen (Mobilfunk, Satellitentelefone)	IT-Leitung
Externe Kommunikation (Kunden)	Hoch	- Aktivierung des Notfallplans zur Kundenkommunikation (z.B. über Radiosender)	Kundenservice
Kommunikation mit Behörden und Partnern	Hoch	- Benachrichtigung von Behörden und kritischen Partnern bei Netzproblemen	DR-Notfallteam

---

3.3 Regelmäßige Schulungen und Übungen

1. **Schulungen**
    - Jährliche Schulungen aller Mitarbeiter zum Thema Disaster Recovery und Notfallprozesse. Technische Teams erhalten spezielle Schulungen zur Wiederherstellung kritischer Systeme.
2. **Notfallübungen**
    - Vierteljährliche Tests der Wiederanlaufpläne für SCADA-Systeme, Netzwerke und physische Infrastrukturen. Die Ergebnisse der Übungen werden dokumentiert und analysiert, um die Pläne zu verbessern.

3.4 Datenschutz und Compliance

1. **Datensicherung**
    - Alle Backup- und Replikationsprozesse müssen den Vorschriften zum Datenschutz (DSGVO) entsprechen. Besonders sensible Daten (z.B. Kundendaten) müssen verschlüsselt gespeichert und übertragen werden.
2. **Audit und Überwachung**
    - Jährliche Audits zur Überprüfung der Disaster-Recovery-Pläne und der Einhaltung gesetzlicher Anforderungen. Externe Auditoren überprüfen die DR-Maßnahmen und die technische Umsetzung.

---

4. Technische Spezifikationen für die Wiederherstellung

4.1 Wiederherstellung von IT-Systemen

System	Wiederherstellungsstrategie	Verantwortlich
SCADA-System	- Spiegelung der Datenbank auf externem Server - Test des Remote-Zugriffs	IT-Leitung
CRM-System	- Tägliches Backup der Kundendaten auf Cloud-Speicher	IT-Abteilung
ERP-System	- Replikation der Abrechnungsdaten - Wiederherstellung aus Cloud-Backup	IT-Abteilung

4.2 Wiederherstellung physischer Infrastrukturen

Ressource	Wiederherstellungsstrategie	Verantwortlich
Stromversorgung	- Wiederherstellung der Stromnetze über Notstromquellen	Abteilungsleiter Strom
Wasserversorgung	- Einsatz von Backup-Pumpen - Priorisierung der Wasserversorgung kritischer Gebiete	Abteilungsleiter Wasser
Gasverteilung	- Umschaltung auf alternative Versorgungsquellen	Abteilungsleiter Gas

---

5. Überprüfung und Aktualisierung des Anforderungskatalogs

Der Anforderungskatalog wird mindestens einmal jährlich überprüft und aktualisiert, um auf neue Bedrohungen, technologische Entwicklungen oder Änderungen in der Organisationsstruktur zu reagieren. Verantwortlich für die Aktualisierung ist das DR-Notfallteam.

Datum der letzten Überprüfung: [Datum]
Verantwortlich für die Überprüfung: [Name]

6.7 Aktivierungsprozess für den Stab bei einer Krise/Notfall

1. Allgemeine Beschreibung

Der Aktivierungsprozess beschreibt die Schritte, die unternommen werden müssen, um den Stab bei einer Krise oder einem Notfall zu aktivieren. Dies geschieht, sobald eine Störung oder Bedrohung identifiziert wird, die die Versorgung der xKundeFirmaName mit xKundeProduktbezeichnung beeinträchtigen könnte. Der Stab wird eingesetzt, um den Notfall zu managen, geeignete Maßnahmen einzuleiten und sicherzustellen, dass die Geschäftsprozesse schnellstmöglich wiederhergestellt werden.

