GAI NetConsult GmbH— Am Borsigturm 58 — 13507 Berlin — www.gai-netconsult.de — Tel: 030/417898-0

Der neue BSI-Baustein „Notfallmanagement"

Holm Diening (GAI NetConsult GmbH)

Juni 2010 Sonderdruck aus Security *Journal* #49

Mit der 11. Ergänzungslieferung der Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat sich wieder einiges getan. Bausteine wie „Samba" oder „Client unter Windows Vista" kamen hinzu, etwas angestaubte Bausteine, die sich noch auf Windows NT oder Kommunikation zwischen Arbeitsplatz PCs bezogen, sind entfallen. Die wahrscheinlich wichtigste Änderung verbirgt sich aber hinter einer zunächst wenig auffälligen Namensänderung: Der Baustein B 1.3 „Notfallvorsorge-Konzept" heißt jetzt „Notfallmanagement". Der Zusatz „-management" ist dabei weit mehr als alter Wein in neuen Schläuchen, sondern erweitert den Betrachtungshorizont der Notfallplanung im BSI-Grundschutz deutlich über den IT-Bereich hinaus.

Der Baustein „Notfallvorsorge-Konzept", wie er bis einschließlich der 10. Ergänzungslieferung hieß, hatte bisher ausschließlich eine auf die IT orientierte Sicht. Hier war der Ausfall der IT die einzig betrachtete Ursache eines Notfalls und dessen möglichst schnelle Beseitigung sollte eben durch die Wiederherstellung der benötigten IT-Funktionen erreicht werden. So ist auch die in der Einleitung des Bausteins getroffene Definition: „Die Notfallvorsorge umfasst Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach (…) Ausfall eines IT-Systems ausgerichtet sind" zu verstehen. Dementsprechend wurde auch der „Ausfall des IT-Systems" als einzige Gefährdung in den Baustein aufgenommen, wobei dieser Ausfall natürlich durch diverse Ursachen (technisches oder menschliches Versagen, Sabotage, höhere Gewalt, etc.) ausgelöst werden konnte. Die durch den Baustein vorgeschlagenen Maßnahmen zur Notfallvorsorge waren dementsprechend auch hauptsächlich auf die Aufrechterhaltung bzw. den schnellen Wiederanlauf der IT-Funktionen in Notsituationen ausgelegt. Wichtige Teilmaßnahmen waren hierbei (zusammen-gefasst):

- Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- Definition des eingeschränkten IT-Betriebs
- Vorsorgemaßnahmen (z.B. Redundanzen)
- Erstellung eines Notfall-Handbuches (inkl. Notfallplänen, Alarmierungsplänen, etc.)
- Durchführung von Notfallübungen

Im Grunde deckte damit der bisherige Baustein „Notfallvorsorge-Konzept" genau das ab, was man aus Sicht von ITIL als „IT-Service Continuity Management" betrachten würde, nämlich die Kontinuität der Bereitstellung von IT-Diensten.

Was allerdings nur rudimentär erfolgte, ist eine genauere Betrachtung des IT-Notfalls aus Sicht des Unternehmens. Welche Geschäftsprozesse sind denn eigentlich wirklich essentiell und auf welche kann ich ggf. kurzzeitig verzichten? Inwiefern hängen diese tatsächlich von der IT ab? Welche temporären Alternativlösungen habe ich für diese Geschäftsprozesse, wenn es ein paar Tage auch mal ohne zentrale IT gehen muss? Wie sieht die Arbeit des Krisenstabes außerhalb der IT aus? Wie organisiere ich die Aufarbeitung des Rückstandes, wenn die Betriebsfähigkeit wieder hergestellt ist? Mit diesen Fragestellungen hat sich der bisherige Baustein zur Notfallplanung nicht auseinander gesetzt. Dies hatte möglicherweise zur Folge, dass ausgerechnet die wertschöpfenden Bereiche einer Organisation weitgehend ohne Notfallkonzept blieben (wenn es nicht gerade ein IT-Dienstleister war).

