e:ndlich
in der IT zu Hause

REGULATORISCHE ANFORDERUNGEN AN DIE IT IM BANKWESEN

Bedeutung für die Instituts-IT in der Praxis

endlich.it

DAS ERWARTET SIE IN DIESEM WHITEPAPER

Die regulatorischen Anforderungen an Banken nehmen in den letzten Jahren stetig zu. In diesem Whitepaper zeigen wir auf, welche Anforderungen die BaFin an die Dokumentation der kritischen IT-Infrastrukturen bei Banken stellt und mit welchen Mitteln diese erfüllt werden können. Dazu nutzen wir das Beispiel des Tools FNT Command. Viel Spaß beim Lesen!

Autor

Nikolai Weidmann,
Senior Consultant für ITSM Beratung,
e:ndlich GmbH & Co. KG.

INHALT

1 Prüfungspraxis in der Finanzbranche

Finanzielle „Erdbeben“ wie der Zusammenbruch einer großen Bank in den Vereinigten Staaten 2008 erfordern laut Jean-Claude Trichet ein rasches und entschiedenes Handeln der zuständigen Stellen.[1] So haben Finanz- und Eurokrise für ein Umdenken in der Finanzbranche gesorgt. Die schon in Basel II enthaltenen Vorgaben zu Eigenkapital und zum Risikomanagement, wurden mit Basel III als eine der Lehren der Finanzkrise deutlich erweitert.

Mit neuen Vorgaben und auf die erkannten Probleme zugeschnittenen Verbesserungen sollten Banken zum Aufbau und zur Nutzung risikosensitiver Modelle bewegt werden. So soll ein besserer Blick darauf gerichtet werden, wo versteckte Risiken liegen (BaFin, 2019). In Deutschland erfolgt dies durch das Kreditwesengesetz (KWG) und den Vorgaben in „MaRisk“, den sogenannten „Mindestanforderungen an das Risikomanagement“. Die Einhaltung dieser Anforderungen wurde bereits vor der Krise regelmäßig überprüft. Seit der Einführung eines einheitlichen Aufsichtsmechanismus durch die Europäische Zentralbank werden systemrelevante Banken jedoch von eben dieser beaufsichtigt und nicht mehr „nur“ durch die länderspezifischen Zentralbanken. Gefühlt weht seither ein „anderer Wind“ im Finanzsektor. Banken, die bisher von allzu intensiven Prüfungen verschont geblieben sind, werden nun unter die Lupe genommen.

Doch wie laufen solche Prüfungen ab? Laut den §§25 und 44 des KWG kann eine solche Prüfung anlassbezogen, aber auch anlassunabhängig durchgeführt werden. Angekündigt wird eine solche Prüfung durch ein offizielles Schreiben der zuständigen Aufsichtsbehörde. In der Regel wird dann zwei Wochen später ein Previsit durchgeführt. Bei diesem Vortermin werden erste Informationen, unter anderem zum Umfang der Prüfung, ausgetauscht. Bereits etwa zehn Tage später beginnt die eigentliche Prüfung. Dabei müssen alle angeforderten Unterlagen vorliegen. Es bleibt also nicht allzu viel Vorbereitungszeit. Getreu dem Motto „Besser Vorsicht als Nachsicht“, sollte man sich daher besser schon vorbereiten, bevor eine Prüfung angekündigt wird.[2]

In diesem Whitepaper möchten wir Ihnen einen Überblick über die regulatorischen Anforderungen an die IT der Finanzbranche geben und die Auswirkungen auf den Alltag aufzeigen. Dabei gibt es eine Vielzahl von Stolperfallen auf dem Weg zur bestandenen EZB Prüfung, die Sie anhand unserer Tipps besser umschiffen können.

[1] https://www.ecb.europa.eu/press/key/date/2009/html/sp091015.de.html („Lehren aus der Finanzkrise“, Jean-Claude Trichet, 15.10.2009)

[2] https://www.rolandeller.de/fileadmin/Redaktion/Fachartikel/Artikel-Matthias-Kurfels-Repeat-Jahrbuch-2014-Par-44-Pr%C3%BCfungen.pdf

2 Regulatorische Anforderungen an die IT im Bankwesen

Doch was hat das mit der IT eines Instituts zu tun? „Basel & Co." handeln doch von Eigenkapital und Risiken im Hinblick auf finanzielle Belange. Ein Blick auf Ereignisse wie dem Cyberangriff auf die Deutsche Kreditbank AG im Januar 2020 zeigt, wie groß die Bedeutung einer funktionierenden IT für Banken heutzutage geworden ist.[3] Insbesondere bei Online-Banken ist eine Nicht-Erreichbarkeit der angebotenen Dienste undenkbar.

Um aufsichtsrechtliche Prüfungen zu bestehen und aber auch dem Katastrophenfall „offline" zu entgehen, bieten MaRisk und BAIT, die Bankaufsichtlichen Anforderungen an die IT, eine solide Grundlage, die insbesondere im IT-Bereich auf gängigen Standards wie ITIL und dem IT-Grundschutz des BSI basieren. Die gesetzliche Grundlage der aufsichtsrechtlichen Vorgaben ist §25a Absatz 1 Satz 3 Nummern 4 und 5 Kreditwesengesetz (KWG). Die BAIT interpretieren, ebenso wie die Mindestanforderungen an das Risikomanagement der Banken, die Inhalte dieses Gesetzes. BAIT und MaRisk konkretisieren, was die Aufsichtsbehörden unter „angemessener technisch-organisatorischer Ausstattung der IT-Systeme" und unter „Berücksichtigung der Anforderungen an die Informationssicherheit sowie eines angemessenen Notfallkonzepts", verstehen. Außerdem wird in der BAIT auch der §25b KWG einbezogen, da immer mehr Institute IT-Services von Dritten beziehen und somit das Thema Auslagerung eine immer größere Bedeutung hat. In der Entwicklung der BAIT wurden vor allem Themen adressiert, welche die Aufsicht bei IT-Prüfungen in den letzten Jahren als die wesentlichsten Mängel identifiziert hat (siehe Abbildung 1).[4]

[3] https://www.netzwelt.de/ist-down/175128-dkb-stoerungen-online-banking-hacking-angriff-noch-immer-eingeschraenkt.html

