Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

KfW-Organisationshandbuch

Richtlinie Nr. RL128087

Titel Absicherung des privilegierten administrati-ven Zugangs zu IT Systemen

GELTUNGSBEREICH	VL IT VL CO VL DEG VL X3f
VERANTWORTLICHE OE	COc2
DOKUMENTVERANTWORTLICH	Robbauer, Bastian
VERTRAULICHKEITSSTUFE	Intern (Stufe 2)
ERSETZT VERÖFFENTLICHUNGSDATUM VOM:	18.09.2018

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

ÄNDERUNGEN ZUR VORVERSION

Änderungs-datum	Kapitel	Inhalte
Dez. 2015	alle	Erstellung Dokument
Juli 2017	2 3 4	Geltungsbereich angepasst und auf IPEX und DEG ausgeweitet Anpassung an aktuelle ISO Maßnahmen Einfügen des Wirkens auf die Schutzziele (Vertraulichkeit-Integrität-Verfügbarkeit)
Februar 2018	3 4	Anpassung der Definition an die Definition der RL128098 Erweiterung PA_VM-01-01
Dez. 2018	alle	Konkretisierung der Vorgaben Überwachung und Kontrollen

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

INHALTSVERZEICHNIS

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

1 KURZBESCHREIBUNG

In dieser IS-Richtlinie werden systematische Sicherheitsmaßnahmen für die Absicherung des privilegierten administrativen Zugangs zu Applikationen und Technologiekomponenten beschrieben.

Regelungsdokumente wie die IS-Richtlinie konkretisieren die ISMS-Leitlinie und dienen als Grund-lage für die operative Umsetzung durch die zuständigen Stellen.

Die IS-Vorgaben stellen keine Lösungen dar, sind aber ausreichend konkret, um auf operativer Ebene (1st Line of Defense) Sicherheitskonzepte entwickeln zu können.

Entstehen in der Praxis Situationen, bei welchen die Vorgaben nicht oder nicht vollständig um-setzbar sind, so sind alternative Lösungen zu entwickeln, die dem angestrebten Sicherheitsniveau entsprechen.

2 GELTUNGSBEREICH

Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG.

Die Töchter weichen lediglich bei institutsspezifischen Besonderheiten (gesetzliche, vertragliche, externe oder geschäftliche Anforderungen) durch spezifische Anpassungen ab. Die Konzernleit- und -richtlinien erlangen nachfolgend erst nach Freigabe durch die jeweilige Geschäftsführung der Töchter („Ratifizierung“) Gültigkeit in den Einzelinstituten DEG/IPEX.
Den Einzelinstituten bleibt es im Übrigen unbenommen, unter Ausschluss von Widersprüchen mit den konzernweit nach den vorstehenden Maßgaben verabschiedeten und geltenden Regelungen konkretisierende Einzelmaßnahmen (Richtlinien, Arbeitsanweisungen) zu verabschieden.

3 ZIELSETZUNG

Ziel dieser Umsetzungsvorgabe ist es, für die operative Festlegung von technischen und organisatorischen Schutzmaßnahmen Informationen zur Verfügung zu stellen und Rahmenbedingungen für Vorgaben festzulegen, die eine zentrale Verwaltung und die sichere Nutzung von privilegierten administrativen Berechtigungen ermöglichen. Zielsetzung ist es, allen privilegierten administrativen Berechtigungen mit Zugang zu Systemen, Applikationen und Funktionen, einen sicheren, nachvollziehbaren und auditierbaren Zugang zu den Zielsystemen in Abhängigkeit des jeweiligen Schutzbedarfs zu geben. Die Maßnahmen

gelten für alle internen und externen IT-Administratoren und müssen die bereits existierende IAM[1] Lösung funktional ergänzen, um potenziellen Schaden durch die Nutzung von Schwachstellen im Account Management oder den bewussten Missbrauch von privilegierten administrativen Berechtigungen für das Unternehmen abzuwenden. (ISO-27002/9.2.1-6, 9.4.1-6, 12.4.1-4)

3.1 Administrative (kritische) Berechtigungen in der KfW

3.1.1 Übersicht über Berechtigungsarten und Kontotypen

In der Richtlinie RL128098 Sicherheitsvorgaben für das Berechtigungsmanagement sind alle Ausprägungen der Berechtigungsarten und Kontotypen User-Account-Typen dokumentiert. Diese Richtlinie regelt die Anforderungen an administrative (kritische) Berechtigungen.

3.2 Kritische Sessions

Als „kritische Sessions“ werden der Login und die durchgeführten Aktivitäten mit administrativ kritischen Berechtigungen (siehe Kapitel 3.1.1) beim Zugriff auf Applikationen inkl. Middleware, Datenbanken, Betriebssystemen mit einem sehr hohen Schutzbedarf bei Vertraulichkeit und/oder Integrität im Sinne der Schutzbedarfsfeststellung, definiert.

4 RISIKOORIENTIERTE VORGEHENSWEISE

Für die KfW wird die nachfolgende Mindestanforderung in Anlehnung an den Schutzbedarf der Applikationen inkl. Middleware, Datenbanken, Betriebssystemen festgelegt.
Entstehen in der Praxis Situationen, bei welchen die Vorgaben nicht identisch umsetzbar sind, so ist eine alternative Lösung zu entwickeln, die dem angestrebten Sicherheitsniveau entspricht.

Protokollierung	**Schutzbedarf von Applikationen** inkl. Middleware, Datenbanken, Betriebssystemen **(Integrität und/oder Vertraulichkeit)**

[1] Identity Access Managementsystem

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

	Sehr hoch (4)	Hoch (3)	Mittel (2) Niedrig (1)
Zugriff mit einem privilegierten administrativen Account (siehe Kapitel 3.1.1)	Die Zugriffe und Aktivitäten mit administrativ kritischen Berechtigungen müssen vollständig protokolliert werden. Die Protokolldaten müssen zentral abgelegt und regelmäßig oder anlassbezogen durch unabhängige Unternehmenseinheiten überprüft sowie ausgewertet werden. (PA_VM-05-01)	Die Zugriffe und Aktivitäten mit administrativ kritischen Berechtigungen müssen vollständig protokolliert werden. Die Protokolldaten müssen zentral abgelegt und können anlassbezogen durch unabhängige Unternehmenseinheiten überprüft sowie ausgewertet werden. (PA_VM-05-01)	Die Protokolldaten müssen lokal oder zentral abgelegt und anlassbezogen ausgewertet werden .
<u>Fernwartung</u> Zugriff von externen Dienstleistern über externe Netze auf produktive KfW-Systeme	Die Zugriffe mit (krititschen) administrativen Berechtigungen müssen vollständig protokolliert werden. Die Protokolldaten müssen zentral abgelegt und regelmäßig oder anlassbezogen durch unabhängige Unternehmenseinheiten überprüft sowie ausgewertet werden. (PA_VM-05-01)		

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

5 VORGABEN ZUR UMSETZUNG VON SCHUTZMASSNAHMEN

5.1 Allgemeine Anforderungen

Kürzel	Anforderung	Schutzziel		
		V	I	V
PA_VM-01-01	**Passwort Richtlinie** Das Passwort eines Administratorkontos MUSS sich vom Passwort des Benutzerkontos derselben Person unterscheiden.	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

5.2 Administrative Funktionskontoen

Kürzel	Anforderung	Schutzziel		
		V	I	V
PA_VM-02-01	**Nachweis der Verwendung von administrativen Funktionskonten** Es muss sichergestellt werden, dass ein unveränderbarer Nachweis der Verwendung eines administrativen Funktionskontos bis auf die Personenebene möglich ist. Es muss jeder Geschäftsvorfall eindeutig einem personalen Benutzer zugeordnet sein. Für die kritischen Sessions muss ein Sprungserver mit einem Passwort Vault Management z.B. eines Privilegierten Identity Management Systems (PIM) mit einer personifizierten Benutzerabfrage eingesetzt werden.	X	X	

5.3 Anlassbezogene autorisierte Änderungen

Kürzel	Anforderung	Schutzziel		
		V	I	V
PA_VM-03-01	**Die Anmeldung in die Zielsysteme darf nur anlassbezogen durchgeführt werden.** Für die kritischen Sessions muss ein Sprungserver mit einem Passwort Vault Management z.B. eines Privilegierten Identity Management (PIM) eingesetzt werden. Kritische Sessions MÜSSEN lückenlos dokumentiert werden. Folgende Zugriffsmöglichkeiten sollten vorgesehen werden: a.) Change Zugriff im Rahmen eines genehmigten Change-Tickets mit Angabe der Change Nummer b.) Adhoc Freigabe durch den Officer on Duty (OoD) c.) Notfall Zugriff nach Freigabe durch Notfallmanager	X	X	

5.4 Protokollierung von kritischen Aktivitäten

Kürzel	Anforderung	Schutzziel		
		V	I	V
PA_VM-04-01	**Vollständige Protokollierung von kritischen Aktivitäten** Kritische Aktivitäten müssen vollständig protokolliert werden. Eine vollständige Protokollierung in diesem Sinne umfasst die eindeutige Zuordnung eines Geschäftsvorfalls auf einem System zu einer natürlichen Person und hält fest, wann, wie lange der Zugriff erfolgte und welche Tätigkeiten wann durchgeführt wurden. Darüber hinaus müssen die Systeme mindestens Protokollmeldungen schreiben, die es ermöglichen, die jeweilige Aktion innerhalb der Anwendung mit allen relevanten Parametern nachzuvollziehen. (Gemäß der RL128090 (Vorgaben zur Sicherheitsüberwachung und Protokollierung von IT-Systemen) Im Folgenden werden typische kritische Aktivitäten bzw. Kontrollmaßnahmen genannt.	X	X	
PA_VM-04-02	**Login - Versuche** Es müssen erfolgreiche, nicht erfolgreiche und ungewöhnliche Login-Versuche kritischer Sessions protokolliert werden. Kennzahlen können hier beispielsweise sein: • Häufung fehlerhafter Login Versuche • Unzulässige interaktive Anmeldung als Verfahrensuser • Login auf privilegierte Accounts außerhalb der normalen Geschäftszeiten und außerhalb des Unternehmensnetzwerks • Intervall zwischen Login und Logout überschreitet oder unterschreitet	X	X	

	typische Administrationsdauer.			
PA_VM-04-03	**Logging darf nicht deaktiviert werden** Das Logging kritischer Aktivitäten darf im Unternehmen nicht deaktiviert werden und kann ein Indiz für genauer zu prüfende Auffälligkeiten sein. Insofern muss protokolliert werden, wie häufig durch welche Accounts erfolgreiche oder missglückte Versuche stattfinden, Protokollierungsmaßnahmen an- oder abzuschalten.	X	X	
PA_VM-04-04	**Sichere Aufbewahrung von Protokollen** Protokolle von kritischen Sessions dürfen nicht verändert werden und müssen gegen unbefugten Zugriff geschützt werden. Insofern muss protokolliert werden, welche Accounts sich wann Zugang zu diesen Systembereichen verschaffen wollen.	X	X	
PA_VM-04-05	**Überwachung von Zugriffsberechtigungen der Administratoren** Da die Vergabe von Zugriffsrechten einen zentralen Gefährdungsfaktor darstellt, muss diese besonders überwacht werden. Hier muss protokolliert werden, ob Administratoren Einzelberechtigungen oder gar Zugriffsrechte an sich selbst oder andere verteilen.	X	X	
PA_VM-04-06	**Zugriff auf besondere Befehle muss protokolliert werden** In IT-Applikationen und Technologien existieren bestimmte Befehle, mit welchen umfangreiche Zugriffsrechte (siehe auch RL128098 Sicherheitsvorgaben für das Berechtigungsmanagement verbunden sind. Als Beispiele können „su“ oder „sudo“ in Unix-Umgebungen beziehungsweise die Transaktion „SE38“ in SAP genannt werden. Der Zugriff auf derartige Befehle müssen protokolliert werden.	X	X	

5.5 Auswertung von kritischen Aktivitäten.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PA_VM-05-01	**Prüfung durch unabhängige Unternehmenseinheiten** Die unter Kapitel 3.2 definierten kritischen Sessions müssen neben der vollständigen Protokollierung regelmäßig oder anlassbezogen durch unabhängige Unternehmenseinheiten überprüft und ausgewertet werden. Dazu sind mindestens nachfolgende Kontrollen einzurichten: 1. Ad-hoc-Kontrollen die auf einen konkreten Verdachtsfall hin durchgeführt werden. 2. Systematische Auswertungen der Protokolldaten, welche Hinweise auf Auffälligkeiten geben können. Die auszuwertenden Aktivitäten müssen definiert und in unterschiedlich kritische Kategorien eingeordnet werden, auf welche unterschiedlich schnell und intensiv reagiert werden muss. Für kritische Applikationen und Technologien müssen durchschnittliche Soll-Werte der Aktivitäten definiert werden, die mit den tatsächlichen Ist-Vorfällen verglichen und, wenn möglich, automatisch auf Abweichungen überwacht werden. 3. Die durchgeführten Tätigkeiten während kritischen Sessions sind mit Hilfe einer Stichprobe auf Auffälligkeiten zu überprüfen.	X	X	
PA_VM-05-02	**Auswertung durch den KfW SIEM Prozess** Die auszuwertenden Aktivitäten sind an den KfW SIEM Prozess zu übergeben. Hierzu ist ein „Event forwarding“ an das SIEM System einzurichten.	X	X	