Gleichzeitig bestand die Gefahr, dass der Einsatz von Ressourcen für die IT-Notfallplanung nicht mit den tatsächlichen Erfordernissen aus Sicht des Geschäftsbetriebes im Einklang stand. Grund hierfür war wohl auch die durch den Baustein vorgeschlagene Vorgehensweise zur Ermittlung der Verfügbarkeitsanforderungen von IT-Komponenten. Hier wurde angeraten „zu den einzelnen IT-Anwendungen den Verfahrensverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen" (M 6.1). Erfahrungsgemäß endet eine solche Befragung eher in einem Wunschkonzert als in einer realistischen Einschätzung, wie hoch die Abhängigkeit von der IT in einem *Notfall* wirklich ist und noch viel wichtiger: welche Priorität der durch den „Verfahrensverantwortlichen" vertretene Geschäftsprozess für die Organisation in einem *Notfall* tatsächlich noch hat.

Genau hier setzt die Neufassung des Bausteins 1.3 mit der Bezeichnung „Notfallmanagement" an.

Überblick zu den Neuerungen

Die neue Fassung des Bausteins B 1.3 „Notfallmanagement" erweitert den Fokus der Notfallthematik deutlich. Inhaltlich basiert er auf dem ca. 120 Seiten umfassenden BSI Standard 100-4

„Notfallmanagement" und fasst dessen wesentliche Aspekte in der gewohnten Nomenklatur der Grundschutzkataloge zusammen. Er sollte daher nicht als isolierter Baustein, sondern immer im Zusammenhang mit dem ihm zugrunde gelegten Standard verwendet werden.

Grundsätzlich neu ist die Betrachtung der Notfallthematik als eigenständige Management-Disziplin. Der Baustein verlangt (wie auch der Standard 100-4), dass die Initiierung des Gesamtprozesses durch die Leitungsebene getrieben wird und diese auch die Steuerung und Überwachung des Notfallmanagements verantwortet. Dabei ist das Notfallmanagement natürlich als Teilbereich des Informationssicherheits-Management-Prozesses zu verstehen und soll nicht etwa ein Eigenleben parallel zu einem ggf. bestehenden ISMS führen. Eine Umsetzung von mehr oder weniger isolierten Notfallkonzepten im IT-Bereich, wie sie noch aus dem alten Baustein herauszulesen war, ist damit aber passé.

Die zweite wesentliche Neuerung ist die Betrachtung der „kritischen Geschäftsprozesse". Anstatt sich gleich auf die Verfügbarkeitsanforderungen von IT-Anwendungen zu konzentrieren, setzt der neue Baustein zunächst „ein tiefgreifendes Verständnis der Geschäftstätigkeit" voraus. Hierfür wird als einer der ersten Schritte im Rahmen der Business Impact Analyse (BIA) eine Vorselektion der wirklich entscheidenden Geschäftsprozesse vorgenommen und anschließend überlegt, wie ein akzeptabler Minimalbetrieb über einen festzulegenden Zeitraum aussehen müsste. An dieser Stelle ist auch die Abhängigkeit von IT-Ressourcen zu analysieren und eine nach Wiederanlaufklassen gestaffelte Wiederherstellung der IT-Dienste zu planen. Ebenso sind auf Basis von Risikoanalysen geeignete Präventivkonzepte zu entwickeln.

