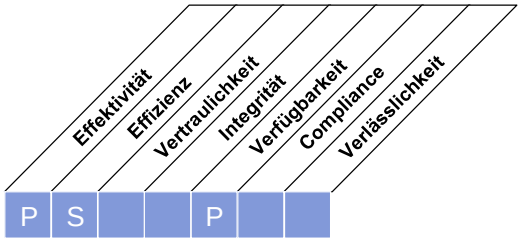
HIGH-LEVEL CONTROL OBJECTIVE

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Die Notwendigkeit, IT-Services kontinuierlich anzubieten, erfordert die Entwicklung, Aufrechterhaltung und den Test von IT-Kontinuitätsplänen, ausgelagerte Aufbewahrung von Backup und das regelmäßige Training des Notfallvorsorgeplans. Ein wirksamer Prozess für kontinuierliche Services minimiert die Wahrscheinlichkeit von bedeutenden Unterbrechungen von IT-Services und deren Auswirkung auf wesentliche Unternehmensfunktionen und -prozesse.



Kontrolle über den IT-Prozess,

Ensure Continuous Service (*Stelle den kontinuierlichen Betrieb sicher*)

der die Anforderung des Unternehmens an die IT bezüglich

der Sicherstellung einer minimalen Auswirkung auf die Geschäftstätigkeit im Falle einer Unterbrechung der IT-Services

durch die Konzentration auf

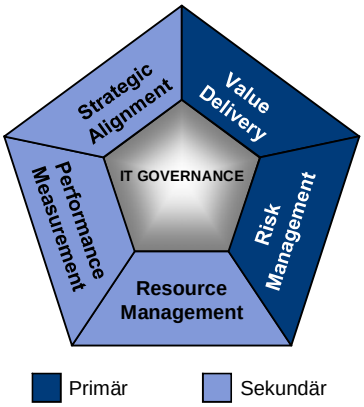
die Integration von Ausfallssicherheit in automatisierte Lösungen und die Entwicklung, Wartung und das Testen von IT-Kontinuitätsplänen, *zufrieden stellt,*

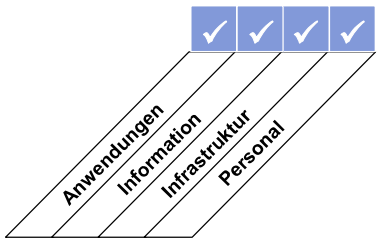
wird erreicht durch

- Entwicklung und Wartung (Verbesserung) einer IT-Notfallplanung
- Schulungen über und Tests von IT-Notfallplänen
- Aufbewahrung von Kopien der Notfallpläne und Daten an einem entfernten Standort

und gemessen durch

- Anzahl verlorener Stunden pro User und Monat aufgrund von ungeplanten Ausfällen
- Anzahl von geschäftskritischen, auf die IT angewiesenen Prozessen, die durch die IT-Notfallplanung nicht abgedeckt werden





DETAILLIERTE CONTROL OBJECTIVES

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

DS4.1 IT Continuity Framework (Framework für IT-Kontinuität)
Entwickle ein Framework für IT-Kontinuität zur Unterstützung eines unternehmensweiten Management der Geschäftskontinuität durch einen konsistenten Prozess. Das Ziel des Frameworks ist die Unterstützung bei der Bestimmung der notwendigen Ausfallssicherheit der Infrastruktur und das Vorantreiben der Entwicklung von Wiederanlauf- und IT-Kontinuitätsplänen (engl.: *disaster recovery and IT contingency plans*). Das Framework sollte die Organisationsstruktur für Kontinuitätsmanagement behandeln, mit den Rollen, Aufgaben und Verantwortlichkeiten von internen und externen Dienstleistern, ihrem Management und ihren Kunden, und die Rollen und Strukturen für Dokumentation, Test und Ausführung der Wiederanlauf- und IT-Kontinuitätsplänen. Der Plan sollte Einzelheiten wie die Identifikation kritischer Ressourcen, das Monitoring und Reporting der Verfügbarkeit kritischer Ressourcen, alternative Verarbeitung und die Grundprinzipien für Backup und Wiederherstellung umfassen.