5.6 Zielgerichtete Angriffe auf privilegierte User

Kürzeln	Anforderung	Schutzziel		
		V	I	V
PA_VM-06-01	**Für kritische Sessions muss PIM eingerichtet werden** Für die kritischen Sessions muss ein Sprungserver mit einem Passwort Vault Management z.B. eines Privilegierten Identity Management Systems (PIM)	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

	eingesetzt werden. Das System muss die Möglichkeit bieten, nach erfolgreicher Authentifizierung die administrative Session zum Zielsystem direkt bereitzustellen und als Proxysystem für die Konfigurationssession zu fungieren. Die Zuweisung der jeweiligen Zugriffsmöglichkeiten muss dabei userbezogen erfolgen. Die Sprungsysteme dürfen keine Internetverbindungen aufbauen. Die Sprungserver und das Passwort Vault Management müssen einer besonderen, dem Einsatzweck angepassten Systemhärtung unterliegen. An den Zielsystemen und den dazwischengeschalteten Sicherheits-Gateways muss gewährleistet werden, dass nur die Sprungsysteme Zugriff auf die jeweiligen Zielsysteme erhalten.			
PA_VM-06-01	**Authentifizierungsverfahren mit 2-Faktor Authentifizierung** Für den Zugriff auf Sprungserver und den Passwort Vault muss ein starkes Authentifizierungsverfahren mit 2-Faktor Authentifizierung verwendet werden.	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

6 RELEVANTE PROZESSE

Keine relevanten Prozesse

7 RELEVANTE UNTERLAGEN

LL001501 Leitlinie-ISMS

RL128093_IS-Organisation und Aufgaben

RL040049 Passwortrichtlinie für IT-Systemen

RL 000081 IS-Werte- und –Risikomanagement

RL128098 Sicherheitsvorgaben für das Berechtigungsmanagement

DV SIEM

DV Privileged Identity Management PIM

DV002020 DV EMail und Internet

8 ANHANG

Kein Anhang

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

KfW-Organisationshandbuch

Richtlinie Nr. RL 128088

Titel Sicherheitsvorgaben für IT Security Architektur

GELTUNGSBEREICH	Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG (s. Kapitel Geltungsbereich)
VERANTWORTLICHE OE	COc2
DOKUMENTVERANTWORTLICH	Waldemar Burghardt
VERTRAULICHKEITSSTUFE	2 (intern)

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

ERSETZT
VERÖFFENTLICHUNGSDATUM VOM: 20.01.2017

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

ÄNDERUNGEN ZUR VORVERSION

Änderungs-datum	**Kapitel**	**Inhalte**
Aug. 2015	alle	Erstellung Dokument
17.01.2017	2	Änderung das Geltungsbereichs auf CO und IT
Juli 2017	2 3,6	Geltungsbereich angepasst und auf IPEX und DEG ausgeweitet Anpassung auf aktuelle ISO Maßnahmen

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

INHALTSVERZEICHNIS

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

9 KURZBESCHREIBUNG

In dieser IS-Richtlinie werden die grundsätzliche Rahmenbdingungen für die Implementierung einer IT Security Architektur beschrieben.

Regelungsdokumente wie die IS-Richtlinie konkretisieren die ISMS-Leitlinie und dienen als Grundlage für die operative Umsetzung durch die zuständigen Stellen.

Die IS-Vorgaben stellen keine Lösungen dar, sind aber ausreichend konkret, um auf operativer Ebene (1st Line of Defense) Sicherheitskonzepte entwickeln zu können.

Entstehen in der Praxis Situationen, bei welchen die Vorgaben nicht oder nicht vollständig umsetzbar sind, so sind alternative Lösungen zu entwickeln, die dem angestrebten Sicherheitsniveau entsprechen.

10 GELTUNGSBEREICH

Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG.

Die Töchter weichen lediglich bei institutsspezifischen Besonderheiten (gesetzliche, vertragliche, externe oder geschäftliche Anforderungen) durch spezifische Anpassungen ab. Die Konzernleit- und -richtlinien erlangen nachfolgend erst nach Freigabe durch die jeweilige Geschäftsführung der Töchter („Ratifizierung“) Gültigkeit in den Einzelinstituten DEG/IPEX.
Den Einzelinstituten bleibt es im Übrigen unbenommen, unter Ausschluss von Widersprüchen mit den konzernweit nach den vorstehenden Maßgaben verabschiedeten und geltenden Regelungen konkretisierende Einzelmaßnahmen (Richtlinien, Arbeitsanweisungen) zu verabschieden.

11 ZIELSETZUNG

Die Zielsetzung der IT Security Architektur ist die

- Verbesserung der Planung und Steuerung der IT Sicherheit
- Konzeption und Weiterentwicklung einer IT Security Architektur der KfW
- Integration der IT Security Architektur in die Gesamtarchitektur der KfW
- Herstellung eines zentralen und systematischen Überblicks des Umsetzungsstands und der Wirksamkeit von IT-Sicherheitsanforderungen. (ISO27002/13.1.1/13.2.2)

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

12 DEFINITION

12.1 IT Security Architektur

Die IT Security Architektur beschreibt die Gesamtheit aller realisierten Sicherheitskonzepte und die daraus abgeleiteten Sicherheitsmaßnahmen des KfW-Konzerns.

Dabei basiert die IT Security Architektur auf einer Kombination von verschiedenen ineinander greifenden Sicherheitsmaßnahmen.

Die IT Security Architektur ist ein Bestandteil der Architektur der KfW und wird über die Geschäftserfordernisse auf der Basis von Schutzbedarfsfeststellungen und IS-Risikoanalysen abgeleitet.

12.2 Cyber Security

Die Informationssicherheit hat zum Ziel die Informationen der KfW hinsichtlich ihrer Vertraulichkeit, Integrität (inkl. Authentizität) und Verfügbarkeit zu schützen. Die Cyber Security betrachtet dabei im speziellen diejenigen Informationen und IT-Systeme der KfW, die über Cyber Raum erreichbar sind. Der Cyber Raum umfasst alle über das Internet bzw. sonstige vergleichbare IT-Netze (z. B. Partnernetze) erreichbaren IT Systeme.

Bei Cyber Angriffen wird in der Regel das Internet als universelles und öffentliches Verbindungs- und Transportnetz als Kommunikationsinfrastruktur verwendet. Durch den öffentlichen Charakter des Internets bietet dieses die Möglichkeit Quelle, Ziele sowie Werkzeuge für kriminelle Handlungen zu sein (z. B. Verteilung von Viren, Trojanern, Phishing-Mails oder Distributed Denial-of-Service-Attacken (DDoS)).

Um Cyber Risiken auf ein angemessenes Niveau zu reduzieren, sind geeignete Sicherheitsmaßnahmen zu ergreifen. Klassische Maßnahmen der IT-Sicherheit müssen hierzu um spezielle Sicherheitsmaßnahmen zur Abwehr von Cyber Angriffen ergänzt werden.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

13 VORGEHENSWEISE DER SICHERHEITSKONZEPTION DER KFW

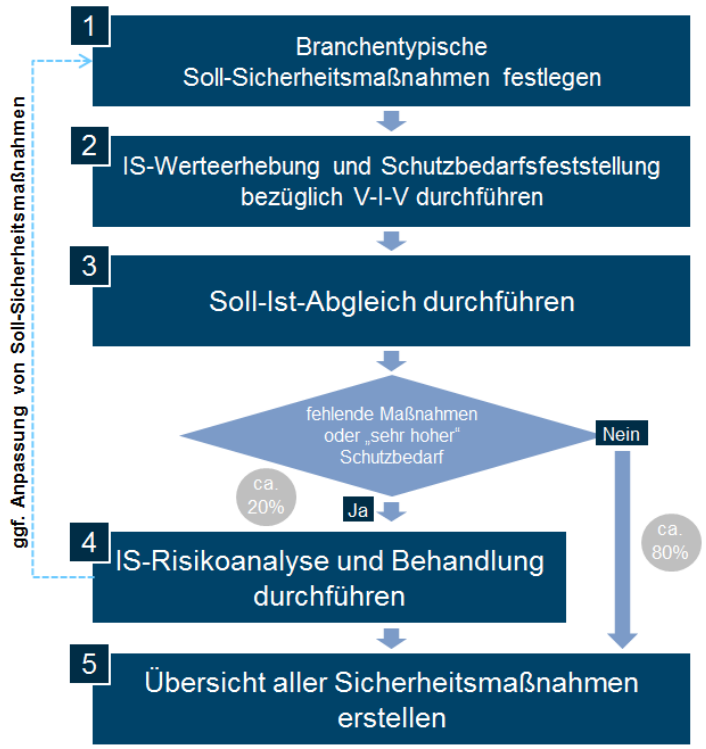

Abbildung 1: Sicherheitskonzeption der KfW

Im **ersten Schritt** werden branchentypische Soll-Sicherheitsmaßnahmen definiert. Diese werden aus gesetzlichen Vorgaben, den Anforderungen der Normenreihe ISO27001/2, den Ergebnissen der IS-Risikoanalysen, Security Audits, IS-Vorfällen und den Anmerkungen der BaFin, WP und IR abgeleitet.

Im **zweiten Schritt** wird eine IS-Werteerhebung durchgeführt. Für die Durchführung der IS-Werteerhebung ist es erforderlich, das Zusammenspiel der Informationswerte, Geschäftsprozesse, der Applikationen zu analysieren und zu dokumentieren. Dabei geht es um die Erfassung der Bestandteile (Informationswerte, Applikationen, IT-Systeme(IT-Infrastruktur), Räume, Kommunikationsbeziehungen(Netzwerkkommunikation)), die zur Erfüllung der im Geltungsbereich festgelegten Geschäftsprozesse oder Fachaufgaben benötigt werden. Anschließend wird der Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit eingestuft.

Im **dritten Schritt** reduziert sich die IS-Risikoanalyse auf einen Soll-Ist-Abgleich zwischen den Soll-Sicherheitsmaßnahmen und den bereits realisierten Maßnahmen. Dabei festgestellte fehlende oder nur unzureichend umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem Sehr hohen Schutzbedarf oder der Nichtumsetzung der Soll-Sicherheitsmaßnahmen muss im **vierten Schritt** zusätzlich eine ergänzende IS-Risikoanalyse durchgeführt werden und unter Beachtung von Kosten-/Wirksamkeitsaspekten eine angemessene Behandlung erarbeitet werden. Im **fünften Schritt** wird eine Übersicht alle sicherheitsrelevanten Maßnahmen erstellt bzw. aktualisiert.

14 VERZAHNUNG IT SECURITY UND IT ARCHITEKTUR

Die IT Architektur umfasst die Ebenen:

- **Funktions- und Datenarchitektur**
- **Applikationsarchitektur**
- **Technologiearchitektur**
- **IT Security Architektur der Schutzsysteme.**

Die IT Security Architektur und die daraus abgeleiteten Sicherheitsmaßnahmen sind integrale Bestandteile der IT Architektur. Auf allen Ebenen der IT Architektur wirken IT Security Anforderungen, die sich aus den normativen und gesetzlichen Anforderungen ableiten.

