# MUSTERLÖSUNG, H.P. KÖNIGS, SPRINGER VIEWEG „IT-RISIKOMANAGEMENT MIT SYSTEM“, 5. AUFLAGE

## KONTROLLFRAGEN UND AUFGABEN ZU KAPITEL 13

**Lösung zu Frage 1**

Der vorrangige Zweck des Geschäftskontinuitätsplans ist die nachhaltige Aufrechterhaltung der Geschäftsfunktionen eines Unternehmens, falls ein Ereignis eintritt, bei dem die Fortführung der Geschäftsfunktionen in erheblichem Masse beeinträchtigt oder gefährdet werden. Somit dient der Geschäftskontinuitätsplan der Planung, Dokumentation und Verifikation von Aktivitäten und Massnahmen zur raschen Fortsetzung der Geschäfte unter möglichst geringen, akzeptablen Schadensauswirkungen beim Eintreten einer erheblichen Störung oder Unterbrechung von Geschäftsfunktionen oder beim Eintreten einer Situation, welche solche Störungen oder Unterbrechungen zur Folge haben kann.

**Lösung zu Frage 2**

Für den Fall, dass infolge einer Katastrophe das Geschäft an einem anderen Ort mit einer anderen Infrastruktur und anderen Ressourcen weitergeführt werden soll, wird manchmal neben dem Geschäftskontinuitäts-Plan ein separater sogenannter „Geschäftswiederer-langungs-Plan“ (Business Recovery Plan) erstellt und unterhalten. Im Gegensatz zum Geschäftskontinuitäts-Plan, welcher alle Vorkehrungen und Massnahmen für eine nachhaltige Aufrechterhaltung der Geschäftsfunktionen eines Unternehmens enthält, ist dieser Plan lediglich auf die Wiedererlangung von gleichen oder annähernd gleichen Bedingungen zur Geschäftsfortführung nach einem Katastrophenereignis fokussiert. Der Plan ist somit Teil des Geschäftskontinuitäts-Plan und oft in diesen integriert.

**Lösung zu Frage 3**

Der **Ausweichplan** kommt dann zur Ausführung, wenn durch ein katastrophales Ereignis, wie Brand im Hauptgebäude, die Geschäftsprozesse mit ihren Support- und Infrastruktur-Einrichtungen (z. B. IT-Systeme, Rechenzentrumsgebäude) über eine längere Zeitdauer ganz aus und/oder nicht in ihrer normalen Funktion betrieben werden können. Somit beschreibt der Plan beispielsweise, wie der Betrieb auf eine Ausweich-Infrastruktur ausgelagert und von dort betrieben werden soll. Der **IT-Notfall-Plan** hingegen adressiert in erster Linie Störungen und Ausfälle von solchen IT-Systemen und Supportprozessen, die normalerweise sowohl der direkten als auch der indirekten Unterstützung der Geschäftsprozesse dienen. Die verschiedenen Supportprozesse und IT-Systeme werden dabei entsprechend ihrem Einfluss auf die kritischen Geschäftsprozesse und deren Priorisierung in den IT-Notfall-Plan einbezogen. Der IT-Notfall-Plan ist deshalb wie der Ausweichplan eng mit dem Geschäftskontinuitäts-Plan verknüpft. Er enthält neben den Massnahmen zur Wiedererlangung und -herstellung der IT-Funktionen auch die allenfalls notwendigen IT-

Support-Massnahmen zur Aufrechterhaltung der Geschäftsprozesse während einer Störung oder einem Ausfall. Im Gegensatz zum Ausweichplan werden im IT-Notfall-Plan auch die für die Geschäftskontinuität ohne Schadensfolge verlaufenden Problemsituationen sowie die Ereignisse mit (noch) geringen Schadensauswirkungen behandelt. Für „unerwartete" und „katastrophale" Ereignisse, die mit physischen Zerstörungen der IT-Infrastruktur einhergehen, wird der IT-Notfall-Plan mit dem Ausweichplan verknüpft.

