Herstellerunterlage zur Unterstützung bei der Erstellung eines

**IT-Sicherheitskonzeptes für**

**KAP**

**Kredit-Auswertungs-Programm**



KAP-Version: 7.5

Stand: Mai 2019

Inhaltsverzeichnis

[1 Einleitung 3](#_Toc443031011)

[2 Vorbemerkung 3](#_Toc443031012)

[2.1 Geltungsbereich 3](#_Toc443031013)

[2.2 Wesentliche Komponenten 3](#_Toc443031014)

[2.3 Bezug zu RS FAIT 1 4](#_Toc443031015)

[2.4 Rechtliche Rahmenbedingungen 4](#_Toc443031016)

[3 Herstellervorsorge 5](#_Toc443031017)

[3.1 Architektur 5](#_Toc443031018)

[3.2 Datenbasis von KAP 5](#_Toc443031019)

[3.2.1 Änderung der Grundeinstellungen 6](#_Toc443031020)

[3.2.2 Kreditauswertungen 6](#_Toc443031021)

[3.2.3 Kontrolle der Kreditdaten 6](#_Toc443031022)

[3.3 Datenherkunft / Datenhaltung 7](#_Toc443031023)

[3.3.1 Datenklassifizierung 7](#_Toc443031024)

[3.3.2 Aufbewahrungspflichten / Auskunft 7](#_Toc443031025)

[3.4 IT-Umfeld 8](#_Toc443031026)

[3.5 Test- und Freigabeverfahren 8](#_Toc443031027)

[3.6 Datensicherheit 8](#_Toc443031028)

[3.7 Benutzerverwaltung 9](#_Toc443031029)

[3.8 Protokollierung 9](#_Toc443031030)

[3.9 Verschlüsselung 9](#_Toc443031031)

[4 Schutzbedarf 9](#_Toc443031032)

[4.1 Schutzbedarfsfeststellung 9](#_Toc443031033)

[4.2 Empfehlungen zur Feststellung des Schutzbedarfs 10](#_Toc443031034)

[4.3 Schutzniveau 10](#_Toc443031035)

[5 Bedrohungsanalyse / Risikobewertung 11](#_Toc443031036)

[5.1 Bedrohungskategorien 11](#_Toc443031037)

[5.2 Ereignisanalyse 12](#_Toc443031038)

[6 Risikomatrix 13](#_Toc443031039)

[7 Restrisiken 14](#_Toc443031040)

# Einleitung

Die sicherere Verarbeitung von Daten ist eine existenzielle Notwendigkeit für Unternehmen, insbesondere im sensiblen Bereich der Finanzdienstleister, Banken und Versicherungen. Ein standardisiertes Vorgehen ist die Voraussetzung für eine sinnvolle Umsetzung eines nachhaltigen Sicherheitskonzeptes. Diese Unterlage soll dazu dienen, die Erstellung eines Sicherheitskonzeptes zu unterstützen, das für die Nutzung der Systemkomponenten von KAP (Kreditauswertungsprogramm) der bundesdeutschen Genossenschaftsverbände notwendig ist.

KAP ist mit der Hilfe der dbs Computer GmbH in Celle erstellt worden. Diese Gesellschaft arbeitet seit 1999 für die Vorgängerprodukte KEB und KAP mit den Verbänden und der FIDUCIA & GAD IT AG zusammen.

# Vorbemerkung

Die vorliegende Herstellerbestätigung dient der sachbezogenen Unterstützung für die beim Anwender nachzuweisende Systemfreigabe. Aus der vorliegenden Herstellerbestätigung leiten sich keine Forderungen an den Hersteller des Softwareproduktes ab. Sie ist keine Software-Bescheinigung im Sinne der OPDV oder des Prüfungsstandards IDW PS 880 und kein Zertifikat nach ISO-Normen. Dieses Dokument enthält notwendige Informationen zur Erstellung eines eigenen Sicherheitskonzeptes. Die aufgeführten Maßnahmen haben empfehlenden Charakter, die im Rahmen der eigenen Organisationsrichtlinien und der unterstützenden Fachinformationen von Rechenzentralen und Verbänden zu interpretieren sind.