[4] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1801_BAIT.html

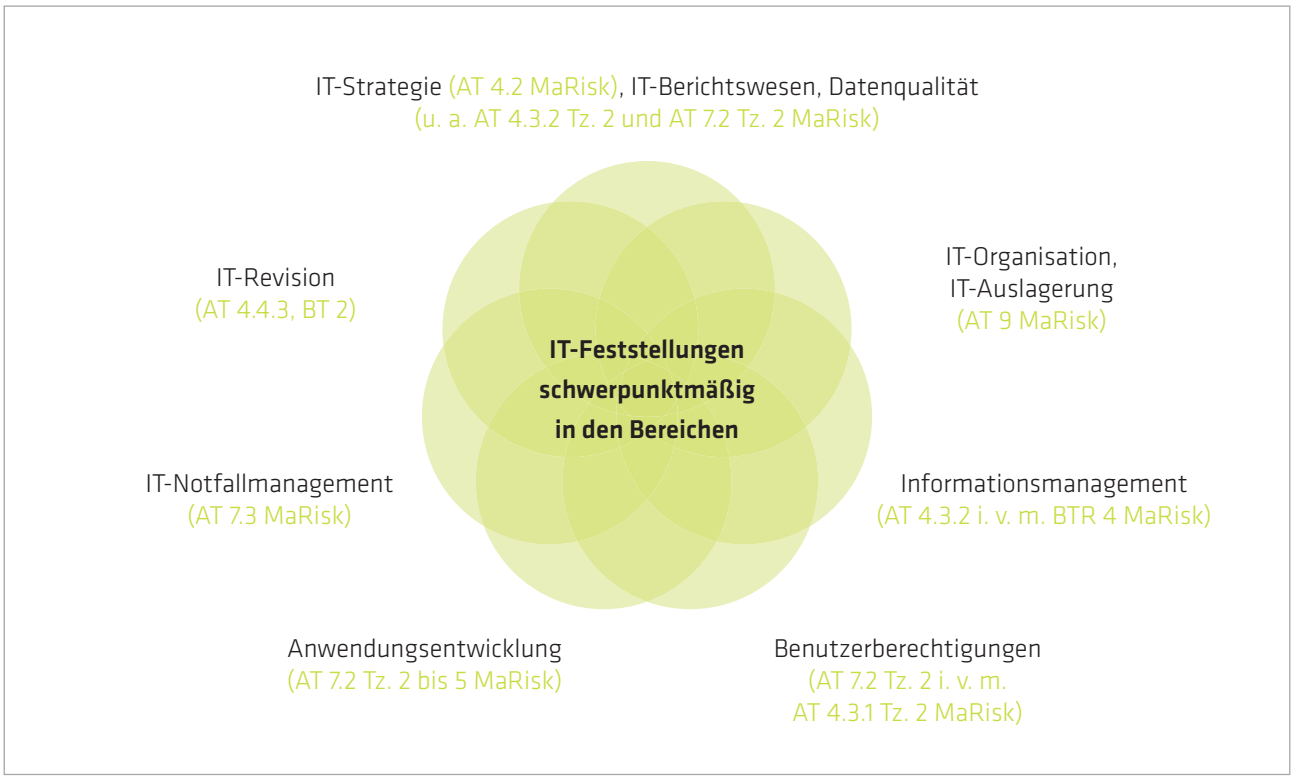


Abbildung 1: Identifizierte IT-Mängel; © BaFin

2.1 BAIT MASSNAHMEN ANHAND HÄUFIGER MÄNGEL

2.1.1 IT-Strategie und IT-Governance

Die erkannten Mängel werden vermieden, indem Risikobewusstsein durch dedizierte Maßnahmen in allen Bereichen der Unternehmens-IT geschaffen wird. Zunächst wird empfohlen, die IT-Strategie auf die Bedürfnisse des Business und dessen Strategie anzupassen. In der IT-Strategie muss die Aufbau- und Ablauforganisation der IT festgelegt werden. Des Weiteren muss entschieden werden, wie mit der Auslagerung von IT-Dienstleistungen umgegangen wird. Eine wichtige Rolle muss auch der strategische Umgang mit der individuellen Datenverarbeitung (IDV) einnehmen.

Diese Strategie soll sich zudem im Governance-Regelwerk wiederfinden und es muss sichergestellt werden, dass die Regelungen in der Praxis wirksam umgesetzt werden. Die Aufsichtsbehörden legen dabei Wert darauf, dass die Personalausstattung so ausreichend ist, dass keine unvereinbaren Tätigkeiten bzw. Rollen in einer Person vorkommen. So werden daraus resultierende Risiken vermieden und so dem Grundsatz gerecht, Risiken zu kennen und entsprechende Maßnahmen daraus abzuleiten.

2.1.2 Informationsrisiko-, Informationssicherheits- und Benutzerberechtigungsmanagement

Dem Management der Risiken dienen zudem die Disziplinen Informationsrisiko-, Informationssicherheits- und Benutzerberechtigungsmanagement. Informationen bzw. Daten sind nicht nur im Finanzsektor ein hohes Gut und daher besonders schützenswert. Zunächst sollte man sich daher mit dem Schutzbedarf der im Institut anfallenden Daten und Informationen beschäftigen. Hierfür ist es hilfreich zunächst Schutzbedarfskategorien festzulegen, die später Basis für Maßnahmen werden. In Abbildung 2 ist ein üblicher Ablauf einer Schutzbedarfsanalyse aufgezeichnet.

Die erarbeiteten Schutzbedarfe können zum Beispiel im Configuration Management System (CMS) an den Applikationen oder Services als Attribute oder eigenes Configuration Item (CI) dokumentiert werden. Die Aufsichtsbehörden legen hier auf einen angemessenen Vererbungsalgorithmus wert. Diese Vererbung kann durch die meisten Tools abgebildet werden. Unterstützt werden sollten dabei die Vererbungstechniken Maximumprinzip, Kumulationseffekt und Verteilungseffekt (Kapitel 4.3.3 IT-Grundschutz Handbuch). Dies ist von großer Bedeutung, da zum Beispiel durch den Verteilungseffekt Maßnahmen wirtschaftlicher gestaltet werden können. Läuft beispielsweise eine Anwendung auf einem Cluster, reduziert sich das Ausfallrisiko und der Schutzbedarf kann so an den einzelnen physischen Servern niedriger angesetzt werden. Man spricht bei einem Failover Cluster daher von einer höheren Schutzbedarfseignung als bei einem einzelnen Server. Das Vorgehen zur Schutzbedarfsanalyse ist im ISO-Standard ISO 27001:2015 sowie den BSI-Standards und Grundschutzkatalogen definiert.

Um die Vererbung der Schutzbedarfe korrekt durchführen zu können, ist es notwendig Informationsverbünde zu identifizieren. Unter einem Informationsverbund ist die Gesamtheit infrastruktureller, organisatorischer, personeller und technischer Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei je nach Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche umfassen, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind.[5]

Die definierten Informationsverbünde dienen allerdings nicht nur der Vererbung der Schutzbedarfe in den Bereichen Vertraulichkeit, Integrität und Verfügbarkeit, sondern werden auch für weitere Überlegungen im Informationssicherheitsmanagement benötigt. Hier wird unter anderem für die Informationsverbünde eine Sicherheitsrichtlinie erstellt. Eine Herausforderung ist hierbei alle beteiligten Organisationseinheiten zu identifizieren, da auch softwarebasierte Schnittstellen in die Richtlinie einzubeziehen sind.

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 („Leitfaden zur Basis-Absicherung nach IT-Grundschutz", BSI, S.26).

Abbildung 2: Ablauf einer Schutzbedarfsanalyse (https://www.computerwoche.de/a/it-sicherheit-das-kalkulierte-risiko,3092357)

Eine der am häufigsten unterschätzten Gefahren für IT-Systeme sind dabei jedoch andere Schnittstellen. Sogenanntes Social Hacking bezeichnet den Versuch eines Hackers mittels Manipulation von Menschen, Zugriff auf ein fremdes Computersystem zu erhalten. Daher legt die BaFin in ihren Prüfungen großen Wert auf konsistente Berechtigungskonzepte. Diese sollten nach dem „Need-to-Know"-Prinzip erstellt werden. Es dürfen also immer nur so viele Zugriffsrechte vergeben werden, wie es für die jeweilige Aufgabenwahrnehmung notwendig ist. Diese Berechtigungen sollen in anwendungsspezifischen Berechtigungskonzepten festgelegt werden. Hier sollte jedoch unbedingt ein Rezertifizierungsprozess vorgesehen werden, um sicherzustellen, dass keine unnötigen Berechtigungen vorliegen. Diese entstehen zum Beispiel, wenn Mitarbeiter die Abteilung wechseln und die alten Berechtigungen nicht entfernt werden. Ebenso wie in den anderen Bereichen der BAIT sollte hier auf gängige Standards gesetzt werden: In diesem Fall z.B. auf das Access Management aus ITIL. So wird eine Minimierung der Risiken aus unnötigen Berechtigungen sichergestellt.