**Lösung zu Frage 4**

Das Top-Management eines Unternehmens stellt sein Commitment zu einem BCMS unter Beweis, u. a. durch:

- Erstellung einer Geschäftskontinuitäts-Policy (z. B. Genehmigung und Erlass durch den Verwaltungsrat); Kommunikation an die Belegschaft von wichtigen das BMCS betreffenden Festlegungen oder über eingetretene Ereignisse;
- Schaffung von Rollen, Verantwortlichkeiten und Kompetenzen sowie Nomination einer oder mehrerer Personen mit den notwendigen Kompetenzen für Leitung, Aufbau und Betrieb des BCMS;
- Vergewisserung, dass adäquate Ziele und Pläne eingesetzt sind und periodische Überprüfung, ob die notwendigen Pläne aktualisiert werden.
- Einbezug der BCMS-Management-Reviews in die Traktanden der reguläre Führungs- und Review-Sitzungen;
- Mitwirkung bei der Festlegung der Test- und Übungsprogramme und Teilnahme in bestimmten Test- und Übungsabschnitten.

**Lösung zu Frage 5**

Die Geschäfts-Impact-Analyse (Business Impact Analyse, BIA) widmet sich vor allem den folgenden Aufgaben:

- Identifikation der kritischen Geschäftsfunktionen, Prozesse und Aktivitäten, welche die wichtigen Geschäftsziele (Key Goals) zur Lieferung von Produkten und/oder Dienstleistungen unterstützen;
- Aufzeigen der Abhängigkeiten und unterstützenden Ressourcen für die kritischen Geschäftsfunktionen, Prozesse und Aktivitäten;
- Bestimmung von Art und Höhe der Geschäfts-Impacts (finanziell, operationell und strategisch) für den Ausfall einer jeden kritischen Geschäftsfunktion;
- Bestimmung der maximal akzeptierbaren Ausfalldauer (MTPD = Maximum Tolerable Period of Disruption oder auch MAO = Maximum Acceptable Outage);
- Ausgehend von ermittelten MTPD-Zeiten und der analysierten Impacts, für jede kritische Geschäftsfunktion (resp. jeden kritischen Geschäftsprozess) die **maximalen Sollzeiten sowie die Prioritäten** für Wiederanlauf und Wiederherstellung sowie die

Zeiten der minimal notwendigen Notbetriebsdauer und der maximal tolerierbaren Notbetriebsdauer festlegen;

- Minimaler „Service Level“ (MBCO = Minimum Business Continuity Objective) für jede kritische Geschäftsfunktion definieren; dabei muss nicht nur die Aufrechterhaltung einer minimalen Produktivität und Verfügbarkeit, sondern auch der durch den Notbetrieb sich allenfalls ergebende Rückstand betrachtet werden.

**Lösung zu Frage 6**

Das Risiko-Assessment im Geschäftskontinuitäts-Prozess erfordert u.a die folgenden Aktivitäten:

- Spezifische Analysen des Unternehmens und seines Umfeldes bezüglich möglicher Bedrohungen der Kontinuität (z. B. Energie-Engpässe, Telekom-Unterbrechungen, Sabotagen, Seuchen, Feuer);
- Analyse der Aktivitäten, Prozesse, Systeme, Informationen, Personal, involvierte Anspruchsgruppen und andere Ressourcen und Akteure auf inhärente Verletzlichkeiten und Abhängigkeiten;
- Aufsuchen der Verletzlichkeiten, Schwachstellen und Abhängigkeiten in den kritischen Geschäftsprozessen;
- Untersuchung der Abhängigkeit der Geschäfts-Prozesse von den Support-Prozessen (z. B. IT-Prozesse, Liefer- und Transportprozesse) und deren Verletzlichkeiten;
- Untersuchung der bereits vorhandenen Umgehungsmassnahmen Workarounds).

