



INTARGIA



Das INTARGIA IT-Kontinuitätsmanagementsystem

IT-Kontinuität mit Augenmaß

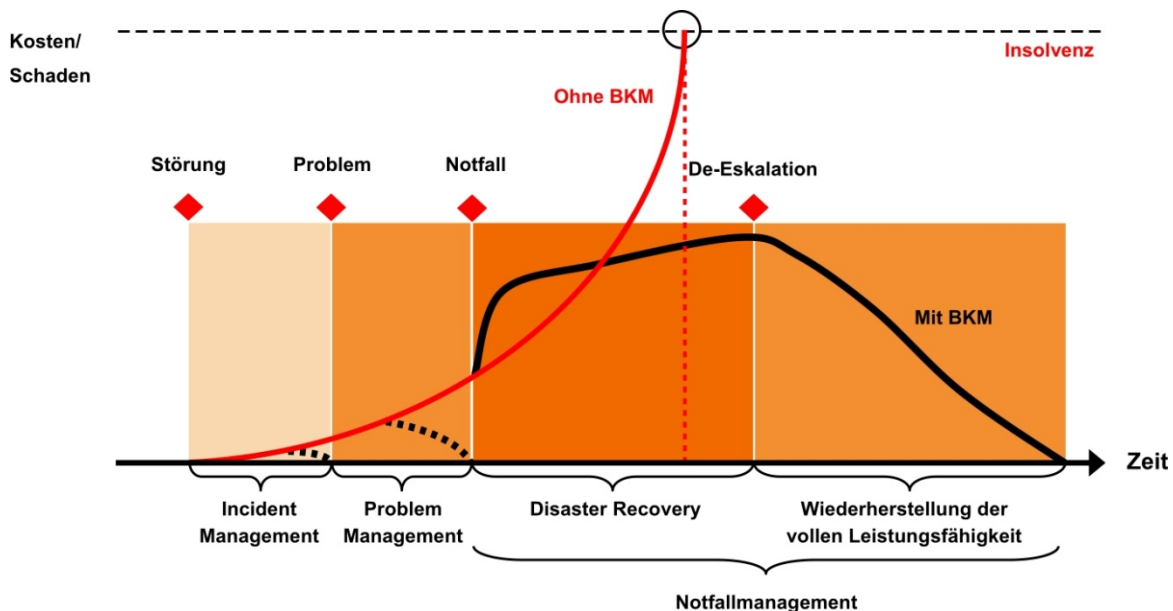
INTARGIA Managementberatung GmbH
Max-Planck-Straße 20
63303 Dreieich

Telefon: +49 (0)6103 / 5086-0
Telefax: +49 (0)6103 / 5086-45
E-Mail: it-risikomanagement@intargia.com
Internet: <http://www.intargia.com>

1. Bedeutung von IT-Kontinuität für das Unternehmen

Unternehmen sind mit einer Vielzahl von Risikofaktoren konfrontiert, welche sich negativ auf die Leistungserbringung des IT-Bereichs auswirken können. Höhere Gewalt, Sabotage, Unfälle sowie technisches und vor allem menschliches Versagen gehören zu den führenden Gründen für den Ausfall von IT-Services und umfassende Datenverluste. Eine 2009 von Forrester und dem Disaster Recovery Journal durchgeführte Studie unter 250 Entscheidern für den Bereich IT-Kontinuität in weltweit tätigen Unternehmen ergab, dass 25% der Befragten innerhalb der letzten fünf Jahre die höchste Bedrohungsstufe ausrufen mussten, um mit einem schweren Zwischenfall umzugehen.

Der professionelle und wirkungsvolle Umgang mit solchen Ausnahmesituationen ist damit entscheidend für den Fortbestand des Unternehmens. Ein umfassendes Kontinuitätsmanagement für die IT-Funktionen eines Unternehmens deckt dabei die volle Bandbreite an Zwischenfällen vom Ausfall einzelner Komponenten bis hin zur umfassenden Katastrophe ab.

