Cyber Incident Response Planung

Digitalisierungsthema 2025

© 2025 - Rewion

XING LinkedIn

Besuchen Sie unseren **Blog**

Ich packe meinen Notfallkoffer…

Ausgedruckte Telefonliste

Notfallhandy

Notfalllaptop, nicht am Netz

Notfallcheckliste

Maßnahmen-Plan

© 2025 - Rewion

Positionierung zwischen Strategie und Systemhaus

REWION

Strategie
Beratung

Systemhaus

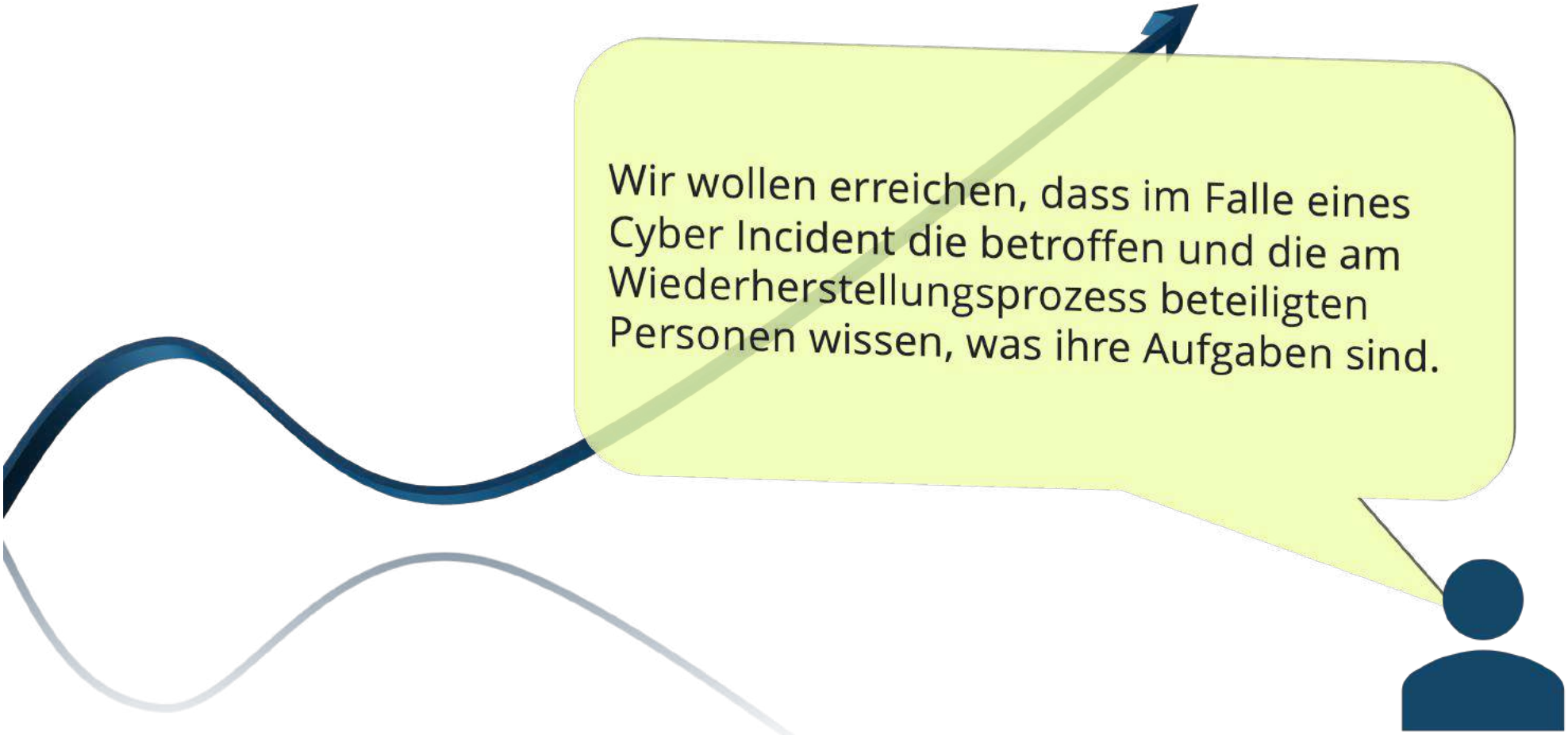
Unabhängig

Ganzheitlich

Umsetzungsstark

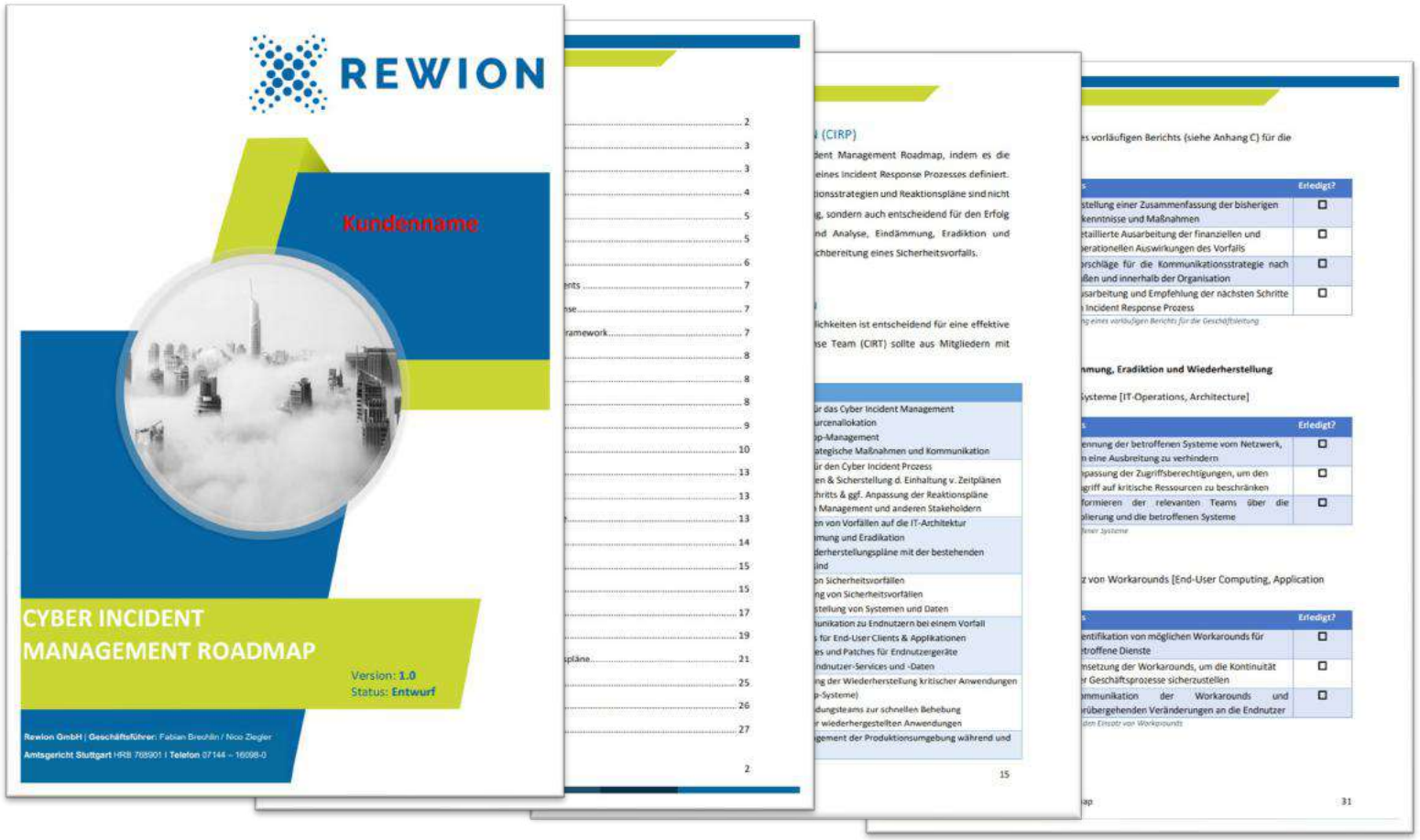
Ihr TRUSTED ADVISOR

Projektziel in einem Satz



© 2025 - Rewion

Das Notfalldokument



Projekttimeline mit den Partnern

© 2025 - Rewion

Projekttimeline

© 2025 - Rewion

Projekttimeline

Kick-Off

- ✓ Gemeinsames Projekt-verständnis

- ✓ Theorie

- ✓ IST-Analyse

Arbeitsphase 1

- ✓ Erste Anpassungen Template auf das eigene KH

- ✓ Anfangsumfrage

Sommercamp

- ✓ Weitere Anpassungen
- ✓ Planung Praxistest
- ✓ Planung weitere Tasks
- ✓ Brainstorming technisches Worksaround mit DMI

D·M·I

Arbeitsphase 2

- ✓ Verbesserung und Finalisierung des Plans

Leadership Summit

- ✓ Vorstellung der Highlights der fertigen Pläne

Arbeitsphase 3

- ✓ ggf. Tests
- ✓ Abschluss-umfrage

Entscheider-Event

- ✓ Abschluss-präsentation

© 2025 - Rewion

Agenda.

