BADEN-WÜRTTEMBERGISCHER
GENOSSENSCHAFTSVERBAND e.V.

Notes-Datenbanken SOIT und Risikomanagement

Stand: März 2019

Ihr Ansprechpartner

Stefan Beck
Beratung Genossenschaftsbanken – Prozesse

Fon: 0174 3478 985
Mail: stefan.beck@bwgv-info.de

bwgvberatung.

Baden-Württembergischer Genossenschaftsverband e.V.
Heilbronner Straße 41 | 70191 Stuttgart | www.wir-leben-genossenschaft.de

Produkt

Notes-Datenbanken

Standard für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT), Risikomanagement (RiMa)

Kurzbeschreibung

Der Standard für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT), interpretiert für alle Genossenschaftsbanken im Finanzverbund die Vorgaben gängiger Standards und konkretisiert diese auf das agree21®- und bank21-Umfeld. Dadurch entsteht ein für die Genossenschaftsbank geeigneter Standard, der durch Anwendung, die Umsetzung der aufsichtsrechtlichen Anforderungen aus MaRisk AT 7.2 zur Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse anhand eines gängigen Standards erfüllt. Autor und Herausgeber des Standards für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT) ist der Arbeitskreis Ordnungsmäßigkeit und Revision.
Sofern eine Bank von einzelnen Anforderungen abweicht, sind daher die Auswirkungen insbesondere auf die Erfüllung der Ordnungsmäßigkeits- und Sicherheitsanforderungen zu untersuchen, ggf. Maßnahmen abzuleiten (z. B. zur Risikoreduzierung), die Ergebnisse im Rahmen einer Risikoanalyse zu dokumentieren und in den hausindividuellen und unternehmensweiten Risikomanagementprozess der operationellen Risiken nachweislich zu tragen. Die Funktionen der Datenbank können darüber hinaus für weitere Risikoanalysen z.B. für Anwendungen in wesentlichen Geschäftsprozessen und zur Dokumentation von regelmäßigen Kontrollhandlungen genutzt werden.

Um den Prozess in den Banken zu etablieren, hat der Baden-Württembergische Genossenschaftsverband (bwgv) die gleichnamige Notes-Datenbank entwickelt, die die Banken bei o. g. Aufgabenstellung praxis- und technikorientiert unterstützt.

Das Modul Risikomanagement (RiMa) erweitert die SOIT-Datenbank. Diese Datenbank dient zur übersichtlichen Darstellung und Auswertung der IT-Risiken für die Berichterstellung. Eine integrierte Schnittstelle zum SOIT ermöglicht eine direkte Übernahme der Risiken. Weiterer Leistungsinhalt des Risikomanagement ist es die Risiken im Einflussbereich der Bank aus den vierteljährlichen Risikoreports des Rechenzentrums dokumentiert auszuwerten und neben weiteren eigenen Risikoanalysen diese ebenfalls in die Berichtserstellung aufzunehmen. Dabei unterstützt die Datenbank die Bank durch einen integrierten Workflow bei der dokumentierten Genehmigung/Kenntnisnahme der Risiken.

Neben der Berichterstellung der IT-Risiken können in dieser Datenbank alle aufsichtsrechtlich geforderten Bestandteile eines Informationsrisikomanagements komplett Medienbruchfrei und arbeitsteilig vorgenommen werden. Dies sind:

- Durchführung eines vollständigen Risikomanagements mit Maßnahmendefinition und deren Nachverfolgung.
- Ermittlung des Schutzbedarfs aller Prozesse mit integrierter Business Impact Analyse (BIA) - „Prozessklassifizierung“.
- Dokumentation aller Schutzobjekte zur Ermittlung deren Schutzniveaus - Sicherheitskonzepte“.
- Dokumentation der Schutzobjekte bezüglich derer MaRisk Relevanz nach AT 7.2 Tz. 6 „Test und Freigabeverfahren“.