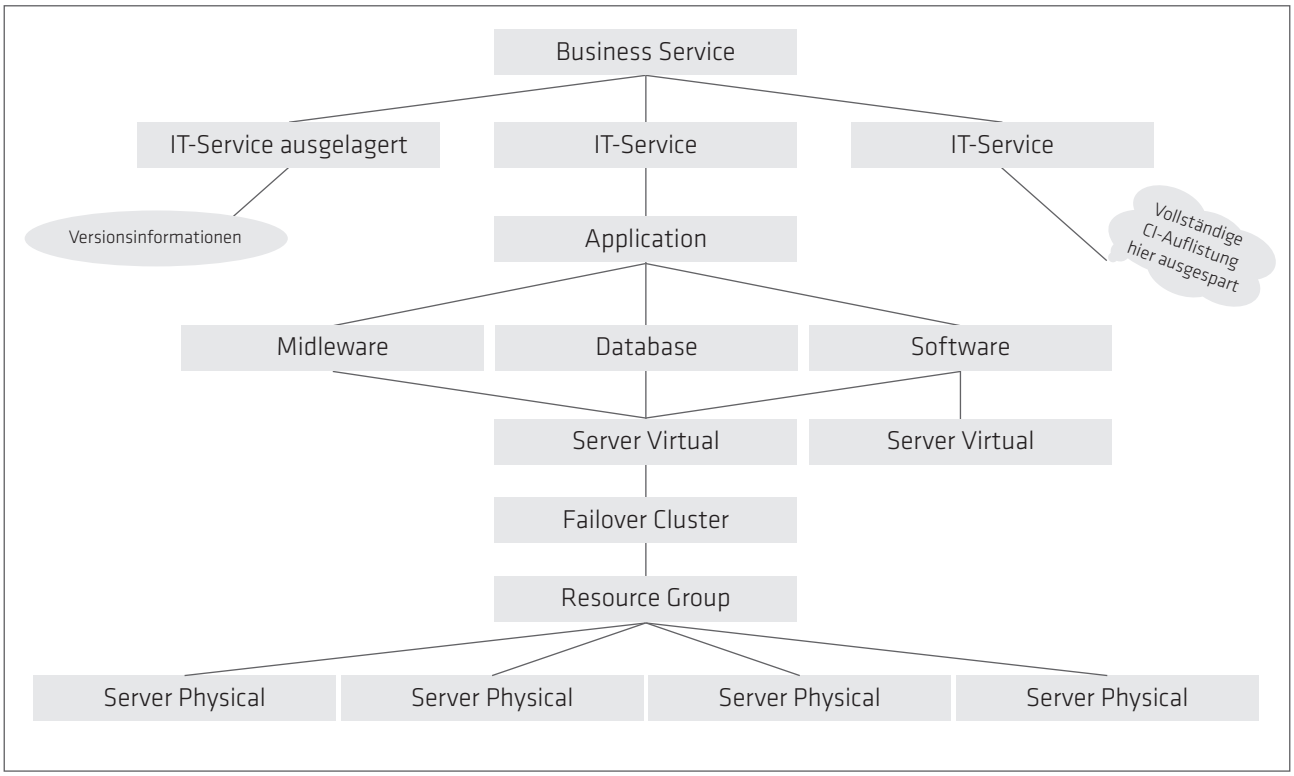


Abbildung 3: Schematisches Beispiel für einen Informationsverbund

2.1.3 IT-Risiken in Projekt und Betrieb

Ebenso soll diese Minimierung für Projekte und die Entwicklung von Anwendungen erreicht werden. Auch hier helfen gängige Standards bzw. Methoden eine Übersicht über Risiken und deren Abhängigkeiten zu erhalten. Um häufige IT-Projektrisiken wie Zeitverzug, Kostenexplosion oder Nicht-Nutzung der Projektergebnisse zu vermeiden, kann zum Beispiel wie in Abbildung 4 vorgegangen werden.

Bereits in der Vorprojektphase der Entwicklung von Anwendungen ist es hilfreich die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität, der in diesem Programm zu verarbeitenden Daten zu analysieren und im weiteren Projektverlauf zu beachten. Diese Informationen helfen, IDVen (sogenannte „Individuelle Datenverarbeitungen", also selbst entwickelte Anwendungen) in Risikoklassen einzuteilen. Anhand derer können dann angemessene Maßnahmen ergriffen werden. Die IDVen sollen zudem in einem zentralen IDV-Register (Abbildung 5) geführt werden.

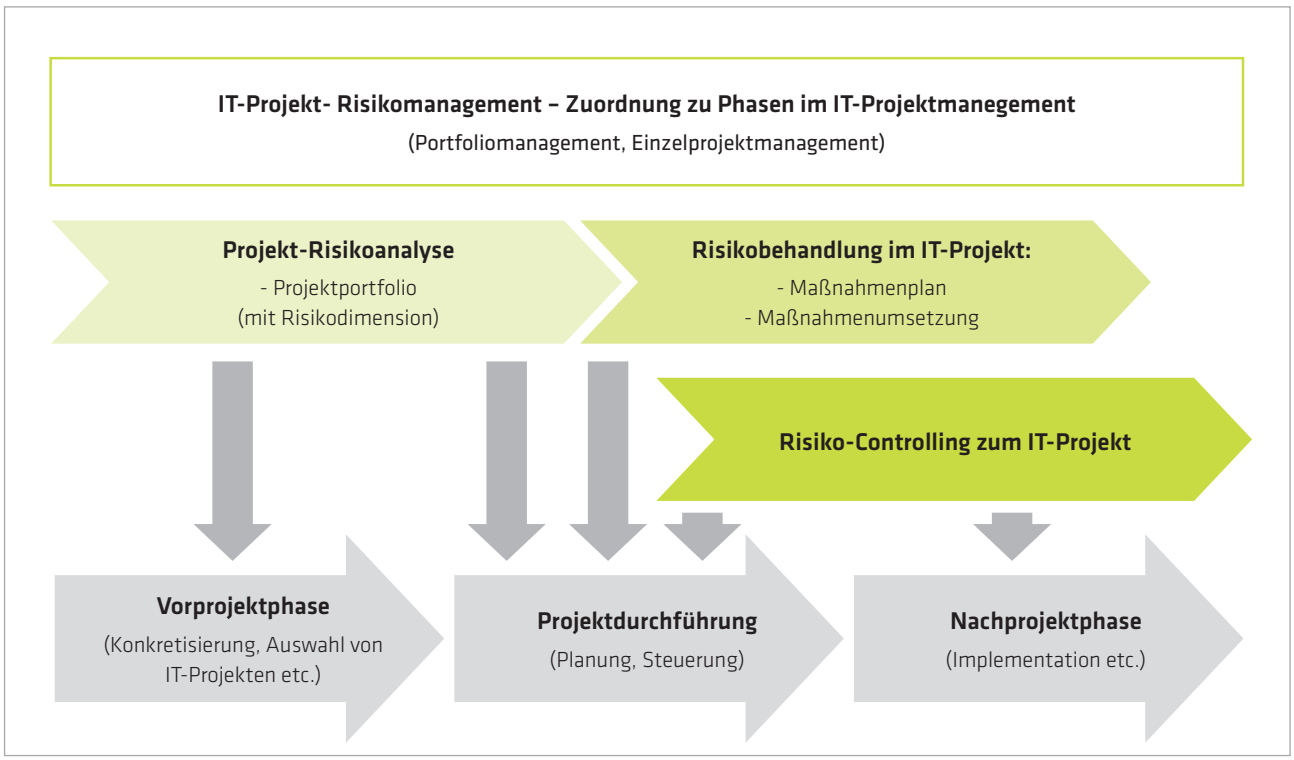


Abbildung 4: IT-Projekt-Risikomanagement – Zuordnung zu Phasen im IT-Projektmanagement (Portfoliomanagement, Einzelprojektmanagement). © Ernst Tiemeyer (https://www.informatik-aktuell.de/management-und-recht/projektmanagement/it-projektrisiken-erfolgreich-managen.html)

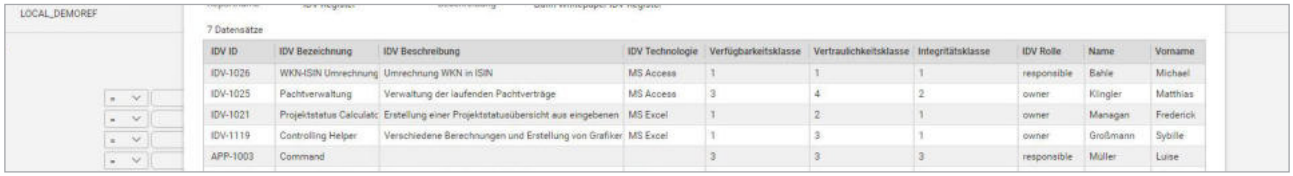


Abbildung 5: Ausschnitt aus einem IDV Register als Report im Query Editor von FNT Command

Dieses Register kann sinnvollerweise in einer Configuration Management Database, kurz CMDB, abgebildet werden. Die CMDB dient zudem der Erkennung von Risiken aus veralteten IT-Systemen. Dazu sollte ihre CMDB ein Produktlebenszyklus-Management unterstützen. Hierbei müssen die Komponenten ihrer IT-Systeme vollständig in der CMDB abgebildet sein. Viele Institute haben dabei bereits einen guten Datenbestand, jedoch reicht das nicht allein, um in diesem Bereich frei von Prüfungsfeststellungen zu bleiben. Die BaFin fordert die Datenqualität durch einen entsprechenden Prozess zu überwachen. Abbildung 6 zeigt beispielhaft einen Datenqualitätsprozess.