1. Ziel der Umfrage
2. Teilnehmernanzahl und Kernthemen
3. Vorstellung der Antwortstruktur/ Ergebnisse
4. Erkenntnisse

© 2025 - Rewion

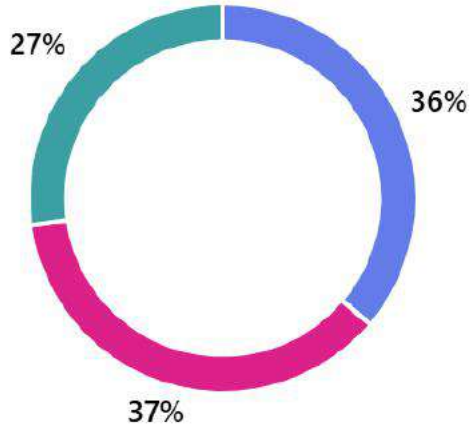
Ziel der Umfrage

... war es, den IST-Zustand zum Thema Cybersicherheit im Krankenhaus zu erfassen – insbesondere das **Wissen, Verhalten und Sicherheitsgefühl** der Mitarbeitenden bei einem Vorfall.

© 2025 - Rewion

Teilnehmeranzahl & Kernthemen

Dr. Fontheim	108
AWO	109
Landeskrankenhaus Andernach	81



Teilnehmeranzahl: 298

Kernthemen der Umfrage

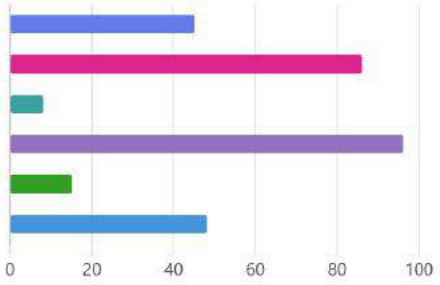
- ✓ Kenntnis über Reaktionswege bei Cyberangriffen
- ✓ Persönliches Sicherheitsgefühl
- ✓ Einschätzung der bisherigen Vorbereitung
- ✓ Bessere Vorbereitung

© 2025 - Rewion

Wer hat an der Umfrage teilgenommen?

4. Welche Funktion erfüllen Sie im Krankenhaus?

Ärztlicher Dienst	45
Pflege & betreuung	86
Medizinisch-technischer Bereich	8
Verwaltung & Management	96
Service & Technik	15
Sonstige (bitte angeben)	48

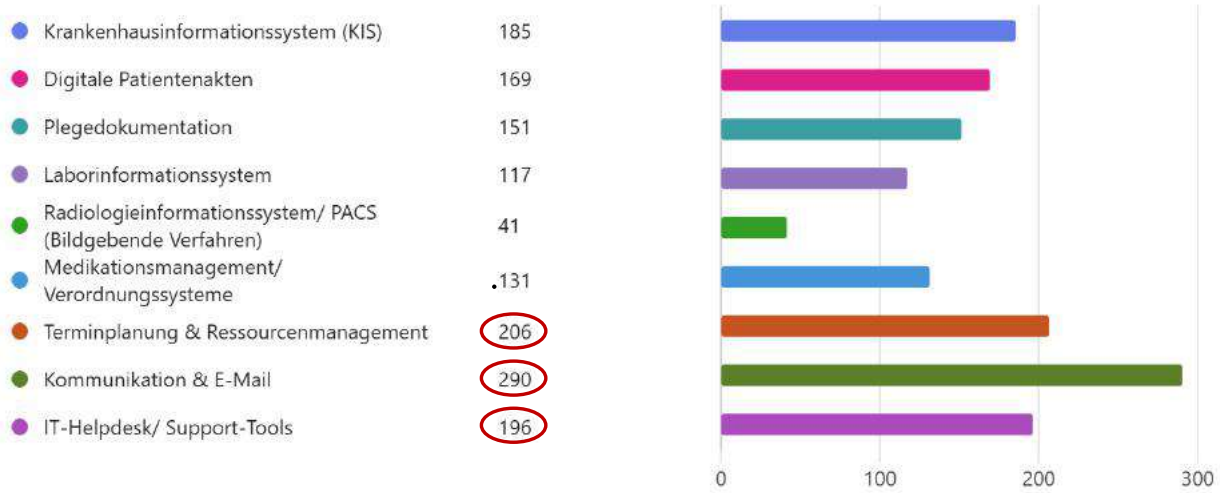


Mehrheit aus den Bereichen
Verwaltung & Management (32%) und
Pflege & Betreuung (29%)

© 2025 - Rewion

Unverzichtbare Programme und digitale Anwendungen

6. Welche digitalen Anwendungen oder Programme sind für Ihre Arbeit im Krankenhaus unverzichtbar?



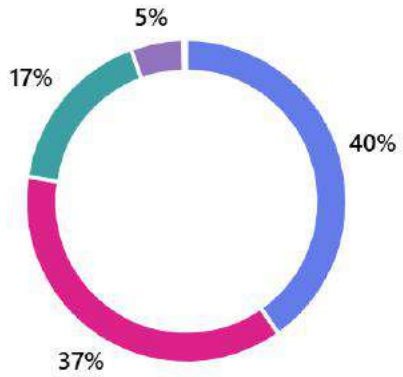
- Kommunikationsanwendungen und E-Mail als unverzichtbare Anwendungen (97%)
- Terminplanung & Ressourcenmanagement (69%)
- IT-Helpdesk/ Support Tools (66%)

© 2025 - Rewion

Handeln bei Fehlfunktion dieser Anwendungen

8. Was tun Sie, wenn diese Anwendungen nicht funktionieren?

Ich kontaktiere den IT-Helpdesk/ IT-Support	288
Ich starte den Rechner/ die Anwendung neu	266
Ich versuche, eine alternative Lösung zu finden	121
Ich warte	38
Ich weiß ehrlich gesagt nicht, was dann zu tun ist	2



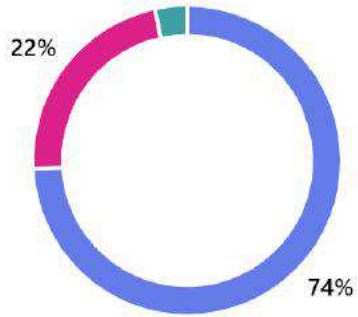
- 97% der Teilnehmer kontaktieren den IT-Hepldesk/-Support
- 89% der Teilnehmer starten den Rechner oder die Anwendung neu

© 2025 - Rewion

Kenntnis über Handlungsschritte bei einem Cyberangriff

10. Sind Ihnen die notwendigen Schritte bekannt, die sie bei einem Cyberangriff durchführen müssen?

Nein	221
Ja, mir ist die offizielle Meldekette (nach BSI) im Falle eines Cyberangriffs bekannt	67
Ja, ich habe bereits eine Schulung zu Cybersecurity-Notfallmaßnahmen (nach BSI) erhalten, aber bin mi...	10



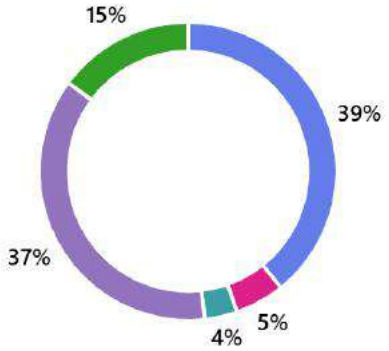
- 74% der Teilnehmenden sind die notwendigen Schritte NICHT bekannt
- 22% ist die offizielle Meldekette nach BSI bekannt
- 3% haben eine Schulung über die BSI-Maßnahmen erhalten, sind sich aber doch unsicher

© 2025 - Rewion

Ergreifen von Maßnahmen

11. Welche konkreten Maßnahmen ergreifen Sie in Ihrem Arbeitsbereich im Falle eines Cyberangriffs?

IT-Abteilung informieren	66
Abwarten und keine voreiligen Maßnahmen ergreifen	9
Gegenmaßnahmen ergreifen	6
verdächtige Mails oder Dateien nicht öffnen und melden	62
Computer vom Netzwerk trennen	25



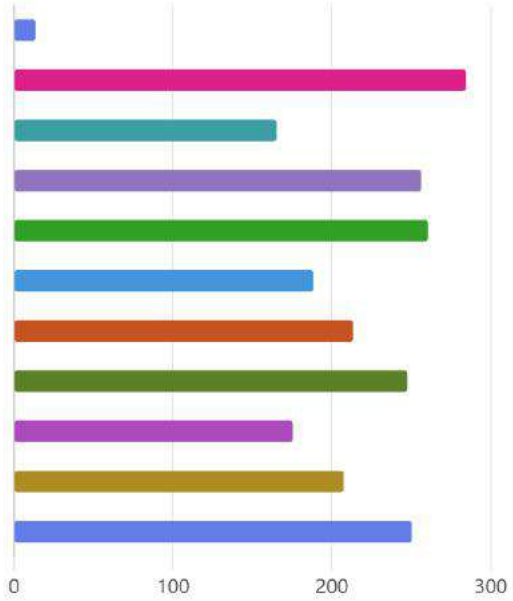
- die Mehrheit informiert die IT-Abteilung oder meldet verdächtige Mails oder Dateien