DS4.2 IT Continuity Plans (IT-Kontinuitätspläne)
Entwickle basierend auf dem Framework IT-Kontinuitätspläne, die auf die Reduktion der Auswirkungen einer wesentlichen Unterbrechung auf die Schlüssel-Geschäftsfunktionen und -Prozesse ausgelegt sind. Die Pläne sollten die Anforderungen für Ausfallsicherheit, alternative Verarbeitung und Wiederherstellungstauglichkeit für alle kritischen IT-Services behandeln. Sie sollten auch Gebrauchsanleitungen, Rollen und Verantwortlichkeiten, Verfahren, Kommunikationsprozesse und das Testvorgehen abdecken.

DS4.3 Critical IT Resources (Kritische IT-Ressourcen)
Lenke die Aufmerksamkeit auf die im IT-Kontinuitätsplan als am kritischsten definierten Elemente, um Ausfallsicherheit einzubauen und um Prioritäten für den Wiederanlauf festzulegen. Vermeide die Ablenkung der Wiederherstellung weniger kritischer Elemente und stelle Reaktion und Wiederanlauf entsprechend den priorisierten Unternehmensbedürfnissen sicher, unter Wahrung der Kosten auf einem akzeptablen Niveau gehalten werden und der Einhaltung regulatorischer und vertraglicher Anforderungen. Beachte Anforderungen für Ausfallsicherheit, Reaktion und Wiederherstellung für verschiedene Abstufungen, zB eine bis vier Stunden, vier bis 24 Stunden, mehr als 24 Stunden und kritische geschäftliche Betriebszeiten.

DS4.4 Maintenance of the IT Continuity Plan (Wartung des IT-Kontinuitätsplans)
Unterstütze das IT-Management bei der Festlegung und Anwendung von Verfahren zur Steuerunv von Changes, um sicherzustellen, dass der IT-Kontinuitätsplan aktuell gehalten wird und fortwährend die aktuellen Geschäftsanforderungen widerspiegelt. Es ist wichtig, dass Veränderungen der Verfahren und Verantwortlichkeiten klar und rechtzeitig kommuniziert werden.

DS4.5 Testing of the IT Continuity Plan (Test des IT-Kontinuitätsplans)
Teste den IT-Kontinuitätsplan regelmäßig, um sicherzustellen, dass alle IT-Systeme wirksam wiederhergestellt werden können, Mängel behandelt werden und die Pläne zweckmäßig bleiben. Dies verlangt eine sorgfältige Vorbereitung, Dokumentation, Berichterstattung über Testergebnisse und – abhängig von den Ergebnissen – die Umsetzung einer Maßnahmenplanung. Erwäge den Umfang für Wiederherstellungstests von einzelnen Anwendungen, integrierten Test-Szenarios bis hin zu durchgehenden Tests und integrierten Anbieter-Tests.

DS4.6 IT Continuity Plan Training (Schulung des IT-Kontinuitätsplans)
Stelle sicher, dass alle betroffenen Parteien regelmäßig Schulungen für die im Ereignis- oder Katastrophenfall anzuwendenden Verfahren sowie ihrer Rollen und Verantwortlichkeiten erhalten. Verifiziere und erweitere Trainings entsprechend den Ergebnissen von Kontinuitätstests.

DS4.7 Distribution of the IT Continuity Plan (Verteilung des IT-Kontinuitätsplans)
Stelle sicher, dass eine festgelegte und gesteuerte Verteilungsstrategie besteht, um sicherzustellen, dass die Pläne genau und sicher an geeignete, autorisierte Interessensgruppen verteilt werden und diesen bei Bedarf – zeitlich und örtlich – zur Verfügung stehen. Es sollte darauf geachtet werden, dass die Pläne für alle Katastrophenszenarien verfügbar gemacht werden.