Die Verzahnung der einzelnen Ebenen wird in der nachfolgenden Grafik dargestellt:

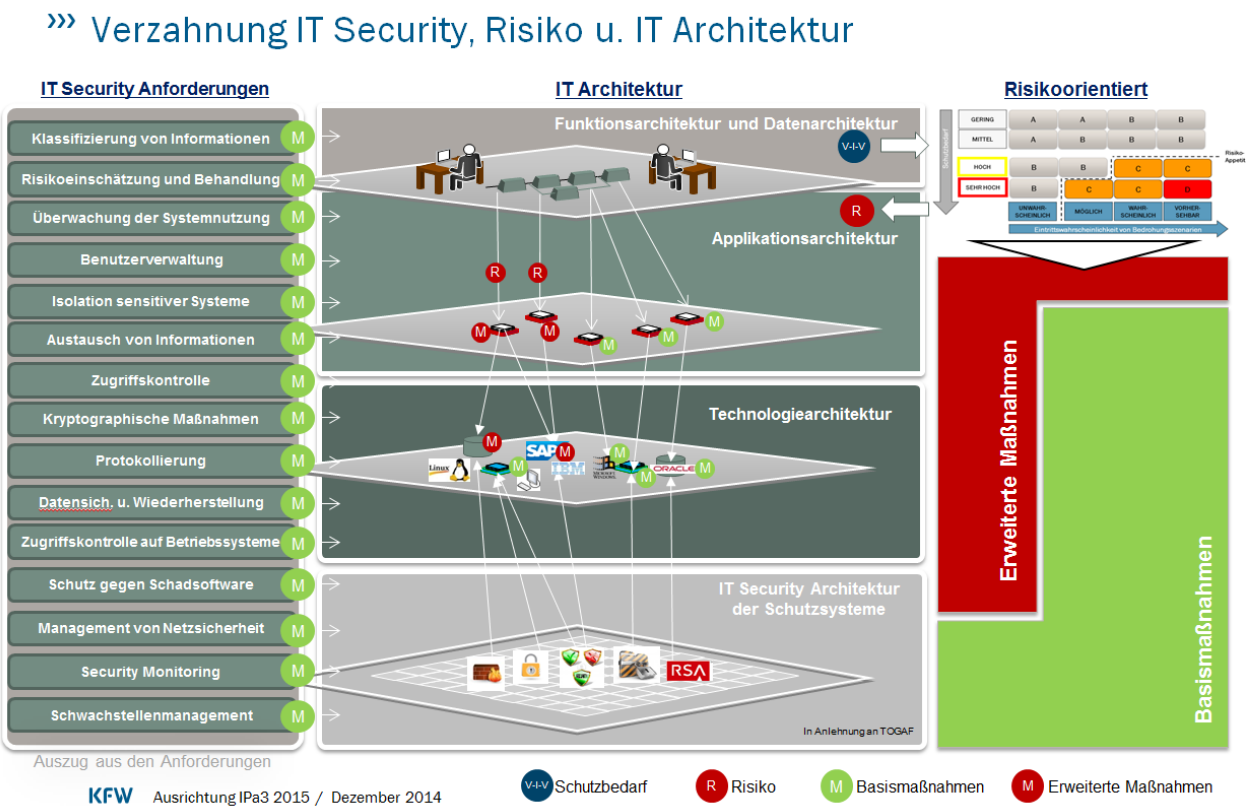

Abbildung 2: Verzahnung IT Security, Risiko und IT Architektur

Die Verzahnung der IT Security, Risiko und IT Architektur wird im Folgenden weiter detailliert und erläutert.

14.1 Funktions- und Datenarchitektur

Auf Basis der Schutzbedarfsfeststellungen von primären Informationswerten (z.B. Daten) durch KfW-Fachbereiche ändert sich der Schutzbedarf der darunterliegenden Ebenen der IT Architektur.

14.2 Applikations- und Technologiearchitektur

Applikationen bzw. Technologien sollten so stark aggregiert wie möglich und so granular wie für die IT Security Konzeption nötig gruppiert werden. Zu diesem Zweck soll für Applikationen bzw. Technologien Strukturanalyse durchgeführt werden. Ziel der Strukturanalyse ist das Zusammenspiel der Applikationen und zugrundeliegender Infrastruktur zu analysieren und darzustellen. Dabei wird die

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

V-I-V Einstufung aus der Schutzbedarfsfeststellung, entsprechend der identifizierten Abhängigkeiten auf genutzte Komponenten (z.B. Server-Plattformen) vererbt.

Die gruppierten Applikationen und Technologien bilden die Basis für Schutzbedarfsfeststellungen, Sicherheitskonzepte und IS-Risikoanalysen.

Weitere Differenzierung der Applikationen in der IT: Die IT unterscheidet die Applikationen welche im Rahmen des SWEP eingeführt oder angepasst werden in nachfolgenden Klassen. Die Einstufung der Anwendung in die Klasse erfolgt anhand der im SWEP verbindlich geregelten Kriterien.

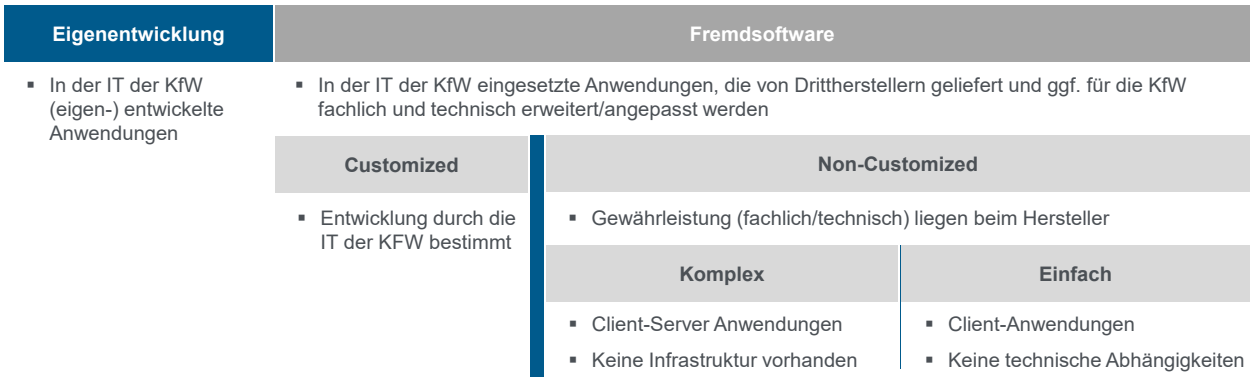

Abbildung 3: Weitere Differenzierung von Applikationen innerhalb der IT

14.2.1 Sicherheitsdokumentation für Applikationen und Technologien

Die Entscheidung über den Umfang der Sicherheitsdokumentation hängt von der Komplexität, den Schutzbedarf und der Gefährdungslage ab.
Für die KfW wird festgelegt, dass für alle IT System die über den Cyber-Raum erreichbar sind Sicherheitskonzepte zu erstellen sind. Für alle anderen IT-Systeme gelten die nachfolgenden Mindestanforderungen.

<table>
<tr><th>Dokumentation
IT Systeme</th><th>Technisches Design</th><th>Sicherheitskonzept</th></tr>
<tr><td>Eigenentwicklung</td><td rowspan="3">Vertraulichkeit
Integrität
Verfügbarkeit
=
niedrig oder mittel</td><td rowspan="3">Vertraulichkeit
Integrität
Verfügbarkeit
=
hoch & sehr hoch</td></tr>
<tr><td>Fremdsoftware
Customized</td></tr>
<tr><td>Technologieprodukte</td></tr>
<tr><td>Fremdsoftware
Non-Customized
(Komplex)</td><td rowspan="2">Vertraulichkeit
Integrität
Verfügbarkeit
=
niedrig bis sehr hoch</td><td rowspan="2"></td></tr>
<tr><td>Fremdsoftware
Non-Customized
(Einfach)</td></tr>
</table>

Abbildung 4: Sicherheitsdokumentation für Applikationen und Technologien

Inhalte der Sicherheitsdokumentation:

Technisches Design	Sicherheitskonzept
• Schutzbedarf • Verfügbarkeitsklassen • Account und Passwortverwaltung • Benutzer und Rollenverwaltung	Inhalte aus dem technischen Design und • Technische Beschreibung • Physische und umgebungsbezogene Sicherheit

• Authentifizierung • Berechtigungsprüfung • Patchmanagement • Physische Sicherheit • Perimeterschutz • Schutz gegen Schadsoftware	• Zugangskontrolle (Authentisierung) • Zugriffskontrolle (Autorisierung) • Protokollierung • Datensicherung und Wiederherstellung • Notfallkonzept • Besondere Sicherheitsmaßnahmen

14.3 IT Security Architektur der Schutzsysteme

Die wesentliche Ebene der IT Security Architektur wird durch die so genannten „Schutzsysteme“ gebildet, die in der IT Security Architektur der Schutzsysteme zusammengefasst sind.

In der IT Security Architektur der Schutzsysteme werden übergreifende Bausteine der IT Security beschrieben, die zum Schutz der in der KfW verwendeten Daten und IT-Systeme verwendet werden.

Die IT Security Architektur der Schutzsysteme basiert auf der Erkenntnis, dass die Schutzziele nicht alleine durch den Einsatz einzelner Schutzmaßnahmen erreicht werden können. Vielmehr bedarf es einer der Situation angemessenen Kombination aus verschiedenen ineinandergreifenden Mechanismen von IT Schutzmaßnahmen, um ein notwendiges Maß an Sicherheit für IT Systeme zu erzeugen. Im Allgemeinen spricht man bei dem gewählten Ansatz von multilateraler Sicherheit bzw. “Verteidigung in der Tiefe“[2].

Die Inhalte der IT Security Architektur der Schutzsysteme sollen dem Service und Produktverantwortlichen helfen die Sicherheit seiner Systeme zu gewährleisten, in dem die wesentlichen notwendigen Bausteine und alle sicherheitsrelevanten Konfigurationen auflistet werden, die innerhalb eines Services betrachtet und - sofern anwendbar - umgesetzt werden müssen.

[2] "Verteidigung in der Tiefe" lautet ein hochgradig wirksamer Ansatz im Bereich Sicherheit. Durch Implementierung voneinander unabhängiger, sich gegenseitig verstärkender Sicherheitsmechanismen auf unterschiedlichen Ebenen werden dabei mehrere Verteidigungslinien geschaffen. Wenn ein Mechanismus ausfällt, springt ein anderer ein. Die "Verteidigung in der Tiefe" ist die logische Konsequenz aus der Einsicht, dass ein Schutzsystem oder eine Schutzfunktion allein auf Dauer niemals ausreichend sein kann.

Im Einzelnen handelt es sich um folgende Sicherheitsthemen und die damit verbundenen Sicherheitsbereiche:

Abbildung 5: IT Security Architektur der Schutzsysteme

14.3.1 IT Security Themen

Die IT Security Themen sind an den Regelungsbereichen des Anhang A der ISO 27001 und der aktuellen Gefährdungslage des Unternehmens orientiert und bilden das erste Ordnungsmerkmal der IT Security Architektur der Schutzsysteme. Die IT Security Themen beschreiben inhaltlich zusammenhängende Schutzziele die einen von der ISO Norm geforderten Regelungsbereiche abdecken (z.B. A.12.2. „Schutz vor Schadsoftware“).

14.3.2 IT Security Bereiche

Die IT Security Bereiche wurden aus der ISO 27002 und Regelungen der IT Sicherheit der KfW abgeleitet. Ein IT Security Thema untergliedert sich spezifische Unterkategorien, die jeweils einzelne Schutzmaßnahmen nochmal thematisch zusammenfassen z.B. „Hostbasierter Schutz gegen Schadcode“.

14.3.3 IT Security Services und Tools

Ein oder mehrere IT Security Tools bilden einen IT Security Service. Unter IT Security Tools werden Technologieprodukte oder Applikationen verstanden, welche die Schutzfunktion ausführen. Generell kann ein IT Security Service aus einem oder mehreren Tools bestehen.

Nachfolgend ein Beispiel zur Darstellung des Zusammenhangs:

- IT Security Thema **„Schutz gegen Schadsoftware“**
- IT Security Bereich **„Hostbasierter Schutz von Schadcode“**
- IT Security Service **„AV-System Windows Client“**
- IT Security Tool **“McAfee Virus Scan Enterprise Client + McAfee Move”**

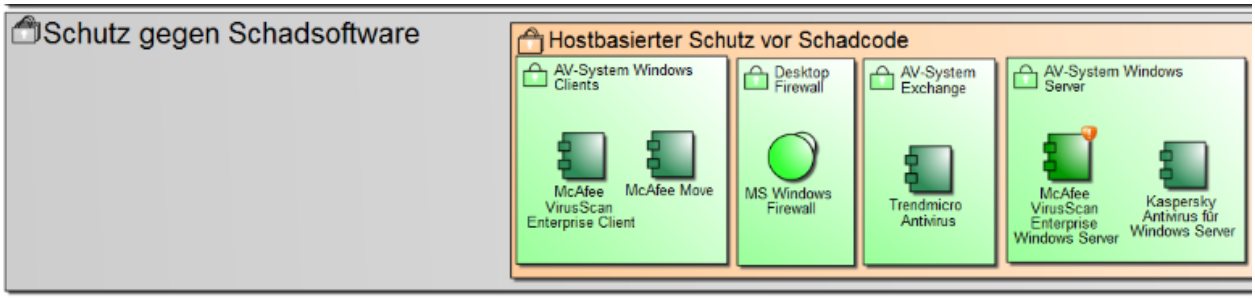

Abbildung 6: IT-Security Thema „Schutz gegen Schadsoftware“ (Auszug)

14.4 Dokumentation der IT Security Architektur

Die IT Security Architektur ist gemäß den oberen Vorgaben zu dokumentieren.