**Lösung zu Frage 7**

Das Kommunikationskonzept im Geschäftskontinuitäts-Prozess beinhaltet u.a. folgende Aktivitäten und Festlegungen:

- Die im Notfall (resp. Katastrophen- oder Störfall) zu erreichenden Informationsempfänger:
  - — Mitarbeiter und allenfalls ihre Familien-Mitglieder;
  - — Aktionäre;
  - — Verwaltungsratsmitglieder;
  - — Medien (z. B. Presse, Radio und Fernsehen);
  - — Behörden, kommunale und staatliche Stellen;
  - — Regulatoren;
  - — Kunden, Lieferanten und Vertragspartner;
  - — usw.
- Zusammenstellung und Dokumentation wie und durch wen im Notfall (resp. Katastrophen- oder Störfall) informiert wird (z. B. CEO, Public-Relation-Stelle, Personalverantwortliche, Vorgesetzte);

- Aufführen der Einschränkungen bezüglich Informationsweitergabe (z. B. Bankgeheimnis, Informationenschutz, vertragliche Geheimhaltungsvereinbarungen);
- Bezeichnung der Stellen durch die eine Abgabe von Informationen autorisiert sein muss;
- Informationsart an die verschiedenen Empfänger und Vorbereitung von Muster-Texten an die verschiedenen Informations-Empfänger unter Annahme verschiedener Szenarien;
- Informationskanäle (z. B. Telefon, Anlaufstellen bei Medien, Fax, Hotline, Homepage) und der Kommunikations-Intervalle für die verschiedenen Empfänger.

**Lösung zu Frage 8**

Die Tests dienen dem Auffinden von allfälligen Mängeln und Fehlern in der Logik der Pläne, den Kapazitäten und den Leistungsfähigkeiten der zur Verfügung stehenden Ressourcen (z.B. Systeme, Einrichtungen, Umschalt- und Ausweichprozesse). Dabei sollen die Tests den aus einzelnen Risiko-Szenarien resultierenden Anforderungen unterworfen werden. Aus den gewonnenen Testresultaten können Schlüsse für die Festlegung von wichtigen Parametern (z. B. Auslegung von Noteinrichtungen, Zeitpunkte der Informationensicherungen) sowie der notwendigen Verbesserungen gezogen werden.

**Lösung zu Frage 9**

**Mit Tests** werden die bei einem Störungs-/Ausfall-ereignis im Einsatz befindlichen oder einzusetzenden Ressourcen möglichst realitätsnahe überprüft (z.B. Abschaltung eines bestimmten Systems, Abschaltung von Strom oder Umschaltung auf Backup-Einrichtungen);

Bei **Übungen** werde für nicht real durchführbare Situationen (z.B. Ausfall eines Systems) die entsprechende Situationen durch Vorgabe von fiktiven Ausgangslagen und fiktiven Situationsbeschreibungen simuliert, worauf die Übungsteilnehmenden entsprechende Entscheide, Anordnungen und Aktionen durchzuführen haben (z. B. Evakuations-Übung aufgrund einer fiktiv angenommenen Katastrophe).

Ziele von Übungen in einem Unternehmen mittlerer Grösse können beispielsweise sein:

- Überprüfung des organisatorischen Ablaufes bei der Notfall- und Krisenbewältigung, z.B. schnelle und reibungslose Evakuationen;
- Schaffung eines angemessenen Risiko- und Sicherheitsbewusstseins der Führungspersonen und Mitarbeiter;
- Vertrauensbildung für Anspruchsgruppen, Führungspersonen und Mitarbeiter (Anspruchsgruppen sollen, wo sinnvoll und möglich, auch in die Plan-Überprüfungen einbezogen werden).

**Lösung zu Frage 10**

**Mit Übungen** sollen vorwiegend die Fähigkeiten des Managements und des Personals zur Bewältigung von Störungs- oder Ausfallereignissen verbessert und überprüft werden. Die

Übungen dienen somit dem Lernen und Überprüfen der notwendigen Kenntnisse und Fertigkeiten zur Bewältigung der Notfälle. Aufgrund realistischer Szenarien wird der Ablauf eines Notfalls vom Zeitpunkt des Ereignis-Eintritts , über die Anpassungen bei der Geschäftsweiterführung bis hin zur Wiederherstellung des Normalbetriebs durchgespielt.