DS4.8 IT-Services Recovery and Resumption (Wiederherstellung und Wiederanlauf von IT-Services)
Plane die Aktionen für den Zeitraum, während die IT wiederhergestellt und die Services wieder aufgenommen werden. Dies kann die Aktivierung von Ausweichsstandorten, die Inbetriebnahme der alternativen Verarbeitung, die Kommunikation mit Kunden und Stakeholdern, Wiederanlaufverfahren etc beinhalten. Stelle sicher, dass die Fachbereiche die IT-Wiederherstellungszeiten und die notwendigen technologischen Investitionen zur Unterstützung der geschäftlichen Bedürfnisse hinsichtlich Wiederherstellung und Wiederanlauf verstehen.

DS4.9 Offsite Backup Storage (Auslagerung von Backup)
Lagere alle kritischen Backup-Medien, Dokumentationen und andere IT-Ressourcen, welche für den IT-Wiederanlauf und die Geschäftskontinuitätspläne notwendig sind, an einem entfernten Standort aus. Der Inhalt der Backup-Aufbewahrung sollte in

Zusammenarbeit zwischen Geschäftsprozesseignern und den IT-Mitarbeiter bestimmt werden. Die Verwaltung der externen Lagereinrichtung sollte dem Datenklassifikationsschema und Unternehmenspraktiken für Medienlagerung folgen. Das IT-Management sollte sicherstellen, dass die Vorkehrungen für Auslagerung periodisch (mindestens jährlich) nach ihrem Inhalt, dem umgebungsbezogenen Schutz und der Sicherheit beurteilt werden. Stelle die Kompatibilität von Hardware und Software sicher, um die archivierten Daten wiederherzustellen, periodisch zu testen und archivierte Daten aufzufrischen.

DS4.10 Post-resumption Review (Review nach dem Wiederanlauf)
Bestimme nach erfolgreichem Wiederanlauf der IT-Funktionen nach einem Unglück, ob das IT-Management Verfahren für die Beurteilung der Angemessenheit der Pläne und für deren dementsprechende Überarbeitung etabliert hat.

MANAGEMENT GUIDELINES

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Von	Inputs
PO2	Klassifizierte Daten
PO9	Risikobewertung
AI2	Verfügbarkeits-, Kontinuitäts- und Recovery-Spezifikation
AI4	Benutzer-, Betriebs-, Support-, technische und administrative Handbücher
DS1	SLAs und OLAs

Outputs	Nach						
Ergebnisse Contingency-Tests	PO9						
Incident- und Katastrophen-Schwellwerte	DS8						
Kritikalität von IT-Configuration Items	DS9						
Plan zur Lagerung und Schutz von Backups	DS11	DS13					
Service-Anforderung für Notfälle (inkl. Rollen und Verantwortlichkeiten)	DS1	DS2					

RACI-CHART*

Aktivitäten \ Funktionen	CEO	CFO	Business Executive	CIO	Geschäftsprozesseigner	Leitung Betrieb	Chief Architect	Leitung Entwicklung	Leitung IT-Administration	Projektbüro	Compliance, Audit, Risk und Security
Entwickle ein Framework für die IT-Kontinuität		C	C	A	C	R	R	R	C	C	R
Führe eine Business-Impact-Analyse und eine Risikobeurteilung durch		C	C	C	C	A/R	C	C	C	C	C
Entwickle und unterhalte IT-Kontinuitätspläne	I	C	C			A/R	C	C	C	C	C
Identifiziere und kategorisiere IT-Ressourcen nach deren Wiederherstellungszielen				C		A/R		C	I	C	I
Definiere und wende Änderungskontrollverfahren an, um sicherzustellen, dass der IT-Kontinuitätsplan auf dem neuesten Stand ist				I		A/R		R	R	R	I
Teste regelmäßig den IT-Kontinuitätsplan				I	I	A/R		C	C	I	I
Entwickle einen Folgeplan basierend auf den Testergebnissen				C	I	A/R	C	R	R	R	I
Plane und führe Trainings für den IT-Wiederanlauf durch				I	R	A/R		C	R	I	I
Plane die Wiederherstellung und den Wiederanlauf von IT-Services		I	I	C	C	A/R	C	R	R	R	C
Plane und implementiere Backup-Archivierung und -Sicherung				I		A/R		C	C	I	I
Führe Verfahren für die Durchführung der Reviews nach dem Wiederanlauf ein				C	I	A/R		C	C		C

* RACI steht für **R**esponsible (zuständig), **A**ccountable (verantwortlich), **C**onsulted (konsultiert) und **I**nformed (informiert).