Besonders wichtig ist dabei die eindeutige Rollenzuordnung. Verantwortlichkeiten sollten niemals geteilt werden, so dass immer klar ersichtlich ist, wer zum Beispiel verantwortlich für die Pflege einer CI-Klasse ist (=CI Owner). Die eigentliche Dokumentationsarbeit kann trotzdem delegiert werden. Die Rolle des Configuration Auditors wird häufig durch eine Kombination aus Toollösungen und der Rolle abgebildet. Klassisch kommen hier mehrstufige Datenqualitätsreports zum Einsatz. Der Librarian koordiniert die Maßnahmen zur Behebung von ungeplanten Abweichungen vom Regelbetrieb. Gegebenenfalls organisiert er auch Notfallmaßnahmen und meldet diese anhand geeigneter Kriterien der Geschäftsleitung.

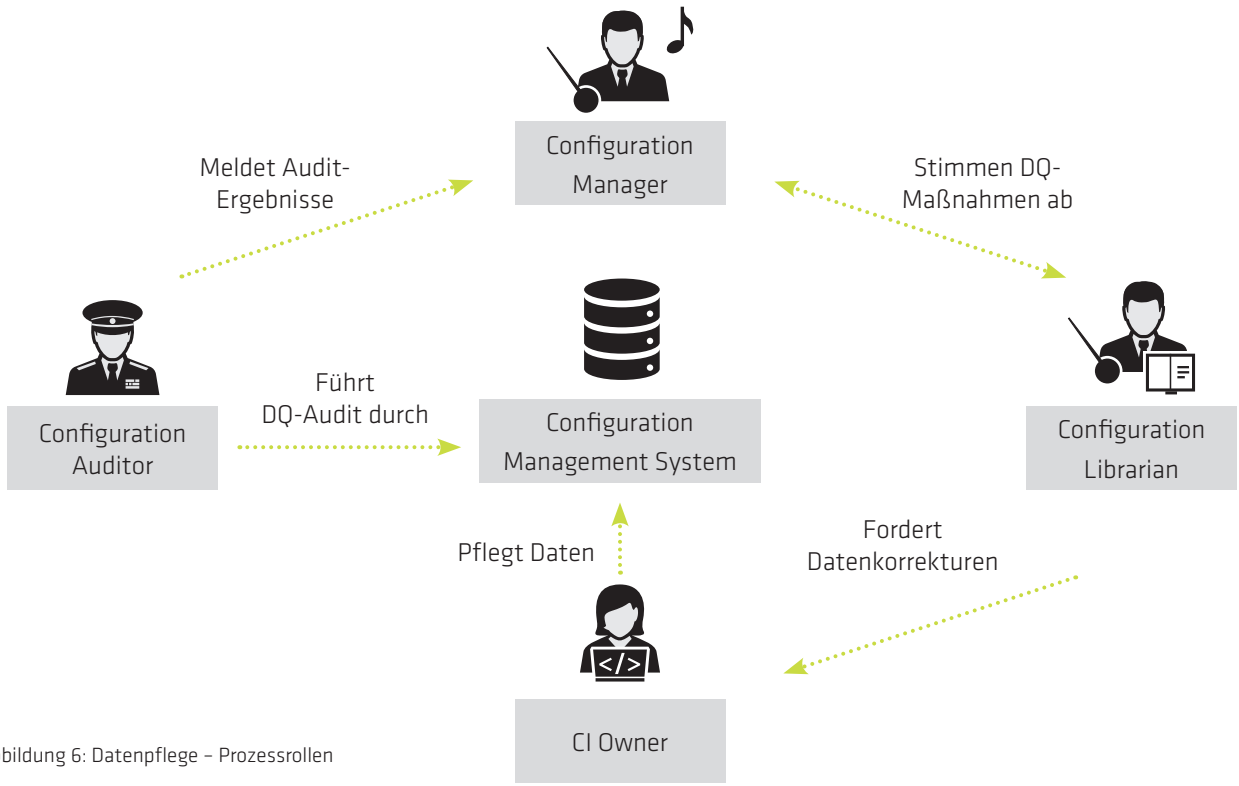


Abbildung 6: Datenpflege – Prozessrollen

Abbildung 7: Ausschnitt aus einem Dashboard für zu prüfende CI mit eindeutiger Zuordnung der Verantwortlichkeit in FNT Command

2.1.4 Neue Elemente in der BAIT

Relativ neu in der BAIT sind die Themen Auslagerung und KRITIS. Immer häufiger werden IT-Dienstleistungen an spezialisierte Anbieter ausgelagert. Dagegen spricht laut BAIT nichts, allerdings müssen die Anforderungen nach AT 9 der MaRisk erfüllt werden. Diese fordert unter anderem eine wirksame Exit-Strategie. Für jede Auslagerung muss zudem eine Risikoanalyse zur Bewertung durchgeführt werden. Aus dieser Analyse sollen Maßnahmen erarbeitet werden und bei der Gestaltung von Verträgen einfließen.

Das KRITIS Gesetz ist der neueste Bestandteil der BAIT. KRITIS steht kurz für Kritische Infrastrukturen und umfasst Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[6] Darunter fällt unter anderem das Finanz- und Versicherungswesen, zum Beispiel mit der Bargeldversorgung. Um die Anforderungen aus dem KRITIS Gesetz zu erfüllen, ist es notwendig eine Erkennung von kritischen Infrastrukturen innerhalb des eigenen Instituts zu etablieren und diese Infrastrukturen zu dokumentieren. Auch das kann direkt am Configuration Item in der CMDB erfolgen. Das Gesetz fordert des Weiteren, dass Incidents an diesen Systemen dem BSI gemeldet werden. Dazu müssen Incident Tool und CMDB/CMS über Schnittstellen technisch und prozessual verbunden werden.

