



Finanz Colloquium
Heidelberg

Banken-Times **SPEZIAL**

IT / ORGA / NEUE MEDIEN

Juli & August 2014

Finanz Colloquium Heidelberg

eMail: info@fc-heidelberg.de

Web: www.fc-heidelberg.de

In Zusammenarbeit mit:



Roland Hein
- Geschäftsführer -

bit Informatik GmbH

WIP - Der Wissenschaftspark Trier
Am Wissenschaftspark 32
54296 Trier

Tel.: +49 651 966 29-112

Fax: +49 651 966 29-100

eMail: roland.hein@bit-informatik.de

Web: www.bit-Informatik.de

Sehr geehrte Damen und Herren,

unser Newsletter enthält in dieser Ausgabe Beiträge zur **Business Impact Analyse** sowie zu den **Revisionsberichten von Bank-Dienstleistern**.

Die Inhalte haben wir zusammen mit unserem [Kooperationspartner bit Informatik](#) gestaltet. bit Informatik bietet Standardsoftware zur Umsetzung von gesetzlichen und bankfachlichen Anforderungen an, Schwerpunkte liegen in der Umsetzung von Programmeinsatzverfahren sowie der Vergabe und Kontrolle von IT-Berechtigungen.

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de. Wenn Sie einen eigenen Gastbeitrag verfassen möchten, freuen wir uns ebenfalls über Ihre Nachricht.

Mit besten Grüßen aus Trier und Heidelberg,

Roland Hein, Geschäftsführer, bit Informatik GmbH

Thomas Göhrig, Geschäftsführer, Finanz Colloquium Heidelberg

Business Impact Analyse – Herzstück eines anforderungsgerechten Business Continuity Managements

Die Anforderung zur Implementierung eines wirksamen **Business Continuity Managements (BCM)** als Bestandteil eines ganzheitlichen Risikomanagements ergibt sich für Finanzinstitute direkt aus MaRisk AT 7.3 „Notfallkonzept“. Hier werden generisch die Rahmenbedingungen definiert, deren Erfüllung der Regulator im Rahmen der Umsetzung im Institut erwartet. Geschäftsfortführungs- und Wiederanlaufpläne werden gefordert, wobei erstere auf die Etablierung von Ersatzprozessen für die Fortführung der Geschäftsprozesse und letztere auf die gesteuerte Wiederherstellung des Regelbetriebs nach einem Notfall abzielen.

Wie bei allen anderen Aktivitäten zur Ausgestaltung des Risikomanagements ist auch hier auf gängige Standards abzustellen. Es können mehrere High-Level-Standards herangezogen werden, exemplarisch genannt seien hier ISO22301 (abgeleitet aus dem British Standard BS25999) mit internationalem Geltungsanspruch sowie der BSI Standard 100-4 Notfallmanagement mit eher nationaler Verbreitung.

Von den im Risikomanagement betrachteten Dimensionen Vertraulichkeit, Integrität, Verbindlichkeit und Verfügbarkeit steht beim BCM naturgemäß die Verfügbarkeit im Vordergrund. Um die gebotene Angemessenheit sicherstellen zu können, müssen die Geschäftsprozesse und ihre Relevanz für die Wertschöpfungskette sowie die Anforderungen der Geschäftsprozesseigner an die Verfügbarkeit der eingesetzten IT-Services identifiziert

werden. Hierfür steht als Standard-Methodik die **Business Impact Analyse (BIA)** zur Verfügung.

In der BIA werden die potentiellen Schadenswirkungen ermittelt, die durch den Ausfall von kritischen Geschäftsprozessen entstehen könnten. Die BIA selbst ist als Prozess zu verstehen, der idealtypisch nach dem **Plan-Do-Check-Act (PDCA)** – Modell aufgebaut sein und mindestens jährlich, besser aber nachvollziehbar risikogesteuert in regelmäßigen Intervallen durchgeführt werden sollte.

Folgende Ziele sollen durch den BIA-Prozess erreicht werden:

- Identifikation geschäftskritischer Prozesse, deren Anforderungen sowie deren benötigte Ressourcen.
- Ermittlung der Auswirkungen eines Ausfalls oder einer Unterbrechung von Geschäftsprozessen.
- Identifikation interner und externer Abhängigkeiten für das Funktionieren aller relevanten Prozesse.

Um dies zu erreichen, müssen Prozesse, Verantwortliche und relevante Ansprechpartner in den betroffenen Fach- und Marktbereichen identifiziert werden. Die Bedrohungskategorien (Reputation, monetär, juristisch etc.) müssen definiert und in Bezug auf den betrachteten Risikoraum (Standorte, Produkte, Märkte etc.) abgebildet werden.