Für die Pflege der IT Security Architektur ist eine Prozess in der jeweiligen 1st Line of Defense zu etablieren. Der Prozess soll einen zentralen und systematischen Überblick bezüglich des Umsetzungsstands, der Wirksamkeit seiner IT-Sicherheitsmaßnahmen sowie der damit einhergehenden Risiken sicherstellen.

Ein solcher systematischer Überblick der einzelnen Themenbereiche ist exemplarisch für das IT Security Asset “Client“ im nachfolgenden Schaubild dargestellt:

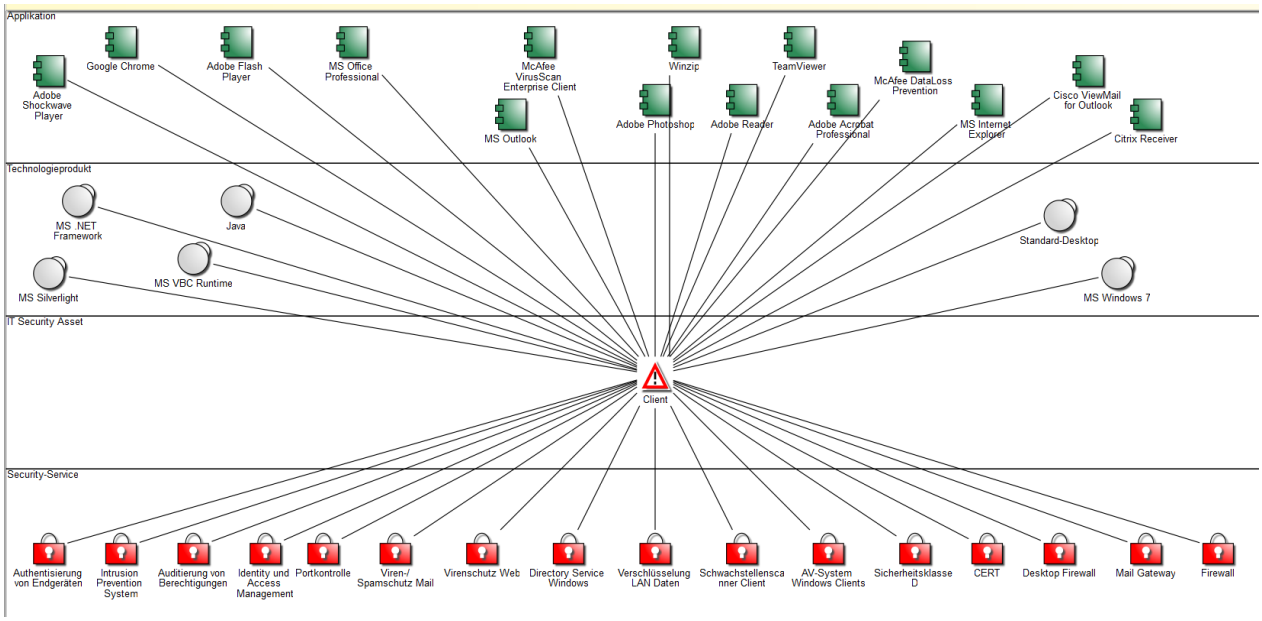

Abbildung 7 : Exemplarischer Überblick für das IT Security Asset „Client“

15 RELEVANTE PROZESSE

Keine relevanten Prozesse

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

16 RELEVANTE DOKUMENTE

RL000081 IS-Werte- und -Risikomanagement

RL128084 Strukturanalyse für Informationssicherheit relevanten Unternehmenswerte

FO040413 Schutz-Niveau-Rechner

RL128093 IS-Organisation und Aufgaben

17 ANHANG

Kein Anhang

KfW-Organisationshandbuch

Richtlinie Nr. RL128089

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Titel Anforderungen an die physikalische Sicherheit von RZ und IT-Räumen

GELTUNGSBEREICH	VL IT VL ZS VL TM
VERANTWORTLICHE OE	TM01
DOKUMENTVERANTWORTLICH	Danz, Uwe
VERTRAULICHKEITSSTUFE	Intern (Stufe 2)
ERSETZT VERÖFFENTLICHUNGSDATUM VOM:	17.04.2018

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

ÄNDERUNGEN ZUR VORVERSION

Änderungs-datum	**Kapitel**	**Inhalte**
Nov 2015	Alle	Initialversion
17.01.2017	2	Änderung das Geltungsbereichs auf CO, ZS und IT
14.02.2017	Alle	Erweiterung des Richtlinieninhalts auf physikaliche Sicherheit von Rechenzentren und IT-Räumen Überarbeitung aller Kapitel
08.04.2017	Alle	Überarbeitung hinsichtlich marktüblicher Standards
28.03.2018	5.2.	Ergänzung SIB-02-013 Umgang mit USB- und sonstigen Daten-Schnittstellen von IT-Servern
11.03.2020	2, 6	Anpassung der Bereichsbezeichnung CO zu TM wegen Umorganisation. Ergänzung Kapitel 6 auf Grund neuer OC-Anforderung

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

INHALTSVERZEICHNIS

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

18 KURZBESCHREIBUNG

Der sichere und störungsfreie Betrieb der IT–Infrastruktur ist eine wesentliche Voraussetzung für den gesamten Geschäftsbetrieb der KFW Bankengruppe. In dieser Richtlinie werden die Anforderungen zur Gewährleistung der physikalischen Sicherheit von Rechenzentren und IT-Räumen, d.h. Räume, in denen IT-Infrastruktur betrieben wird, beschrieben. Die Vorgaben gliedern sich hierbei in die Bereiche

- Sicherheitsbereiche, Organisation und Dokumentation
- Sicherheitssysteme
- Umfeld und Baukonstruktion, Brandschutz,
- Unterbrechungsfreie Energieversorgung
- Klimatisierung und Belüftung.

19 GELTUNGSBEREICH

Bereiche IT, ZS, TM

19.1 Erläuterungen & Abgrenzungen

Ein „IT Raum“ ist ein Raum in dem IT Infrastruktur vorhanden oder administriert wird. Hierzu gehören auch aktive Netzwerkkomponenten. Alle anderen Räume liegen nicht im Geltungsbereich dieses Dokuments.

20 ZIEL

Schutz vor unerlaubtem Zutritt und Beschädigung, Störung von IT Systemen und dazugehörenden Informationen. (auf Basis der ISO 27002/9.1)

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

21 RISIKOORIENTIERTE VORGEHENSWEISE

Sicherheitsrelevante Bereiche benötigen Schutz gemäß deren ermittelten Schutzbedarfsklassen. Gebäude oder Räume, die IT-Systeme enthalten oder zum Betrieb von IT-Systemen dienen, müssen auf Basis einer Risikobetrachtung einer Sicherheitsklasse zugeordnet werden. Die Zuordnung der Sicherheitsklasse muss von einem für den Raum verantwortlichen IT Mitarbeiter durchgeführt werden.

Die Umsetzung der erforderlichen Schutzmaßnahmen zur physischen Sicherung und die korrekte technische Umsetzung muss transparent dokumentiert und mit dem Betreiber der Zutrittskontrollsysteme klar geregelt sein.

Sicherheitsklassen und Mindestanforderungen abhängig von der Risikoeinschätzung:

Sicherheits-klasse	Zutrittsschutz (Mindestsicherung)	Sicherheitsbereich
A	Sicherheitsdienst 2-Faktor-Authentifizierung mit Protokollierung	Rechenzentren Serverräume
B	Sicherheitsdienst 1-Faktor Authentifizierung oder Schlüssel	Operatingzonen Testzonen Lagerräume Netzwerkverteilerräume Räume mit USV und NEA, Stromverteilung, Trafos und Klimaanlagen

22 VORGABEN ZUR UMSETZUNG

22.1 Klassifizierung von Sicherheitsbereichen

Kürzel	Beschreibung
SIB-01-01	**Klassifizierung von Sicherheitsbereichen** Jeder Sicherheitsbereich muss einer Sicherheitsklasse zugeordnet werden. Für jeden Sicherheitsbereich muss eine verantwortliche Person benannt sein.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

22.2 Allgemeine Anforderungen an alle Sicherheitsbereiche

Kürzel	Beschreibung
SIB-02-01	**Ausweise und Schlüssel** Ausweise und Schlüssel für den Zutritt zu Sicherheitsbereichen müssen personenbezogen ausgegeben werden.
SIB-02-02	**Zutrittsberechtigungen für Dritte** Die Zutrittsberechtigungen für externe Mitarbeiter und Besucher müssen in einem geregelten Verfahren festgelegt, dokumentiert und aktualisiert werden.
SIB-02-03	**Funktionsausweise Ausgabe und Rücknahme** Die Ausgabe und Rücknahme von Funktionsausweisen muss dokumentiert werden.
SIB-02-04	**Funktionsausweise Rückgabe** Funktionsausweise müssen beim Verlassen des Standorts der ausgebenden Stelle unverzüglich zurückgegeben werden.
SIB-02-05	**Austritt und Abteilungswechsel** Bei Wechsel der Abteilung oder Austritt aus dem Unternehmen müssen dem jeweiligen Mitarbeiter alle Zutrittsrechte zu Sicherheitsbereichen unverzüglich und vollständig entzogen werden. Der Mitarbeiter muss alle erhaltenen Zutrittsmittel zurückgeben.
SIB-02-06	**Zutrittsrechte zu IT-Räumen** Zutrittsrechte zu IT-Räumen müssen aufgabenbezogen vergeben und auf das unbedingt notwendige Maß beschränkt werden.
SIB-02-07	**Zutrittsgenehmigung** Der Zutritt in Sicherheitsbereiche ist durch einen formalen Genehmigungsprozess zu erteilen. Unbegleitetes, externes Personal muss einen sichtbaren Ausweis tragen.
SIB-02-08	**Protokollierung von Zutritten zu Sicherheitsbereichen**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
	Der Zutritt zu allen Sicherheitsbereichen muss protokolliert werden. Die Log-Audits/Files sind sicher zu verwahren. Auswertungen sind sicher und unter Einhaltung der internen und regulativen Vorgaben zu archivieren.
SIB-02-09	**Prüfung der Zutrittsberechtigungen** Die erteilten Zutrittsberechtigungen sind in festgelegten Frequenzen auf Ordnungsmäßigkeit zu prüfen. Frequenz und Umfang sind dabei entsprechend der Risikolage des Objekts festzulegen.
SIB-02-10	**Entsorgung** Alle Informationsträger (Daten, Hardware, etc.) müssen gemäß den KfW Entsorgungsrichtlinien entsorgt oder vernichtet werden.
SIB-02-11	**Umgang mit Datenträgern** Informationen jeglicher Art und Form (Daten, gespeichert auf Festplatten etc.) dürfen aus den Sicherheitsbereichen nicht entfernt werden. Der Umgang mit Ausnahmen muss geregelt werden.
SIB-02-12	**Heißarbeiten in Sicherheitsbereiche** Heißarbeiten in Sicherheitsbereichen sind anzumelden und zu genehmigen. Es gelten ergänzend die einschlägigen Vorschriften der KfW (Brandschutz).
SIB-02-13	**Umgang mit USB- und sonstigen Daten-Schnittstellen von IT-Servern** Alle Datenschnittstellen, z.B. USB, CD/DVD-Leser/-Brenner, FireWire, etc. sind grundsätzlich organisatorisch und technisch vor Missbrauch zu schützen.

22.3 Besondere Anforderungen an den Schutz von technischen Anlagen in Gebäuden bzw. der Räumen der Sicherheitsklasse A

22.3.1 Anforderungen an das Umfeld von Rechenzentren

Kürzel	Beschreibung
SIB-03-01	Hochwasser- und Überschwemmungsgebiete sollten gemieden werden. Standorte mit leichtem Risiko von Überschwemmungen sind akzeptabel, sofern ausreichende bauliche Maßnahmen zum Schutz vor eindringendem Wasser getroffen wurden. In die Betrachtung sind alle Infrastrukturkomponenten des Rechenzentrums einzubeziehen.
SIB-03-02	Die Umgebung von Betrieben mit Schadstoffausstoß in Hauptwindrichtung des zu betrachtenden Objekts sollten gemieden werden. Als Alternative dazu kann eine Betriebsbeeinträchtigung durch Schadstoff- und Staubbelastung durch geeignete technische Schutzmaßnahmen verhindern werden.
SIB-03-03	Starke elektromagnetische Quellen, wie Sendeanlagen und Hochspannungsleitungen sollten gemieden werden. Abhängig von der Stärke der Quelle sind Sicherheitsabstände oder evtl. Maßnahmen wie z. B. Schirmung sicherzustellen, die eine Betriebsbeeinträchtigung verhindern.
SIB-03-04	Jegliche Quellen in der Umgebung. wie Walz- und Hammerwerke. Straßen mit hoher Schwerverkehrsbelastung und Bahntrassen, sollten gemieden werden, soweit nicht eine konstruktive Schwingungsentkopplung gegeben ist.
SIB-03-05	Folgende Mindestabstände sollten eingehalten werden: Hauptverkehrsstraße und Bahntrassen: 75 m, Wasserwege: 150 m, Flughäfen: außerhalb des Anflugsektors. Geringere Abstände sind tolerierbar, wenn Maßnahmen risikobehaftete Abstände kompensieren können.