Die dritte bedeutsame Erweiterung des Bausteins ist die Integration von nicht-IT Aspekten in die eigentliche Notfallplanung. Dies betrifft sowohl die im Notfall benötigten Ressourcen (Gebäude, Räume, Fahrzeuge, etc.), als auch die Einbindung der „normalen Anwender" in die Notfallkonzeption. Letzteres soll vor allem erreicht werden durch:

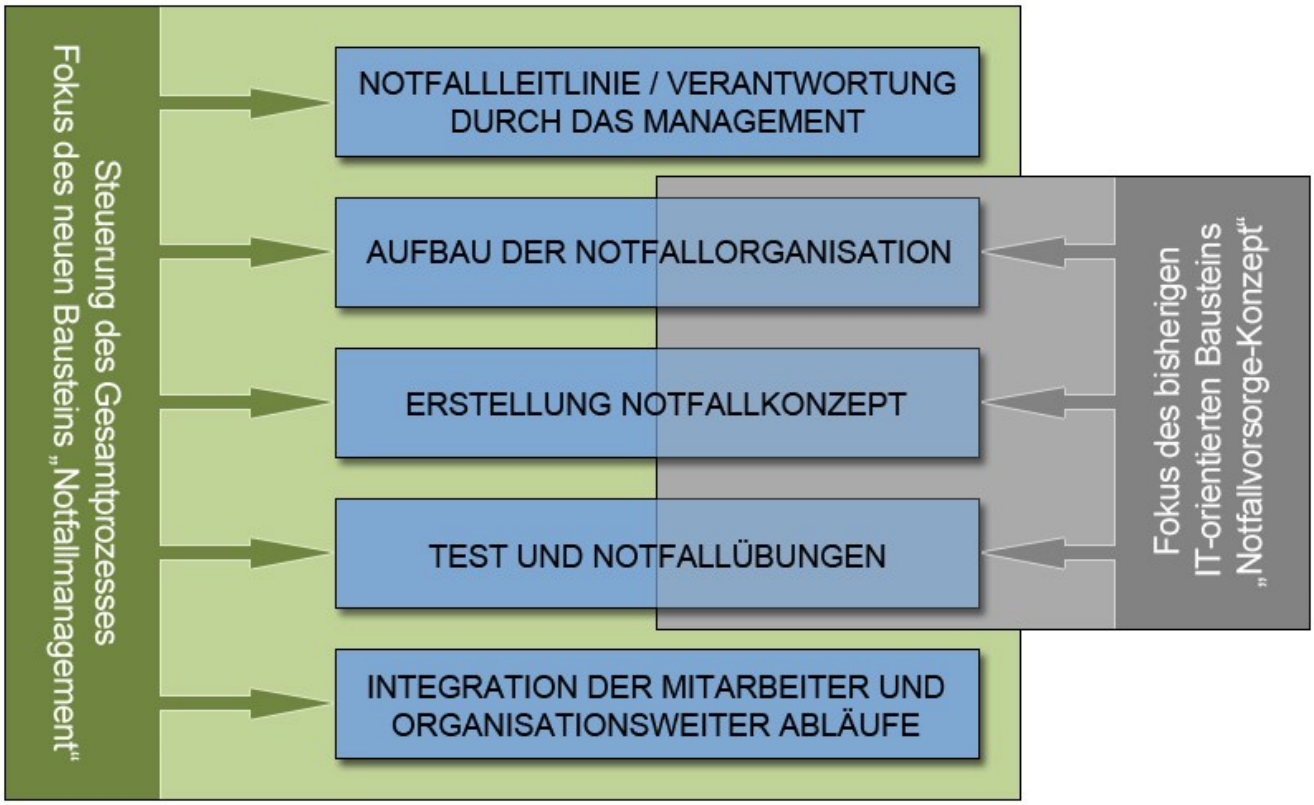

Abbildung-1: Der alte Baustein „Notfallvorsorge-Konzept" deckte nur Teilaspekte des Notfallmanagements ab. Und auch hier nur den IT-Bereich

- Aktive Mitgestaltung der Notfallkonzepte durch die Mitarbeiter
- Schulungs- und Sensibilisierungsmaßnahmen zur Vorbeugung von Notfällen und zu den Aufgaben innerhalb des Notfallkonzeptes
- Beteiligung an Übungen