ZIELE UND METRIKEN

Aktivitätsziele

- Entwicklung und Aufrechterhaltung (Verbesserung) einer IT-Notfallplanung
- Schulungen über und Tests von IT-Kontinuitätsplänen
- Aufbewahrung von Kopien der Notfallpläne und Daten an entfernten Standorten

werden gemessen durch

Key Performance Indicators

- Zeitspanne zwischen den Tests von jeglichen Bestandteilen des IT-Kontinuitätsplans
- Schulungsstunden über die IT-Kontinuität pro Jahr und betroffenem IT-Mitarbeiter
- % der kritischen Infrastrukturkomponenten mit automatisierter Verfügbarkeits-überwachung
- Häufigkeit von Reviews des IT-Kontinuitätsplans

treiben

Prozessziele

- Führe einen IT-Kontinuitätsplan ein, der die Kontinuitätspläne der Geschäftsbereiche unterstützt
- Entwickle durchführbare IT-Kontinuitäts-pläne, die getestet und gewartet werden
- Minimiere die Wahrscheinlichkeit einer IT-Service-Unterbrechung

werden gemessen durch

Key Goal Indicators

- % der Verfügbarkeiten, die die SLAs erfüllen
- Anzahl von geschäftskritischen, auf IT angewiesene Prozessen, die durch die IT-Notfallplanung nicht abgedeckt wurde
- % der Tests, die die Zielsetzungen bezüglich Wiederherstellung erreichen
- Häufigkeit der Service-Unterbrechungen bei kritischen Systemen

treiben

IT-Ziele

- Stelle die Verfügbarkeit der IT-Services gemäß den Anforderungen sicher
- Stelle sicher, dass der Einfluss einer IT-Service-Störung oder -Änderung auf das Geschäft minimiert ist
- Stelle sicher, dass IT-Services und Infrastruktur Ausfälle auf Grund von Fehlern, bewussten Angriffen oder Katastrophen standhalten können und ihre Wiederherstellung gewährleistet ist

werden gemessen durch

IT Key Goal Indicators

- Anzahl der verlorenen Stunden pro User und Monat auf Grund von ungeplanten Ausfällen

MATURITY MODEL

DS4 Ensure Continuous Service *(Stelle den kontinuierlichen Betrieb sicher)*

Die Reife des Management des Prozesses *Ensure Continuous Service (Stelle den kontinuierlichen Betrieb sicher)*, der die Geschäftsanforderungen an die IT der Sicherstellung einer minimalen Auswirkung auf die Geschäftstätigkeit im Falle einer Unterbrechung der IT-Services, ist:

0 Non-existent (nicht existent):
Es besteht kein Verständnis für die Risiken, Verletzbarkeiten und Bedrohungen für den IT-Betrieb oder die Auswirkungen eines Ausfalls der IT-Services auf das Unternehmen. Service-Kontinuität wird nicht betrachtet, Aufmerksamkeit des Management zu benötigen.

1 Initial (initial):
Die Verantwortlichkeiten für kontinuierliche Services sind informell und die Kompetenz, die Pflichten auszuüben, ist begrenzt. Das Management erkennt das Risiko bei und die Notwendigkeit für kontinuierliche Services. Der Fokus der Aufmerksamkeit des Managements in Bezug auf kontinuierliche Services liegt auf Infrastruktur-Ressourcen und weniger auf IT-Services. Die Anwender setzen provisorische Lösungen als Reaktion auf Service-Incidents ein. Die Reaktionen der IT auf größere Unterbrechungen sind reaktiv und unvorbereitet. Vorgesehene Ausfälle werden eingeplant, um die IT-Anforderungen zu erfüllen, berücksichtigen jedoch keine betrieblichen Anforderungen.