22.3.2 Anforderungen an die Baukonstruktion von Rechenzentren

Kürzel	Beschreibung
SIB-04-01	Befindet sich die RZ-Fläche innerhalb eines Bürogebäudes, muss die Lage unauffällig

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

	(nicht exponiert) sein. Es sollte eine Tiefenstaffelung hinsichtlich des Sicherheitsbereichs (SB) im Gebäude existieren. Der SB liegt abseits von Besucherverkehr, Personen- und Materialströmen. Es gibt keine Hinweise auf die Existenz und Lage des SB. Auf Lagehinweise ist zu verzichten.
SIB-04-02	Gebäudebereiche mit Gefährdungspotenzial sind zu meiden. Räume, die unmittelbar an IT- und Technik-Räume (T) grenzen und die aufgrund ihrer Nutzung eine Gefährdung für diese Technik-Räume und auch für die Versorgungstrassen (Energie, Datennetz) darstellen, müssen gemieden werden, es sei denn, das Risiko wird durch geeignete Gegenmaßnahmen kompensiert. Hohes Gefährdungspotenzial weisen z. B. auf: Gasanschluss- oder zentrale Heizräume, explosionsgefährdete Produktionsbereiche oder Räume, in denen leicht entzündliche Gegenstände lagern
SIB-04-03	Der Sicherheitsbereich wird durch Technik- (T-), Funktions- (F-) und IT-Räume gebildet. F-Räume sind z. B. Schleusen, Flure, Vorbereitungsräume, etc. Die IT-Räume und die zugehörigen F-Räume bilden einen zusammenhängenden Sicherheitsbereich.
SIB-04-04	Es muss auf eine sinnvolle Raumaufteilung mit brandschutztechnischer Trennung geachtet werden. Es wird dem Prinzip der Trennung von Grob- (T-Räume) und Feintechnik (IT-Räume) gefolgt. Redundante Komponenten befinden sich in unterschiedlichen brandschutztechnisch voneinander getrennten Räumen. IT-Räume bilden hierbei einen eigenen Brandabschnitt.
SIB-04-05	Die Fläche, Höhe und Statik der IT Räume ist ausreichend zu dimensionieren. Ein ungehinderter Transport und eine barrierefreie Wartung der Geräte muss gegeben sein. Die Raum- und Doppelbodenhöhen erlauben eine ungehinderte Luftzirkulation und die Tragfähigkeit des Doppelbodens muss so ausgelegt sein, dass er auch schwere Lasten aufnehmen kann. Die Auslegung erfolgt so, dass Wartungen an den Komponenten möglich sind, Luftzirkulationen nicht behindert werden und die Tragfähigkeit des Bodens auf das Equipment angepasst ist.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

SIB-04-06	Unmittelbar neben, über oder unter IT-Räumen dürfen keine Parkmöglichkeiten existieren, soweit nicht zusätzliche Maßnahmen des Brandschutzes, des Anfahrschutzes und der Zufahrtskontrolle getroffen werden.
SIB-04-07	Das Gebäude muss über einen äußeren Blitzschutz verfügen. Alle Dachaufbauten sind derart in den Blitzschutz eingebunden, dass sie vor direkter Blitzeinwirkung geschützt sind. Die Ableitung mit entsprechender Erdung ist sichergestellt. Die Anlage muss mindestens der Blitzschutzklasse III gemäß EN 62305 entsprechen.
SIB-04-08	Raumtrennungen und Decken müssen in massiver Bauweise ausgeführt werden, so dass sie Brandschutz, Gasdichtigkeit und Einbruchhemmung bieten.
SIB-04-09	Zumindest die einzelnen IT-Räume oder alternativ das gesamte RZ müssen in Bezug auf ihre bauliche Ausführung - Türen, Fenster, Kanäle - einbruchhemmend gemäß EN 1627 mit definierten Widerstandsklassen (Resistance Class (RC)) ausgeführt werden. Direkte Inner- und Außengrenzen zur Öffentlichkeit sind einbruchhemmend auszuführen. Ferner ist durch technische Maßnahmen sicher zu stellen, dass die IT-Räume, oder alternativ das gesamte RZ (Zone), jederzeit verschlossen ist. Alle Türen der IT-Räume sind mit einem Knauf ausgestattet.
SIB-04-10	Für IT-Räume sollten über keine Fenster verfügen. Dennoch vorhandene Fenster sind zur Reduzierung des damit verbundenen Risikos (Einbruch, Brand, Wärmeeintrag und Einsicht) besonders abgesichert.
SIB-04-11	Kanäle, Steigschächte & Außenöffnungen sind mit Sabotage und Durchstiegssicherungen sind an der Zonengrenze durch geeignete Maßnahemn, z.B. einbruchhemmende Gitter, zu sichern.
SIB-04-12	Versorgungstrassen müssen mit Schutz vor mechanischen Beschädigungen in das Gebäude ausgeführt sein.
SIB-04-13	In IT-Räumen und RZ sind möglichst keine brennbare Materialien zu verbringen. In IT-Räumen findet keine Lagerhaltung statt.
SIB-04-14	Türen, Fenster und Abschlüsse sind gegen Brand und Rauch gemäß EN 13501 abzusichern. Der Brandübertritt ist für mindesten 30 Minuten zu verhindern.
SIB-04-15	Für durchzuführende Komponenten, wie z.B Verkabelungen müssen geeignete, zugelassene Brandschotts eingesetzt werden, die gekennzeichnet sind und stets

	geschlossen gehalten werden.
SIB-04-16	Gegen die Gefährdung durch das Eindringen von Wasser in IT-Räume oder RZ sind bauliche oder konstruktive Maßnahmen zu treffen, die das Eindringen von Wasser verhindern. Es sind bauliche/konstruktive Maßnahmen zur Begrenzung von Leckagen in IT-Räumen zu treffen.
SIB-04-17	Durch Räume der Energieversorgung dürfen keine flüssigkeitsführende Leitungen verlaufen, die nicht der Versorgung der IT dienen. In IT-Räumen sind, nicht zwingend dem Zwecke der IT dienende, flüssigkeitsführende Leitungen möglichst vollständig zu vermeiden, weisen aber in jedem Fall eine begrenzte Flüssigkeitsmenge auf. Erforderliche Leitungen (z. B. Rackkühlung) sind gefährdungsfrei und auf kurzen Wegen zu verlegen. Es sollte zusätzlich die Möglichkeit der Abschieberung eines havarierten Flüssigkeitskreislaufes geben. Im Einzelfall sind Flüssigkeiten führende Leitungen zulässig, sofern wirksame Maßnahmen zum Leckageschutz getroffen wurden.
SIB-04-17	Sofern technische Komponenten der Zutrittssicherung ausschließlich elektrisch betrieben sind, müssen diese notstromversorgt sein.
SIB-04-18	In den IT-Räumen sowie allen Funktionsräumen sind die Fluchtwege ausgeschildert. Zusätzlich gibt es eine Notbeleuchtung, die eine sichere Bedienung ermöglicht und die Ausleuchtung der Fluchtwege in der Art und Weise gewährleistet, dass eine Fluchtmöglichkeit für Personen im Gefahrenfall jederzeit gegeben ist. Für kritische Räume muss eine Notbeleuchtung mit einer Umschaltzeit < 1 Sekunde vorhanden sein.
SIB-04-19	WAN-Trassen sind auf Wegen ohne besondere Gefährdungen durch Brand und mechanischer Beeinflussung und kreuzungsfrei zu errichten

22.3.3 Anforderungen an die Brandmelde und Löschtechnik

Kürzel	Beschreibung
SIB-05-01	Es muss eine geeignete Brandmeldeanlage nach Stand der Technik eingesetzt werden. Die Brandmeldeanlage (BMA) muss die Einteilung in Melderbereiche und -gruppen erlauben und eine sichere Energieversorgung wie auch gesicherte Übertragungswege aufweisen.Zusätzlich ist die BMA auf die Feuerwehr oder eine andere ständig besetzte Stelle (Sicherheitszentrale) aufzuschalten.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

SIB-05-02	Die IT-Bereiche, wie auch die zur Versorgung der IT notwendigen Technik-räume, sind auf Brand zu überwachen. Zusätzlich sind die Räume auf Brand zu überwachen, durch die Versorgungstrassen geführt werden.
SIB-05-03	Alle an IT-Räume angrenzenden Räume sind auf Brand zu überwachen. Hierzu gehören auch darüber und darunter liegende Räume. Entfernt liegende Räume im Gebäude mit hohen Brandrisiken, die im selben baulichen Brandabschnitt wie der Sicherheitsbereich liegen, sind ebenfalls zu überwachen.
SIB-05-04	Die einzelnen Raum-Melder der BMA decken einen definierten maximalen Überwachungsbereich ab. Dabei sind die Anforderungen einer ggf. vorhandenen Löscheinrichtung (z. B. Verdopplung der Melderdichte) zu berücksichtigen. Der max. Überwachungsbereich eines Melders im Raum beträgt 30 qm, im Doppelboden 40 qm.
SIB-05-05	Die eingesetzten Melder müssen eine zuverlässige Detektion sicherstellen und ausfallsicher sein. Fehlfunktionen müssen erkennbar sein und sie müssen mit einer Sensorik ausgestattet sein, mit welcher Fehlalarme vermieden werden.
SIB-05-06	In IT-Bereichen sind Ansaugrauchmelder mit einer Ansprechempfindlichkeit < 1,5 % Lufttrübung pro Meter zur Brandfrühesterkennung einzusetzen.
SIB-05-07	Zur wirksamen und frühzeitigen Schadensbegrenzung sind unabhängig von automatischen Gaslöschanlagen CO2-Handfeuerlöscher zu installieren. Dies trifft für Räume zu, welche eine Größe von 50 qm überschreiten
SIB-05-08	Schalträume müssen in die konventionelle Brandüberwachung durch eine BMA einbezogen sein. Zusätzlich ist das Brandrisiko durch weitere Maßnahmen zu minimieren. Die Brandlastenfreiheit des Schaltraumes muss gewährleistet sein und es muss in regelmäßigen Abständen eine Thermografie der Verteiler vorgenommen werden.
SIB-05-09	Zur Schadensbegrenzung ist auf den IT-Flächen eine automatische Lösch- / Inertisierungsanlage oder Brandvermeidungsanlage zu installieren. Auf eine entsprechende Anlage kann verzichtet werden, wenn eine ständige Besetzung mit in der Brandbekämpfung geschultes Personal und eine brandlastenarme Installation gegeben ist. Löschmittel in ausreichender Menge (z. B. 30 kg-Löscher) sind vorzuhalten.

SIB-05-10	Bei Einsatz einer Gaslöschanlage ist die Löschmittelbevorratung auf Schwund zu überwachen. Eine Brandvermeidungsanlage ist auf Funktion zu überwachen. Die Überwachung mindestens mindestens wöchentlich durch manuelle Kontrollen erfolgen.
SIB-05-11	Löschbatterien bzw. die Brandvermeidungsanlage sind gefährdungsfrei in einem eigenen, zutrittsgeschützten Raum zu positionieren. Entsprächende Räume sind zu belüften. Löschgase mit abweichender Zulassung, wie bspw. FM200, dürfen abweichend hiervon gem. Zulassung gelagert werden.
SIB-05-12	Brandschutzklappen zu Räumen mit IT-Technik oder Elektronik müssen mit einem ansteuerbaren Schließmechanismus wie z. B. Federrücklaufmotoren ausgestattet sein. Der ausschließliche Einsatz von Schmelzloten ist zu vermeiden.
SIB-05-13	Die BMA und die BLA sind mindestens jährlich durch Fachkräfte zu warten. Wartungsprotokolle sind zu archivieren.