2. Stufen der Aktivierung

Der Aktivierungsprozess erfolgt in mehreren Stufen, je nach Schweregrad des Vorfalls:

Stufe 1 – Frühwarnung

- Ein potenzieller Vorfall wird identifiziert (z.B. extreme Wetterbedingungen, technische Warnungen).
- Die verantwortlichen Abteilungsleiter und das IT-Team werden informiert und zur Situation beraten.
- Es erfolgt eine Bewertung, ob der Vorfall eskalieren könnte.

Stufe 2 – Aktivierung des Stabs

- Ein Vorfall hat sich ereignet oder droht sich zu ereignen und beeinträchtigt die reguläre Versorgung oder kritische Geschäftsprozesse.
- Der Stab wird aktiviert, bestehend aus:
    - **Stabsleiter (Geschäftsführung)**
    - **Leitung IT**
    - **Leitung Stromversorgung**
    - **Leitung Gasversorgung**
    - **Leitung Wasserversorgung**
    - **Kundenservice-Verantwortliche**
    - **Leitung Krisenkommunikation**
- Die Mitglieder des Stabs werden innerhalb von 15 Minuten informiert und müssen sich in den Krisenraum begeben oder über alternative Kommunikationswege (z.B. Notruftelefon, Satellitentelefon) zur Verfügung stehen.

Stufe 3 – Eskalation und Koordination

- Der Vorfall wird als Notfall oder Krise eingestuft.
- Der Stab übernimmt die vollständige Koordination der Wiederherstellungsmaßnahmen und der Krisenkommunikation.
- Der Aktivierungsprozess wird an alle betroffenen Abteilungen weitergeleitet, und die vordefinierten Notfallpläne werden in Kraft gesetzt.

3. Rollen und Verantwortlichkeiten

Rolle	Verantwortlichkeiten im Aktivierungsprozess
Stabsleiter	- Entscheidung über die Aktivierung des Stabs - Oberste Verantwortung für alle Notfallmaßnahmen - Kommunikation mit Behörden und externen Stakeholdern
IT-Leitung	- Bewertung und Koordination der IT-Wiederherstellungsmaßnahmen - Sicherstellung der IT-Infrastruktur und Netzwerksysteme
Leitung Stromversorgung	- Sicherstellung der Stromversorgung - Koordination mit externen Energieversorgern - Wiederanlauf der Stromnetze und Sicherung der kritischen Bereiche
Leitung Gasversorgung	- Sicherstellung der Gasversorgung - Überwachung der Druckkontrollen und Sicherung der Gasnetze
Leitung Wasserversorgung	- Sicherstellung der Wasserversorgung - Überwachung der Pumpen und Wasserwerke
Leitung Kundenservice	- Sicherstellung der Kommunikation mit Kunden - Koordination von Maßnahmen zur Information der Bevölkerung
Leitung Krisenkommunikation	- Öffentliche Kommunikation über Medienkanäle (z.B. Radio, Internet) - Sicherstellung der internen Kommunikation innerhalb des Stabs

---

4. Detaillierte Schritte zur Aktivierung des Stabs

4.1 Erkennung des Vorfalls

Schritt	Beschreibung	Verantwortlich	Status
1. Meldung des Vorfalls	Ein kritischer Vorfall wird von einem Abteilungsleiter oder durch IT-Systemüberwachung gemeldet.	Abteilungsleiter / IT-Leitung	☐
2. Bewertung der Lage	Die Auswirkungen des Vorfalls werden durch die jeweiligen Abteilungen bewertet.	Stabsleiter	☐
3. Entscheidung zur Aktivierung	Der Stabsleiter entscheidet, ob der Stab aktiviert wird.	Stabsleiter	☐

4.2 Benachrichtigung und Zusammenkunft des Stabs

Schritt	Beschreibung	Verantwortlich	Status
1. Benachrichtigung des Stabs	Der Stab wird per Telefon oder über Notfallkommunikationswege informiert.	Stabsleiter / IT-Leitung	☐
2. Krisenraum / Kommunikationskanal	Die Mitglieder des Stabs treffen sich im Krisenraum oder schalten sich per Notfalltelefon hinzu.	Alle Mitglieder des Stabs	☐
3. Lagebesprechung	Erster Überblick über den Vorfall und Abstimmung der nächsten Schritte.	Stabsleiter	☐