[6] https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

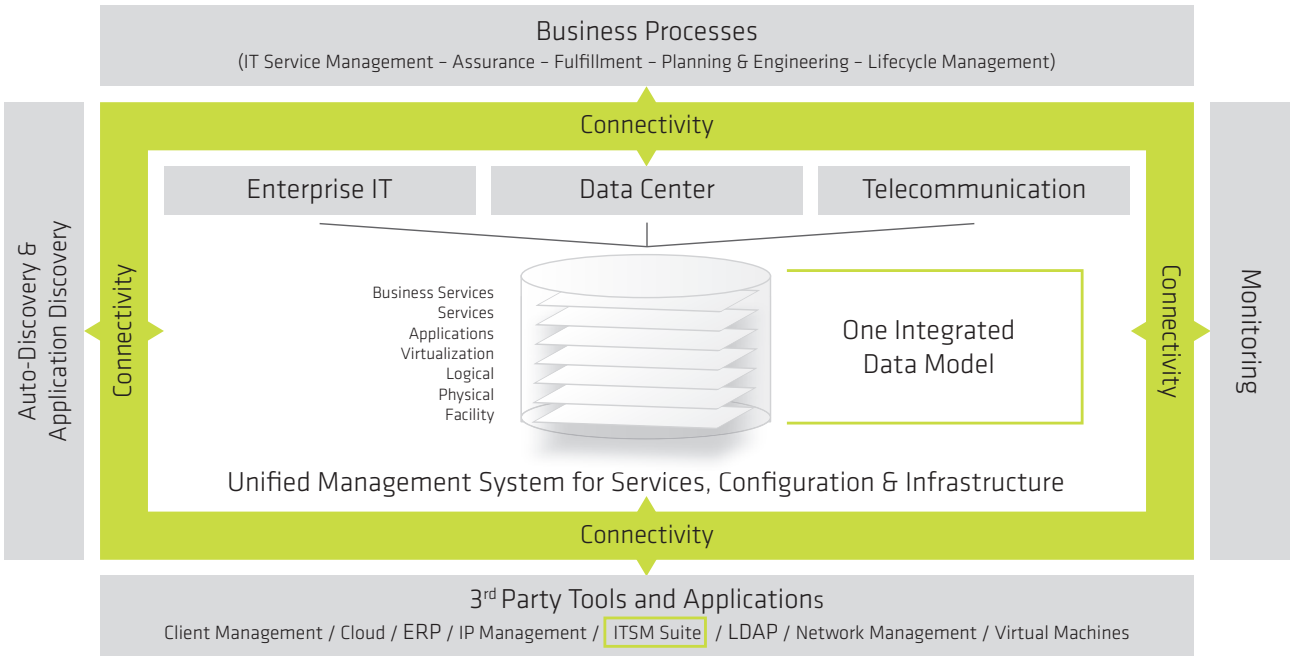


Abbildung 8: Einbindung des Configuration Managements in die Unternehmens-IT wie unter anderem für die Abbildung der KRITIS Anforderungen sinnvoll

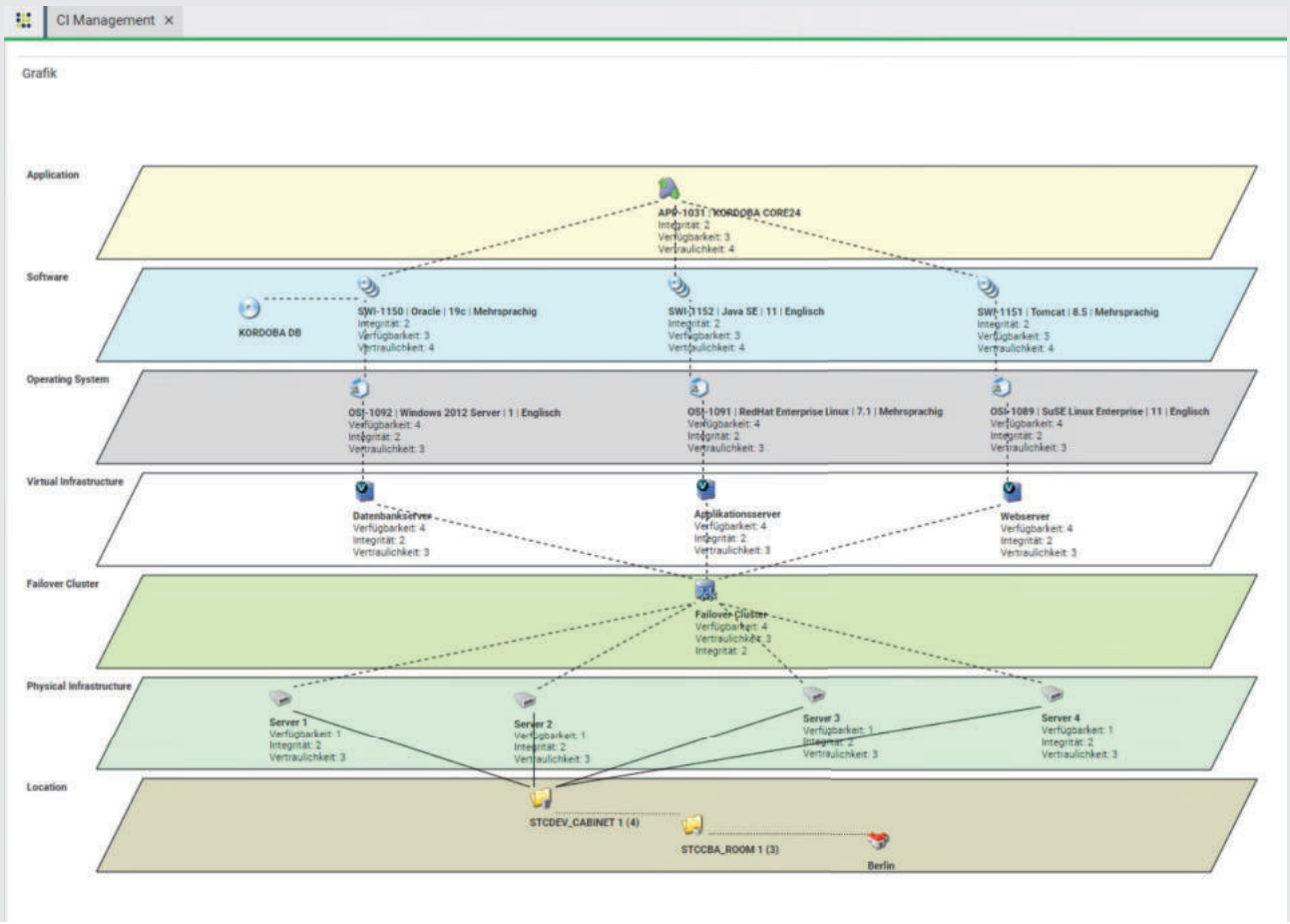


Abbildung 9: Beispiel für den Verteilungseffekt bei der Vererbung von Schutzbedarfen innerhalb eines Informationsverbundes für die Applikation Kordoba in FNT Command

3 Auswirkungen in der Praxis

Die Umsetzung der Anforderungen ändert das tägliche Leben der IT-Abteilung deutlich. Doch die BAIT bringt dabei mehr als nur Dokumentationsaufgaben. Das sich durch die Maßnahmen entwickelnde Risikobewusstsein fördert auch das Verständnis für die Arbeit der Instituts-IT. Nachfolgend wird beschrieben, wie sich normale Tätigkeiten des Betriebs durch die regulatorischen Anforderungen verändern.

3.1 ANFORDERUNG AUS DEM BUSINESS

Als Beispiel dient hier eine Veränderung an einem Business Service. Bisher wurden dort Börsendaten verarbeitet, jedoch bestand keine Verbindung zu den Portfolio-Daten der Kunden. Nun soll diese Anbindung geschaffen werden. Ohne MaRisk und BAIT wäre das nur eine Anforderung für ETL-Entwickler. Außerdem würde man die Vorgaben der Datenschutzgrundverordnung (DSGVO) in Betracht ziehen, da es sich um personenbezogene Daten handelt. Dies hat zur Folge, dass - auch wenn es sich dabei auf den ersten Blick nur um Änderungen an Applikationen bzw. deren Erweiterung um eine entsprechende Schnittstelle handelt – nun der vollständige Informationsverbund betrachtet und die Änderungen analysiert werden werden müssen.

3.2 SCHUTZBEDARFSANALYSE

Das Werkzeug der Wahl hierfür ist in diesem Beispiel die Schutzbedarfsanalyse. Klassisch wird der Schutzbedarf für Daten, Dokumente und IT-Anwendungen ermittelt. In diesem Fall sollte mindestens ab der Anwendungsebene neu analysiert werden, da dort die personenbezogenen Daten zusätzlich verarbeitet werden. Dies erfolgt auf Basis von Templates oder ISMS-Tools durch das Informationssicherheitsmanagement in den Fachbereichen. Die ermittelten Werte für Integrität, Vertraulichkeit und Authentizität werden anschließend auf die dahinter liegenden IT-Systeme, Netzwerke und -komponenten vererbt.[7]

Die Darstellung im Tool (ISMS, CMDB) kann auch in Form eines klassischen Reports erfolgen, ist dann aber weniger übersichtlich. Der vererbte Schutzbedarf wird häufig als Schutzbedarfseignung bezeichnet. Damit wird verdeutlicht, dass zum Beispiel der Server selbst keinen Schutzbedarf hat, aber in der Nutzung für einen bestimmten Schutzbedarf geeignet ist.