Um dem Zusatz „-management" gerecht zu werden, darf im neuen Baustein letztlich auch die „Überprüfung und Steuerung des Notfallmanagement-Systems" nicht fehlen. Im Gegensatz zur alten Fassung, bei der eine Anpassung der Notfallkonzeption im

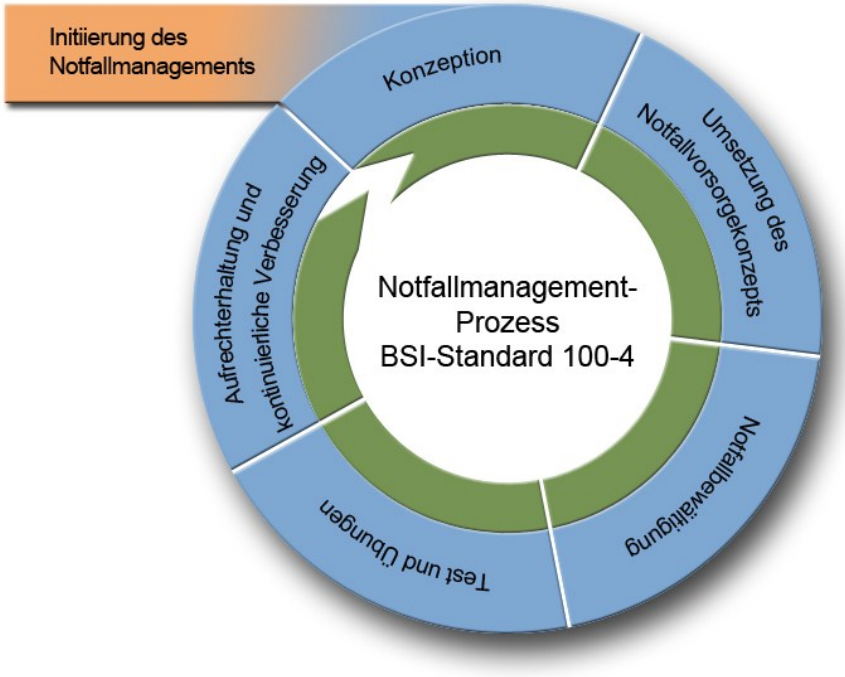

Abbildung-2: Notfallmanagement Prozess nach BSI 100-4

Wesentlichen „nur" auf Basis von Tests und Übungen erfolgte, erwartet die neue Version ein regelmäßiges und umfassendes Review des Notfallmanagements. Hierzu soll unter anderem ein Management-Bericht erstellt werden, der unter anderem folgende Punkte umfasst:

- Ergebnisse von internen Revisionen sowie Überprüfungen bei Outsourcing-Dienstleistern
- Ergebnisse der Tests und Übungen
- Berichte über aktuelle Risikolage, Schwachstellen und Schadensereignisse, sowie daraus abgeleitete Erkenntnisse und Empfehlungen
- Berichte über Änderungen, die Auswirkungen auf das Notfallmanagement haben können
- Statusberichte zu den etablierten Notfallmaßnahmen, Realisierungs- und Verbesserungsvorhaben
- Berichte über Schulungs- und Sensibilisierungsmaßnahmen

Auf Grundlage dieser Management-Berichte wird die Geschäftsleitung anschließend über notwendige Änderungen, Anpassungen und das weitere Vorgehen im Notfallmanagement-Prozess entscheiden.

Damit beschreibt der Baustein 1.3 erstmals einen in sich geschlossenen Management-Kreislauf für den Umgang mit Notsituationen (siehe Abbildung 2). Er basiert auf den Vorgaben des BSI 100-4 und verdichtet diese in die klassischen Maßnahmenbausteine der Grundschutzkataloge. Dabei wird in der Formulierung zwar wieder ein etwas stärkerer Bezug auf das *IT*-Notfallmanagement genommen, als es im Standard der Fall ist, ohne dabei jedoch die Integration in das übergeordnete Notfallmanagement der Organisation aus den Augen zu verlieren.