Sowie weitere Funktionen die den Arbeitsablauf des Informationsrisikomanagements optimieren und vereinfachen.

Kundennutzen

- Tool zur Umsetzung eines gängigen Standards im Sinne der Anforderungen aus MaRisk AT 7.2
- revisionssichere Dokumentationsplattform der im SOIT dargestellten Checklisten Fragen
- Elektronische Unterstützung des Updateprozesses
- Identifizierung von IT-Risiken und Dokumentation der Umsetzung von Sicherheitsmaßnahmen durch elektronische Workflowunterstützung
- Übersichtliche Darstellung aller IT-Risiken zu Auswertungszwecken

Weitere Anmerkungen

Einzelpreis Datenbanken ohne Beratungsleistung:

Der Preis für die Datenbanken und Updates richtet sich nach der Bilanzsumme der Bank zum 31.12. des Vorjahres der Bestellung bzw. Auslieferung des Updates gemäß folgender Staffel:

Bilanzsumme per 31.12. des Vorjahres in Mio. Euro BWGV-Mitgliedsbanken*)	Erstauslieferung (netto in Euro)	Abo-Preis je Update (netto in Euro)
bis 250	1.000,00	150,00
251 bis 500	1.000,00	200,00
501 bis 1.000	1.200,00	250,00
1.001 bis 1.500	1.200,00	300,00
1.501 bis 2.000	1.200,00	350,00
2.001 bis 3.000	1.400,00	400,00
ab 3.001	1.600,00	500,00

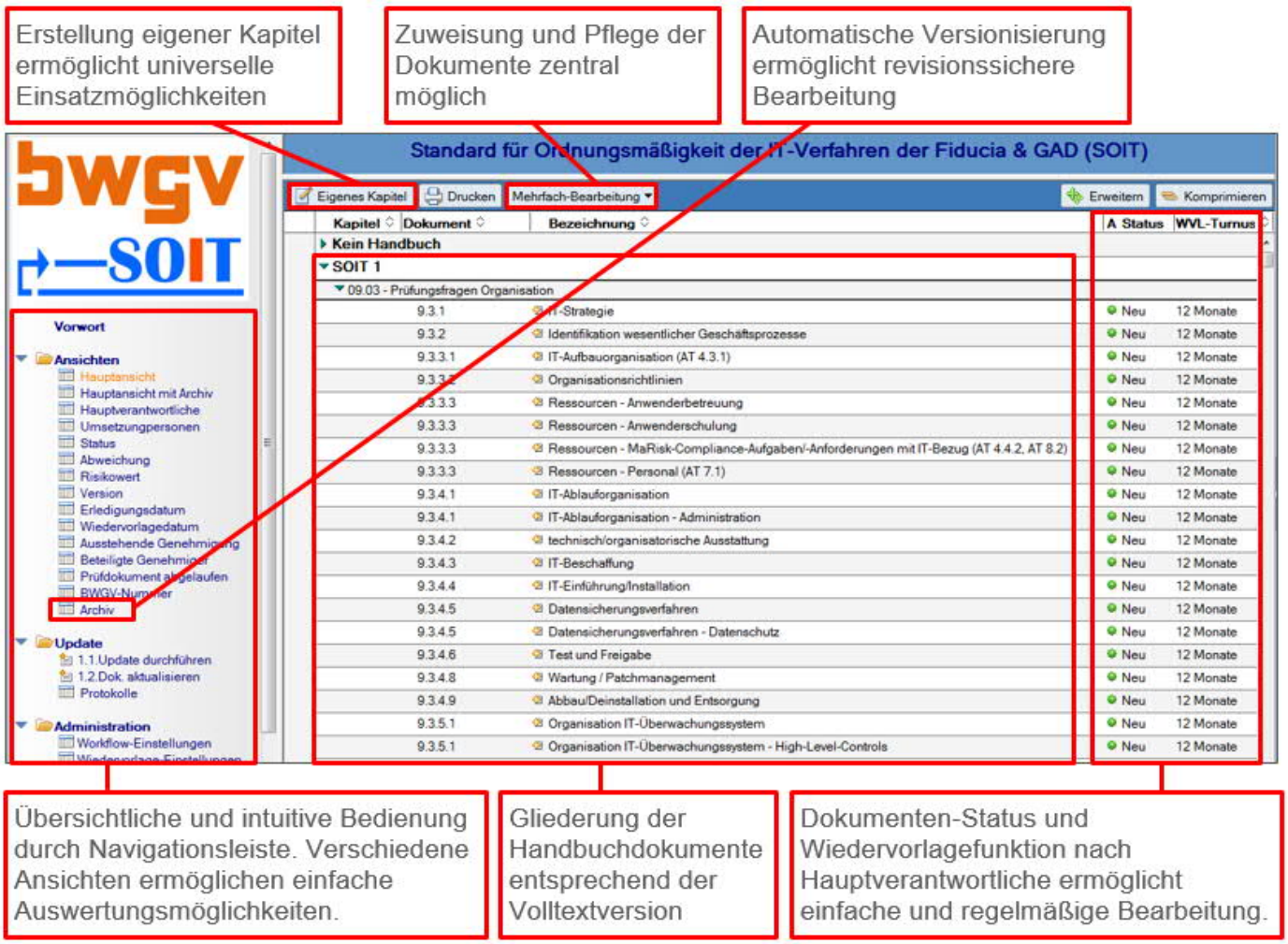
*) für Nichtmitglieder des BWGV: Abo-Preis je Update zzgl. 50,00 EUR; Erstauslieferung zzgl. 200,00 EUR