© 2025 - Rewion

Erkennen eines Cyberangriffs

14. Welche Erkennungsmerkmale eines Cyberangriffs sind Ihnen bekannt?

Ich weiß nicht, wie ich einen Cyberangriff erkennen kann	13
Unerwartete oder verdächtige E-Mails mit Anhängen oder Links (Phishing-Mails)	284
Plötzliche verlangsamte oder nicht reagierende Systeme	165
Unbekannte oder verdächtige Programme, die sich selbst installieren	256
Pop-ups oder Warnmeldungen, die zur Eingabe von Passwörtern auffordern	260
Dateien oder Dokumente sind plötzlich nicht mehr zugänglich oder verschlüsselt	188
Unerwartete Änderungen an Passwörtern oder Zugriffsrechten	213
Ungewohnte Aktivitäten in E-Mails (z. B. versendete Nachrichten, die man nicht...	247
Unbekannte oder nicht autorisierte Geräte im Netzwerk	175
Plötzlicher Datenverlust oder Manipulation von Dateien	207
Antivirus- oder Sicherheitssysteme melden ungewöhnliche Aktivitäten	250



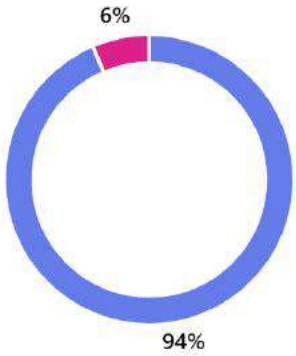
- Phishing-Mails, verdächtige Programme
- plötzliche Passworteingabe
- Meldung ungewöhnlicher Aktivitäten sind am bekanntesten

© 2025 - Rewion

Verantwortungsbewusstsein Cyberangriff

19. Fühlen Sie sich verantwortlich, bei einem Cyberangriff zu handeln?

Ja, natürlich!	279
Nein, nicht wirklich	19



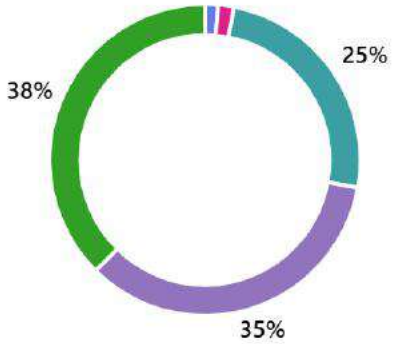
- 94% der Teilnehmer fühlt sich zum Handeln verpflichtet
- 6% fühlen sich nicht wirklich verantwortlich

© 2025 - Rewion

Risikoeinschätzung Cyberangriff

20. Wie hoch schätzen Sie das Risiko ein, dass Krankenhäuser Opfer eines Cyberangriffs werden?

sehr unwahrscheinlich	4
eher unwahrscheinlich	5
möglich	74
wahrscheinlich	103
sehr wahrscheinlich	112



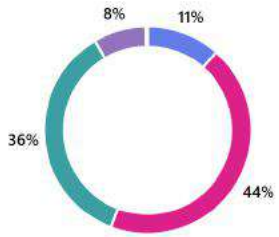
- 73% der Teilnehmer halten einen Angriff für wahrscheinlich bis sehr wahrscheinlich

© 2025 - Rewion

Vorbereitung Cyberangriff

21. Wie gut fühlen Sie sich auf einen Cyberangriff vorbereitet?

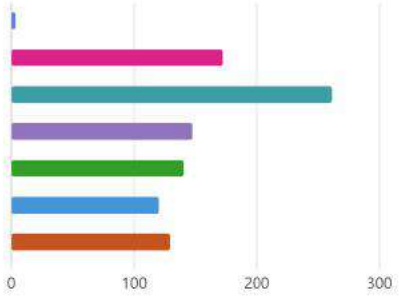
Ich habe keine Ahnung, was ich tun sollte.	35
Ich kenne eine paar grundlegende Maßnahmen, bin mir aber unsicher.	135
Ich kenne die wichtigsten Schritte, bin mir aber nicht 100% sicher.	109
Ich bin gut vorbereitet und weiß, welche Maßnahmen ich ergreifen muss.	25
Ich bin sehr gut vorbereitet und weiß genau, was ich zu tun habe.	1



- nur ein Teilnehmer gibt an, genau zu wissen, was zu tun ist
- 80% geben an, unsicher zu sein
- 8% fühlen sich gut vorbereitet
- 11% fühlen sich garnicht vorbereitet

22. Was würde Ihnen helfen, sich besser vorbereitet zu fühlen?

nichts davon, ich weiß genau, was ich zu tun habe	3
Schulungen oder Workshops zur IT-Sicherheit	172
Klare Handlungsanweisungen für den Ernstfall (z. B. Notfallplan, Checkliste)	261
Mehr Informationen über aktuelle Bedrohungen und Angriffsmethoden	147
Bessere Erreichbarkeit der IT-Abteilung im Notfall	140
Eine einfachere Meldemöglichkeit für verdächtige Vorfälle	120
Technische Unterstützung durch automatische Sicherheitssysteme	129

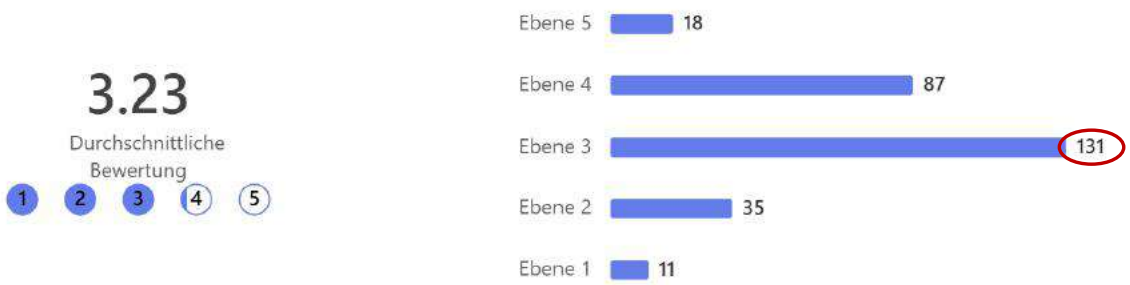


- 88% der Teilnehmenden wünschen sich einen Notfallplan/Checkliste
- 58% wünschen sich Schulungen oder Workshops
- 47% wünschen sich eine bessere Erreichbarkeit der IT-Abteilung

© 2025 - Rewion

Einschätzung Vorbereitung Cyberangriff

26. Wie gut ist Ihr Krankenhaus Ihrer Meinung nach auf einen Cyberangriff vorbereitet (1-sehr schlecht, 5-sehr gut)?



- 44% schätzen ihr Krankenhaus als durchschnittlich vorbereitet ein
- 29% schätzen es als gut vorbereitet ein

© 2025 - Rewion

Erkenntnisse aus der Mitarbeiterumfrage

- **74%** der Teilnehmenden sind die notwendigen Schritte bei einem Cyberangriff **nicht bekannt**
- Nur 27% wissen, wie ein Cyberangriff erkannt werden kann
- 73% wissen nicht, wie ein Cyberangriff erkannt werden kann oder sind sich unsicher
- **Verantwortungsbewusstsein** der Krankenhausmitarbeiter ist **stark**, aber das know-how fehlt
- das Risiko eines Angriffs wird eher als hoch eingeschätzt (35%-wahrscheinlich, 38%-sehr wahrscheinlich, 25%-möglich)
- 80% fühlen sich nicht gut vorbereitet oder unsicher, auch wenn ihnen bereits ein paar Maßnahmen bekannt sind
- **88% wünschen** sich einen **Notfallplan/Checkliste** für den Ernstfall
- die Teilnehmer sehen in Sachen Cybersicherheit bei dem eigenen Krankenhaus Potenzial nach oben