22.3.4 Anforderungen an die Sicherheitssysteme und -organisation

Kürzel	Beschreibung
SIB-06-01	Für den Zutritt zu Sicherheitsbereichen muss eine geeignete Zutrittskontrollanlage (ZKA) installiert sein. Diese muss über einen hohen Schutz gegen Überwindungsversuche und eine hohe Verfügbarkeit verfügen. Hierzu gehören eine Sabo- tageüberwachung, eine gesicherte Energieversorgung, ein sicheres Codeverfahren sowie die Signalisierung von Notöffnungen. Zutrittsmöglichkeiten sind hierbei auf den geschlossenen Zustand zu überwachen.
SIB-06-02	Die ZKA muss in einem Raum installiert sein, der denselben Einbruchschutz aufweist wie IT-Räume, zutrittsgeschützt und alarmüberwacht ist und nur über ZKA-Funktion betreten werden kann
SIB-06-03	Die Leitungen der ZKA sind gegen Manipulation zu schützen. Unterbrechung und Kurzschluss müssen erkannt werden. Die Übertragung zwischen den Konzentratoren und den ZKA-Servern muss auf einem IT-Datennetz verschlüsselt erfolgen oder in einem eigenen, abgetrennten und außerhalb des SB zugangsgeschützten Sicherheitsnetzes. Die Leitungen müssen über eine Funktion zur Sabotageüberwachung verfügen. Eine signalisierte Sabotage muss entsprechend eines Alarms der EMA gehandhabt werden.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

SIB-06-04	Türöffner, Zuhaltungen (insbesondere elektromagnetische), Auswerteeinheiten, Konzentratoren und die ZKA Zentrale müssen an einer unterbrechungsfreien Stromversorgung angeschlossen sein.
SIB-06-05	Kartenleser müssen gegen Öffnen geschützt sein und Eingaben von PIN-Codes dürfen nicht nachvollziehbar oder beobachtbar sein. Die Leser müssen über einen Sabotagekontakt verfügen oder als Vollgussgehäuse ausgelegt sein. Eine signalisierte Sabotage muss entsprechend eines Alarms der EMA gehandhabt werden.
SIB-06-06	Der Identifikationsmerkmalträger (IMT) wird personenbezogen ausgegeben und eingesetzt. Die nicht personalisierten IMTs werden sicher aufbewahrt. Zusätzlich sind nicht komromittierbare Codierungsverfahren einzusetzen.
SIB-06-07	Jeder Versuch des Zutritts einer mit einer ZKA gesicherten Tür ist mindestens mit IMT-Code, Datum und Uhrzeit zu protokollieren. Die Daten sind mindestens 30 Tage aufzubewahren. Fehlversuche sind durch die ZKA zentral anzuzeigen.
SIB-06-08	Die Ausbildung von Sicherheitszonen muss sich in der Profilierung der Zutrittsberechtigungen abbilden lassen. Anti-Passback oder zumindest Bereichswechselkontrolle muss realisiert werden. Zusätzlich muss die ZKA auch die Möglichkeit einer zeitlichen Eingrenzung der Zutritte bieten.
SIB-06-09	Wenn eine Tür zu IT- oder strategisch wichtigen Räumen (z. B. technische Sicherheitszentrale) zu lange offen steht, muss eine Alarmierung vor Ort erfolgen. Die Alarmierung muss nach maximal 1 Minute Offenstand erfolgen. Nach zwei Minuten Offenstand muss die Alarmierung auch an eine ständig besetzte Stelle geleitet werden. Als Reaktion auf die Meldung sind organisatorische Maßnahmen vorzusehen.
SIB-06-10	Die Einbruchmeldeanalage (EMA) muss über einen erhöhten Schutz gegen Überwindungsversuche im scharfen sowie im unscharfen Zustand verfügen. Meldungen sind an eine ständig besetzte Stelle zu signalisieren. Die EMA muss ihre eigenen sicherheitsrelevanten Funktionen, einschließlich der Sabotage der angeschlossenen Komponenten wie Scharfschalteeinrichtungen und Melder, überwachen. Für den Alarmfall müssen organisatorische Maßnahmen zur unverzüglichen Alarmverfolgung nachgewiesen werden.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

SIB-06-11	Die eingesetzten Melder müssen abhängig von der Überwachungsaufgabe ausgewählt werden, eine sichere Detektion gewährleisten und einen stabilen Betrieb ohne Fehlalarme sicherstellen. Es ist bspw. durch regelmäßige Kontrollgänge sicherzustellen, dass Manipulationen an Meldern erkannt werden (z. B. Besprühen von Bewegungsmel- dern oder das Abnehmen von Glasbruchmeldern). Entsprechende Kontrollgänge sind zu protokollieren.
SIB-06-12	Zur Erkennung von Einschleichtätern oder bei leichter Überwindung von Umfassungswänden sind Bewegungsmelder als Fallenüberwachung zu installieren.
SIB-06-13	Technikräume sind in die EMA-Überwachung einzubeziehen. Alle Technikräume bzw. der Gesamttechnikbereich sind zu überwachen. Bei Überwachung einer Zone mit mehreren Technikräumen kann auf die Einzelüberwachung eines Raumes verzichtet werden.
SIB-06-14	Flure mit Zutritten zu IT-Räumen sind mit Videokameras zu überwachen. Die Bilder sind an eine ständig besetzte Stelle zu übertragen und für mindestens 30 Tage aufzuzeichnen. Es kann auf eine Videoüberwachung verzichtet werden, wenn ein für das Objekt zuständiger Sicherheitsdienstleister vor Ort existiert und die Räume einbruchüberwacht sind.
SIB-06-15	Die Außengrenze ist so zu überwachen, dass ein Eindringen bzw. Überschreiten der Grenze detektiert werden kann. Die zu überwachende Außengrenze kann entlang der Fassade (Handbereich) des Objektes verlaufen, in dem sich das Rechenzentrum befindet.
SIB-06-16	Der Zutritt zum IT-Bereich oder zum gesamten Sicherheitsbereich (IT-Bereich & Technikbereich) muss über eine Personenvereinzelung erfolgen. Es kann auch eine Kombination aus technischer und organisatorischer Lösung, etwa durch Videoüberwachung und Fernfreigabe einer Schleusentür, eingesetzt werden.
SIB-06-17	Bei den Komponenten der Sicherheitseinrichtung wird durch einen Wartungsvertrag sichergestellt, dass sie regelmäßig nach Herstellerangaben (jedoch mindestens jährlich) gewartet werden. Es sind vierteljährlich Inspektionen durchgeführtdurchzuführen und zu protokollieren..

SIB-06-18	Die Vergabe der IMTs muss formalisiert und nachvollziehbar erfolgen. Die Medien sind gesichert aufzubewahren und die Administration der Medien wie der ZKA selbst erfolgt nur nach vorausgegangener Authentifizierung. Der Bildschirmarbeitsplatz ist zusätzlich mit einem Kennwort bei Inaktivität gesichert. Es sind vierteljährlich Inspektionen durchzuführen und zu protokollieren.
SIB-06-19	Für die Verfolgung von Alarmen ist Sicherheitspersonal mit einer ständig besetzten Zentrale zu verpflichten.
SIB-06-20	Das Sicherheitspersonal muss sich durchgehend am Objekt befinden. Die Sicherheitszentrale sollte mit mindestens zwei Personen besetzt werden. Die Sicherheitszentrale kann sich auch in räumlicher Nähe zum Objekt befinden, wenn eine Videoüberwachung und kurze Interventionszeit gegeben sind.

22.3.5 Anforderungen an die Energieversorgung

Kürzel	Beschreibung
SIB-07-01	Die Energieversorgung im Gebäude muss auf einem 5-Leiter-Netz basieren. PE und N sind getrennt verlegt. Der Neutralleiter ist isoliert verlegt und nur am ZEP mit PE gebrückt. Der N-Leiter wird ohne reduzierten Querschnitt geführt. Ein Erdungskonzept für die zentrale Erdung ist zu erstellen.
SIB-07-02	Die Stromversorgung erfolgt über Primär- und Sekundärversorgungen. Stromquellen sind Versorgungen aus dem öffentlichen Netz und Netzersatzanlagen (NEA). Die Leitungen sind möglichst auf getrennten Wegen oder mit besonderem Schutz gegen äußere Einwirkungen zu führen. Die Primärversorgung muss von der Sekundärversorgung unabhängig sein.
SIB-07-03	Die Sekundärversorgung muss bei Ausfall der Primärversorgung die Last automatisch übernehmen.
SIB-07-04	Redundante Sekundärversorgung Jeder Versorgungspfad der A/B-Versorgung muss eine eigene Sekundärversorgung (über USV /NEA) aufweisen, die zu 100% die Versorgung sicherstellen kann. Die Steuerungen für die Sekundärversorgungen müssen unabhängig voneinander aufgebaut sein.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
SIB-07-05	Die Stromtrassen sind in halböffentlichen und betriebseigenen Bereichen gegen mechanische Beschädigung, Brand und Wasser zu schützen.
SIB-07-06	Die Verteiler der IT-Räume bzw. RZ-Zonen werden mit einer eigenen Zuleitung aus der Niederspannungshauptversorgung (NSHV) / Unterbrechungsfreienstromversorgung (USV) versorgt. Eine abgezweigte Zuleitung ist nur dann zulässig, wenn dieseunter eigener Kontrolle des RZ-Betreibers steht.
SIB-07-07	Die Stromverteiler der IT-Räume bzw. RZ-Zonen dienen ausschließlich der Stromversorgung der IT-Systeme. Sie versorgen keine Fremdsysteme oder haben Abzweige zu Verteilern in Fremdbereichen.
SIB-07-08	Anschlüsse von Rackeinspeisungen sind so zu gestalten, dass ein versehentliches Lösen, z. B. bei Arbeiten im Doppelboden, unwahrscheinlich ist. Erfordelichenfalls sindausreichende Zugentlastungen herzustellen.
SIB-07-09	Die Kabelverlegung erfolgt geordnet, möglichst auf Kabelwannen und unter Trennung von Starkstrom- und Daten- bzw. Schwachstromkabel. Eine gegenseitige Beeinflussung der Kabel durch elektromagnetische Felder ist durch voneinander getrennte Kabelführungen zu minimieren.
SIB-07-10	Für die Energieversorgung ist ein gestaffelter Überspannungsschutz gemäß DIN EN 61643 vorzusehen. Lange Versorgungswege erfordern aufgrund der Einkopplungsgefahr einen zusätzlichen, ggf. kaskadierten Mittelschutz in den Unterverteilungen.
SIB-07-11	Alle elektrischen Leitungen, wie bspw. die der Telekommunikation, EMA, ZKA und der Videoanlage, sind bei der Hauseinführung mit geeigneten Überspannungsschutzeinrichtungen gemäß DIN EN 61643 zu versehen.
SIB-07-12	In IT-Räumen sind eigene Sammelschienen für einen niederimpedanten Potenzialausgleich zur Verringerung der Auswirkungen von Ableit- und Ausgleichsströmen erforderlich. Daran sind alle metallischen Gegenstände, wie Racks, Kabelwannen, Verrohrungen und Doppelbodenstützen, anzuschließen
SIB-07-13	Zentrale Fehlerstromschutzeinrichtungen für IT-Verteiler und zentrale Steuerungen sind zu vermeiden.
SIB-07-14	Wichtige Messwerte des IT-Versorgungsnetzes (z. B. Spannungen, Ströme und Leistungen) sind zentral zu erfassen. Eine regelmäßige manuelle Aufnahme und

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
	Kontrolle der Messwerte ist zulässig.
SIB-07-15	Die Energieversorgung der IT Verbraucher ist durch eine zentrale unterbrechungsfreie Stromversorgung (USV) in einem eigenen brandgeschützten Raum abzusichern.
SIB-07-16	Für bspw. den Fall eines Brands im USV-Raum oder bei Arbeiten an der USV-Anlage ist der Betrieb durch eine Leitungsumgehung des Raums mit geschütztem Schalter zu gewährleisten.
SIB-07-17	Der Komplettausfall eines USV-Systems darf nicht zu Versorgungseng pässen führen. Es ist eine Komponentenredundanz bei USV-Systemen von n+1 oder eine zweite Versorgung vorzusehen.
SIB-07-18	Um eine gegenseitige Einflussnahme durch Konzentration der USV-Batterien zu verhindern (Temperatur, Ausgase, Brandgefährdung), ist eine Trennung bei der Aufstellung von USV und Batterien in brandschutztechnisch getrennten Räumen vorzusehen. Die Trennung ist zwingend bei Einsatz offener Batterien erforderlich.
SIB-07-19	Auslegung einer USV-Anlage mit Leistungsreserven: In der jeweiligen Ausbaustufe sind Sicherheitsreserven bei den Leistungskomponenten vorzusehen.
SIB-07-20	Im Falle eines Stromausfalls muss in hinreichend kurzer Zeit eine Netzersatzanlage (NEA) bereitgestellt werden. Der Anschluss muss vorbereitet und getestet sein. Vertragliche Vereinbarungen zur NEA-Bereitstellung müssen vorgelegt werden.
SIB-07-21	In der jeweiligen Ausbaustufe sind Leistungsreserven der Netzersatzanlage vorzusehen.
SIB-07-22	Es muss sichergestellt sein, dass immer ein ausreichender Kraftstoffvorrat für einen Volllastbetrieb der gesamten, für den Weiterbetrieb des RZ notwendigen Last, für 48 h vorhanden ist. Der Nachweis eines Liefervertrages für die zuverlässige Treibstofflieferung im Notfall ist ausreichend, sofern der Treibstoffvorrat die für 24 h Volllastbetrieb erforderliche Menge nicht unterschreitet
SIB-07-23	Die Einsatzbereitschaft der NEA ist durch regelmäßige Lastprobeläufe zu testen.
SIB-07-24	Die Aufstellung der Umschalteinrichtung hat so zu erfolgen, dass ein Zutrittsschutz gegeben ist und dass bei Ausfall der Primärversorgung die Sekundärversorgung

Kürzel	Beschreibung
	gewährleistet ist.
SIB-07-25	Es ist eine Selektivitätsbetrachtung bzw. eine vollständige Berechnung des Lastflusses und der Kurzschlussströme für alle relevanten Betriebsarten durchzuführen. Eine argumentativ geführte Selektivitätsbetrachtung hinsichtlich der Auslegung und Staffelung der Sicherungselemente/IS-Strombegrenzer ist vorzunehmen.
SIB-07-26	Wichtige Betriebszustände der Elektroversorgung (z. B. USV, NEA) sowie die Verfügbarkeit der Versorgungsspannung sind zu überwachen. Dies kann durch regelmäßige manuelle Kontrollen und Dokumentation der oben genannten Komponenten und ihrer Parameter erfolgen.
SIB-07-27	Technische Störmeldungen sind direkt an eine ständig besetzte Stelle weiterzuleiten. Die Meldung kann an einen Bereitschaftsdienst erfolgen.
SIB-07-28	Bei den elektrischen Anlagen muss durch einen auf die jeweilige Komponente abgestimmten Wartungsvertrag sichergestellt sein, dass sie regelmäßig (mindestens jährlich) gewartet werden. Es ist mindestens der Abschluss von Wartungsverträgen für die USV, die Batterien und die NEA nachzuweisen.