Neustrukturierung der Gefährdungen und Maßnahmen

Wie spiegeln sich nun diese Neuerungen in der Struktur des Bausteins wider? Zunächst fällt die Erweiterung der betrachteten Gefährdungen ins Auge. Während in der Vorgängerversion des Bausteins nur die Gefährdung „Ausfall von IT-Systemen" betrachtet wurde, werden jetzt unter anderem auch die Gefährdungen

- Personalausfall
- Ausfall eines Gebäudes und
- Ausfall eines Dienstleisters oder Zulieferers

mit in die Notfallplanung einbezogen. Diese Gefährdungen sind allerdings noch mit „Altlasten" belegt und beziehen sich teilweise doch wieder auf IT-Probleme. So ist der betrachtete „Personalausfall" in den genannten Beispielen wieder der Ausfall von Systemadministratoren oder anderem Fachpersonal mit entsprechenden Auswirkungen auf den IT-Betrieb. An dieser Stelle kann sicher noch nachgebessert werden, obwohl es sich hier natürlich nur um eine kleine Unschönheit handelt, die keinen Einfluss auf die Anwendbarkeit des Bausteines hat.

Die Auflistung der umzusetzenden Maßnahmen dagegen ist optisch deutlich kürzer geworden, hat es aber in sich: Im Prinzip sind alle Einzelmaßnahmen des alten Bausteins, welche die Erstellung eines Notfallvorsorge-Konzeptes zum Gegenstand hatten (siehe erster Abschnitt) „verschwunden" und werden jetzt durch die Einzelmaßnahme „Erstellung eines Notfallkonzepts" abgedeckt. An dieser Stelle verlangt der Baustein nichts Geringeres, als die Umsetzung der Vorgehensweise des BSI Standards 100-4 „Notfallmanagement" im Abschnitt 5 „Konzeption". Die Maßnahme selbst fasst diese Methodik nur in kurzer Form zusammen, kann aber ohne die Zuhilfenahme des Standards nicht eigenständig umgesetzt werden.

Flankierend zur „Erstellung eines Notfallkonzeptes" wurden weitere Maßnahmen hinzugefügt, welche die verbleibenden Aspekte des Gesamtkreislaufes im „Notfall-

management" abdecken. Die Wichtigsten sind dabei zusammengefasst:

- Übernahme der Gesamtverantwortung durch die Leitungsebene (Leitlinie)
- Bereitstellung angemessener Ressourcen
- Integration der Mitarbeiter und organisationsweiter Abläufe
- Tests und Notfallübungen (auch für nicht-IT)
- Aufrechterhaltung, Überprüfung und Steuerung des Notfallmanagement-Systems

Im Unterschied zum bisherigen Baustein werden damit auch die nicht-IT Bereiche in die Notfallkonzeption mit eingebunden. Gleichzeitig erfolgt ein Transfer der Gesamtverantwortung auf die Führung der Organisation und eine Integration der Notfallplanung in die wertschöpfenden Geschäftsprozesse.

Hintergrund ISO 27001

Die radikale Erweiterung des Bausteins „Notfallmanagement" ist bis dato recht einzigartig im Vergleich zur Entwicklung der anderen Bestandteile des Grundschutzkataloges (abgesehen vom Baustein B 1.0 „Sicherheitsmanagement" natürlich). Allerdings war dieser Umbau auch dringend notwendig.

Seit 2006 vergibt das BSI auch ISO 27001 Zertifikate auf Basis von IT-Grundschutz. Dabei sind die Grundschutzkataloge vergleichbar mit der Umsetzung des Anhang A der ISO, in welchem 11 Managementgebiete der Informationssicherheit auf 136 Maßnahmenziele („Controls") aufgeteilt werden. Während diese Maßnahmenziele in der internationalen Norm lediglich als Anforderungen formuliert sind, ohne eine konkrete Umsetzung vorzugeben, verstehen sich die Grundschutzkataloge als direkt implementierbare Maßnahmensammlung für IT-Umgebungen normalen Schutzbedarfs.