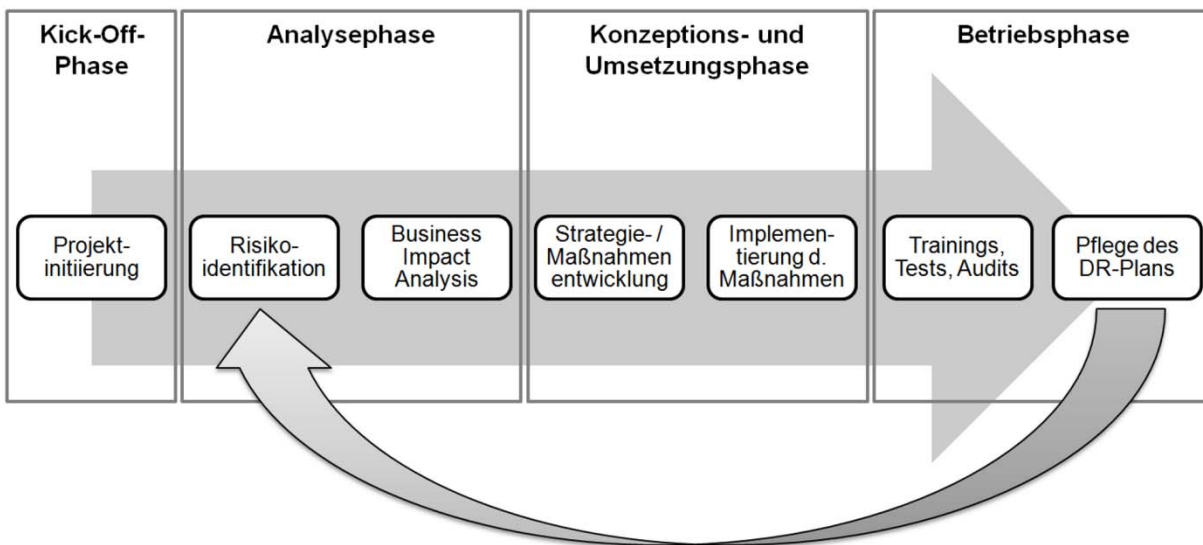


Wie die Grafik zeigt entwickeln sich die Kosten bzw. Schäden, welche durch einen Zwischenfall, der nicht von den Standardfunktionen abgefangen werden kann, exponentiell und können schnell zur Insolvenz des Unternehmens führen, wenn Sie nicht durch ein wirksames Notfallmanagement und zügige Wiederherstellung der vollen Leistungsfähigkeit abgefangen werden.

Dass diese Darstellung der Realität entspricht demonstriert eine 2005 von Cummings, Haag und McCubbrey veröffentlichte Studie. Die Untersuchung umfasst Unternehmen, die einen bedeutenden Datenverlust (z. B. durch eine Katastrophe, technisches bzw. menschliches Versagen oder Sabotage) erlitten hatten, ohne auf einen Kontinuitätsplan zurückgreifen zu können. In 43 % der Fälle wurde der Betrieb nicht wieder aufgenommen, weitere 51 % der Firmen schlossen innerhalb von zwei Jahren. Nur 6 % überlebten langfristig, was einer Mortalitätsrate von 94 % entspricht.

2. Implementierung eines wirksamen IT-Kontinuitätsmanagementsystems

Das Projekt zur Einführung eines IT-Kontinuitätsmanagementsystems kann als lineare Abfolge von Schritten betrachtet werden, welche vor dem Hintergrund der Anpassung an sich ändernde Bedingungen zur Sicherstellung der Wirksamkeit und der kontinuierlichen Verbesserung regelmäßig in weniger umfangreicher Form wiederholt werden. Hieraus ergibt sich ein zyklisch zu durchlaufendes Modell zur kontinuierlichen Verbesserung des IT-Kontinuitätsmanagements, wie in folgender Grafik kurz zusammengefasst:



Kick-Off-Phase: Das Projekt wird initiiert und im gehobenen Management verankert, Mitarbeiter verpflichtet sowie die benötigte Projektorganisation geschaffen.

Analysephase: Das Team beschäftigt sich mit dem Unternehmen und seinem Umfeld, potentielle Risiken für die Aufrechterhaltung des IT-Betriebs werden identifiziert und deren Auswirkungen bei Eintritt auf die verschiedenen Einrichtungen, Systeme und Applikationen analysiert. Existiert bereits ein (IT-)Risikomanagement im Unternehmen wird hier eine Schnittstelle geschaffen, um auf bereits vorliegende Analysen zurückgreifen und diese einbeziehen zu können.