2 Repeatable but Intuitive (wiederholbar aber intuitiv):
Die Verantwortlichkeit für die Gewährleistung kontinuierlicher Services ist zugewiesen. Die Ansätze für die Gewährleistung der Servicekontinuität sind bruchstückhaft. Die Berichterstattung über die Systemverfügbarkeit ist sporadisch, kann unvollständig sein und berücksichtigt die geschäftlichen Auswirkungen nicht. Es besteht kein dokumentierter IT-Kontinuitätsplan, obwohl Verpflichtungen für die kontinuierliche Verfügbarkeit von Services vorhanden sind und die wesentlichen Grundprinzipien bekannt sind. Ein Verzeichnis kritischer Systeme und Komponenten ist vorhanden, ist jedoch nicht unbedingt zuverlässig. Praktiken zur Servicekontinuität entstehen, aber ihr Erfolg hängt von einzelnen Personen ab.

3 Defined (definiert):
Die Verantwortlichkeiten für die Verwaltung der Servicekontinuität sind eindeutig. Die Aufgaben für die Planung und das Testen der Servicekontinuität sind klar festgelegt und zugewiesen. Der IT-Kontinuitätsplan ist dokumentiert und basiert auf der Kritikalität der Systeme und den betrieblichen Auswirkungen. Eine periodische Berichterstattung über Tests der Servicekontinuität ist vorhanden. Einzelne Personen ergreifen die Initiative, um Standards zu befolgen und Schulungen über den Umgang mit bedeutenden Ereignissen oder Katastrophen zu erhalten. Das Management kommuniziert konsistent die Notwendigkeit der Planung für die Gewährleistung kontinuierlicher Services. Hoch-verfügbare Komponenten und System-Redundanz werden eingesetzt. Ein Verzeichnis kritischer Systeme und Komponenten wird gepflegt.

4 Managed and measurable (gemanaged und messbar):
Die Verantwortlichkeiten und Standards für kontinuierliche Services werden durchgesetzt. Die Verantwortung für die Pflege des Servicekontinuitätplans ist festgelegt. Die Pflegeaktivitäten basieren auf den Ergebnissen der Tests der Servicekontinuität, internen Good Practices und den Veränderungen der IT- und Betriebsumgebung. Strukturierte Daten über die Servicekontinuität werden gesammelt, analysiert, gemeldet und danach gehandelt. Formelle und vorgeschriebene Schulungen über die Prozesse für die Servicekontinuität werden bereitgestellt. Good Practices der Systemverfügbarkeit werden konsistent genutzt. Die Praktiken für die Verfügbarkeit und die Planung der Servicekontinuität beeinflussen einander gegenseitig. Unterbrechungen werden klassifiziert und der jeweilige Eskalationspfad ist allen involvierten Personen gut bekannt. Die KGIs und KPIs für die Servicekontinuität wurden entwickelt und vereinbart, werden aber teilweise inkonsistent gemessen.

5 Optimised (optimiert):
Integrierte Prozesse für die Servicekontinuität berücksichtigen Benchmarking und die besten externen Praktiken. Der IT-Kontinuitätsplan ist in die betrieblichen Kontinuitätspläne integriert und wird routinemäßig gepflegt. Die Anforderungen für die Gewährleistung der Servicekontinuität werden durch die Anbieter und wesentlichen Zulieferer gesichert. Globale Tests für die IT-Kontinuitätsplanung werden ausgeführt und die Testergebnisse werden als Eingabe für die Aktualisierung des Plans verwendet. Die Erfassung und Analyse von Daten werden für die kontinuierliche Verbesserung des Prozesses verwendet. Die Verfügbarkeitspraktiken und die Planung der Servicekontinuität sind vollständig abgestimmt. Das Management gewährleistet, dass keine Katastrophe oder ein größeres Ereignis auf Grund eines Single Point of Failure auftritt. Die Praktiken zur Eskalation werden verstanden und uneingeschränkt durchgesetzt. Die KGIs und KPIs für die Erreichung kontinuierlicher Services werden systematisch gemessen. Das Management richtet die Planung der Servicekontinuität in Reaktion auf die KGIs und KPIs aus.