Für den Nachweis der Kompatibilität der Grundschutzmethodik mit der ISO 27001, veröffentlicht das BSI eine Gegenüberstellung zwischen den 136 Maßnahmenzielen der Norm mit den Bausteinen oder einzelnen Maßnahmen der Grundschutzkataloge. Diese Vergleichstabelle wird mit jeder neuen Ergänzungslieferung aktualisiert.

Zur Abdeckung des ISO Management-Gebietes „Business Continuity Management" wurde dabei bisher immer auf die Bausteine „Notfallvorsorge-Konzept" und „Behandlung von Sicherheitsvorfällen" verwiesen. Dabei war diese Zuordnung so eigentlich gar nicht gerechtfertigt. Die ISO 27001 fordert in diesem Bereich nämlich unter anderem:

A.14.1.1 „**Einbeziehung** der Informationssicherheit **in den Prozess zur Sicherstellung des Geschäftsbetriebs**":

- In der **gesamten Organisation** muss ein **gelenkter Prozess** zur **Sicherstellung des Geschäftsbetriebs** entwickelt und aufrechterhalten werden, der die für die Sicherstellung des Geschäftsbetriebs (…) erforderlichen Informationssicherheitsanforderungen (…) behandelt.

Gefordert wird also eindeutig ein Notfallmanagement in der gesamten Organisation aus Sicht der Geschäftsprozesse. Informationssicherheit sollte dabei in die (als bereits bestehend vorausgesetzte) Gesamtnotfallplanung der Organisation eingebettet werden. An erster Stelle die Aufrechterhaltung der IT-Dienste. Deutlicher wird die Intention dieses Maßnahmenzieles noch in den Implementierungshinweisen der ISO 27002. Die ist zwar nicht maßgeblich für eine Zertifizierung, hilft aber auch, die Zielsetzung und die Hintergründe der einzelnen Maßnahmenziele besser zu verstehen. Die in der ISO 27002 formulierte Zielsetzung des gerade erwähnten Controls konkretisiert hier: „Dieser Prozess sollte die kritischen Geschäftsprozesse identifizieren und die Informationssicherheitsanforderungen bei der Sicherstellung des Geschäftsbetriebs in andere Anforderungen integrieren, die sich auf Aspekte wie Betrieb, Personal, Material, Transport und Einrichtungen beziehen."

Damit greift der ursprüngliche Baustein in Bezug auf die Forderungen der ISO 27001 etwas zu kurz, da dieser, wie bereits erwähnt, eher „IT-Service Continuity Management" im Fokus hatte als „Business Continuity Management". Diese Lücken füllt nun der neue Baustein „Notfallmanagement" sehr gut aus und über den Standard 100-4 „Notfallmanagement" liefert das BSI den Standard für das Rahmen-Notfallmanagement aus betrieblicher Sicht gleich mit, in den sich dann der kleinere Baustein „Notfallmanagement" im Sinne der Forderungen der ISO 27001 einbetten kann.

Konsequenzen für die interne Revision

Für die Revision, die nunmehr die Umsetzung der neuen Fassung des Bausteines 1.3 „Notfallmanagement" als Prüfgrundlage verwenden soll, kommen damit gegenüber der bisherigen Vorgehensweise eine Reihe erweiterter Prüfaspekte hinzu. Die Untersuchung des Notfallmanagements könnte dadurch zum Beispiel um folgende Kontrollfragen erweitert werden:

- Kann die Initiative des Managements im Notfallprozess nachgewiesen werden?
- Werden ausreichend Ressourcen zur Verfügung gestellt?
- Erfolgte die Notfallkonzeption auf Basis kritischer Geschäftsprozesse?
- Wie ist der eingeschränkte Geschäftsbetrieb definiert?