Methodisch kann dies – idealerweise initiiert durch den Verantwortlichen für Informationssicherheit / OpRisk oder durch das Management selbst – durch moderierte Workshops oder Interviews erreicht werden. Denkbar sind auch analoge oder digitale Fragebögen, wobei der direkte Austausch mit den Prozessverantwortlichen am effektivsten ist und eine optimale Bindung aller Beteiligten (Awareness) an den Prozess sicherstellt.

Als Ergebnis der ersten Iteration des Prozesses sollten folgende Informationen vorliegen:

- Alle geschäftskritischen Prozesse und deren benötigte Ressourcen (Personal, Services, Daten etc.).
- Die Auswirkungen eines Ausfalls oder einer Unterbrechung eines Geschäftsprozesses.
- Die maximal akzeptable Unterbrechungszeit (Maximum Tolerable Period of Disruption, MTPD) für jeden betrachteten Geschäftsprozess.
- Der angestrebte Zeitraum bis zur Wiederherstellung des Regelbetriebes nach Ausfall (Recovery Time Objective, RTO) der Services pro Geschäftsprozess.
- Zeitpunkt der letzten Sicherung der vom Geschäftsprozess benötigten Daten (Recovery Point Objective, RPO).

Die BIA unterstützt das Management bei Definition und Fortschreibung einer **Strategie für die Notfallvorsorge und -planung**. Auf der Basis dieser Strategie und der Ergebnisse der BIA können die Verantwortlichen im IT-Servicemanagement auf technischer und organisatorischer Ebene geeignete Maßnahmen für die Sicherstellung der geforderten Verfügbarkeiten bzw. Wiederherstellungszeiten definieren und umsetzen. Grundlegende Voraussetzung hierfür ist eine valide Zuordnung der IT-Systeme und -services zu den Geschäftsprozessen.

Eine Iteration des BIA-Prozesses gliedert sich in Konzeptions-, Durchführungs- und Nachbereitungsphase:

In der Konzeptionsphase werden die Schadenskategorien und Betrachtungshorizonte sowie das Risikoakzeptanzniveau des Managements festgelegt bzw. einem Review unterzogen. Daraus resultieren nachvollziehbare und reproduzierbare Kenngrößen zu Schadensbewertung und Kritikalitätseinstufung von Prozessen. Des Weiteren wird die Vorgehensweise zur Erhebung der benötigten Daten festgelegt. Um die Komplexität zu reduzieren, sollten nicht mehr als ca. 10 Prozesse pro Bereich definiert werden.

In der Durchführungsphase wird der Prozess im Rahmen einer Awareness-Maßnahme den beteiligten Stakeholdern vorgestellt. Danach werden die relevanten Informationen mittels der in der Konzeptionsphase festgelegten Methodik (Workshop, Interview etc.) erhoben und erfasst.

Qualitätssicherung und Datenaufbereitung bilden den Fokus der Nachbereitungsphase. Hier werden unter anderem Berichte für das Management erstellt, die die Grundlage für die Fortentwicklung der Notfallstrategie und -planung bilden. Eine anschließende Wirtschaftlichkeitsanalyse stellt die Balance zwischen Anforderungen und Kosten her.

Natürlich muss ein solcher Prozess durch IT-Werkzeuge gestützt werden. Die Spannweite reicht hier von mehr oder minder komplexen Excel-Sheets oder Datenbanken bis hin zu spezialisierten Anwendungen, je nach Art und Umfang der Anforderungen des Instituts. In der Praxis finden sich allerdings – vor allem in kleinen und mittelgroßen Instituten – häufig nicht die notwendigen personellen und organisatorischen Ressourcen, um den skizzierten BIA-Prozess und das BCM idealtypisch umzusetzen. Geschäftsprozesse sind oftmals nicht in einer formal standardisierten Form definiert und dargestellt. Hier empfiehlt sich eine möglichst pragmatische Herangehensweise im Dialog mit den Prozess- und Durchführungsverantwortlichen, die dann in den meisten Fällen eher applikationszentrisch als prozessorientiert ausfallen wird.

Mittel- bis langfristig sollten sich aber **alle Institute** intensiv mit der Aufgabenstellung auseinandersetzen, da leider keine Anpassung der aufsichtsrechtlichen Anforderungen an Institute mit prinzipiell risikoarmem Geschäftsmodell in Sicht zu sein scheint.

