Bundesanstalt für Finanzdienstleistungsaufsicht

Postfach 50 01 54
60391 Frankfurt
Konsultation-04-18@bafin.de

Dr.-Ing. Klaus-Rainer Müller
Fachbuchautor
Senior Management Consultant

64846 Groß-Zimmern

Groß-Zimmern, den 17. April 2018

Geschäftszeichen: VA 36-I 2802-2018/0001
Betreff: Stellungnahme im Rahmen der Konsultation 04-2018

Sehr geehrte Damen und Herren,

mit Interesse habe ich die VAIT gelesen, die Sie zur Konsultation gestellt haben. Die dort genannten Auslegungshinweise begrüße ich, da sie Versicherungen Feststellungen bei Prüfungen ersparen können. Gerne möchte ich folgende Anregungen geben:

II. Anforderungen, 1. IT-Strategie, Tz. 2b, Erläuterungsspalte	
„Zu b) Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse des Unternehmens sowie Darstellung des avisierten Implementierungsumfangs der jeweiligen Standards;“	Empfehlenswert erscheint es mir, an dieser Stelle Hinweise auf gängige Standards zu geben. Dazu zähle ich in diesem Kontext die relevanten Standards aus der ISO-27000-Familie zur Informationssicherheit, insbesondere auch einschließlich der ISO 27005 zum Informationssicherheitsrisikomanagement und der ISO 27031 zur IT-Service-Kontinuität (IRBC), die BSI-Standards und das BSI-Grundschutz-Kompendium, die ISO 20000 zum Service Management sowie die ISO 38500 in Bezug auf die IT-Governance. Im Hinblick auf KRITIS-Betreiber könnte der Verweis auf die BSI B3S hilfreich sein. Meiner Einschätzung nach müsste es statt „avisiert“ „anvisiert“ oder „angestrebt“ heißen.
II. Anforderungen, 1. IT-Strategie, Tz. 2c:	
„c) Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation;“ Erläuterung: „Zu c) Beschreibung der Bedeutung der Informationssicherheit im Unternehmen sowie der Einbettung der Informationssicherheit in die Fachbereiche und in das jeweilige Zusammenarbeitsmodell mit den IT-Dienstleistern;“	Die Informationssicherheit ist der IT-Sicherheit übergeordnet und dementsprechend oberhalb der IT-Strategie angesiedelt. Von daher erscheint es mir empfehlenswert, dass die Bedeutung der Informationssicherheit und deren Einbettung in die Fachbereiche an anderer Stelle, z. B. im Rahmen der Informationssicherheitsleitlinie/-politik (Tz. 26) beschrieben wird. In der IT-Strategie erscheinen mir Aussagen dazu empfehlenswert, wie die Anforderungen zur Informationssicherheit in der IT,

	genauer der IKT, und in der IKT-Sicherheit umgesetzt werden.
II. Anforderungen, 1. IT-Strategie, Tz. 2e:	
„e) Aussagen zum Notfallmanagement unter Berücksichtigung der IT-Belange;“	Empfehlenswert erscheint mir an dieser Stelle der Hinweis, dass derartige Aussagen verschiedentlich als ICT Service Continuity Strategy bezeichnet werden. Der Standard ISO 27031 verwendet den Begriff IRBC-Strategy. Eine derartige Strategie bezieht alle in Bezug auf einen Notfall relevanten Ressourcengruppen ein, z. B. Personen, Gebäude, IKT-Systeme, Daten und Dienstleister.
II. Anforderungen, 3. Informationsrisikomanagement, Tz. 23, Erläuterungsspalte	
„IT-Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit.“	Wenngleich Standards den Begriff „risk appetite“ (Risikoappetit) nutzen, erscheint es mir empfehlenswert, den sachlich-neutraleren Begriff „Risikobereitschaft“ zu verwenden. Ebenfalls empfehlenswert erscheint mir der Hinweis, dass die Risikobereitschaft kleiner als die Risikotragfähigkeit sein muss.
II. Anforderungen, 4. Informationssicherheitsmanagement, Tz 26	
„Die Geschäftsleitung hat eine schriftliche Informationssicherheitsleitlinie zu beschließen und innerhalb des Unternehmens angemessen zu kommunizieren. Die Informationssicherheitsleitlinie hat im Einklang mit den Strategien des Unternehmens zu stehen.“	Empfehlenswert erscheint es mir, darauf hinzuweisen, dass der Begriff „Informationssicherheitsleitlinie“ gleichbedeutend mit dem Begriff „Informationssicherheitspolitik“ der DIN EN ISO/IEC 27001:2017-06 und der DIN EN ISO/IEC 27002:2017-06 ist. Dieser Begriff ist für Personen zudem tendenziell leichter unterscheidbar von dem Begriff „Informationssicherheitsrichtlinie“
II. Anforderungen, 4. Informationssicherheitsmanagement, Tz. 27	
„Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.“	Empfehlenswert erscheint es mir, den Satz aufzutrennen und bei den genannten Teilprozessen zu konkretisieren, worauf sich diese beziehen, z. B. auf die Identifizierung von Bedrohungen, den Schutz von Assets, die Reaktion auf Sicherheitsvorfälle etc., z. B.: „Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der

	Technik berücksichtigende Informations-sicherheitsrichtlinien zu definieren. Informationssicherheitsprozesse müssen Teilprozesse berücksichtigen, die sich auf die Identifizierung, den Schutz, die Entdeckung, die Behandlung und die Wiederherstellung beziehen. Beispiele dafür sind die Identifizierung von Bedrohungen und Schwachstellen, der Schutz vor Bedrohungen, die Entdeckung von Sicherheitsvorfällen, die Behandlung von Sicherheitsvorfällen und Notfällen, die Wiederherstellung von Assets und Services.“
Notfallmanagement unter Berücksichtigung der IT-Belange	
k. A.	Es erscheint mir empfehlenswert, ein eigenes Kapitel mit Auslegungshinweisen zum Notfallmanagement in Bezug auf die IKT anzulegen, das beispielsweise auf die Tz. 293 bis 298 der MaGo Bezug nimmt. Diese Auslegungshinweise können sich u. a. auf die Ableitung der Kontinuitätsanforde-rungen für die IKT aus Business-Impact-Analysen, Kontinuitätsziele, Optionen für Kontinuitätsstrategien und konkrete Kontinuitätsstrategien, die Distanz von Gebäuden, Notfallszenarien, Dienstleister, Kontinuitätspläne, Test- und Übungsarten sowie Tests und Übungen, Leistungsfähigkeit und Berichtswesen beziehen.

Freundliche Grüße sendet Ihnen

Dr.-Ing. Klaus-Rainer Müller