Grundlage dieser Bestätigung ist das Kreditauswertungsprogramm KAP in der Version 7.x, ein Revisionsinstrument für die Kreditprüfung, das eine unterstützende Datenaufbereitung der Kreditprüfungsergebnisse liefert. Das System ist ein Produkt der bundesdeutschen Genossenschaftsverbände (nachfolgend Verbände).

## Geltungsbereich

Wesentlicher Nutzerkreis sind externe und interne Kreditrevisoren im technischen Umfeld der Rechenzentrale FIDUCIA & GAD IT AG. Das technische Umfeld wird in dieser Unterlage nicht betrachtet und ist auf Basis unseres Kenntnisstandes in eigens dafür erstellten Sicherheitskonzepten abgehandelt.

## Wesentliche Komponenten

Die wesentlichen Komponenten sind:

* Unterstützung einer Kreditselektion auf Basis kundenbezogener Daten für den Auftrag der Innenrevision zur Feststellung und Bestätigung der wesentlichen Risiken im Kreditgeschäft
* Bearbeitung der ausgewählten Kreditdaten und Erstellung von Prüfungsprogrammen
* Dokumentation der festgestellten Kreditrisiken auf Einzelkreditbasis
* Auswertung aller geprüften Kredite und Bericht gegenüber dem Vorstand
* Durchsprache der Feststellungen mit der zuständigen Abteilung im Kreditbereich
* Nachschau getätigter Feststellungen

Dabei werden im Bereich der Innenrevision personenbezogene Daten durch KAP verarbeitet.

## Bezug zu RS FAIT 1

Voraussetzung für die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung ist neben der Gesetzesentsprechung des Rechnungslegungssystems die Sicherheit der verarbeiteten rechnungslegungsrelevanten Daten.

Nur bei Vorliegen sicherer rechnungslegungsrelevanter Daten und IT-Systeme kann die Verlässlichkeit der in Buchführung, Jahresabschluss und Lagebericht enthaltenen Informationen gewährleistet werden.

Hieraus folgt, dass die gesetzlichen Vertreter auch für die Einhaltung der Sicherheit der IT-Systeme und der rechnungslegungsrelevanten Daten verantwortlich sind. Dazu ist für das Unternehmen ein geeignetes Sicherheitskonzept zu entwickeln, einzuführen und aufrecht zu erhalten, das den erforderlichen Grad an Informationssicherheit gewährleistet.

Das Sicherheitskonzept beinhaltet die Bewertung der Sicherheitsrisiken aus dem Einsatz von IT aus Sicht der gesetzlichen Vertreter und daraus abgeleitet die technologischen und organisatorischen Maßnahmen, um eine angemessene IT-Infrastruktur für die IT-Anwendungen zu gewährleisten sowie die ordnungsmäßige und sichere Abwicklung der IT-gestützten Geschäftsprozesse sicherzustellen.

IDW RS FAIT 1 TZ 19 bis 22

Da KAP keine rechnungslegungsrelevanten Daten verarbeitet oder weiterleitet ist keine Softwarebescheinigung nach IDW PS 880 erforderlich. Sollte von der Bank KAP für Funktionen mit Rechnungslegungs- bzw. Steuerungsrelevanz eingesetzt werden, sind die aufsichtsrechtlichen und gesetzlichen Vorgaben zu beachten.

## Rechtliche Rahmenbedingungen

Mit dem Einsatz von KAP sind die datenschutzrechtlichen Bestimmungen aufgrund der Verarbeitung von personenbezogenen Daten zu beachten und anzuwenden.

Ergänzend sind die Anforderungen der MaRisk zu berücksichtigen:

**AT 7.2 – Textziffer 2**

Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen

 die 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 grundsätzlich auf gängige Standards umzustellen, insbesondere sind Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich. Die Eignung der IT-Systeme und der zugehörigen Prozesse ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.

# Herstellervorsorge

Die Verarbeitung der Vorgänge wird durch die Innenrevision auf bankeigenen Rechnern vorgenommen.