4.3 Eskalation und Einsatz der Notfallpläne

Schritt	Beschreibung	Verantwortlich	Status
1. Bewertung der Auswirkungen	Der Stab bewertet die Auswirkungen des Vorfalls auf die Versorgung und die kritischen Systeme.	Alle Mitglieder des Stabs	☐
2. Einleitung der Wiederanlaufpläne	Die Wiederanlaufpläne der betroffenen Bereiche (Strom, Gas, Wasser, IT) werden aktiviert.	Abteilungsleiter	☐
3. Eskalation an externe Partner	Externe Partner und Behörden werden je nach Schwere des Vorfalls informiert und in die Maßnahmen einbezogen.	Leitung Krisenkommunikation	☐

4.4 Kommunikation und Berichterstattung

Schritt	Beschreibung	Verantwortlich	Status
1. Interne Kommunikation	Alle internen Teams und Abteilungen werden über den Vorfall und den Status der Maßnahmen informiert.	Leitung Krisenkommunikation	☐
2. Externe Kommunikation	Kunden, Behörden und die Öffentlichkeit werden regelmäßig über den Stand der Wiederherstellungsmaßnahmen informiert.	Leitung Krisenkommunikation	☐
3. Berichterstattung an die Geschäftsführung	Der Stab berichtet regelmäßig an die Geschäftsführung über den Fortschritt der Wiederherstellungsmaßnahmen.	Stabsleiter	☐

5. Eskalationsstufen

Die Eskalation erfolgt stufenweise, basierend auf der Schwere des Vorfalls und der Fähigkeit des Stabs, den Vorfall zu bewältigen.

Stufe	Beschreibung	Maßnahme
Stufe 1	Vorfall ist unter Kontrolle, Wiederanlaufpläne funktionieren.	Regelmäßige Berichterstattung, Kommunikation mit Behörden und Partnern, Krisenteam bleibt aktiv.
Stufe 2	Vorfall erfordert zusätzliche Unterstützung.	Externe Dienstleister und Lieferanten werden hinzugezogen, zusätzliche Ressourcen werden aktiviert.
Stufe 3	Vorfall ist außer Kontrolle, Versorgung gefährdet.	Katastrophenfall wird ausgerufen, volle Koordination mit lokalen Behörden, Eskalation an Krisenzentralen.

---

6. Nachbereitung und Dokumentation

Nach der Bewältigung des Vorfalls führt der Stab eine Nachbesprechung durch und dokumentiert alle Maßnahmen und Erkenntnisse. Es wird ein Abschlussbericht erstellt, der folgende Punkte enthält:

1. **Beschreibung des Vorfalls**
2. **Durchgeführte Maßnahmen**
3. **Ergebnisse und Erkenntnisse**
4. **Verbesserungsvorschläge für den DR-Plan**

Verantwortlicher für die Dokumentation: [Name]

---

7 Prozess: Sicherstellung der organisatorischen und technischen Voraussetzungen für den Wiederanlaufplan

1. Zielsetzung

Der Prozess stellt sicher, dass alle organisatorischen und technischen Bedingungen erfüllt sind, bevor der Wiederanlaufplan oder der Wiederherstellungsplan aktiviert werden kann. Diese Voraussetzungen sind notwendig, um den reibungslosen Betrieb der xKundeFirmaName nach einem Vorfall (z.B. IT-Ausfall, Naturkatastrophe, Netzproblem) sicherzustellen.

---

2. Organisatorische Voraussetzungen

Die organisatorischen Voraussetzungen betreffen die Koordination und Kommunikation zwischen den Beteiligten sowie die Verfügbarkeit von Personal, Dokumentation und anderen Ressourcen.