22.3.6 Anforderungen an die raumlufttechnischen Anlagen

Kürzel	Beschreibung
SIB-08-01	Die klimatischen Raumbedingungen (Temperatur und Feuchte) sind auf den Betrieb von IT-Technik anzupassen. Es ist die Überwachung und Regelung der Temperatur und der Feuchte erforderlich.
SIB-08-02	Eine ausreichende Belüftung für den sicheren und auslegungskonformen Betrieb von technischen Komponenten, wie z. B. NEA, Trafo, ist sicherzustellen.
SIB-08-03	Für eine ausreichende Luftwechselrate gemäß Batteriehersteller ist Sorge zu tragen.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
SIB-08-04	Die Klimageräte der USV-Räume müssen an die Notstromversorgung angeschlossen werden.
SIB-08-05	Klimageräte sind gefährdungsfrei und luftströmungsoptimal aufzustellen. Diese Forderung betrifft sowohl die Aufstellung der Umluftkühlgeräte (ULK) wie auch die Anordnung der Rackreihen. Ziel ist eine ungehinderte Luftströmung, Meidung von Wärmenestern und sichere Wartbarkeit der Geräte.
SIB-08-06	Es sind sowohl Maßnahmen zur Leckageüberwachung als auch zur aktiven Begrenzung der austretenden Flüssigkeitsmenge erforderlich. Dabei sind alle IT-Räume und elektrischen Betriebsräume mit Flüssigkeiten führenden Leitungen zu berücksichtigen.
SIB-08-07	Je nach Anlagenkonzept und Anlagenkomponente ist eine redundante Auslegung zu realisieren. Dies betrifft aktive Teile wie Rückkühlwerke, Kältemaschinen, Umluftkühlgeräte (ULK) und Pumpen. Aktive Teile, wie Rückkühlwerke, Kältemaschinen, ULK und Pumpen sind in (n+1)-Redundanz auszuführen.
SIB-08-08	Die Filterung der Raumluft ist in allen Umluftklimageräten für IT-Bereiche für den Schutz der Elektronik sowie der Klimageräte ausreichend zu dimensionieren. Die Filter müssen mindestens der Klasse M5 entsprechen oder die Luftqualität muss an Hand einer Messung nachgewiesen werden.
SIB-08-09	Die IT-Räume aber auch Räume mit Steuerelektronik oder USV-Anlagen sind rauchdicht auszuführen.
SIB-08-10	Das Eindringen von Rauch und Staub in IT-Räume über die Außenluftzuführung ist zu detektieren, die Reinheit der von außen zugeführten Luft ist im Zentralgerät mit einer zweistufigen Filterung zu gewährleisten. Der Verschluss der Außenluftansaugung ist bei Außenkontamination automatisch sicherzustellen, Regional spezifische Risiken sind zu berücksichtigen. Als Außenluftfilter sind mindestens die Klassen M5 und F7 einzusetzen.
SIB-08-11	Durch eine örtlich getrennte Aufstellung von Schalteinheiten, Leistungsteilen und Steuerungen ist das Risiko zu minimieren, dass lokale Brände unmittelbar auf weitere Anlagenteile übergreifen.

Sachgebiet **Fehler! Verweisquelle konnte nicht gefunden werden.**

Teilgebiet **Fehler! Verweisquelle konnte nicht gefunden werden.**

Titel **Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
SIB-08-11	Rückkühlwerke sind gegen sabotage zu schützen. Der freie Zugang zu Rückkühlwerken ist wirksam zu verhindern. Bei Zaunanlagen sind weitere Maßnahmen zu berücksichtigen, wie frühzeitige Detektion, Verhinderung von Manipulationen von außen.
SIB-08-12	Rückkühlwerke sind ausreichend zu dimensionieren. Temperaturauslegung der Rückkühlwerke auf regionale Extremwerte und luftströmungsoptimierte Aufstellung, damit keine Leistungsminderungen auftreten können.
SIB-08-13	Kälteanlagen sind plankonform auszulegen und wartungsfreundlich aufzustellen. Die Nutzkälteleistung hat den errechneten Anforderungen zu entsprechen.
SIB-08-14	Elementar wichtige Steuerungen von Klima- und Raumluftanalagen sind entweder einschließlich ihrer Energieversorgung hochverfügbar auszulegen oder so, dass bei Ausfall ein Rückfall auf eine Notsteuerebene erfolgt. Ein Handeingriff ist nur bei sehr trägen Prozessen möglich bzw. wenn durchgehend Personal vor Ort ist. Die relevanten Steuerungen - insbesondere solche mit langen Hochlaufzeiten - müssen USV-versorgt sein.
SIB-08-15	Wichtige Betriebszustände der Hauptkomponenten Klima- und Raumluftanalagen sowie der geförderten Medien sind zu überwachen und zu dokumentieren. Die Überwachung betrifft im Allgemeinen Temperatur, Feuchte, Lastzustände, Anlagendrücke und Massenströme. Eine engmaschige manuelle Kontrolle und Dokumentation wird akzeptiert.
SIB-08-16	Risiken im Zusammenhang mit unentdeckten Fehlfunktionen der Klimasteuerung sind mit einer zusätzlichen, unabhängigen Überwachung der Raumluftkonditionen in den IT-Räumen zu minimieren. Dabei ist die Raumtemperatur zu überwachen
SIB-08-17	Es sind die vollständigen Abnahmedokumente vorzulegen, insbesondere die Nachweise der Druck-/Dichtheitsprüfung sowie die Prüfung der Ausführung des Korrosionsschutzes und der Dämmung.
SIB-08-18	Alle Anlagenteile wie z. B. ULK, Rückkühlwerke, Kältemaschinen, Armaturen, etc. sind mindestens einmal im Jahr zu warten und regelmäßig zu inspizieren.
SIB-08-19	Technische Störmeldungen sind an eine ständig besetzte Stelle sicher zu übertragen und Fachpersonal zur Fehlerbeurteilung und Störungsbehebung unmittelbar heranzurufen. Die Meldung kann auch an eine Rufbereitschaft erfolgen.

22.3.7 Anforderung an die Organisation von Rechenzentren

Kürzel	Beschreibung
SIB-09-01	IT-Produktion und Datenarchivierung/-sicherung sind voneinander zu trennen. Die Daten der Sicherung (Spiegelung) sind in einen anderen Brandabschnitt zu verbringen.
SIB-09-02	Unabhängig von einer allgemeinen den gesamten Betrieb betreffenden Regelung zum Rauchverbot ist der Sicherheitsbereich zusätzlich mit Rauchverbotshinweisen auszuschildern.
SIB-09-03	Die IT-Räume, alle relevanten Technikräume, Trassen und Außeninstallationen sind zur Sichtkontrolle mindestens einmal pro Woche zu begehen.
SIB-09-04	Die Ordnungsmäßigkeit hinsichtlich Einhaltung von Regeln, Ordnung, Sauberkeit, Zugänglichkeit, Beschriftung, Entsorgung, etc. muss gegeben sein. Die Überprüfung erfolgt im Rahmen der Begehung des Rechenzentrums.
SIB-09-05	Die Zutrittsberechtigung ist formal zu beantragen und entsprechend zu Protokollieren. Zusätzlich sind Zutrittsregelungen und ihre Kontrolle schriftlich darzulegen und die Anzahl der Zutrittsberechtigten ist regelmäßig auf Plausibilität zu prüfen.
SIB-09-06	IT-Systemerweiterungen sind zwischen IT-Betrieb und dem Facilitymanagement abzustimmen.
SIB-09-07	Bei einer Erstinbetriebnahme müssen alle Anlagenteile auf Funktion und Zusammenwirken in den möglichen Betriebszuständen getestet und in einem Testprotokoll dokumentiert werden.
SIB-09-08	Zu allen, für den Betrieb relevanten Gewerken, sind Wartungsverträge abzuschließen.
SIB-09-09	Der Umgang mit Fremdpersonal, der Abstimmungsprozess für Wartungsfenster, Vorkehrungen für bestimmte Tätigkeiten oder Schalthandlungen sowie Besonderheiten im Rahmen von Wartungs- und Reparaturarbeiten sind in Betriebsanweisungen zu beschreiben.
SIB-09-10	Das Personal muss jährlich, sowie neue Mitarbeiter bei Dienstantritt, eine Sicherheitsunterweisung (Brandschutz, Löschung, elektr. Betriebsräume, etc.) erhalten. Dies erfolgt, soweit möglich, über die verpflichtende Arbeitsschutzunterweisung. Nachweise über den Umfang und die Teilnahme an den

Kürzel	Beschreibung
	Unterweisungen sind zu archivieren
SIB-09-11	Die technische Infrastruktur ist durch entsprechend qualifiziertes Personal zu betreuen. Zusätzlich ist sicherzustellen, dass Vertretungspersonal und Regelungen für den Einsatz gegeben sind.
SIB-09-12	Lagehinweise zum Rechenzentrum sind zu meiden. Hierzu zählen Beschilderungen im Außenbereich, Raumschilder, Etagenübersichten an Eingängen oder Aufzügen sowie sicherheitsrelevante Hinweise in Broschüren und Web-Auftritten.