## Architektur

KAP ist ein Revisionswerkzeug zur Unterstützung der Innenrevision im Bereich der Kreditprüfung.

Die SQL-Datenbank kann von mehreren Clientnutzern im Netzwerkbetrieb gleichzeitig genutzt werden. Die Anforderungen an einen sicheren Netzwerkbetrieb werden durch die ausschließliche Nutzung des KAP im Fiducia & GAD-Netzwerk erfüllt.

## Datenbasis von KAP

KAP steht in der aktuellen Version 7.5 zur Verfügung.

Die Datenhaltung in KAP erfolgt in einer MS SQL Datenbank. Die Datenbank kann vom Nutzer auf ein Netzwerklaufwerk der Bank als komprimierte SQL-Datenbank gesichert werden, falls ein Übertrag auf einen anderen Rechner erforderlich sein sollte. Die Zugriffsrechte auf das Tauschlaufwerk sind nach dem Prinzip der minimalen Berechtigungsvergabe zu steuern. Die Bank hat entsprechende Vorgaben in ihr Benutzergruppenkonzept aufgenommen.

Die Regelungen zur Behandlung von externen Speichermedien zur Übertragung der gesicherten SQL-Datenbanken sind besonders zu beachten.

### Änderung der Grundeinstellungen

Administrative Funktionen wie Datenbankbereinigungen, Jahresabschluss und Datenrücksicherungen sind immer nur von einem Nutzer, dem Administrator, möglich.

Empfohlen wird die Programminstallation auf den Anwenderclient. Die Datenbank selbst kann auf einem Netzwerkverzeichnis liegen. Änderungen an den Quellcodes oder den Rechenroutinen in der Datenbank sind nicht möglich. Die Änderungsmöglichkeiten beschränken sich auf die inhaltliche Anpassung einzelner XML-Dateien. Diese Einstellungen (z.B. Textbausteine, Funktionsprüfungsfragen) sind mit Programmierkenntnissen im Programm mithilfe des Administrators änderbar.

Die Bank stellt über ein Benutzergruppenkonzept die Beschränkung auf den berechtigten Nutzerkreis sicher.

### Kreditauswertungen

Das Herzstück bildet die Kreditauswertung für geprüfte Einzelkredite.

Dafür stehen umfassende Reports zur Verfügung, die auch auf dem Bildschirm erstellt werden und in mehrere gängige Formate (PDF, RTF, XLS) zur Weiterverarbeitung exportiert werden können.

Darüber hinaus ist unter wave eine Schnittstelle zum Revisionsprodukt revisWEB erstellt worden, mit dem in einer ersten Version die Hinweise / Einzelfeststellungen zu einem geprüften Kunden-kredit übertragen und in der Prüfungsnachschau mit revisWEB verarbeitet werden.

Die exportierten Daten werden in Netzwerkverzeichnissen abgelegt, auf deren Inhalte die Bank keinen Zugriff hat.

### Kontrolle der Kreditdaten

KAP 7.5 stellt dem Anwender mit den Reports Funktionen bereit, mit denen er unplausible Erfassungen prüfen kann.

Auch werden Datenimporte und -exporte protokolliert und unplausibel importierte Daten in einem Protokoll erfasst.



## Datenherkunft / Datenhaltung

Alle Daten, die in KAP 7 importiert werden, sind juristische Daten aus den Systemen der Rechenzentrale der Banken.

Die Aufgabe von KAP 7 ist die Bündelung von revisionserheblichen Daten, um eine Einzelerhebung der wichtigsten Beurteilungswerte eines Kredites zu verhindern und so eine effiziente Kreditprüfung zu ermöglichen.

Die Importe können auf Anforderung der Verbände und Banken an geänderte Rahmenbedingungen oder die Datenqualität angepasst werden. Die Standardimporte werden im Rahmen der Supportleistung durch die Verbände bei den Rechenzentralen beauftragt. Der Anwender kann die Importroutinen nicht eigenständig verändern.

Die nach KAP zu importierenden agree21/bank21-Rohdaten werden in einem Netzwerkordner bereitgestellt, auf den nur ein berechtigter Personenkreis Zugriff haben soll. Den Zeitpunkt des Datenimports legt die Bank selbst fest.