2.1 Verfügbarkeit des Personals

Schritt	Beschreibung	Verantwortlich	Status
1. Aktivierung des Stabs	Der Stab wird aktiviert, und alle Mitglieder sind ansprechbar. Die Kommunikationswege sind etabliert.	Stabsleiter	☐
2. Festlegung der Verantwortlichkeiten	Jeder Bereich (Strom, Gas, Wasser, IT) hat klare Verantwortliche, die die Wiederanlauf- und Wiederherstellungsmaßnahmen koordinieren.	Stabsleiter / Abteilungsleiter	☐
3. Notfallkontakte verfügbar	Eine aktuelle Liste aller internen und externen Notfallkontakte ist vorhanden und für den Krisenstab zugänglich.	Leitung Krisenkommunikation	☐
4. Schulung und Übung	Das Notfallteam ist geschult und hat die Notfallpläne bei vorangegangenen Übungen getestet.	Abteilungsleiter	☐
5. Benennung externer Partner	Externe Dienstleister (z.B. für IT, Gas, Wasser, Strom) wurden informiert und stehen zur Unterstützung bereit.	Beschaffungsabteilung	☐

2.2 Verfügbarkeit der Notfalldokumentation

Schritt	Beschreibung	Verantwortlich	Status
1. Notfallpläne zugänglich	Alle relevanten Notfallpläne (Wiederanlaufpläne, Handlungsanweisungen) sind zugänglich und aktuell.	IT-Abteilung / Abteilungsleiter	☐
2. Kommunikationsplan verfügbar	Ein klar definierter Kommunikationsplan liegt vor und kann sofort aktiviert werden.	Leitung Krisenkommunikation	☐
3. Zugriffsrechte vorhanden	Die verantwortlichen Personen haben Zugriff auf kritische IT-Systeme und physische Standorte (z.B. Rechenzentren, Kraftwerke).	IT-Leitung / Facility Management	☐
4. Protokollierung der Maßnahmen	Alle Wiederherstellungsmaßnahmen werden dokumentiert, und es gibt klare Protokollierungsrichtlinien.	IT-Leitung	☐

3. Technische Voraussetzungen

Die technischen Voraussetzungen beziehen sich auf die Verfügbarkeit der IT-Infrastruktur, die Versorgungssysteme und die physischen Ressourcen, die zur Wiederherstellung und zum Betrieb der xKundeFirmaName benötigt werden.

3.1 IT-Infrastruktur und Netzwerke

Schritt	Beschreibung	Verantwortlich	Status
1. Notstromversorgung aktiv	Die Notstromversorgung an kritischen Standorten (Rechenzentrum, SCADA, Pumpen) ist aktiv und getestet.	Facility Management	☐
2. Server und Netzwerkverbindungen verfügbar	Alle Server und Netzwerkverbindungen sind getestet und bereit für den Wiederanlauf (primär und sekundär).	IT-Leitung	☐
3. Backup-Systeme einsatzbereit	Backup-Systeme (Offsite-Backups, Cloud-Replikation) stehen zur Verfügung und sind aktuell.	IT-Leitung	☐
4. Kommunikationssysteme verfügbar	Notfallkommunikationssysteme (Satellitentelefon, Mobilfunk, Notruftelefone) sind betriebsbereit.	IT-Leitung / Krisenteam	☐
5. Redundante IT-Systeme geprüft	Alle kritischen IT-Systeme (SCADA, CRM, ERP) sind durch redundante Systeme gesichert.	IT-Leitung	☐