- Welche präventiven und reaktiven Maßnahmen sieht das neue Notfallkonzept auch außerhalb der IT-Bereiche vor?
- Wie sehen die Notfallkonzepte mit stark eingeschränkter oder sogar ohne IT aus?
- Wie sind die Anwender in die Notfallkonzeption eingebunden?
- Welche Planungen gibt es zur Rückstandsaufarbeitung nach der Wiederherstellung des Normalzustandes?
- Können übergreifende Notfalltests nachgewiesen werden (IT und nicht-IT) oder werden nach wie vor nur reine IT-Übungen durchgeführt?
- Fließen die Ergebnisse der Tests in die neue Notfallkonzeption ein?
- Wie erfolgt die proaktive Anpassung der Notfallplanung, wenn sich die Prioritäten innerhalb der Geschäftstätigkeit der Organisation verschieben?

Wie sich aus den vorstehenden Fragestellungen leicht ableiten lässt, ist der Sprung von der alten auf die neue Fassung des Bausteins 1.3 „Notfallmanagement" ein gewaltiger. Nachdem die 11. Ergänzungslieferung erst Ende 2009 erschienen ist, können hier noch keine Wunder in der Umsetzungsreife erwartet werden, sofern der BSI Standard 100-4 nicht schon unabhängig von den Grundschutzkatalogen umgesetzt wurde. Andererseits sollte die interne Revision schon frühzeitig damit beginnen nach den neuen Vorgaben zu prüfen, um in den Revisionsberichten (angemes-sene Wertung vorausgesetzt) auf die gestiegenen Anforderungen des neuen Bausteins hinzuweisen.

Fazit

Mit dem neuen Baustein „Notfallmanagement" hat das BSI wieder einen Schritt in die richtige Richtung getan: weg von der reinen IT-Denkweise, hin zur Betrachtung der übergeordneten Aufgabenstellungen aus Sicht der Organisation. Gerade im Bereich der Notfallvorsorge ist eine ausschließliche Fokussierung auf die Wiederherstellung von IT-Ressourcen nicht zielführend, wenn es doch im Grunde um den Erhalt der Arbeitsfähigkeit und damit das Überleben des Unternehmens in Notsituationen geht. Die Neufassung des Bausteins ist damit ein wichtiger Lückenschluss zwischen reiner IT-Notfallplanung und betrieblichem Kontinuitätsmanagement und dient ebenso auch der angestrebten Kompatibilität der Grundschutzmethodik mit den Forderungen der ISO 27001. Allerdings haben sich durch den weiter gefassten Rahmen auch der für die Umsetzung zu veranschlagende Aufwand und das erforderliche Fachwissen deutlich erhöht. Zudem dürfte der neue Baustein auch Probleme für diejenigen mit sich bringen, für die der „IT-Grundschutz", wie dem Namen nach zu erwarten wäre, auch tatsächlich nur im IT-Bereich angesiedelt wäre. Die geforderte Integration des Notfallmanagements in die betrieblichen Abläufe wird aus der Position eines IT-Verantwortlichen heraus in vielen Organisationen nur schwer zu vermitteln sein. Die Notwendigkeit eines übergeordneten Notfallmanagements ergibt sich aber auch aus externen Anforderungen. Als Beispiele wären hier der KRITIS-Umsetzungsplan des Bundeministeriums des Innern für Betreiber kritischer Infrastrukturen oder die „Mindestanforderungen an das Risikomanagement" (MaRisk) des BaFin für die Finanzwirtschaft zu nennen. In beiden Fällen wird die Umsetzung einer Notfallvorsorge auf Basis gängiger Standards gefordert. Hier sollte für die Einführung des BSI Standards 100-4 „Notfallmanagement" plädiert werden, da dessen Anforderungen zunächst wenig IT-lastig sind. Eingebettet in diesen übergeordneten Prozess kann dann in einem grundschutzorientierten IT-Bereich die Einführung des Notfallmanagements als Umsetzung des neuen Grundschutz-Bausteines erfolgen.