Im Rahmen der Nutzung von KAP können manuelle Daten im System erfasst werden. Auch neue Kredite können manuell angelegt werden, wenn dies aus Effizienzgründen sinnvoll ist.

Kreditnehmerstrukturen können den tatsächlichen / korrekten Verhältnissen durch die Revision angepasst werden, damit die Berichterstattung an den Vorstand / an die beurteilte Stelle richtig gestellt ist.

Importierte Werte bleiben aber erhalten, um so auch später mögliche Veränderungen am Datenbestand erkennen zu können. Veränderte Werte / Kredite sind am Bildschirm erkennbar.

### Datenklassifizierung

Die Datenklassifizierung erfolgt im Rahmen des Informationssicherheitsmanagements des Anwenders, die dementsprechend berücksichtigt werden muss.

Folgende Daten werden im System erfasst:

 Personendaten

o Kundendaten im Rahmen der selektierten Kreditfälle durch Datenimport aus den RZ-Systemen

o Mitarbeiterdaten/Anwenderkürzel im Rahmen des Prüfungsvorgehens

 Geschäftsdaten

o aggregierte Kontodaten aus der Finanzbuchhaltung

 Technische Daten

o Benutzerdaten (Anwenderkürzel)

o Passwörter (verschlüsselt)

o Steuerungsparameter

### Aufbewahrungspflichten / Auskunft

Die AO enthalten Bestimmungen über die Aufbewahrungspflicht von Unterlagen. Da die Daten in KAP 7 aus den juristischen Vorsystemen stammen, greift dort auch die Umsetzung der Aufbewahrungspflicht, insbesondere für die Auskunftspflicht entsprechend der GDPdU.

Daten, die in KAP erfasst werden und aufbewahrungspflichtig sind, wie z .B. Daten im Rahmen der einzelnen Kreditprüfungen im Laufe eines Jahres, aufzubewahren. Es ist darauf zu achten, dass eine dem Backup entsprechende Programmversion vorzuhalten ist. Wobei eine Aufwärtskompatibilität gewährleistet ist.

Die sachkundige Nutzung und Bedienung von KAP 7 gewährleistet, dass auf Verlangen eines berechtigten Dritten (z. B. Finanzbehörde, Abschlussprüfer) in angemessener Zeit die gespeicherten Daten lesbar gemacht werden können. Zur Unterstützung dient die vom Anwender erstellte Verfahrensbeschreibung.

Es wird ausdrücklich darauf hingewiesen, dass KAP 7 nicht die Anforderungen an ein juristisches DMS erfüllt. Es besteht jedoch die Möglichkeit, diese Daten in vom Anwender unterhaltene DMS-Systeme zu archivieren.

Datensicherungen sollten bedacht und sicher aufbewahrt werden, wenn dies nicht bereits im Rechenzentrumsbetrieb sichergestellt ist.

Die Verfahrensdokumentation gehört zu den Arbeitsanweisungen und sonstigen Organisationsunterlagen im Sinne des § 257 Abs. 1 HGB bzw. § 147 Abs. 1 AO und ist grundsätzlich zehn Jahre aufzubewahren.

## IT-Umfeld

KAP 7 ist auf Basis einer Citrix-Technik in die Client-Server-Umgebung der Bank eingebunden und unterliegt infolgedessen den definierten Sicherheitsrichtlinien von Bank und Rechenzentrum. Im Bereich der FiduciaGAD ist KAP 7 im Rahmen der sicherheitstechnischen Prüfung zertifiziert. KAP 7 benötigt keine Verbindung nach außen, wie z.B. das Internet.

## Test- und Freigabeverfahren

Im Rahmen der Implementierung ist diese Software einem regulären Test- und Freigabeverfahren zu unterziehen. Verantwortlich für die Durchführung und die Dokumentation ist hierfür die jeweilige Bank, auf deren System die Anwendung installiert werden soll.