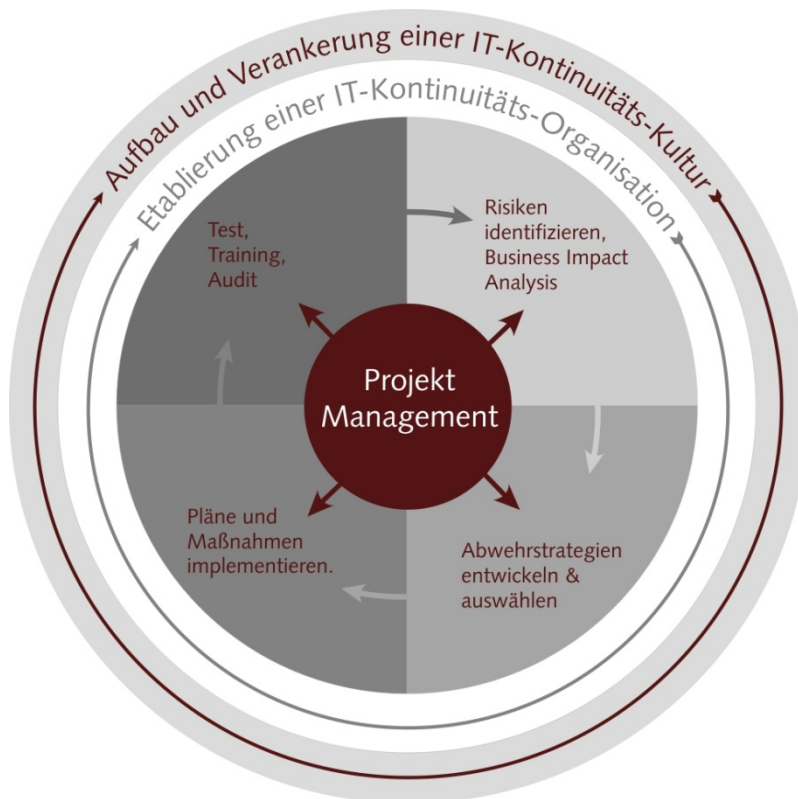
Konzeptions- und Umsetzungsphase: Strategien und Maßnahmen zur Abwehr bzw. Reduzierung bestehender Risiken und deren Auswirkungen bei Eintritt werden entwickelt sowie implementiert. Dies kann z. B. in Form von Schutzmaßnahmen, Notfallplänen oder Aufbau zusätzlicher Ressourcen geschehen.

Betriebsphase: Mitarbeiter werden im Hinblick auf die implementierten Maßnahmen geschult, regelmäßige Tests und Übungen finden statt, das entstandene Managementsystem kann auditiert und zertifiziert werden. Neue interne und externe Entwicklungen und Einflüsse sowie Resultate aus Tests und Audits werden zur Pflege und Erweiterung des Disaster-Recovery-Plans herangezogen. Ausgehend hiervon erfolgt die regelmäßige Wiederholung der drei Hauptphasen.

Die dargestellten Anforderungen an das IT-Kontinuitätsmanagement orientieren sich an anerkannten Standards und Best Practices, konkret BS 25999, BSI 100-4, ISO 27001 und ITIL ITSCM sowie der einschlägigen internationalen Fachliteratur zum Thema.

3. INTARGIA: IT-Kontinuität mit Augenmaß

INTARGIA hat speziell für die Anforderungen des Mittelstands ein pragmatisches IT-Kontinuitätsmanagementsystem entwickelt, welches mit Augenmaß den wirksamen Schutz wichtiger Geschäftsprozesse bei Zwischenfällen sicherstellt und jederzeit die Wirtschaftlichkeit der Maßnahmen sicherstellt.



Von professionellem Projektmanagement begleitet durchlaufen unsere ISO 27001-zertifizierten Berater mit unseren Mandanten die Analysephase, identifizieren Risiken und bewerten den Eintritt dieser auf die Leistungsfähigkeit der Geschäftsprozesse. Darauf aufbauend werden eine IT-Kontinuitätsstrategie sowie passende taktische und operative Maßnahmen entwickelt, welche stets auf Wirtschaftlichkeit und Effektivität geprüft werden. INTARGIA unterstützt mit breiter Erfahrung bei der Implementierung der Maßnahmen und koordiniert in enger Zusammenarbeit mit unseren Mandanten deren Tests, Trainings und Audits. Begleitend wird sichergestellt, dass die notwendigen Aspekte in Organisation und Kultur des Unternehmens verankert werden.

Der Umfang der Leistungen kann je nach Bedarf, Kompetenz und Ressourcensituation auf Seiten des Mandanten angepasst werden und reicht von Begleitung und Coaching der Projektverantwortlichen bis hin zu Steuerung, Management und Dokumentation des Projekts durch ein INTARGIA-Team.