DGI® Deutsche Gesellschaft für Informationssicherheit AG

Management der Durchführung einer Business Impact Analyse (BIA)

- Konzept -

Prüfung und Freigabe

Geprüft am	Durch	Unterschrift
TT.MM.JJJJ		

Freigabe am	Durch	Unterschrift
TT.MM.JJJJ		

Änderungshistorie

Version	Geändert am	Durch	Änderungen
	TT.MM.JJJJ		
	TT.MM.JJJJ		
	TT.MM.JJJJ		

Dokumentensteuerung und Verteilerkreis

A accountable – rechenschaftspflichtig
R responsible – verantwortlich
C consulted - beratend einzubeziehen
I informed - zu informieren

	Erstellung	Prüfung	Freigabe	Verteilung
Arbeitssicherheit				
Aufsichtsrat				
Betriebsrat / Personalrat				
Buchhaltung / Rechnungswesen				
Business Continuity Management				
Compliance				
Datenschutz				
Einkauf				
Fertigung / Produktion				
Finanzen				
Forschung und Entwicklung				
Geschäftsführung				
Gesellschafter				
Hausverwaltung / Facility Management				
Informationssicherheit				
IT				
IT-Sicherheit				
Kundenbetreuung				
Logistik / Materialwirtschaft				
Marketing				
Personal				
Public Relations				
Qualitätssicherung				
Qualitätsmanagement				
Recht				
Risikomanagement				
Verkauf / Vertrieb				
Sonstige				

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Ziel und Zweck

Diese Regelung bestimmt die einzuhaltenden Vorgaben für das Management der Durchführung einer BIA.

Durch die Einhaltung der Vorgaben dieser Regelung soll insbesondere Folgendes sichergestellt werden

- Die Identifikation der wesentlichen Abhängigkeiten und Wechselwirkungen der Geschäftsprozesse, Kernprozesse und Teilprozesse, die für die Organisation relevant sind
- Die Bestimmung der spezifischen Zeitkritikalität von Aktivitäten und Aufgaben, die für die Durchführung der Geschäftsprozesse relevant sind
- Die Steigerung der Transparenz sowie der Effektivität und Effizienz bei der Durchführung einer BIA
- Die Einhaltung gesetzlicher und vertraglicher Anforderungen zur Risikofrüherkennung sowie der Umsetzung von technischen und organisatorischen Maßnahmen (Compliance)
- Die Umsetzung von Maßnahmen für die Aufrechterhaltung bzw. Wiederherstellung der

Verantwortlich für die Überwachung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.

Verantwortlich für die Aufrechterhaltung und Verbesserung der Vorgaben dieser Regelung ist die Rolle/Name der Abteilung.

4 Begriffe

Die den Begriffen zugehörigen Begriffsbestimmungen und Begriffsdefinitionen sind dem Glossar zu entnehmen.

Um die Lesbarkeit dieser Regelung zu erleichtern, wird nachfolgend teilweise

- für „Services, Hardware, Software, Infrastruktur-Komponenten oder technischen Schnittstellen“ der verallgemeinernde Begriff „System“
- für „Teilprozess“ der Begriff „Aktivitäten und Aufgaben“

synonym verwendet.

5 Management der Durchführung einer BIA

5.1 Änderungsmanagement

Bei jeglicher Änderung und Anpassung dieser Regelung sowie bei der Maßnahmenumsetzung der Planung, der Umsetzung, der Überwachung sowie der Aufrechterhaltung und Verbesserung bedarf es einer Beurteilung der möglichen Auswirkungen für den ordnungsgemäßen, sicheren und konformen Geschäftsbetrieb und darf die Integrität des Geschäftsbetriebs nicht gefährden.

Die Prozesse des ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs sind hinsichtlich der Wechselwirkungen eng miteinander verzahnt, weswegen Änderungen und Anpassungen stets unter Berücksichtigung der Auswirkungen evaluiert und durch definierte Freigabeprozesse zur Umsetzung kommen müssen.

Grundsätzlich müssen für jede Umsetzung eines Vorhabens alle Schritte der Planungsphase durchlaufen werden, um die Anforderungen an einen ordnungsgemäßen, sicheren und konformen Geschäftsbetrieb zu gewährleisten.

Die Planungsphase soll die Umsetzung der erforderlichen Maßnahmen für die Einführung dieser Regelung in den nachfolgenden Phasen sicherstellen, was bedingt, dass einzelne Planungsschritte parallel zur Maßnahmenumsetzung der nachfolgenden Phasen umgesetzt werden können.