[7] https://www.bcm-news.de/2016/07/12/business-impact-und-schutzbedarfsanalyse-gemeinsamkeiten-und-unterschiede/

Im Beispiel der neuen Schnittstelle ändert sich die Vertraulichkeitsbewertung. Dies erfordert, dass die genutzten virtuellen Server gegebenenfalls besser abgesichert werden. Das BSI empfiehlt für virtuelle Server unter anderem grundsätzlich auf Verschlüsselung zu setzen. Weitere Maßnahmen zur Absicherung und damit der Erhöhung der Vertraulichkeitseignung eines virtuellen Servers sind im IT-Grundschutz Kompendium unter SYS.1.5.A8 ff zu finden.[8]

Darauf sollte man achten:

- **Datenqualität:** Informationsverbund ist nicht durchgängig definiert (➔ ISMS)
- **Regeln für Bestimmung/Vererbung nicht bekannt:** Schutzbedarfe/-eignung ist für bestimmte Komponenten nicht klar
- **Fehlende Relationen:** Zusammenhänge innerhalb des IV sind nicht oder nur teilweise dokumentiert
- **Vererbung nicht vollständig oder falsch durchgeführt:** Mangelhafte/nicht vorhandene Vererbung von Schutzbedarfseignungen

3.3 CHANGE-VORBEREITUNG

Die neue Schutzbedarfsanalyse liefert daher neben neuen Bedarfsinformationen auch Hinweise zu notwendigen Änderungen an den Komponenten des Informationsverbundes. Nach ITIL werden solche Anpassungen im Rahmen eines oder mehrerer Changes umgesetzt. Auch dabei sollten alle Risiken bekannt sein, um einen reibungslosen IT-Betrieb sicherzustellen. Soweit stimmen ITIL und BAIT überein. Für die Vorbereitung des Changes stehen aber möglicherweise bisher nicht durchgeführte Tätigkeiten an.

Neben der Anpassung des EAM Bauplans sollte unbedingt eines Auswirkungsanalyse, als Risikoanalyse im Sinne von BAIT, durchgeführt werden. Dabei wird beantwortet, welche Auswirkungen der Change auf die Komponenten des Informationsverbundes und damit auf die Bereitstellung des Business Service hat. Zudem müssen die zu informierenden Stellen identifiziert werden. Die Auswirkungsanalyse beschreitet im Informationsverbund den umgekehrten Weg der Schutzbedarfsvererbung. Dabei gelten vergleichbare Regeln im Hinblick auf die Verfügbarkeit. Änderungen an einem physischen Server innerhalb eines Clusters hat weniger Auswirkung auf die Verfügbarkeit eines Service als in unserem Beispielfall die Änderung an einem virtuellen Server.

Darauf sollte man achten:

- **Fehlende Methodenkenntnis:** Das Change Management und auch die Auswirkungsanalyse sind keine Disziplinen, die jedem bekannt sind.
- **Fehlende Daten im Informationsverbund:** Der Analyseerfolg steht und fällt mit der Datenqualität.
- **Mangelhafte Verknüpfung von CMS und EAM**

Als Ergebnis der Analyse stehen also Informationen zu den Change-Risiken und ggf. ein angepasster EAM Bauplan. Für den eigentlichen Change können so Maßnahmen zur Ausfallminimierung vorgesehen werden.

[8] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_5_Virtualisierung.html?nn=10137184#doc10095768bodyText16

3.4 UMSETZUNG UND DOKUMENTATION DER NOTWENDIGEN ÄNDERUNGEN

Im Rahmen der Change-Durchführung muss die ordnungsgemäße Dokumentation der Änderungen sichergestellt werden. Hierzu hat es sich bewährt den Change-Management Prozess mit dem Configuration Management eng zu verschränken. Aus Prozesssicht kann das über eine gemeinsame Vereinbarung der beiden Prozess Owner über Zuständigkeiten und Vorgehensweisen geschaffen werden. Die Tools der Prozesse sollten ebenso verbunden werden. Eine Schnittstelle aus dem CMS in das Change Tool liefert Daten zu den Configuration Items. So können CI Informationen im Change dokumentiert werden. Änderungen im CMS werden dabei immer unter Angabe einer Begründung und einer Change oder Request ID dokumentiert. Viele CMDBs bieten die Möglichkeit, Attribute wie diese beiden als Pflichtfelder zu markieren, was sicherstellt, dass diese Angaben bei jeder Änderung angegeben werden muss. In regelmäßigen Auditreports wird geprüft, ob korrekte und ausschließlich genehmigte Changes bzw. Requests für Änderungen in der CMDB verwendet wurden. Für den Request Fullfilment Prozess sollte geprüft werden, ob jeder Request Typ für Änderungen im Configuration Management sinnvoll ist und damit Änderungen an der Dokumentation genehmigt werden können.

Darauf sollte man achten:

- **Pflege der CMDB-Daten erfolgt nur im Configuration Management durch ein dediziertes „Pflegeteam“:** Nein, besser nicht! Denken Sie prozessorientiert.
- **Mangelhafte Datenqualität:** Ist die Datenqualität zu gering, fehlt die Verlässlichkeit der CMDB und das Vertrauen in Selbige geht verloren.
- **Verifikations- und Kontrollmechanismen zu spät oder gar nicht eingeführt:** Planen Sie Verifikations- und Kontrollmechanismen bereits vor Erstbefüllung der CMDB ein.

3.5 SOLL-IST-ABGLEICH

Zur weiteren Sicherung der Dokumentationsqualität muss periodisch ein Soll-Ist-Abgleich durchgeführt werden. Der Abgleich kann aber auch situativ zum Beispiel im Nachgang eines Changes durchlaufen werden, um die Qualität in Bezug auf diesen Change zu prüfen. Dieser wird anhand der Dokumentation im CMS (Soll) und der Daten in den Bestandssystemen (Ist) erstellt. Der Abgleich kann über Reports durchgeführt werden. Als Ergebnis erhält man Informationen zu Vollständigkeit und Korrektheit der Dokumentation. Im Configuration Management ist für die Ableitung von Maßnahmen zur Datenkorrektur die Rolle des Configuration Librarian vorgesehen.

Darauf sollte man achten:

- **Ermittlung Datenbestand IST nicht möglich:** Insbesondere die von der Prüfung explizit geforderte Überwachung von IDVen macht häufig Schwierigkeiten, da zum Beispiel Excel-Dateien von außen nicht als IDV zu erkennen sind, aber eine solche sein können.
- **Ermittlung Datenbestand SOLL nicht möglich** (z.B. „Was heißt ‚produktiv‘ wirklich?“)
- **Unregelmäßige Durchführung von Audits:** Häufig wird der Aufwand für Audits gescheut und daher zu selten durchgeführt.
- **Zuarbeit der Fachabteilungen nicht ausreichend:** Häufig wird in den Fachabteilungen der Datenpflege und -korrektur keine Priorität eingeräumt.