## Datensicherheit

Das Softwaresystem KAP 7 basiert auf einem hohen Niveau der Datensicherheit. Die Datensicherheit wird z.B. erreicht durch:

 zuverlässige, relationale Datenbanksysteme (MS SQL)

 Zugriffsrechte auf Funktionsbausteine und Prozessebenen

 passwortgeschützte Zugangsberechtigung

Die regelmäßige Sicherung und Sicherstellung der Daten obliegt dem verantwortlichen Anwender. Die Arbeiten zur Datensicherheit sind in einer Arbeitsvorschrift des Anwenders zu fixieren und durch den Anwender zu bestätigen.

Die Verfügbarkeit der erforderlichen Hardware und der Betriebssysteme sichert der Anwender. Den Schutz der Informationen gegen unberechtigte Veränderungen gewährleistet KAP durch wirksame Zugriffs- bzw. Zugangskontrollen. Darüber hinaus ist aufgrund des vorhandenen Arbeitsplatzzugangs in Verbindung mit einem Benutzergruppenkonzept eine ausreichende Sicherheit hergestellt.

Die Durchführung von (periodischen) Datensicherungsprozeduren obliegt dem Anwender, wenn dies nicht durch die Administration bereits gewährleistet ist, durch die tägliche Sicherung der SQL-Datenbanken.

Zur Wiederauffindbarkeit und zur Vermeidung (unbeabsichtigter) Vernichtungen der gesicherten Daten sind dokumentierte, strukturierte Verzeichnisse zu verwenden. Das Datensicherungskonzept des Unternehmens ist durch den Anwender zu bestätigen.

## Benutzerverwaltung

KAP verfügt über eine Benutzerverwaltung. Eine weitergehende Aufteilung von Rechten ist nicht implementiert und nach bisherigen Anwendungserfahrungen auch nicht erforderlich.

Eine Session wird nicht automatisch nach einer Zeit der Inaktivität beendet. Dieses ist über die Bildschirmsperre zu kompensieren.

## Protokollierung

Das Importieren und Verändern von Kreditdaten wird in KAP 7 protokolliert.

Die Protokolle umfassen die Anlage einer Datenbasis und die Anzahl importierter Daten zum Abgleich mit den Datensets der Rechenzentrale. Die Protokolle sind durch den Anwender aus dem Programm heraus nicht änderbar.

Ferner sind veränderte Daten am Bildschirm erkennbar.

## Verschlüsselung

Da KAP 7 in der Regel im gesicherten Netz des Anwenders betrieben wird, werden die Daten zwischen Server und Client nicht verschlüsselt.

# Schutzbedarf

Die Verbände als Hersteller bestätigen hiermit, dass alle Maßnahmen bei der Programmentwicklung, dem Test der fachlichen und der technischen Funktionen und bei der Dokumentation von KAP 7 in der aktuellen Version ergriffen wurden, um die Ordnungsmäßigkeit in Anlehnung an die Anforderungen einzuhalten.

Es werden von Seiten der Verbände planmäßig Kontrollen durchgeführt.

Diese Herstellerbestätigung ersetzt nicht die Freigabe dieses Softwareproduktes durch den Anwender und stellt keine Softwarebescheinigung gemäß IDW PS 880 dar.

## Schutzbedarfsfeststellung

Die Festlegung über Art und Umfang der zu sichernden KAP-Daten bestimmt der Anwender bzw. die zuständige IT-Organisation der anwendenden Bank. Grundsätzlich ist anzumerken, dass KAP 7 auf dem hauseigenen IT-Umfeld, welches durch die Rechenzentrale zur Verfügung gestellt wird, läuft. Die KAP-Datenbank soll auf ein Serverlaufwerk gelegt und somit von mehreren Nutzern bestückt und Daten eingepflegt werden. Der Kreis der Zugriffsberechtigten ergibt sich aus dem Berechtigungskonzept der Bank. Klassischerweise werden diese Zentrallaufwerke im Ganzen durch die IT gesichert.

Dem Anwender steht zusätzlich eine Datensicherungsfunktion durch das Programm zur Verfügung. Somit lassen sich zeitunabhängige Datensicherungen alternativ durch den Nutzer erstellen.