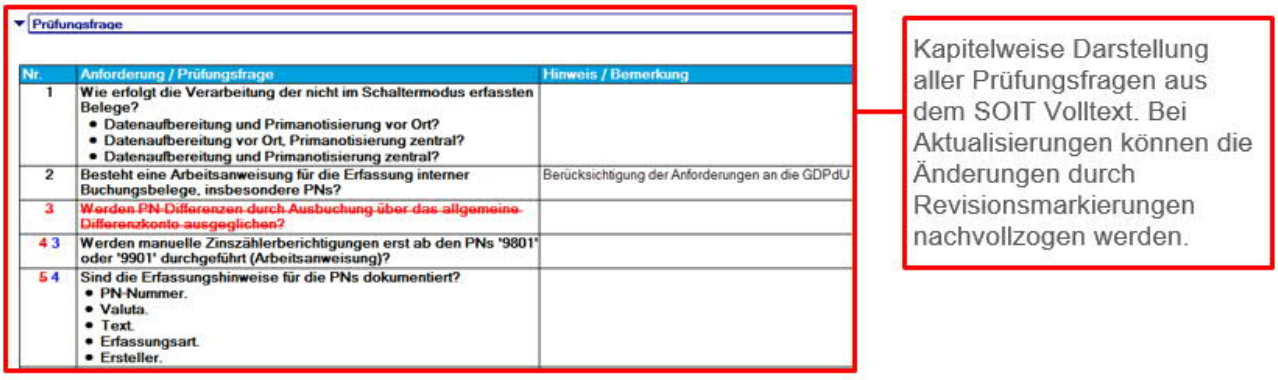
Beratungsleistungen:
zzgl. Beratungsumfang zur Einrichtung der Datenbanken, nach aktuellem Tagessatz:

- ca. 0,5 Beratertag technische Ingangsetzung der Datenbanken
- ca. 0,5 Beratertag Schulung der Mitarbeiter

In der Folge erforderliche Einzelleistungen werden nach Aufwand berechnet.