© 2025 - Rewion

ENTSCHEIDERFABRIK
Eco System ENTSCHEIDERFABRIK - der eHealth Inkubator

REWION

Cyber Incident Response Planung

Sommercamp

Landeskrankenhaus

DR. FONTHEIM
Mentale Gesundheit

AWO
Niedersachsen gGmbH
AWO Psychiatriezentrum

D·M·I

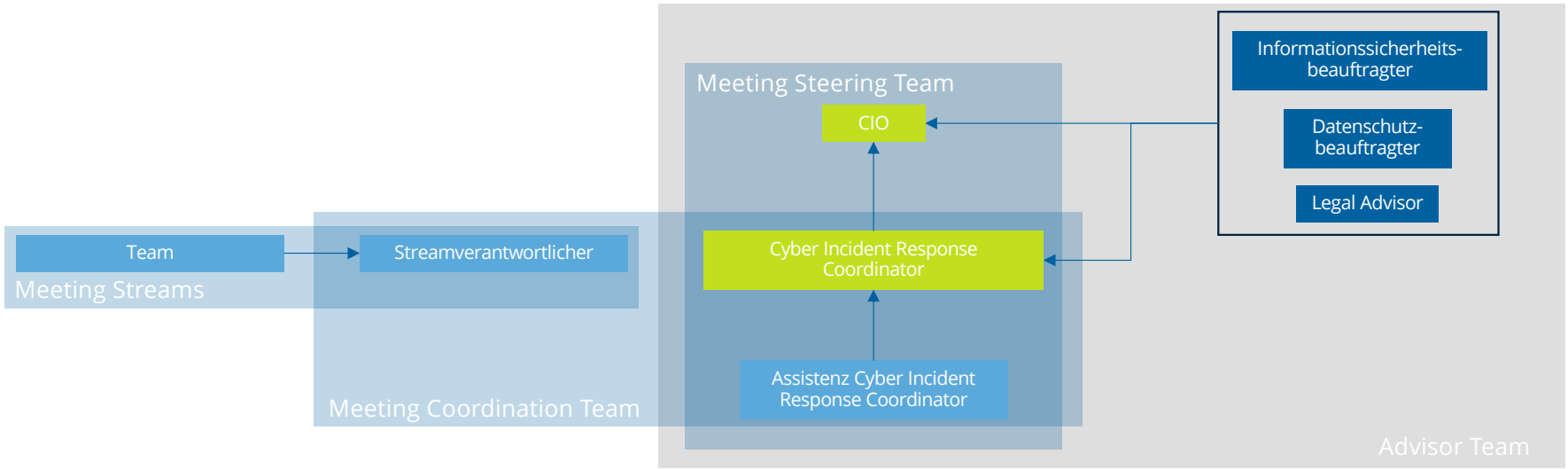
XING LinkedIn

Besuchen Sie unseren **Blog**

© 2025 - Rewion

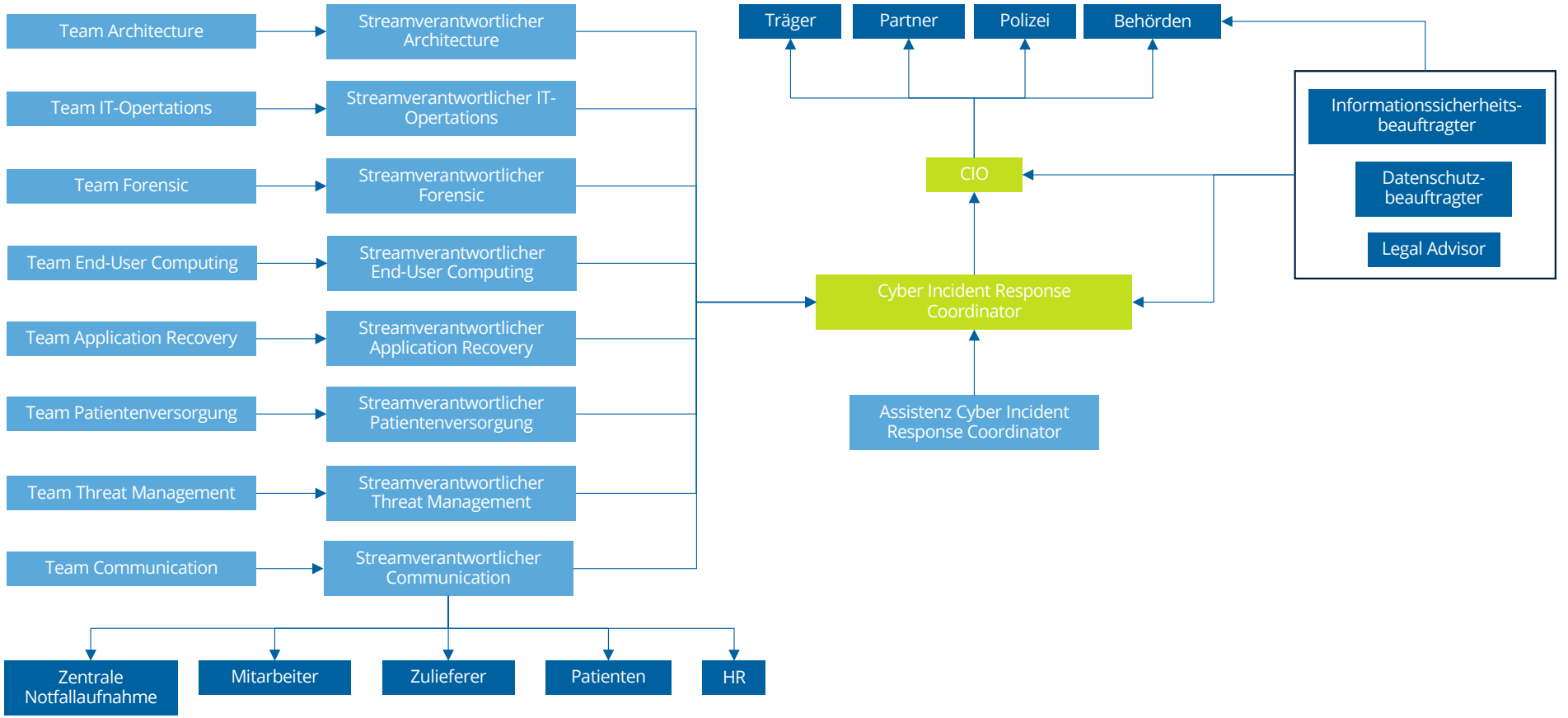
Arbeitsauftrag: Verantwortlichkeiten festlegen

Überlegen Sie sich (falls noch nicht geschehen), wie Sie ihre Mitarbeiter aufteilen und schreiben Sie die Namen in das Organigramm. Passen Sie das Organigramm so an, dass nach Möglichkeit jeder Name nur einmal vor kommt. Hier können Streams zusammengefasst werden und Vernutzen neu sortiert werden.



© 2025 - Rewion

Berichterstattung/Kommunikation



© 2025 - Rewion

Arbeitsauftrag: Praxistest vorbereiten

Wir wollen den einen Praxistest planen. Dafür müssen wir wissen, welche Abteilung wofür IT-Support benötigt, wie die Workarounds sind und in welcher Priorität die IT wiederhergestellt werden muss.

Aufteilung Abteilungen
Überlegen Sie, welche Abteilungen bei Ihnen in der Klinik vorhanden sind.

Eingesetzte IT
Überlegen Sie ausgehend vom Behandlungsprozess und Arbeitsalltag/Patientenjourney, wo welche IT in den Abteilungen zum Einsatz kommt.

Workarounds
Wo kann für die IT ein Workaround gefunden werden und wie sieht dieser aus?

Prioritäten festlegen
In welcher Priorität werden die Applikationen wieder hergestellt/Server hochgefahren?

© 2025 - Rewion

Abteilungen

01 IT
- IT Admin (KIS)
- IT Admin (ERP)
- IT Admin (Infrastruktur)
- IT Mitarbeiter
- IT Leitung

02 Verwaltung
- Personaler/-entwicklung
- Controller
- Buchhaltung
- GF
- Projektmanagement
- Einkauf
- Kommunikation
- Recht
- QM

03 Medizinisches Personal
- ÄrztInnen
- Pflegende
- Stationsleitende
- Pflegedirektion
- Chefärzte/Oberärzte
- Spezialtherapeuten
- Therapeutische Leitung

04 Labor intern
- Laborleitung
- Labormitarbeitende

Labor extern
- Externe Firma

05 Unterstützung
- Transport
- Sicherheitsdienst
- Küche
- Technik
- Studienassistenten
- Medizintechnik
- Lager
- Reinigung
- Garten

06 Externe
- Azubis
- Praktikanten
- Dienstleister
- Kooperationskliniken
- Pflegeschule
- Honorarärzte
- Akademie

07 Maßregelvollzug
- Psychiatrische Forensik

Akutstation
- Mitarbeiter Akutstation

© 2025 - Rewion

Hardware (I)

Alarmsystem

Smartphone

Private Smartphones (BYOD)

Tablets

Telefon

Laptops

Anzeigen

Barcodescanner

Gegensprechanlage

Piepser

Infotainment

Zubehör

Drucker

PC

Qumea

Patienten-monitoring

Visitenwagen

Diagnostik

Laborgräte

OP Geräte

© 2025 - Rewion

Hardware (II)

Router

Server

Switches

Firewall

Externe Server

Voice over IP / Telefonanlage

© 2025 - Rewion

Unverzichtbare Programme und digitale Anwendungen

6. Welche digitalen Anwendungen oder Programme sind für Ihre Arbeit im Krankenhaus unverzichtbar?

- Kommunikationsanwendungen und E-Mail als unverzichtbare Anwendungen (97%)
- Terminplanung & Ressourcenmanagement (69%)
- IT-Helpdesk/ Support Tools (66%)