## Empfehlungen zur Feststellung des Schutzbedarfs

In KAP 7 werden personenbezogene Daten von Kunden erfasst und verarbeitet.

Die Schutzziele Vertraulichkeit, Integrität und Authentizität (VIA) werden nicht getrennt bewertet sondern zu einer Gruppe zusammengefasst. Eine getrennte Bewertung erhöht die Komplexität. Daher wird die Gruppe am weitreichendsten Schutzbedarf ausgerichtet.

**Vertraulichkeit V = 3**

In KAP 7 werden die aus den juristischen Vorsystemen gelieferten Kunden- und Geschäftsdaten gespeichert. Für die Bank kann eine nicht vertrauliche Behandlung von Daten zu einem Imageschaden führen.

**Integrität I = 3**

Da eine begrenzte Möglichkeit besteht, dass aufgrund der Daten in KAP 7 Entscheidungen getroffen werden, die für den Anwender wirtschaftliche Folgen oder eine Imagewirkung hat, bekommt die Unverfälschbarkeit der Daten eine hohe Bedeutung.

**Authentizität A = 3**

Begleitend zur Vertraulichkeit und Integrität der Daten ist es bedeutend, die an Prozessen Beteiligten im Falle einer Schutzverletzung identifizieren zu können.

**Verfügbarkeit V(f) = 1**

Der Ausfall des Systems kann je nach Intensität der Nutzung zu einer Erschwernis bei der Aufgabenerfüllung führen, dies wird aber in der Regel nicht zu einem nachhaltigen Ertragsschaden oder Imageschaden führen. Die Anwendung wird nicht für den Betrieb zeitkritischer Prozesse benötigt.

**KAP unterstützt folgenden Geschäftsprozess:**

Interne Prozesse -> Unternehmensorganisation -> **Interne Revision**

**KAP ist von folgenden Schutzobjekten abhängig
(in kursiver Schrift Bezeichnungen aus bank21-Umfeld):**

* IT-Cloud / *Wave\** (rz-seitig zur Verfügung gestellte zentralisierte Anwendungs- und Datenlandschaft)
* agree Net / *MPLS Express* (Verbindung zum Rechenzentrum)
* LAN inkl. der hierfür verwendeten Komponenten (internes Netzwerk)
* agree21-Client / *BI Thin- und FAT Client* (Bankarbeitsplatz)

## Schutzniveau

Für die Anwendung KAP kann unter Berücksichtigung der bereits umgesetzten und vorbehaltlich der Umsetzung der empfohlenen Maßnahmen grundsätzlich das folgende IT-Sicherheitsniveau erreicht werden:

Vertraulichkeit V3

Integrität I3

Authentizität A3

Verfügbarkeit Vf2

# Bedrohungsanalyse / Risikobewertung

Die Analyse dient der Definition der wesentlichen Bedrohungen sowie dessen Bewertung für mögliche Risiken. Dies ist die Basis für Maßnahmen, die ein Unternehmen einleiten muss, um Risiken abzuwenden oder bewusst zu tragen. In den weiteren Ausführungen wird auf Bedrohungen eingegangen und es werden Maßnahmen aufgezeigt, die vom Hersteller ergriffen wurden und dem Systemanwender empfohlen werden. Die Umsetzung der Maßnahmen im Einflussbereich des Anwenders obliegen dessen Risikostrategie und Einschätzung. Die nachfolgenden Ansätze sind nicht abschließend vollständig und dienen lediglich der Orientierung. Die Bedrohungen werden in Anlehnung an den IT-Grundschutzkatalog dargestellt. Es wird nur auf die Bedrohungen eingegangen, die direkten Bezug zur Anwendung haben. Die Kategorien in der Analysematrix werden nachfolgend beschrieben.

## Bedrohungskategorien

Die nachfolgenden Bedrohungskategorien sind aus dem IT-Grundschutzkatalog abgeleitet.

**Elementare Bedrohungen G0**

KAP wird in der Regel in der bestehenden Infrastruktur eines Unternehmens betrieben. Die hier bereits ergriffenen notwendigen Maßnahmen im Rahmen eines IT-Sicherheitskonzepts sind maßgeblich und hängen nicht von dem Einsatz der Anwendung ab.