**Lösung zu Frage 11**

**Ein Incident** ist eine Situation, welche eine Unterbrechung, ein Verlust, ein Notfall

oder eine Krise sein oder dazu führen könnte.“ Somit ist es sinnvoll, alle extern und auch intern anfallenden Ausnahme-Ereignisse, auch solche ohne unmittelbaren Schaden, die aber zu grossen Schadensereignissen eskalieren könnten, in diesen Management-Prozess einzubeziehen. Dabei kümmert sich das Incident-Management jeweils in erster Linie um die schnellstmögliche Kontinuitätssicherung des Geschäftsbetriebs, aber auch um das Ziel, den uneingeschränkten „Normalbetrieb“ in nützlicher Frist wieder herzustellen. Zur Erfüllung dieser Ziele gehört die unmittelbare Mitteilung des eingetretenen Ereignisses an die für die Behandlung des Ereignisses zuständigen Stellen sowie die Bewertung und Aufzeichnung des Ereignisses hinsichtlich des allenfalls nötigen Nachvollzugs und des Lernens bezüglich einer kontinuierlichen Verbesserung der Sicherheitslage.

**Das Vulnerability-Management** verfolgt das Ziel, die für die Risikoobjekte relevanten Schwachstellen möglichst zeitnah zu erkennen und mit entsprechenden Massnahmen hinsichtlich eines geringen Risikos zu beheben. Eine organisatorische Verknüpfung des Vulnerability-Managements mit dem Incident-Management in einem gemeinsamen Vulnerability- /Incident-Mangement-Plan ist zweckmässig, da die Behebung von Vulnerabilities oft in unvorhergesehener Weise notwendig wird und oft unverzüglich durchgeführt werden muss. Solche Incidents ergeben sich beispielsweise durch plötzlich bekannt werdende „Exploits“, die mit entsprechenden Massnahmen (u. a. Software Patches) behoben werden sollen, um Cyber-Attacken wie Hackings, Einschleusen von Viren und Trojanische Pferde zu vermeiden.

**Lösung zu Frage 12**

Die sogenannten **„Scouts“** führen die Aufgaben von sogenannten unternehmensinternen Incident Response Teams (IRT) aus. Die Aufgabe der Scouts besteht darin, im zugeteilten Aufgabengebiet (z. B. Windows Clients, Firewalls/Loadbalancing, Server-Betriebssysteme, Oracle Datenbank) die aktuellen für das Unternehmen relevanten „Events“ und „Incidents“ zu überwachen und die möglichen Gefahren und Schwachstellen zu erkunden, z. B. Überwachung mit den zugeteilten Monitoring-Systemen und tägliche Sichtung von prädestinierten Quellen für entsprechende Sicherheits-Informationen, z. B. externe CERTs.

Die **„Taskforce“** ist eine aus den Scouts im betreffenden Fachgebiet zusammengestellte Gruppe von Fachpersonen, welche sich ab einer bestimmten Risiko-Stufe der näheren Beurteilung, Problemlösung und womöglich zeitnahen Behebung von Schwachstellen und konkreten Störungen annimmt (z. B. Patching oder Malwarebeseitigung). Eine Schlüsselrolle kommt dem ebenfalls nominierten permanenten Leiter einer Taskforce zu. Dieser Taskforce-Leiter beruft bei gegebener Risikosituation seine Taskforce ein und ist Ansprechstelle für

Fragen, welche die Taskforce und die aktuelle Problemlösung betreffen. Die beispielhaft genannte **„Office-Taskforce**“ behandelt beispielsweise die Incidents, Bedrohungen und Schwachstellen im Bereich der Office-Systeme einschliesslich der Probleme (z. B. Malware) im Desktop- und Mobil-Computing-Bereich.

**Lösung zu Frage 13**

Das „Service Desk“ als Kommunikationsplattform nimmt als Anlaufstelle u. a. wichtige kommunikative Aktivitäten des Incident-Managements wahr. Solche Aktivitäten sind:

- Entgegennahme von Events und Incidents von den Anwendern
- Alarmieren und Aufbieten der zur Behandlung der Ereignisse vorgesehenen Management- und Fachpersonen;
- Bereitstellung einer „Hotline“, die permanent besetzt ist und Auskünfte gibt bei Problemen, die den Betrieb/Service akut beeinflussen;
- Verwaltung der Massnahmen für die Prävention von Störungs- und Ausfallereignissen im Sinne eines ständigen Verbesserungsprozesses wie die Kategorisierung und Priorisierung aller Incidents.