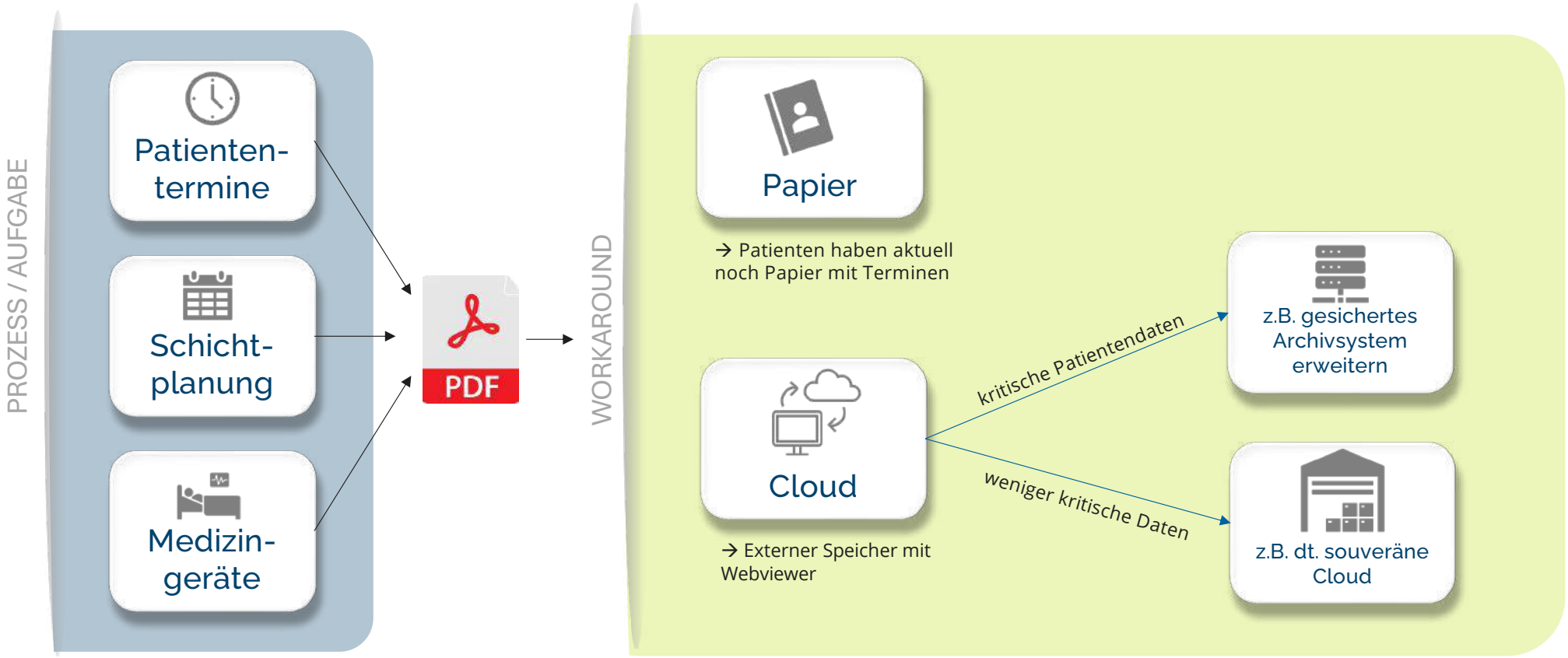
© 2025 - Rewion

Kommunikation wiederherstellen

ART DES AUSFALLS	ABSCHWÄCHUNG	HINWEIS
Netzwerkinfiltration	Vorhalten eines Mailservers im Cold-Standby in einem komplett separaten Netz (eigene Hardware)	Diese Art des Ausfalls Bedarf das Herunterfahren der betroffenen Netzwerkkomponenten
Beeinträchtigung der Kommunikationskanäle	Notfallkommunikation über Cloud-Messanger mit Firmen- oder BYOD-Mobiltelefonen Alternative Mailserver z.B. Freemailer nutzen	Datenschutz, Dokumentation und Sicherheit müssen beachtet werden Zum Beispiel durch Wahl eines deutschen Anbieters

© 2025 - Rewion

Terminplanung und Ressourcenmanagement

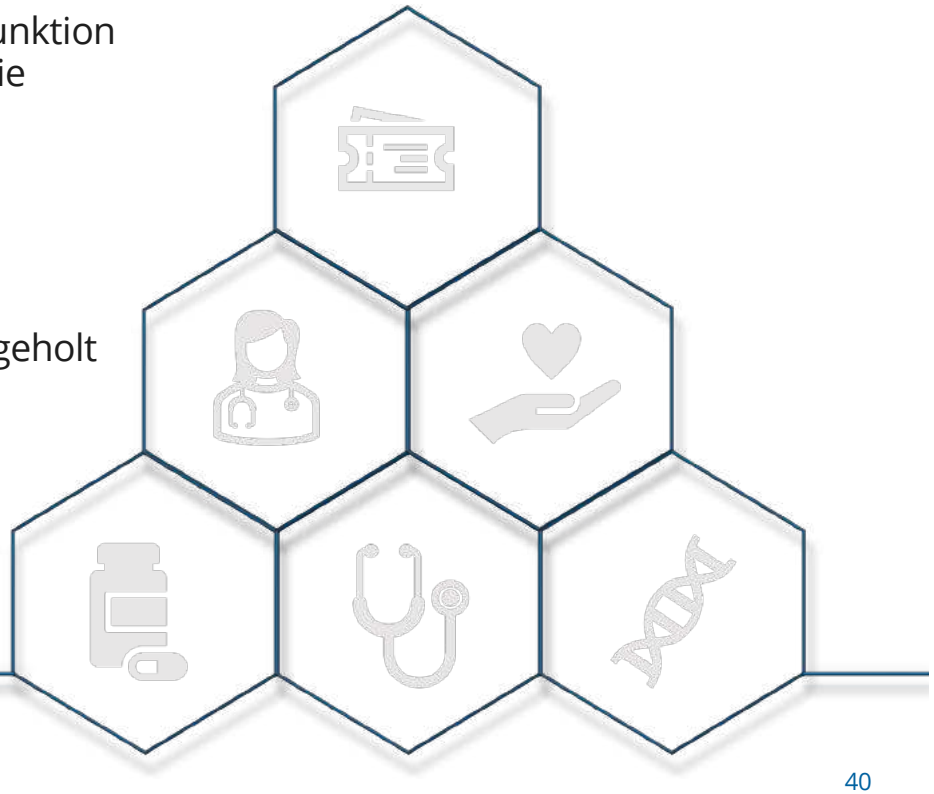


© 2025 - Rewion

Helpdesk

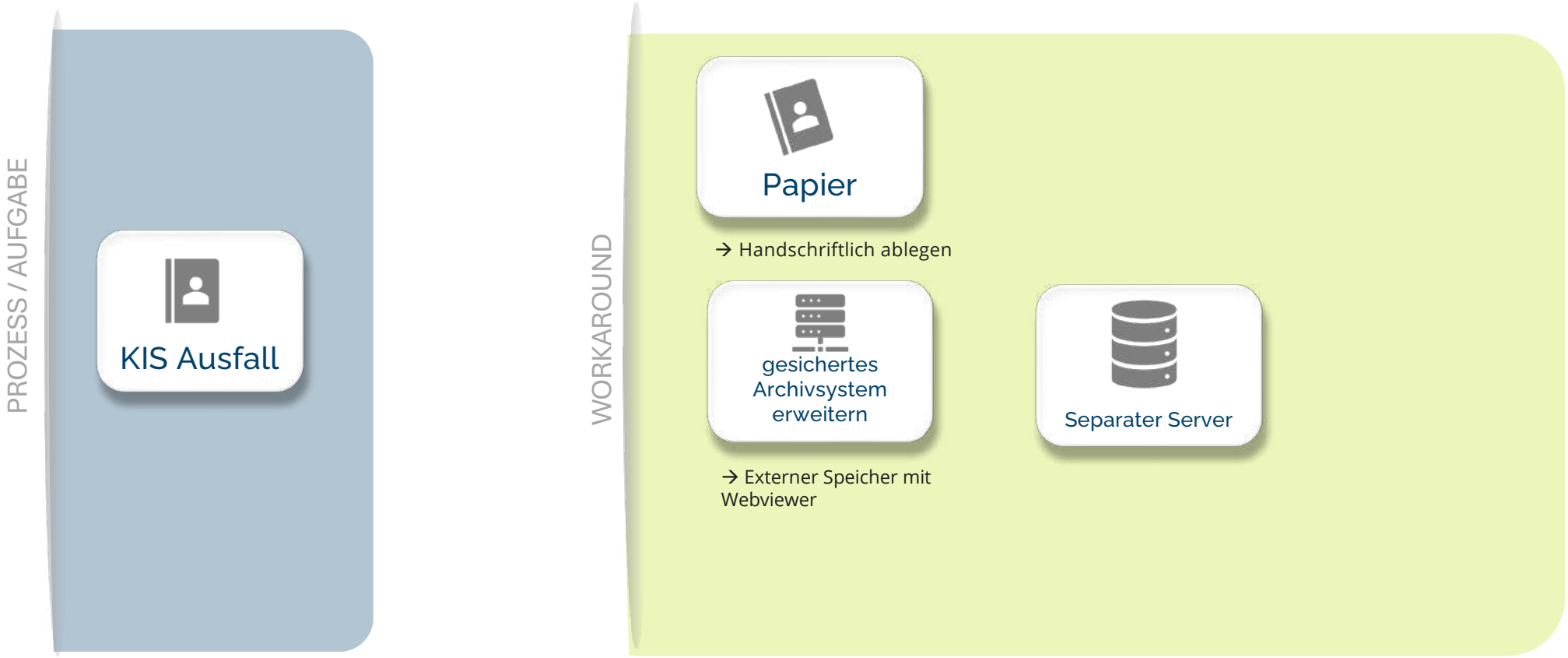
- Die Konfiguration der ACD-Anlage (Anrufverteilung) muss das Ausfallszenario berücksichtigen
- Benutzung von **cloudbasierten VoIP-Anbietern** mit Softphone Funktion für Firmenhandys, um eine geordnete Verteilung der Anrufe auf die Firmenhandys zu leiten
- Alternativ kann ein **Anrufbeantworter** konfiguriert werden

  → Es sollte nicht nur eine interne Durchwahl für den Helpdesk existieren, sondern auch eine öffentliche Nummer
- Dokumentation kann im Notfallszenario auch erst hinterher nachgeholt werden
- Es sollte eine **extra Rufnummer** für IT-Notfälle geben