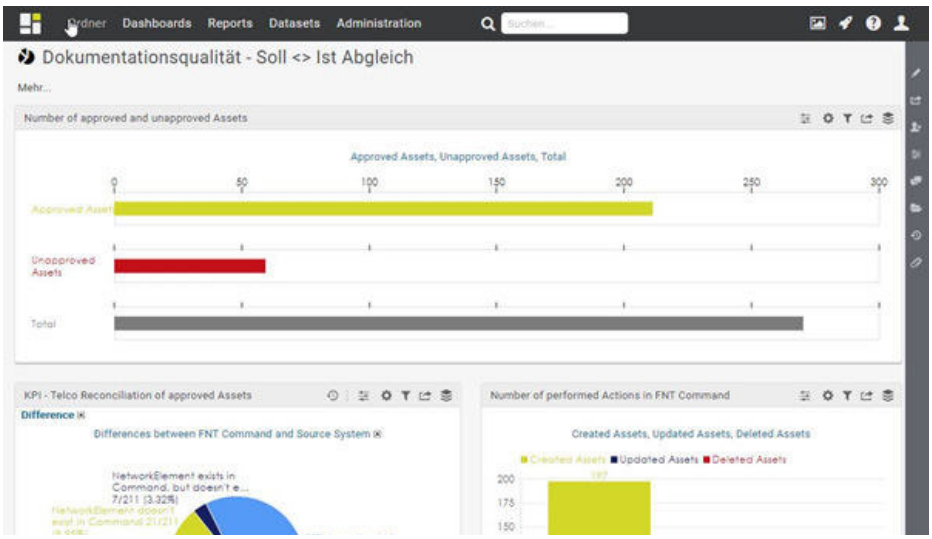


Abbildung 10: Beispiel für ein Dashboard zum Soll-Ist-Abgleich in FNT Command

4 Fazit und Tipps kompakt

Das Beispiel zeigt, wie sinnvoll es ist, der Empfehlung der BaFin zu gängigen Standards nachzugehen. MaRisk und insbesondere BAIT erfinden nämlich nicht wirklich etwas neu. Viel mehr dient die BAIT als Leitwerk für die Verfeinerung zumeist sowieso vorhandener Prozesse und Tools. Dabei ist es viel wichtiger, auf der Prozessebene die ersten Schritte zu machen als neue Tools einzuführen. Häufig lassen sich dort bereits vorhandene Funktionen, wie z.B. das Reporting, für die Anforderungen aus der BAIT nutzen.

Allerdings wird der Service-Gedanke nun Pflicht. Es reicht nicht, nur den eigenen Bereich zu sehen. Stattdessen fordert die BaFin Risikobewusstsein auf allen Ebenen und das funktioniert nur mit Überblick über die genutzten Informationsverbünde. Eine große Hilfe kann ein gut gepflegtes Configuration Management System sein. Das CMS hilft als übergreifendes Tool eine gemeinsame Sprache zwischen den IT-Silos zu finden, so dass der organisatorische Change gelingen kann.

In der Praxis finden wir hier sehr oft FNT Command als Tool vor, mit dem nahezu alle Anforderungen sinnvoll abgedeckt werden können.

Rechtzeitig anzufangen, also nicht erst dann, wenn BaFin oder EZB zur Prüfung kommen, lohnt sich also nicht nur, um eben diese zu bestehen. In den meisten Unternehmen lassen sich weitere Erfolge erzielen. Durch den gewonnenen Überblick lassen sich Services verschlanken und immer wieder ungenutzte Datenbanken und ähnlich kostspielige Komponenten entdecken. Zudem wird ein IT-Betrieb ohne unnötigen Ballast und mit so geringem Risiko wie möglich immer wichtiger. Denn mit der Idee „Bank als App“ ist zukünftig jede Downtime undenkbar.

Führen Sie daher einen „BAIT-Readiness-Check“ durch und erarbeiten Sie ein Vorgehen, um die Anforderungen der BAIT vollständig zu erfüllen. Nur so können Sie entspannt auf etwaige Prüfungen zu gehen und haben damit auch einen Trigger, um Ihre IT in die Zukunft zu führen.

Sinnvolle erste Schritte:

- Definition von Informationsverbünden und Festlegen der Bestandteile der Organisation / Prozesse und IT
- Durchführung einer Strukturanalyse und Dokumentation von IT-Infrastrukturen des Informationsverbundes in einem zentralen Register (CMDB)
- Dokumentation von Anwendungen des Unternehmens (ADV und IDV) samt Ansprechpartner, SLA und Schutzbedarfsinformationen
- Erheben der IT-technischen Abhängigkeiten und Schnittstellen
- Definition von Schutzzielen zu Vertraulichkeit, Verfügbarkeit und Integrität
- Schutzbedarfsvererbung auf IT-Infrastrukturen definieren und umsetzen, idealerweise am CI in der CMDB
- Definition von IKS Kontrollen (und Aufbau eines unterstützenden Reportings hierfür)
- Aufbau eines Datenqualitätsreportings zur Messung von Vollständigkeit, Korrektheit und Aktualität der Daten, z.B. CMDB Datenqualität

Langfristige Schritte:

- Projekt aufsetzen: Zumeist sind die Aufgaben zur Umsetzung der regulatorischen Anforderungen nicht neben dem Alltag zu schaffen. Schaffen Sie daher einen angemessenen Rahmen.
- Tools: Folgende Anforderungen sollten erfüllt werden:
  - Erweiterbarkeit: Es fehlen Funktionen für die Umsetzung der reg. Anforderungen? Kein Problem, wenn Ihre Tools erweiterbar sind.
  - Visualisierung: Durch grafische Darstellung lassen sich Informationsverbünde besser erarbeiten.
  - Schnittstellen: Schnittstellen sind das A und O, um zum Beispiel einen vollständigen Überblick über Ihre CI schaffen zu können.
  - Weitere Anforderungen: Berechtigungskonzept, Mandantenfähigkeit, Historisierung, Baselining, Updatefähigkeit (keine Neukonzeption für Majorreleases).

5 Abkürzungsverzeichnis und Glossar

5.1 ABKÜRZUNGSVERZEICHNIS

BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

BAIT Bankaufsichtliche Anforderungen an die IT

BSI Bundesamt für Sicherheit in der Informationstechnik

CI Configuration Item

CMS Configuration Management System

DSGVO Datenschutzgrundverordnung

EAM Enterprise Architecture Management

ETL Extract, Transform, Load

IDV individuelle Datenverarbeitung

ISMS Informationssicherheitsmanagementsystem

Kritis Kritische Infrastrukturen

KWG Kreditwesengesetz

MaRisk Mindestanforderungen an das Risikomanagement

5.2 GLOSSAR

BSI-Standards und Grundschutzkataloge Die IT-Grundschutz-Kataloge (vor 2005: IT-Grundschutzhandbuch) sind eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die der Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IT-Umgebungen (IT-Verbund) dienen. Die Sammlung umfasst mit Einleitung und Katalogen über 4.800 Seiten (15. Ergänzungslieferung aus 2016) und dient Unternehmen und Behörden als Grundlage zum Erlangen einer Zertifizierung nach IT-Grundschutz. Durch die Zertifizierung zeigt ein Unternehmen, dass es geeignete Maßnahmen zur Absicherung seiner IT-Systeme gegen IT-Sicherheitsbedrohungen unternommen hat.

Basel III bezeichnet Vorschriften des Basler Ausschusses der Bank für Internationalen Zahlungsausgleich (BIZ) zur Regulierung von Banken. Seit 2013 löst Basel III schrittweise die Basel II genannten Vorläuferregeln ab. Grund der Reform waren Schwächen der bisherigen Bankenregulierung, die durch die Finanzkrise ab 2007 offengelegt wurden.

Configuration Management System Das Configuration Management System (CMS) ist eine Kombination von Tools und Daten, die zum Sammeln, Speichern, Managen, Aktualisieren, Analysieren und zur Präsentation von Daten zu allen Configuration Items und deren Beziehungen eingesetzt wird. Ein CMS kann ein oder mehrere physikalische Configuration Management Databases (CMDB) verwalten. Die dem CMS zugrundeliegende Struktur wird definiert durch ein Configuration-Modell, ein logisches Modell der Service Assets einer IT-Organisation.