PRAXISTIPPS

- Gehen Sie in den Dialog mit den Geschäftsprozessverantwortlichen und überzeugen Sie sie von den möglichen Mehrwerten durch den BIA-Prozess.
- Verschaffen Sie sich nachhaltige Unterstützung durch die Geschäftsführung – ohne diese wird der Prozess nicht dauerhaft funktionieren.
- Ziehen Sie für Planung, Design und initiale Implementierung des Prozesses in Ihrer Organisation spezialisierte externe Unterstützung in Betracht.
- Identifizieren Sie nicht-kritische Bereiche, die keine oder nur geringe Relevanz für die Wertschöpfungskette haben und grenzen Sie diese vom BIA-Prozess ab.

Weiterführende Informationen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf

https://en.wikipedia.org/wiki/Business_impact_analysis

<http://www.iso22301online.org>

Steffen Nagel, CISA, Leiter IT, Frankfurter Volksbank eG

Seminartipp zum Thema:

[Wirksame Notfallprozesse und Wiederanlaufplanung, 12. November 2014, Berlin](#)

Weitere aktuelle Veranstaltungen im 2. Halbjahr 2014:

[IT-Projekte & neuer AT 8.2, 17. November 2014, Düsseldorf](#)

[Grauzone Individuelle Datenverarbeitung \(Excel & Co.\), 18. November 2014, Düsseldorf](#)

[Neu-Produkt-Prozess \(NPP\): Umsetzung & Prüfung, 20. November 2014, Düsseldorf](#)

[Prüfung der Arbeitsplatz- und Unternehmenssicherheit, 26. November 2014, Köln](#)

[Jahrestreffen IT-Revision, 27.-28. November 2014, Köln](#)

Fachbeiträge auf unserem FCH Blog

Auf unserem Blog <http://blog.fc-heidelberg.de/> stellen wir ausgewählte Fachbeiträge unserer Banken-Times und Banken-Times SPEZIAL Newsletter sowie die Praxistipps der Zeitschriften-Artikel kostenlos zur Verfügung.

Übersicht der interessanten und aktuellen Fachbeiträge auf unserem Blog:

[Zusammenarbeit von Aufsichtsrat und Interner Revision in Kreditinstituten](#)

[Wie viele halbe Revisoren wollen Sie sich leisten?](#)

[Aufbau eines Soll-Rollenkonzepts](#)

[Datengetriebene Dokumentation und Prozesse von Programmeinsatzverfahren](#)

Überprüfung Revisionsberichte Dienstleister

Dienstleister, die für Unternehmen der Kreditwirtschaft tätig sind, müssen aufgrund der Anforderungen der MaRisk AT 9 in regelmäßigen Abständen, mindestens jedoch einmal im Jahr, ihren Kunden Revisionsberichte über ihren mit den Kreditinstituten getroffenen Outsourcing Verträgen zusenden. Somit sind Dienstleister den Kreditinstituten rechenschaftspflichtig, heißt aktuelle und vollständige Berichte über alle IT-Risiken des eigenen Hauses die für das Kreditinstitut relevant sind, vorzulegen.

Da keine genormten Standard Revisionsberichte existieren, bestehen die Herausforderungen sowohl für den Dienstleister als auch für das Kreditinstitut einen „Kundenrevisionsbericht“ zu erstellen, der den Anforderungen eines Institutes genügt. Somit muss aus Sicht des Kreditinstitutes schon in der Phase der Sondierung einer möglichen Auslagerung das Thema Aufbau und Inhalt eines Revisionsberichtes in die Verhandlungen mit den Dienstleister mit aufgenommen werden.

Der Revisionsbericht sollte zu Beginn den Dienstleister beschreiben, heißt das Organigramm abbilden und erläutern. Damit kann das Kreditinstitut Einblick nehmen, wie zum Beispiel die Entwicklungsabteilung oder die Hotline personell aufgestellt sind. Im Revisionskopf sollten dann auch zentrale Personen des Dienstleisters wie zum Beispiel den zuständigen Risikomanager, Geschäftsführung, IT-Sicherheitsbeauftragten, Revision, etc. namentlich aufgeführt werden.

Der Dienstleister der oftmals für mehrere Institute tätig ist, sollte zuerst alle möglichen Risiken seines Unternehmens erfassen und gegebenenfalls nach dem Bankensäulensystem in S-Finanzgruppe, Genossenschaftsverbund oder Privatbanken klassifizieren bzw. gewichten, da hier im Detail doch einige Unterschiede existieren. Sind alle Risiken vom Dienstleister erfasst, muss in einem weiteren Schritt geprüft werden, welche Risiken in den Revisionsbericht mit aufgenommen werden müssen und welche nicht. Sinnvollerweise kann dies hier in einem Abstimmungsgespräch zwischen Dienstleister und dem Kunden/Kreditinstitut erfolgen. Zu jedem Risiko sollte der Dienstleister dokumentieren, welche Maßnahmen er bei Eintritt des Risikos unternehmen wird, welche gegebenenfalls schon unternommen wurden um das Risiko zu minimieren und welche Eskalationsstufen, zum Beispiel Information an das eigene Management automatisch bei Eintritt anlaufen. Hier kann auch vereinbart werden, dass der Kunde, d.h. das Kreditinstitut, in die Abläufe der Eskalation eingebunden wird.