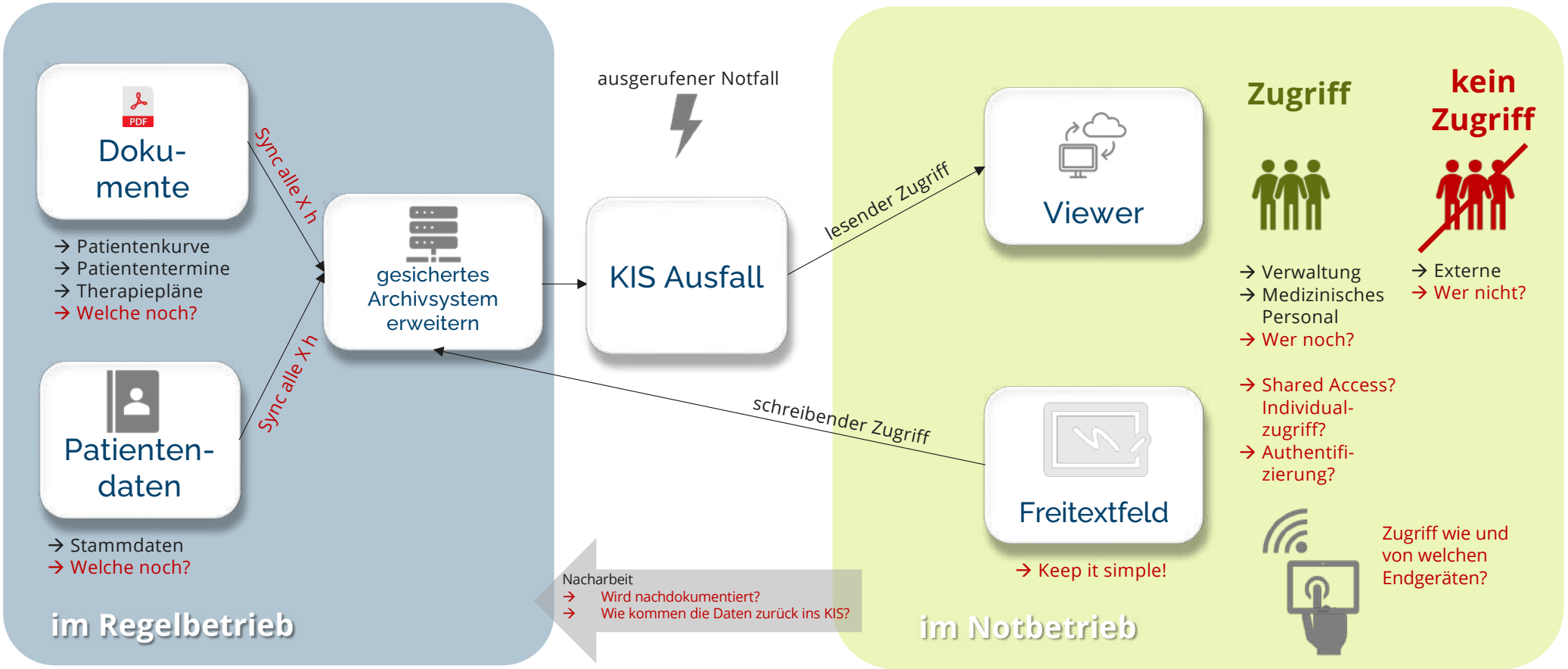
© 2025 - Rewion

Ausfall KIS



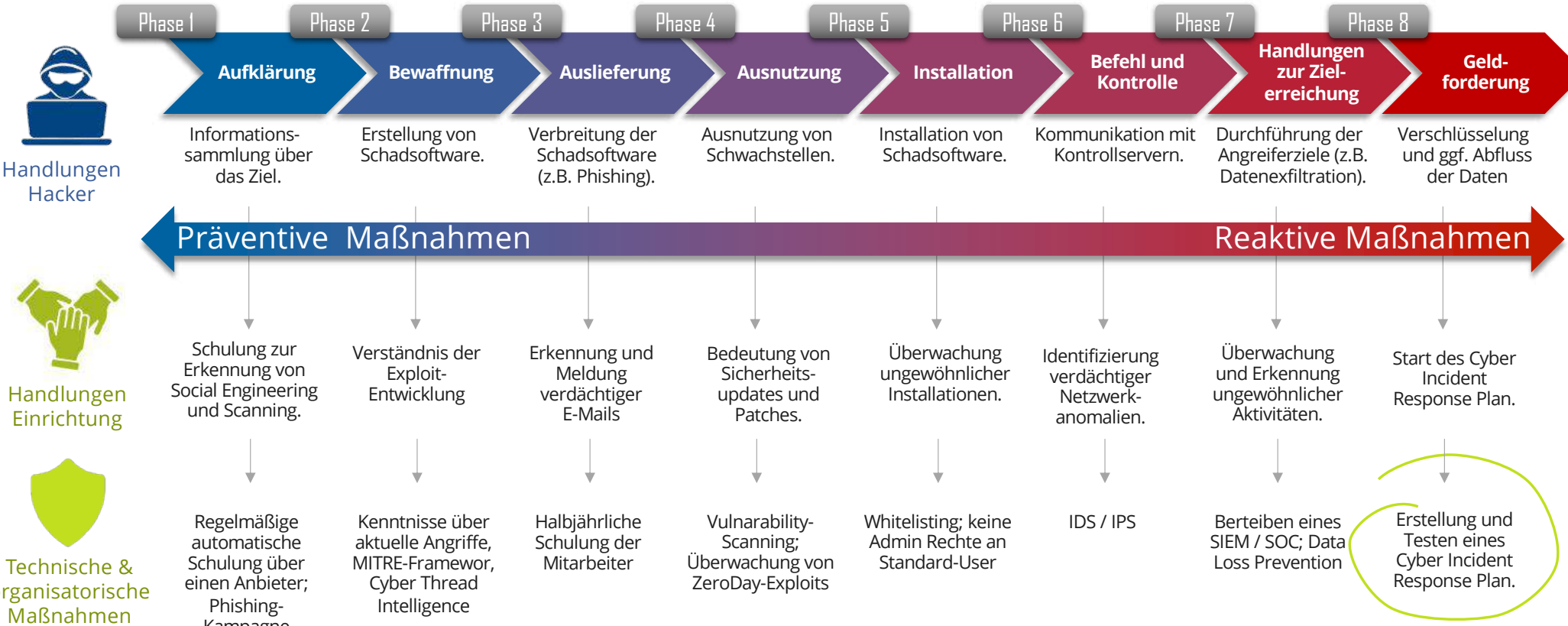
© 2025 - Rewion

Ausfall



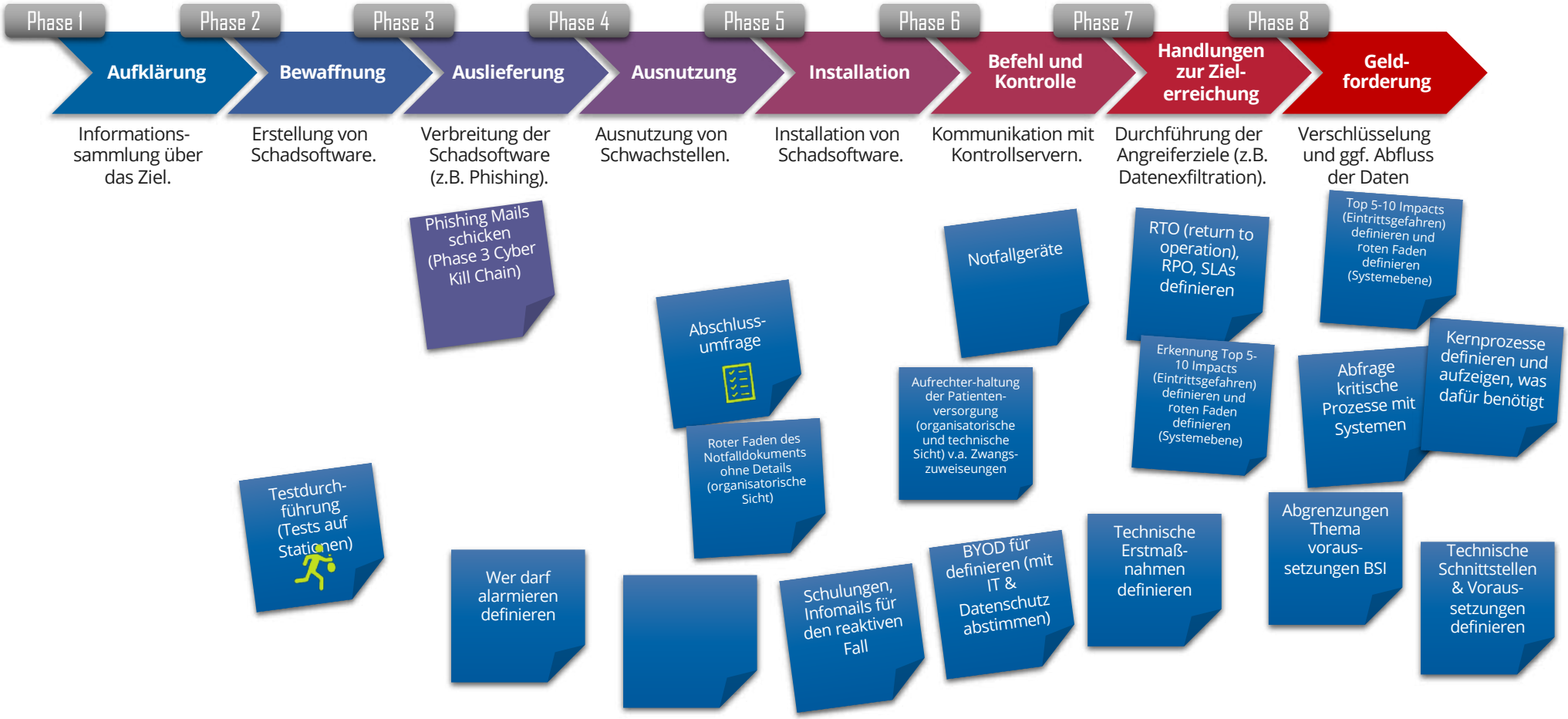
© 2025 - Rewion

Maßnahmen Entgegen der Cyber Kill Chain



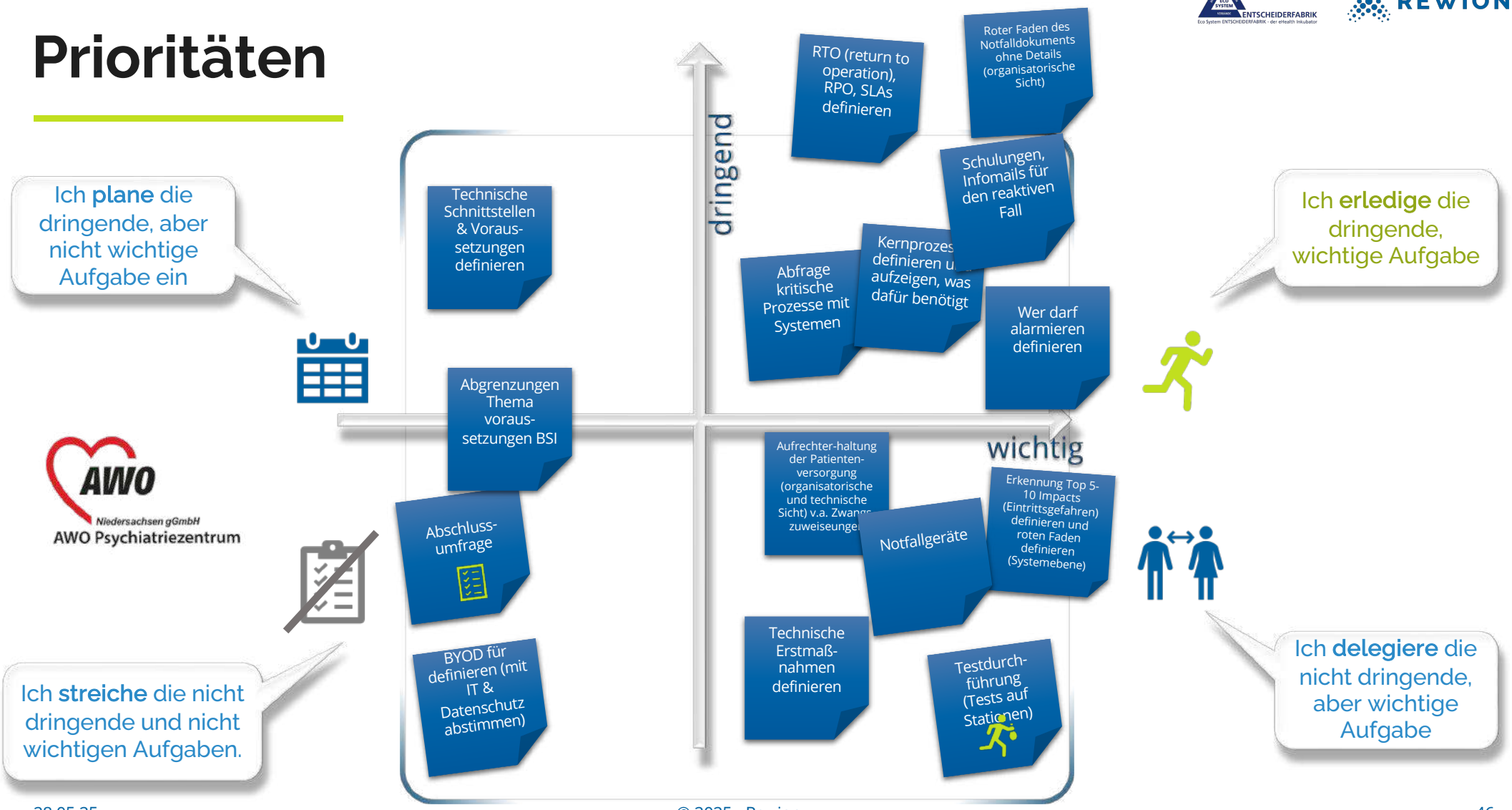
© 2025 - Rewion

Was wollen wir bis Dezember erreichen?



© 2025 - Rewion

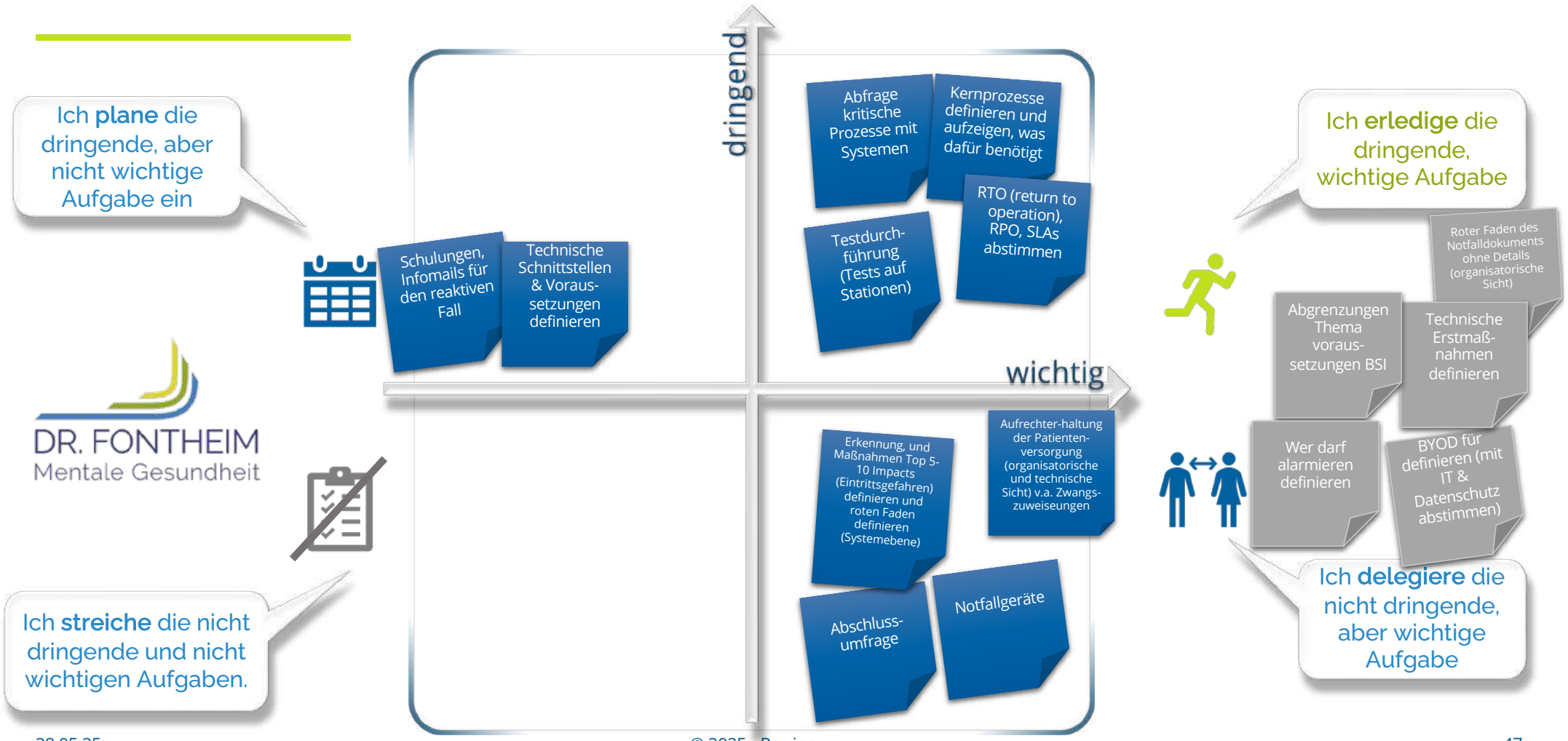
Prioritäten



AWO Niedersachsen gGmbH
AWO Psychiatriezentrum

© 2025 - Rewion

Prioritäten



© 2025 - Rewion

Fragen!?

© 2025 - Rewion

Ablaufplan Praxistest

© 2025 - Rewion

SWOT Analyse des Incident Plans

- Text
- Text

- Text
- Text

- Text
- Text

- Text
- Text

© 2025 - Rewion

Referenzen

© 2025 - Rewion

Partner

© 2025 - Rewion

We level **IT** up.

Kontaktieren Sie uns .

Website besuchen!

REWION

+49 7144 160 980

www.rewion.com

info@rewion.com

Besuchen Sie unseren Blog

© 2025 - Rewion

REWION

Dr. Larissa Hütter.

Manager Digital Health
IT Consultant

+49 160 92126810
larissa.huetter@rewion.com
www.rewion.com

Auf LinkedIn vernetzen.

Termin vereinbaren

REWION

Julian Steil .