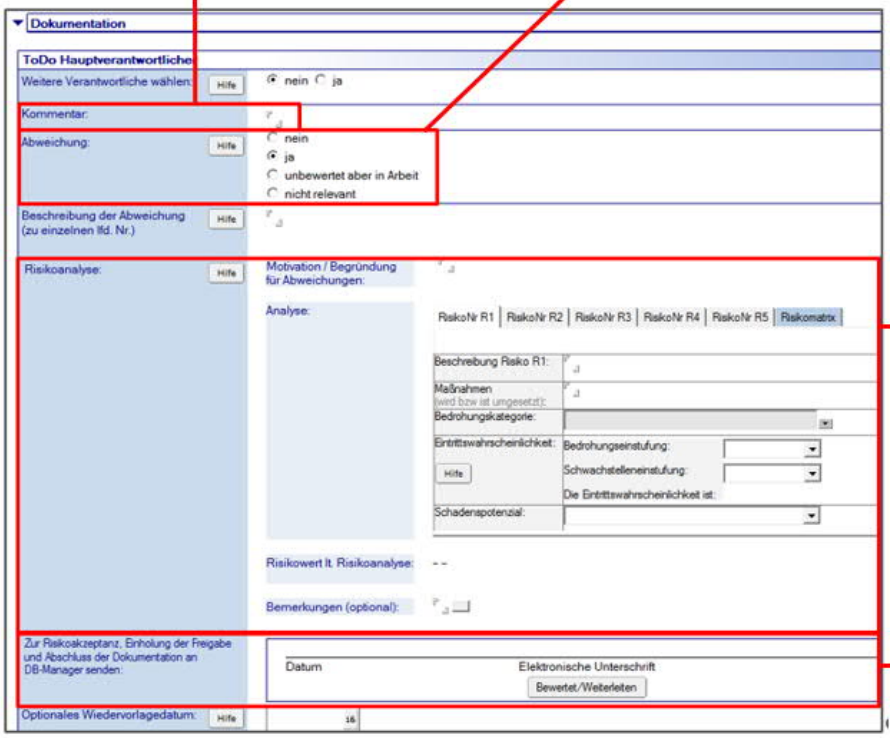
Screenshots





Kommentarfeld ermöglicht die Beantwortung jeder Frage. Die Dokumentation bleibt dabei auch bei Aktualisierungen vorhanden und erleichtert Überprüfung.

Einschätzung des Kapitels und Beantwortung der Fragen stellt die Grundlage für die Bewertung und weitere Bearbeitung des Dokuments.



Integrierte Risikoanalyse ermöglicht bei Abweichung entsprechend des Standards einer Risikobewertung diese durchzuführen.

Direkte Schnittstelle zur Risiko-management-Datenbank und diverse Auswertungsmöglichkeiten ermöglichen es die festgestellten Risiken in das Risikocontrolling zu übernehmen.

Elektronische Unterschrift dokumentiert Beantwortung und evtl. Risikoanalyse.

Artikel im Genograph vom September 2015:

© magele - fotolia.com

Das „Handbuch Ordnungsmäßigkeitsfragen der Agree-Bankorganisation" (HB OF) bildet die Vorgaben gängiger Standards ab und konkretisiert diese für das Agree-Umfeld.

Die Einhaltung gängiger Standards effizient umsetzen

von Stefan Beck

GENOGRAPH 9/2015

Nur wer seine Prozesse und die eingesetzten IT-Systeme genau kennt, kann diese optimal auf die sich ständig verändernde Umwelt anpassen. Neben den betriebswirtschaftlichen Aspekten sind auch die aufsichtsrechtlichen Anforderungen der Mindestanforderungen an das Risikomanagement (MaRisk) zu erfüllen. Nach den MaRisk ist eine angemessene technisch-organisatorische Ausstattung von IT-Systemen und den dazugehörigen IT-Prozessen notwendig. Dabei müssen diese die Schutzziele Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse auf gängige Standards abzustellen. Diese Anforderung gilt unabhängig davon, ob die IT-Systeme und -Prozesse von der Bank selbst betrieben werden, ob diese ausgelagert sind, oder die Leistung anderweitig von externer Stelle bezogen wird.