Sinnvoll ist es die Risiken in Kategorien wie Finanzielle Ausstattung, Produktion, Personal, DV-Infrastruktur, etc. zu gruppieren. Diese definierten Kategorien wiederum enthalten dann Unterkategorien wie zum Beispiel bei der Kategorie Personal die Punkte KnowHow, Weiterbildung, Fluktuation, etc. des eigenen Personals oder unter der Kategorie DV-Infrastruktur die Aspekte Telekommunikation, Datensicherheit, Netzwerk, etc. Auf der dritten Ebene folgen dann die einzelnen Risiken zum Beispiel Ausfall der Telefonanlage unter der Kategorie DV-Infrastruktur/Telekommunikation.

In einem weiteren Schritt erfolgt die Bewertung der Risiken. Mögliche Parameter können hier die Verwendung einer Ampelfunktion (rot, gelb, grün) oder Parameter wie zum Beispiel hoch, mittel oder gering herangezogen werden.

Als Gesamtergebnis enthält der Revisionsbericht die Informationen über mögliche Risikofelder, der Risiken gruppiert nach Bereichen, ihre Bewertung sowie Maßnahmen, die der Dienstleister schon in Angriff genommen hat, um die Risiken zu minimieren.

Zur Weitergabe und Bericht an das Management der Bank sollte der Dienstleister prüfen, inwieweit die weichen Informationen des Revisionsberichtes in einem Summary Report auf einer Seite aufbereitet und zusammengefasst werden können. Ideal wäre auch eine Funktion, vergangene Revisionsberichte mit dem aktuellen zu vergleichen, um Veränderungen direkt zu erkennen.

Aus Sicht des Kreditinstitutes ist der Revisionsbericht ein Dokument eingebunden in einer Mappe bestehend aus dem Outsourcing Vertrag, der Risikoanalyse des Outsourcing Vertrages, der jährlich stattfindenden Beurteilungsgespräche mit dem Dienstleister, eventuell angefallene und damit dokumentierte Vertragsverletzungen und der Service Level Parameter, die mit dem Dienstleister vereinbart wurden.

Roland Hein, Geschäftsführer, bit Informatik GmbH

Seminartipps zum Thema:

[Operatives Dienstleistermanagement, 10. November 2014, Berlin](#)

[Prüfung Dienstleistermanagement, 11. November 2014, Berlin](#)

Aktuelle Fachliteratur:

[Bearbeitungs- und Prüfungsleitfaden Datenschutz & IT-Sicherheit 3. Auflage](#)

[Prüfung IT im Fokus von MaRisk und Bundesbank](#)

[Bearbeitungs- und Prüfungsleitfaden Social Media](#)

[MaRisk-Prozessänderungen und Projektmanagement](#)

Hier können Sie unseren aktuellen [Buchkatalog](#) für das 2. Halbjahr 2014 herunterladen.

Checklisten-Download und Banken-Times Archiv online

Für alle Bücher aus der Reihe unserer „**Bearbeitungs- und Prüfungsleitfäden**“ stellen wir die enthaltenen Checklisten auf unserer Webseite unter „[Mein FCH](#)“ als veränderbare WORD-Datei zum Download zur Verfügung. Den Zugangscode finden Sie im Buch.

Zusätzlich stehen im Bereich „Mein FCH“ auch alle erschienenen **Banken-Times** und Banken-Times SPEZIAL Ausgaben als PDF zum Download bereit.

Impressum

Finanz Colloquium Heidelberg GmbH – Plöck 32a – 69117 Heidelberg

VisdP: Thomas Göhrig

Telefon: 0 62 21 / 99 89 8-0 - Telefax: 0 62 21 / 99 89 8-99

E-Mail: Info@FC-Heidelberg.de – Internet: www.FC-Heidelberg.de

Geschäftsführer:

Dr. Christian Göbes, Frank Sator, Dr. Patrick Rösler, Marcus Michel, Michael Helfer, Thomas Göhrig

Sitz der Gesellschaft ist Heidelberg, Amtsgericht Mannheim, HRB Nr. 335598

Zur Abbestellung dieses Newsletters oder zur Aufnahme von Kollegen/Kolleginnen in den Verteiler senden Sie uns bitte eine eMail an btspezial@fc-heidelberg.de.