IT Security Consultant

+49 171 1906728

julian.steil@rewion.com

www.rewion.com

Hier einen Termin vereinbaren

REWION

David Morva.

Manager Datenschutz & Security
Zertifizierter Berater im Datenschutzrecht (FernUniversität in Hagen)

+49 1511 052 7687
david.morva@rewion.com
www.rewion.com

Hier einen Termin vereinbaren

REWION

Tim Szostakowski.

IT-Consultant

+49 170 249 1192

Tim.Szostakowski@rewion.com

www.rewion.com

Hier einen Termin vereinbaren

Abteilungen

DR. FONTHEIM
Mentale Gesundheit

01 IT
- IT Admin
- IT Mitarbeiter

02 Verwaltung
- Personaler
- Controller
- Rechnungswesen
- GF
- PMSC (Projektmanagement)
- Einkauf
- Kommunikation
- Recht

03 Medizinisches Personal
- ÄrztInnen
- Pflegende
- Stationsleitende
- Pflegedirektion
- Chefärzte/Oberärzte

04 Labor
- Laborleitung
- Labormitarbeitende
- Steri

05 Unterstützung
- Transport
- Sicherheitsdienst
- Küche
- Technik
- Studienassistenten
- Medizintechnik
- Lager

06 Externe
- Azubis
- Praktikanten
- Dienstleister
- Kooperationskliniken

07 Forschung
- Forschungsleitung
- Forschungsmitarbeiter
- Gastwissenschaftler

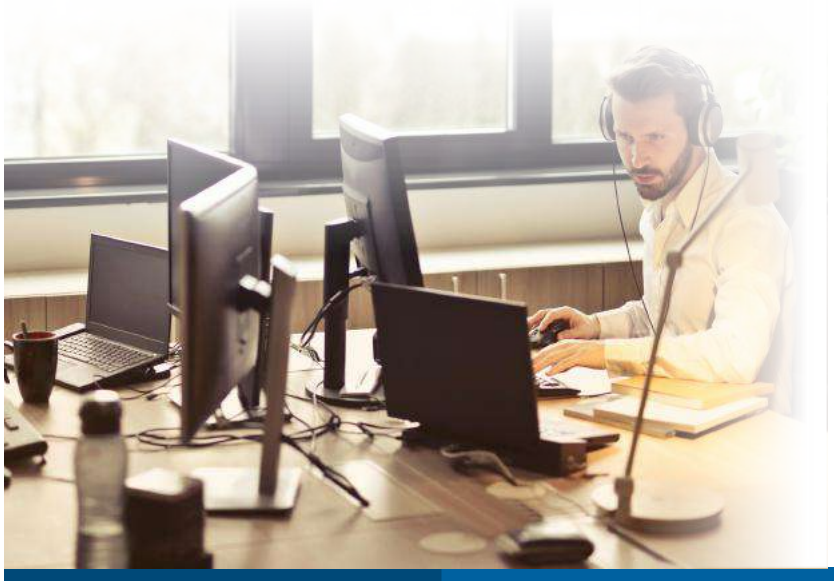
© 2025 - Rewion

Eingesetzte IT: IT-Abteilung

01

IT

- IT Admin
- IT Mitarbeiter



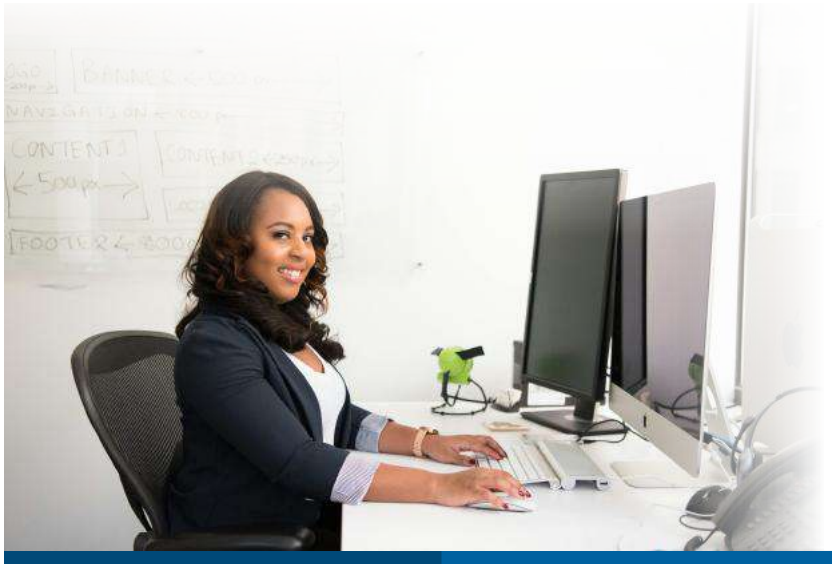
	PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01	Service Desk	Freshdesk, TeamViewer, Intune	Support per Telefon, Papierformular für Meldungen	3
02	Benutzerverwaltung	AD, Intune	Manuelle Zugangskontrolle	
03	Gerätemanagement	Endpoint Manager		
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				

© 2025 - Rewion

Eingesetzte IT: Verwaltung

02 Verwaltung

- Personaler
- Controller
- Rechnungswesen
- GF
- Projektmanagement
- Einkauf
- Kommunikation
- Recht



PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			

© 2025 - Rewion

Eingesetzte IT : Medizinisches Personal

03

Medizinisches Personal

- ÄrztInnen
- Pflegende
- Stationsleitende
- Pflegedirektion
- Chefärzte/Oberärzte

	PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01	Kommunikation & E-Mail			
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				

© 2025 - Rewion

Eingesetzte IT: Labor

04

Labor

- Laborleitung
- Labormitarbeitende
- Steri

	PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01				
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				

© 2025 - Rewion

Eingesetzte IT: Unterstützende Abteilungen

05

Unterstützung

- Transport
- Sicherheitsdienst
- Küche
- Technik
- Studienassistenten
- Medizintechnik
- Lager

PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			

© 2025 - Rewion

Eingesetzte IT: Externe

06

Externe

- Azubis
- Praktikanten
- Dienstleister
- Kooperationskliniken

PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			

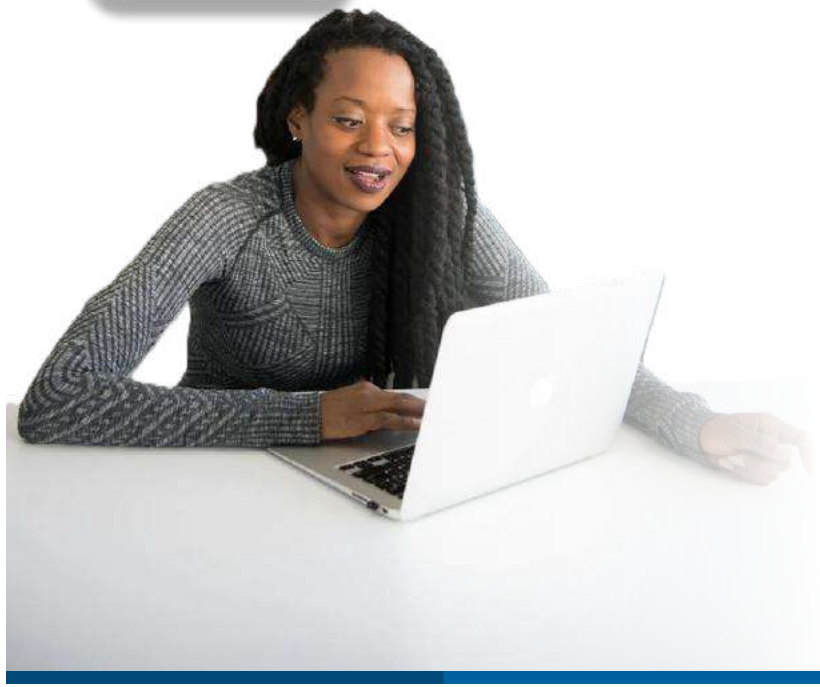
© 2025 - Rewion

Eingesetzte IT: Forschung

07

Forschung

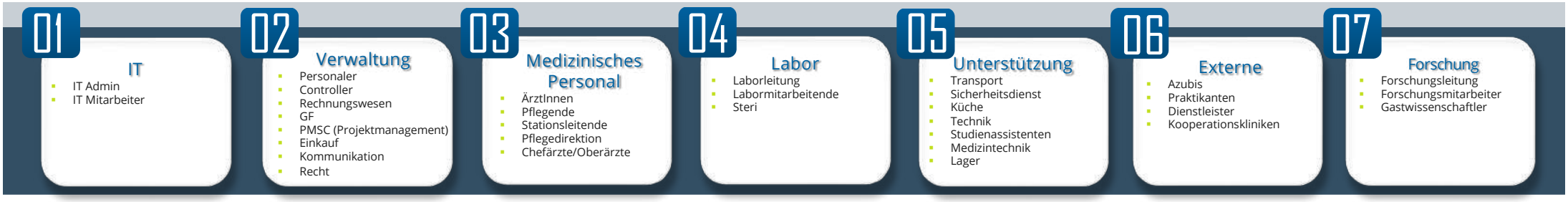
- Forschungsleitung
- Forschungsmitarbeiter
- Gastwissenschaftler



PROZESS / AUFGABE	SOFTWARE	WORKAROUND	PRIO
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			

© 2025 - Rewion

Aufteilung eingesetzte IT Arbeitsphase



© 2025 - Rewion