3.2 Physische Ressourcen

Schritt	Beschreibung	Verantwortlich	Status
1. Verfügbarkeit von Gas, Wasser, Strom	Die Verteilungsnetze für Gas, Wasser und Strom sind einsatzbereit, und die Betriebssysteme wurden geprüft.	Abteilungsleiter Gas, Wasser, Strom	☐
2. Zugang zu kritischen Standorten	Alle kritischen Standorte (z.B. Wasserwerke, Gasverteilungsanlagen, Stromnetzknotenpunkte) sind zugänglich.	Facility Management	☐
3. Ersatzteile und Materialien vorhanden	Notwendige Ersatzteile und Materialien (z.B. für Stromnetzwerke, Pumpen, Gasleitungen) sind in ausreichender Menge vorhanden und leicht zugänglich.	Beschaffung / Logistik	☐
4. Mobile Einsatzkräfte bereit	Mobile Einsatzteams (Techniker) sind bereit, vor Ort Störungen zu beheben.	Logistikabteilung / Abteilungsleiter	☐

3.3 Tests und Prüfungen

Schritt	Beschreibung	Verantwortlich	Status
1. IT-Systeme getestet	Ein Funktionstest der Backup- und Replikationssysteme wurde durchgeführt.	IT-Leitung	☐
2. Notstromversorgung getestet	Regelmäßige Tests der Notstromgeneratoren wurden durchgeführt, und alle Systeme laufen stabil.	Facility Management	☐
3. Physische Systeme überprüft	Alle kritischen physischen Systeme (Strom, Gas, Wasser) wurden auf ihre Funktionalität getestet.	Abteilungsleiter	☐
4. Kommunikationssysteme getestet	Notfallkommunikationssysteme wurden auf Funktionalität geprüft.	Krisenteam	☐

4. Koordinierung und Freigabe des Wiederanlaufs

4.1 Koordinierung des Wiederanlaufs

Schritt	Beschreibung	Verantwortlich	Status
1. Abstimmung zwischen den Abteilungen	Die Abteilungsleiter (IT, Strom, Wasser, Gas) koordinieren die Wiederanlaufmaßnahmen und tauschen Informationen über den Status aus.	Stabsleiter / Abteilungsleiter	☐
2. Kommunikation mit externen Partnern	Externe Dienstleister (z.B. IT-Dienstleister, Zulieferer) wurden in den Prozess einbezogen und sind einsatzbereit.	Stabsleiter / Abteilungsleiter	☐
3. Priorisierung der Wiederherstellungsmaßnahmen	Die Maßnahmen werden priorisiert: IT-Systeme, kritische Infrastruktur, Kundenkommunikation.	Stabsleiter	☐
4. Entscheidung zur Freigabe	Der Stabsleiter gibt grünes Licht für den Wiederanlauf, sobald alle Voraussetzungen erfüllt sind.	Stabsleiter	☐

4.2 Überwachung und Dokumentation des Wiederanlaufs

Schritt	Beschreibung	Verantwortlich	Status
1. Überwachung des Wiederanlaufs	Der Wiederanlauf wird kontinuierlich überwacht, um sicherzustellen, dass alle Systeme ordnungsgemäß funktionieren.	IT-Leitung / Abteilungsleiter	☐
2. Dokumentation der Maßnahmen	Alle durchgeführten Maßnahmen, sowie potenzielle Probleme und deren Lösungen werden in Echtzeit dokumentiert.	IT-Leitung / Krisenteam	☐
3. Prüfung der Wiederherstellungsqualität	Nach Abschluss des Wiederanlaufs wird die Qualität der Wiederherstellungsmaßnahmen überprüft.	IT-Leitung	☐

---

5. Abschluss und Freigabe des Normalbetriebs

5.1 Abschluss des Wiederanlaufs

Sobald der Wiederanlauf abgeschlossen ist und alle Systeme und physischen Infrastrukturen stabil laufen

---

Pink Naarden
Gooimeer 18
1411 DE Naarden
Phone: +31(0)88 235 66 55

Pink Den Bosch
Rietveldenweg 40
5222 AR's-Hertogenbosch
Phone: +31(0)88 235 66 55

Pink Zuid
Australiëlaan 21
6199 AA Maastricht-Airport
Phone: +31(0)43 88 000 88

GERMANY
Reuterweg 51-53
60323 Frankfurt am Main

Centroallee 273
46047 Oberhausen

Phone: +49 541 962 590 04