Eine Bank ist daher verpflichtet, anhand eines solchen Standards regelmäßig zu überprüfen, ob ihre IT-Systeme und -Prozesse diese Anforderungen (noch) erfüllen. Da diese Prüfung sowohl Bestandteil der internen als auch der externen Compliance-Prüfungen ist, sollte diese so durchgeführt werden, dass ein sachverständiger Dritter dies jederzeit leicht nachvollziehen kann.

Das „Handbuch Ordnungsmäßigkeitsfragen der Agree-Bankorganisation" (HB OF) bildet die Vorgaben gängiger Standards ab und konkretisiert diese für das Agree-Umfeld. Dadurch stellt das HB OF selbst den geeigneten Standard zur Erfüllung der aufsichtsrechtlichen Anforderungen für den Großteil der Genossenschaftsbanken dar. Dies auch deshalb, weil die Beachtung der Inhalte aus dem Handbuch ebenfalls Bestandteil des Rahmendienstleistungsvertrags (§4) zwischen der jeweiligen Bank und der Fiducia & GAD IT AG ist.

Handbuch wird regelmäßig aktualisiert

Das Handbuch wird durch den Arbeitskreis „Revision und Kontrolle" herausgegeben und regelmäßig aktualisiert. Die inhaltliche Verantwortung trägt der Arbeitskreis als Herausgeber des Handbuchs. Durch die Kooperation zwischen Rechenzentrale, Vertretern der regionalen Prüfungsverbände und Partnerbanken im Arbeitskreis Ordnungsmäßigkeitsfragen ist sichergestellt, dass sowohl die Anforderungen der täglichen Praxis als auch die prüferischen Aspekte berücksichtigt werden. Innovationen und aufsichtsrechtliche Neuerungen im sich ständig ändernden Umfeld werden im Handbuch in praxisnahe Anforderungen formuliert. Dabei dient das Handbuch auch als Arbeitshilfe zur Umsetzung der in den MaRisk geforderten Prüfung des internen Kontrollsystems. Zeitgleich werden die

AUTOR

Stefan Beck
BWGV-Bereich Beratung
Genossenschaftsbanken-Prozesse
Berater Kostenmanagement/IT

Anwender des Handbuchs für Themen der Ordnungsmäßigkeit und Sicherheit sensibilisiert, um damit die Einhaltung der Compliance-Anforderungen gewährleisten zu können.

BWGV-Datenbank zur Unterstützung

Zur Unterstützung und effizienten Ausgestaltung der Aufsichtsanforderung hat der BWGV die Notes-Datenbank „Handbuch Ordnungsmäßigkeitsfragen der Bankorganisation" entwickelt. Dieses Hilfsmittel unterstützt die Banken dabei, die umfassenden Prüfungsfragen aus dem HB OF praxis- und technikorientiert sowie nachvollziehbar zu bearbeiten und zu dokumentieren. Durch die Evaluierung des Inhalts des HB OF und insbesondere der darin enthaltenen Prüfungsfragen ist es möglich, ein effizientes internes Kontrollsystem unter Kosten-, Nutzen- und Risikoaspekten zu entwickeln. Eine kapitelweise Darstellung der Prüfungsfragen innerhalb der Datenbank ermöglicht es, die thematischen Zusammenhänge beizubehalten.

Nach jeder Veröffentlichung einer Aktualisierung des Handbuchs sind bei sich ergebenden Veränderungen die bisherigen Regelungen der Bank zu dem aktualisierten Themenbereich auf den Prüfstand zu stellen und entsprechend anzupassen. Durch die Bereitstellung von Updates der Datenbank unterstützt der BWGV gezielt die Banken dabei, die Neuerungen zu bearbeiten und diese ressourcenschonend umzusetzen. Durch die Zuweisung von Verantwortlichkeiten sowie einem integrierten Workflow-System ist die revisionssichere Bearbeitung jederzeit gewährleistet. Darüber hinaus bietet die Datenbank ein umfangreiches Wiedervorlagesystem, um der Anforderung der jährlichen regelmäßigen Überprüfung ebenfalls gerecht zu werden.