**Höhere Gewalt G1**

Höhere Gewalt ist ein von außen einwirkendes Ereignis, was nicht in der Natur der Sache begründet werden kann und auch bei größter Sorgfalt nicht hätte abgewendet werden können.

**Organisatorische Mängel G2**

Organisatorische Regelungen sind notwendiger Bestandteil eines ordnungsgemäßen Geschäftsbetriebes. Unzureichende Regelungen für die Nutzung eines IT-Systems können zu Risiken führen.

**Menschliche Fehlhandlungen G3**

Menschen die in einer Organisationseinheit nach dem Prinzip Aufgabe, Verantwortung und Kompetenz Ihrer Verrichtung nachgehen, können durch Unwissenheit und Fahrlässigkeit Fehlhandlungen ausführen. Diese Fehlhandlungen können dem Unternehmen schaden.

**Technisches Versagen G4**

IT-Systeme sind aus arbeitsteiligen Organisationen nicht mehr wegzudenken. Fallen diese IT-Systeme aus, werden Arbeitsabläufe gestört oder kommen vollständig zum Erliegen. Dies führt zu erheblichen Risiken und Schäden für ein Unternehmen, insbesondere im Finanzdienstleistungssektor.

**Vorsätzliche Handlungen G5**

Vorsätzliches Handeln liegt vor, wenn die ausführende Person mit Wissen und Wollen eine Tatbestandsverwirklichung verfolgt, die eine Rechtswidrigkeit darstellt. Motivation für Vorsatz ist häufig Rache, Böswilligkeit und Frust. Es ist sehr schwer gegen Vorsatz Sicherheitsvorkehrungen zu treffen. Grundsätzliche Vorkehrungen helfen aber, die Schwelle der Verwirklichung höher zu legen und so Schaden vom Unternehmen abzuwenden.

## ****Risikoanalyse****

Die nachfolgende Tabelle zeigt die Schadenklassen bezogen auf Programm und KAP-Daten. Die Bank bzw. der Anwender bestimmt das Sicherungskonzept selbst (Hinweis: Punkt 3.1). Diese Maßnahmen muss die Bank abschließend selbst bestimmen, die aufgeführten Beispiele dienen nur der Orientierung und erheben nicht den Anspruch der Vollständigkeit.