Die Betrachtung der Wirkzusammenhänge der einzelnen Planungsschritte, mit den nachfolgenden Phasen der Umsetzung, der Überwachung sowie der Aufrechterhaltung und Verbesserung, sollte insbesondere die Auswirkungen, Abhängigkeiten und Wechselwirkungen folgender Prozessschritte berücksichtigen

- Bei den einzelnen Prozessplanungen, Tätigkeiten und Arbeitspaketen
- Bei der Ablaufplanung und Terminierung
- Bei der Kostenplanung und Finanzplanung
- Bei der Ressourcenplanung
- Bei der Planung von Querschnittsprozessen und Querschnittstätigkeiten, wie Schulung und Unterweisung, Information, Kommunikation und Dokumentation

Die Umsetzung der Maßnahmen für die Planung müssen kontinuierlich sowie anlassbezogen aktualisiert, angepasst und verbessert werden.

In der Planungsphase sollten die gängigen Standards, wie die ISO 223xx-Normenfamilie sowie etablierte Methoden des IT Service Management einbezogen werden.

5.2.2 Risikomanagement

Die Planung sollte mögliche Risikofaktoren und Bedrohungslagen berücksichtigen, das heißt es sollten Aktivitäten der Risikoidentifizierung sowie der Risikoabschätzung erfolgen und die Risikolagen, unter Einbeziehung der Risikobehandlungsoptionen, der Eruierung von Restrisiken sowie der Bestimmung der Risikoakzeptanz, gemanagt und gesteuert werden.

Das Risikomanagement sollte, um die strukturierte, vollständige und konforme Durchführung von BIA zu ermöglichen, erforderliche IT Risk Assessments respektive Datenschutzfolgenabschätzungen eruieren sowie deren Durchführung initiieren.

Um das ordnungsgemäße Management bei der Durchführung einer BIA sicherzustellen, sollten mindestens folgende Informationen erhoben und in die Planung einbezogen werden:

- Informationsbeschaffung aus unsicheren oder unzuverlässigen Quellen
- Missbrauch personenbezogener Daten
- Unberechtigte Offenlegung von personenbezogenen Daten
- Fehlende oder unzureichende Sicherstellung der Lesbarkeit von Informationen

5.2.3 Ressourcen

Die erforderlichen Ressourcen zum Zweck der Umsetzung der Maßnahmen für die Einhaltung dieser Regelung, wie für die Erlangung relevanter Informationen, für die Bestimmung des erforderlichen Budgets, des Personals sowie der Prozessstrukturen für die Integration dieser Regelung in die bestehende Aufbau- und Ablauforganisation, sollten vor der Durchführung einer BIA berücksichtigt und bereitgestellt werden.

5.2.4 Beschaffung

Die Auswahl geeigneter Tools sollte durch den jeweiligen Fachbereich in Abstimmung mit den Bereichen Informationssicherheit, Datenschutz und IT-Betrieb erfolgen.

Die Beschaffung geeigneter Tools muss die Anforderungen an einen ordnungsgemäßen, sicheren und konformen Betrieb berücksichtigen. Hierbei müssen Vorgaben der Informationssicherheit und des Datenschutzes, insbesondere die Umsetzung der Maßnahmen gemäß dem Stand der Technik, sowie die Vorgaben des Privacy und Security by Design sowie des Privacy und Security by Default umgesetzt werden.

Bei der Beschaffung muss insbesondere die Gewährleistung des rechtskonformen Einsatzes sowie der fortlaufenden Aktualisierung der Tools sichergestellt sein.

5.2.6 Informationssicherheitsvorfall

Soweit im Rahmen der Durchführung einer BIA ein Informationssicherheitsvorfall auftritt, muss unverzüglich eine Meldung gemäß dem Prozess „Meldung eines Informationssicherheitsvorfalls“ erfolgen.

Potenzielle Informationssicherheitsvorfälle bei der Durchführung einer BIA können Sicherheitslücken und Schwachstellen der für die BIA eingesetzten Tools oder die Weitergabe oder Übermittlung von Informationen an unberechtigte Dritte sein.

5.2.7 Schulung und Unterweisung

Allen Nutzern und Administratoren müssen die erforderlichen Informationen für das Management der Durchführung einer BIA zur Verfügung gestellt, die eigene Verantwortung bei der Einhaltung der