Transparenz über Prozesslandschaft und internes Kontrollsystem

Die Bearbeitung der Prüfungsfragen ist nicht nur notwendig, um bei Abweichungen vom Standard Risiken transparent zu machen und als operationelle Risiken in das Risikomanagement der Bank zu überführen, sondern ebenfalls, um Transparenz über die Prozesslandschaft und das interne Kontrollsystem in der Bank zu schaffen. Dabei gilt es zu beachten, dass im Allgemeinen jede Abweichung vom Standard meist mindestens ein oder auch mehrere Risiken auslösen und dadurch den Prozess zumindest aus Risikogesichtspunkten negativ beeinflussen kann. Die Identifizierung von Abweichungen und daraus resultierenden operationellen Risiken sollte möglichst effizient ohne große Aufwendungen umgesetzt werden.

Da es sich vorwiegend um die Verhinderung potenzieller Schäden dreht, ist eine Erfolgsmessung durch direkt messbare Ertragsrückflüsse kaum möglich. Entscheidend für den wirtschaftlichen Erfolg ist daher, bei der Beantwortung der Prüfungsfragen neben den notwendigen aufsichtsrechtlichen Anforderungen an die Ordnungsmäßigkeit noch Optimierungspotenziale für die Bank erkennen und heben zu können. Dabei bietet insbesondere das Kapitel 6 im Teil II des Handbuchs praktische Tipps, welche Prozessoptimierungsmöglichkeiten im Agree-Umfeld möglich sind.

Die Datenbank unterstützt die Bank bei diesem Vorhaben, indem beispielsweise bei identifizierten Abweichungen von im Standard genannten Anforderungen unmittelbar eine Risikoanalyse durchgeführt werden kann. Im Anschluss werden die Risiken über diverse Ansichten übersichtlich dargestellt, um damit eine Übertragung in das übergreifende Risikocontrolling der Bank zu ermöglichen. Bei der Verwendung des BWGV-Risikomanagements kann dieser Schritt über eine integrierte Schnittstelle vollautomatisch ausgeführt werden. Die Funktionen der Datenbank können darüber hinaus für weitere Risikoanalysen zum Beispiel für Anwendungen in wesentlichen Geschäftsprozessen und zur Dokumentation von regelmäßigen Kontrollhandlungen genutzt werden.

Frage der bewussten Übernahme von Risiken

Die zielorientierte Ausgestaltung des internen Kontrollsystems mit der Festlegung technisch-organisatorischer Maßnahmen zur Sicherstellung der Ordnungsmäßigkeit samt der Optimierung der Prozesse ist damit nicht nur eine Frage der Erfüllung aufsichtsrechtlicher Anforderungen, sondern auch eine Frage der bewussten Übernahme von Risiken und übergeordneten Managemententscheidungen, die in der besonderen Verantwortung von Vorstand und Führungskräften liegt. ■

Bezug der Datenbank

Zum Bezug der Datenbank „Handbuch Ordnungsmäßigkeitsfragen der Bankorganisation" sowie für Unterstützungen bei der effizienten Ausgestaltung und Umsetzung eines IT-Sicherheitsmanagement-Systems in der Praxis wenden Sie sich bitte an die Beratung Genossenschaftsbanken-Prozesse, Team Kostenmanagement/IT (E-Mail: GP-Prozesse@bwgv-info.de).

Das Team Kostenmanagement/IT

Stephan Klockner, Senior Berater Kostenmanagement/IT
Jürgen Matt, Berater Kostenmanagement/IT
Frank Schowalter, Berater Kostenmanagement/IT