| KZ | Bezeichnung | Umgesetzte Maßnahmen KAP | Vorschlag zur Umsetzung in der Bank |
| --- | --- | --- | --- |
|  |  |  |
| G01 | Ausspähen, Abhören | Eine Verschlüsselung der Daten zwischen Client und der Datenbank auf dem File-Server findet nicht statt. | Betrieb in der sicheren Infrastruktur des RZ. BSI-konforme Passwortregeln, Nutzung SSL-Verschlüsselung. |
|  | Eintrittswahrscheinlichkeit: unwahrscheinlichSchadenspotenzial: mittel |  |
| G02 | Manipulation der Software | Die Programme sind mit Softwarestandards programmiert. Der einfache Zugriff auf den Code ist nicht möglich. | Originalsoftware und Administrator-Passwörter werden entsprechend der betrieblichen Organisationsanweisung sicher verwahrt. Stichprobenkontrollen im Rahmen des internen Kontrollsystems. |
|  | Eintrittswahrscheinlichkeit: unwahrscheinlichSchadenspotenzial: mittel |  |
| G03 | Datenverlust | Bei Ablage der Datenbank auf dem SQL-Server, automatische Datensicherung der KAP-Daten Darüber hinaus eigene Datensicherungen möglich. | Organisatorische Regelungen der erforderlichen Datensicherungen. Regelmäßige Stichproben für erfolgreich durchgeführte Sicherungen. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G11 | Personalausfall | Umfassendes Handbuch für das System, Supporthilfe durch Verbände. | Diversifizierung der Aufgaben mit Vertretungsregelung und Organisationsanweisungen. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G21 | Fehlende Wartung | Rundschreiben der Verbänden  | Organisatorische Regelung der erforderlichen Wartungsaufgaben. Regelmäßige Stichproben im Rahmen des internen Kontrollsystems. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G22 | Fehlende Test- und Freigabeverfahren | Interne Test- und Freigabeverfahren vor Auslieferung, Pilotphase bei Testbanken. | Vorhalten eines Testsystems zur Wahrnehmung der notwendigen Tests mit dokumentierter Freigabe der getesteten Standardfunktionen. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G31 | Fehler von Anwendern | Rücksicherung der letzten Tagessicherung, manuelle Detailkorrektur oder erneuter Datenimport. | Organisatorische Regelungen für nachhaltige Schulungen und Einweisungen. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G32 | Fehler von Administratoren | Umfassendes Handbuch, Seminare, IR-Workshops und ggfs. Coaching. wird herabgestuft auf C | Umfassende allgemeine Schulung für die Administration und Diversifikation der Tätigkeiten auf Fachbereiche. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G33 | Fehler in Prozessen | Umfassendes Handbuch, Seminare, Support und ggfs. Coaching.  | Organisatorische Regelungen für die Abnahme und Freigabe von Prozessen vor dem Einsatz im Echtsystem. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G41 | Technisches Versagen | Automatische Logdateien protokollieren auftretende Fehler | Regelmäßige Überprüfung der Protokolle sowie Wartungsmaßnahmen. Ausreichende Planung der erforderlichen HardwareRessourcen. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |
| G51 | Missbrauch von Rechten | Verwendung von Passwörtern, Zugang nur über den gesicherten Bankrechner, Protokollierung der Anmeldungen, Datenrücksicherungen. | Installation der Systeme entsprechend der Vorgaben des Herstellers. Parametrisierung der technischen Vorgaben im organisatorisch geregelten 4-Augenprinzip. Die Vergabe von Benutzerberechtigungen erfolgt detailliert und funktionsgerecht im organisatorisch geregelten 4-Augenprinzip. Regelmäßige Überprüfung der Logfiles. |
|  | Eintrittswahrscheinlichkeit: möglichSchadenspotenzial: mittel |  |

# Risikomatrix

Die in der Bedrohungsanalyse festgestellten Bedrohungen im Rahmen dieses Sicherheitskonzeptes wurden zur schnellen Übersicht in die nachfolgende Risikomatrix übertragen.





Das Ergebnis ist dabei so zu interpretieren, dass der Eintritt eines Schadens als unwahrscheinlich angesehen wird, wobei der mögliche Schadenswert für Vertraulichkeit, Integrität und Authentizität hoch bewertet wird und für die Verfügbarkeit als Mittel.

Diese Bewertung erfolgt auch aufgrund des Umstandes, dass bei Ausfall des Systems der Geschäftsbetrieb nicht zum Erliegen kommt, da alle wesentlichen Daten im juristischen System verfügbar sind. Im Umkehrschluss kann KAP beim Ausfall des Host-Systems auch die Funktion eines Notfallsystems übernehmen und so die Risiken der Verfügbarkeit reduzieren.

Allesamt werden die Risiken *als nicht relevant / vernachlässigbar / gering* bewertet *(Hinweis: nicht zutreffendes streichen).* Die Verbände als Hersteller des Systems sind im Rahmen der laufenden Qualitätsverbesserung bestrebt, erkannte Schwachstellen zu beseitigen und Hinweise von Kunden aufzunehmen, insbesondere sind gesetzliche Regularien ordnungsgemäß zu erfüllen.

Ein hoher Grad an Sicherheit ist bereits erreicht wobei 100 % aufgrund heutiger Erkenntnisse nie erreichbar sind.

# Restrisiken

Die bestehenden Restrisiken sind nicht elementar für das einsetzende Unternehmen. Existenzielle Gefährdungen werden nicht gesehen und die Restrisiken sollten unter diesen Erkenntnissen tragbar sein. Dies muss das Unternehmen im Rahmen der organisatorischen Regelungen seiner IT-Strategie und dem daraus resultierenden IT-Sicherheitskonzept eigenverantwortlich beurteilen.