Governance – oft übersetzt als Regierungs-, Amts- bzw. Unternehmensführung –, auch Lenkungsform, bezeichnet allgemein das Steuerungs- und Regelungssystem im Sinn von Strukturen einer politisch-gesellschaftlichen Einheit wie Staat, Verwaltung, Gemeinde, privater oder öffentlicher Organisation.

Schutzbedarf Der Schutzbedarf umfasst die Anforderungen einer Anwendung oder ein Service hinsichtlich der Schutzziele „Integrität", „Verfügbarkeit", „Vertraulichkeit" und "Authentizität".

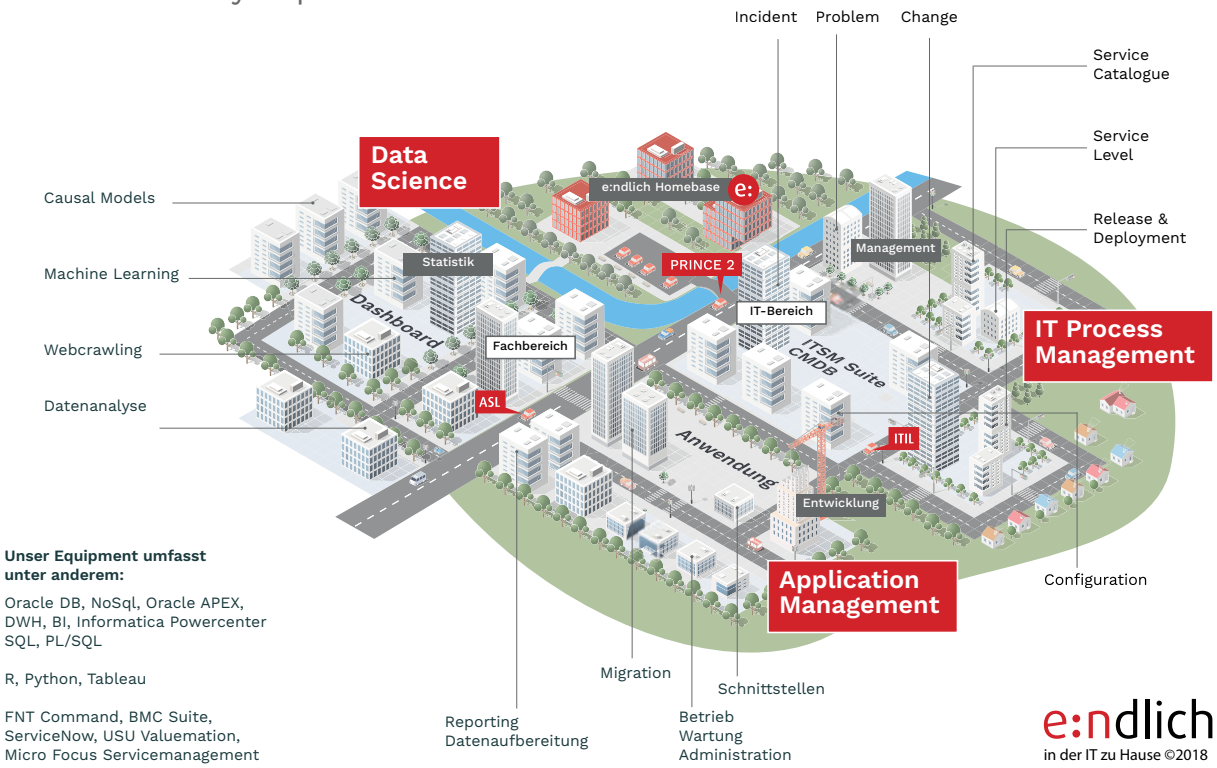
Maximumprinzip In der IT-Sicherheit wird der jeweils höchste Schutzbedarf eines Objektes (Anwendung, Arbeitsplatzrechner, Server, Raum) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit auf das übergeordnete Objekt übertragen.

Kumulationseffekt Als Kumulationseffekt (von lateinisch cumulare = aufhäufen) bezeichnet man im Bereich der IT-Sicherheit einen Effekt, der durch Anhäufung mehrerer (auch kleinerer) Schäden auf einem IT-System einen insgesamt höheren Gesamtschaden entstehen lässt.

Verteilungseffekt Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

ISO 27001:2015 Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation. Darüber hinaus beinhaltet die Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Hierbei werden sämtliche Arten von Organisationen berücksichtigt. Die Norm wurde auch als DIN-Norm veröffentlicht und ist Teil der ISO/IEC 2700x-Familie.

In der IT zu Hause
die e:ndlich citymap



Einsatzbereiche von e:ndlich im Bereich ITSM und Configuration Management

Wir gewährleisten die Transparenz Ihrer technischen Infrastrukturen und sichern Ihr operatives Geschäft:

Mit unserer Expertise aus unterschiedlichsten ITSM-Projekten bieten wir Ihnen hochwertige, fachliche Leistungen in der Strategie, Konzeption, Entwicklung, Einführung und dem Rollout von ITSM Prozessen und Systemen.

Im Configuration Management Umfeld verfügen wir über 10 Jahre Erfahrung in den Branchen Automobil, IT-Dienstleister, Banken und Versicherungen und kennen intensiv die Sorgen unserer langjährigen Kunden und beraten im Prozess- und Systemumfeld. Technisch unterstützen wir Sie bei einer bestehenden CMDB im Bereich der CMDB Schnittstellen, der Staging Area und dem CMDB Reporting.

Informationen zum Autor

Nikolai Weidmann ist Senior Consultant für ITSM Beratung bei der e:ndlich GmbH & Co. KG. Parallel zu seiner Arbeit hat er ein berufsbegleitendes Studium zum Bachelor of Science Wirtschaftsinformatik erfolgreich abgeschlossen. Schwerpunktmäßig ist Herr Weidmann in der Beratung, Konzeption, Entwicklung und dem Rollout von IT-Service Management Tools sowie deren Toolschnittstellen tätig. Sein tiefes Prozess Know-How vornehmlich im Incident, Problem, Change und Configuration Management runden seine Expertise ab. Darüber hinaus beschäftigt er sich mit komplexen Themen, wie dem Business Intelligence, und ist Trainer für Inhouse- oder Offsite-Seminare.

Kontakt:

e:ndlich GmbH & Co. KG
Moststraße 33
90762 Fürth
E-Mail: info@endlich.it
Web: www.endlich.it
Telefon: +49 911 4087-0555

Über FNT

Leistungsfähige, störungsfreie und flexible Infrastrukturen sind die Basis für alle digitalen Geschäftsprozesse und Anwendungen, sei es Smart Cities, Industrie 4.0 oder auch 5G. Mit den standardisierten Softwarelösungen der FNT GmbH erfassen, dokumentieren und managen Unternehmen und Behörden ihre komplexen und heterogenen IT-, Telekommunikations- und Rechenzentrumsinfrastrukturen – von der physikalischen Ebene bis zum Business Service herstellerunabhängig und nach einem einheitlichen Datenmodell.

FNT liefert damit die nötige Transparenz und Tools, um die IT-, RZ- und TK-Landschaft einfacher planen und verwalten, Störungen schneller beseitigen, Ressourcen und Bedarfe optimal synchronisieren und neue digitale Services flexibel und automatisiert bereitstellen zu können. Zu den Kunden zählen mehr als 500 Unternehmen und Behörden weltweit, darunter mehr als die Hälfte der im DAX30 notierten Konzerne. FNT hat seinen Hauptsitz in Ellwangen (Jagst) und betreibt Niederlassungen in den USA (Parsippany, New Jersey), Singapur, Dubai und Russland (Moskau). In zahlreichen Ländern bietet FNT seine Software über Partnerschaften mit den marktführenden IT-Service-Providern und Systemintegratoren an.

FNT GmbH, Röhlinger Straße 11, 73479 Ellwangen, Deutschland, Tel. +49 7961 9039-0, info@fntsoftware.com // **fntsoftware.com**

e:ndlich
in der IT zu Hause

Moststr. 33
D-90762 Fürth
www.endlich.it

Oktober 2020