22.3.8 Anforderungen an die Dokumentation

Kürzel	Beschreibung
SIB-10-01	Für die IT-Infrastruktur ist ein Sicherheitskonzept mit Gefährdungsanalyse, Herleitung der Sicherheitsanforderungen, Darlegung der Umsetzungskonzepte und Ausführungsbeschreibung inkl. Lastenbilanzierungen (Strom/Kälte) zu erstellen.
SIB-10-02	Es ist eine Risikoanalyse für das Umfeld des Rechenzentrumsstandortes zu erstellen. Im Umkreis von 500 m sind alle Objekte mit Entfernungsangabe zu identifizieren und hinsichtlich des Gefährdungsgrades einzuschätzen, getroffene Gegenmaßnahmen sind zu benennen. Im Umkreis von 2000 m sind diejenigen Objekte mit Entfernungsangabe zu benennen, denen grundsätzlich eine Gefährdung unterstellt wird.
SIB-10-03	Ein Alarmplan mit Auflistung der Ereignisse/Störmeldungen, Erstmaßnahmen und Informationskette ist bereitzustellen. Alternativ kann eine direkte Umsetzung in einem Gebäudemanagement- oder Alarmverfolgungssystem erfolgen. Es ist ein Notfallkonzept bereitzustellen.
SIB-10-04	Ein Brandschutzkonzept mit den baulichen, technischen und organisatorischen sowie den Rechenzentrum-spezifischen Vorgaben ist bereitzustellen.
SIB-10-05	Es sind aussagekräftige Gelände- und Gebäudepläne vorzuhalten.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Beschreibung
SIB-10-06	Es sind Raumgrundrisspläne der Etagen(bereiche) vorzulegen, die IT- und Technikflächen, Trassen und Verkehrsflächen beherbergen, sowie Bereiche, die sich unmittelbar in Nachbarschaft hierzu befinden (auch oberhalb und unterhalb). Zu den Technikbereichen zählen auch Außenanlagen, z. B. NEA und Dachinstallationen (Kälte, Blitzschutz).
SIB-10-07	Es sind Trassenpläne der Hauptversorgungswege Elektro / Kälte / WAN vorzuhalten.
SIB-10-08	Es sind Strangschemata für die Elektroversorgung vorzulegen. Im Strangschema sollten Raumbezüge berücksichtigt werden, Abgänge bezeichnet, Kabeltypen, Leistungsschalter und Hauptsicherungen aufgeführt sein.
SIB-10-09	Es sind die Rohr- und Instrumentierungspläne der Kälteversorgung vorzuhalten.
SIB-10-10	Es sind Übersichten der Brandlinien- und Melder vorzuhalten.
SIB-10-11	Es sind Übersichten der Lösch- und Brandvermeidungseinrichtungen vorzuhalten.
SIB-10-12	Projektionen der Sicherheitseinrichtungen auf die Grundrisspläne sind bereitzustellen, ebenso Schemata der Anlagen.
SIB-10-13	Ein Jahreswartungsplan sowie eine Liste der zu wartenden Gewerke mit Angaben zum Vertragspartner, Wartungszyklus, Wartungsumfang sind bereitzustellen. Es sind Reaktions-/Instandsetzungsvereinbarungen bereitzustellen.
SIB-10-14	Es sind Betriebsanweisungen für Sonderfälle und Ausnahmesituationen bereitzustellen, wie z. B. außergewöhnliche Schalthandlungen, Noteinspeisungen, etc.
SIB-10-15	Eine Liste aller, für den Rechenzentrumsbetrieb, relevanten Räume und Örtlichkeiten ist unter Angabe der Raumbezeichnung, -nutzung, -lage, -größe und den möglichen Eigenschaften einbruchhemmend, zutrittskontrolliert über ZKA, brandüberwacht, gelöscht bereitzustellen.
SIB-10-16	Es sind Nachweise über die Durchführung von Leistungs- und Funktionstests bei Inbetriebnahme zu erstellen. Die Nachweise zu den Funktionstests beziehen sich auf die Elektro- und Kälteversorgung sowie auf die Sicherheitssysteme im Rahmen der Inbetriebnahme

22.3.9 Anforderungen an der Rechenzentrumsverbund

Kürzel	Beschreibung
SIB-11-01	Der Rechenzentrumsbetrieb muss in einem Rechenzentrumsverbund mit mindesetns zwei Rechenzentren stattfinden. Es wird davon ausgegangen, dass die Systeme und Applikationen unabhängig voneinander in beiden Rechenzentren ohne Einschränkung laufen können.
SIB-11-02	Jedes der Rechenzentren hat eine eigene Energie- und Kälteversorgung mit eigener Außenanbindung.
SIB-11-03	Zwischen den beiden Rechenzentren gibt es mind. zwei Datenverbindungen auf unterschiedlichen Wegen.
SIB-11-04	Die Anforderungen aus ENV sind gemäß nachfolgender Tabellen insoweit zu erfüllen, als Risiken aus dem Umfeld sich nicht gleichzeitig auf beide Rechenzentren auswirken können.

23 EINORDNUNG DOKUMENTEN-/PROZESSHIERARCHIE

Übergeordnete Dokumente bzw. Prozesse:

- LL001501 Leitlinie ISMS

Nachgelagerte Dokumente bzw. Prozesse: keine

24 RELEVANTE PROZESSE

Keine relevanten Prozesse

25 RELEVANTE DOKUMENTE

- LL001501 Leitlinie ISMS
- RL128092 Außerbetriebsetzung und Entsorgung von Medien
- RL128090 Sicherheitsvorgaben zur Überwachung und Protokollierung von IT-Systemen

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

26 ANHANG

Kein Anhang

KfW-Organisationshandbuch

Richtlinie Nr. RL 128090

Titel Vorgaben zur Sicherheitsüberwachung und Protokollierung von IT-Systemen

GELTUNGSBEREICH: Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG (s. Kapitel Geltungsbereich)

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

VERANTWORTLICHE OE	COc2
DOKUMENTVERANTWORTLICH	Waldemar Burghardt
VERTRAULICHKEITSSTUFE	2 (intern)
ERSETZT VERÖFFENTLICHUNGSDATUM VOM:	02.11.2017

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

ÄNDERUNGEN ZUR VORVERSION

Änderungs-datum	**Kapitel**	**Inhalte**
Nov. 2015	alle	Erstellung Dokument
Dez. 2016	4.1	Redaktionelle Änderung.
Jan. 2017	2	Geltungsbereich auf CO und IT geändert.
Jul. 2017	2 3 4	Geltungsbereich angepasst und auf IPEX und DEG ausgeweitet Anpassung auf aktuelle ISO Maßnahmen Einfügen des Wirkens auf die Schutzziele (Vertraulichkeit-Integrität-Verfügbarkeit)
Jan 2018	alle	Ausweitung des Umfangs der zu überwachenden Systeme im SIEM um alle IT-Systeme (Großrechner, Server, Datenbanken, Schutzsysteme, Firewalls, Workstations, etc.). Erweiterung der Mindestanforderung für Log-Daten und Speicherfristen (neue MaRisk Novelle – 5 Jahre). Anwendung der Bedrohungs- und Risikobetrachtung für den konkreten Umfang der Protokollierung der individuelle IT-Systeme. Anforderungen an Auswertung mit SIEM-System.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

INHALTSVERZEICHNIS

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

27 KURZBESCHREIBUNG

In dieser IS-Richtlinie werden systematische Sicherheitsmaßnahmen für die Überwachung und Protokollierung von Informationssicherheitsereignissen beschrieben.

Regelungsdokumente wie die IS-Richtlinie konkretisieren die ISMS-Leitlinie und dienen als Grundlage für die operative Umsetzung durch die zuständigen Stellen.

Die IS-Vorgaben stellen keine Lösungen dar, sind aber ausreichend konkret, um auf operativer Ebene (1st Line of Defense) Sicherheitskonzepte entwickeln zu können.

Entstehen in der Praxis Situationen, bei welchen die Vorgaben nicht oder nicht vollständig umsetzbar sind, so sind alternative Lösungen zu entwickeln, die dem angestrebten Sicherheitsniveau entsprechen.

28 GELTUNGSBEREICH

Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG.

Der Geltungsbereich dieser Richtlinie bezieht dabei alle Bereiche ein, die Sicherheitsvorgaben dieser Richtlinie operativ umsetzen.

Die Töchter weichen lediglich bei institutsspezifischen Besonderheiten (gesetzliche, vertragliche, externe oder geschäftliche Anforderungen) durch spezifische Anpassungen ab. Die Konzernleit- und -richtlinien erlangen nachfolgend erst nach Freigabe durch die jeweilige Geschäftsführung der Töchter („Ratifizierung“) Gültigkeit in den Einzelinstituten DEG/IPEX.

Den Einzelinstituten bleibt es im Übrigen unbenommen, unter Ausschluss von Widersprüchen mit den konzernweit nach den vorstehenden Maßgaben verabschiedeten und geltenden Regelungen konkretisierende Einzelmaßnahmen (Richtlinien, Arbeitsanweisungen) zu verabschieden.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

29 ZIELSETZUNG

Aufdeckung nicht genehmigter informationsverarbeitender Aktivitäten. Systeme müssen überwacht und Informationssicherheitsereignisse müssen aufgezeichnet werden. Protokollierungen der Administrationstätigkeiten und von Fehlern müssen dazu genutzt werden sicherzustellen, dass Probleme bei Informationssystemen identifiziert werden.

Alle Organisationen müssen die gesetzlichen Anforderungen an die Überwachung und Protokollierung erfüllen. Systemüberwachung sollte dazu genutzt werden, die Effektivität der getroffenen Maßnahmen und die Konformität zur Zugriffskontrollregelung zu prüfen. (ISO-27002/12.4)

29.1 RISIKOORIENTIERTE VORGEHENSWEISE

Grundsätzlich gelten für alle IT-Systeme (Großrechner, Server, Datenbanken, Schutzsysteme, Workstations, etc.) der KfW die Mindestanforderung für die Überwachung und Protokollierung gemäß nachfolgender Kapitel.

Der konkrete Umfang der Protokollierung, der für individuelle Systeme notwendig ist, muss durch eine Bedrohungs- und Risikobetrachtung (RL000081 „IS-Werte- und –Risikomanagement“) ermittelt werden.

Die Protokollierung kann einen Einfluss auf die Leistungsfähigkeit eines Systems haben. Diese Protokollierung sollte nur durch erfahrenes Personal aktiviert werden. Ggfs. ist eine Hardwareaufrüstung des jeweils betroffenen Systems rechtzeitig zu planen.

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

30 VORGABEN ZUR UMSETZUNG

30.1 ALLGEMEINE PROTOKOLLIERUNGSANFORDERUNGEN

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-01-01	**Protokollierungskonzept** Protokollierung kann auf allen Ebenen der Anwendungs- und Systemarchitektur erfolgen (Speichermedien, Betriebssysteme, Datenbankmanagementsystem, Middleware, eigentliche Anwendung, Systemprogramme, Kommunikations-Gateways wie z. B. RAS). Abhängig von den fachlichen und gesetzlichen Anforderungen muss ein Protokollierungskonzept erstellt werden. Das Protokollierungskonzept kann Bestandteil des Sicherhetiskonzeptes oder des technischen Designkonzeptes sein. Für die Erstellung des Protokollierungskonzepts ist der jeweilige Applikationssystem-Verantwortliche verantwortlich.	X	X	
PRT-01-02	**Rahmeninformationen von Systemmeldungen** Grundsätzlich müssen alle Systemmeldungen mindestens die folgenden Rahmeninformationen beinhalten: › Datum › Uhrzeit › Ereigniskennung und Details zum jeweiligen Ereignis, soweit diese zum Verständnis notwendig sind › Rechnernamen und IP Adressen des betroffenen Systems › Rechnernamen und IP Adressen aller weiterer beteiligten Systeme › Auslösende Benutzerkennung, soweit diese für das jeweilige Ereignis protokollierbar sind › Betroffene Benutzerkennung, soweit diese für das jeweilige Ereignis protokollierbar sind › Protokollierung der Änderung, d.h. alter und neuer Wert	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-01-03	**Auditprotokolle für administrative Tätigkeiten** Für alle administrativen Tätigkeiten müssen Auditprotokolle erstellt werden, in denen Aktivitäten, Fehler und Informationssicherheitsvorfälle festgehalten werden. Folgende Ereignisse müssen mindestens in den Auditlogs enthalten sein: › Aufzeichnungen von erfolgreichen und zurückgewiesenen Systemzugriffsversuchen › Aufzeichnungen von erfolgreichen und zurückgewiesenen Zugriffen auf Daten und auf andere Ressourcen › Alle mit Administratorrechten abgesetzte Kommandos › Änderungen der Systemkonfiguration › Verwendung von Berechtigungen anderer User Accounts (z.B. SU, sudo, „run as“) › Nutzung von Systemwerkzeugen › Nutzung von Anwendungen › Alarmierungen durch das Zugriffskontrollsystem › Aktivierung und Deaktivierung von Schutzsystemen wie Virenscannern und Eindringmeldesystemen › Änderung von wichtigen Systemdateien › Änderungen an Logs Soweit dies technisch möglich ist, sollten auch Dateizugriffe und Zugriffsversuche einschließlich der Art des Zugriffs (lesend/schreibend) protokolliert werden.	X	X	
PRT-01-04	**Protokollierung von Benutzeraktivitäten** Für alle Benutzeraktivitäten müssen Protokolle erstellt werden, in denen Aktivitäten, Fehler und Informationssicherheitsvorfälle festgehalten werden. Folgende Ereignisse müssen mindestens in den Auditlogs enthalten sein: › Aufzeichnungen von erfolgreichen und zurückgewiesenen	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
	Systemzugriffsversuchen › Aufzeichnungen von zurückgewiesenen Zugriffen auf Daten und auf andere Ressourcen › Verwendung von Berechtigungen (wie z.B. sudo Kommando) › Nutzung von Systemwerkzeugen › Alarmierungen durch das Zugriffskontrollsystem Versuchte Deaktivierung von Schutzsystemen wie Virenscannern und Eindringmeldesystemen. Versuchte bzw. Änderung von Systemdateien. Soweit dies technisch möglich ist, sollten auch Dateizugriffe und Zugriffsversuche einschließlich der Art des Zugriffs (lesend/schreibend) protokolliert werden.			
PRT-01-05	**Protokollierung von Systemänderungen** Mindestens nachfolgende Systemänderungen müssen protokolliert werden: › Starten von Prozessen mit mindestens folgenden Parametern: Datum, Zeit, Parentprozess, Owner › Installation von Programmen › Erstellen von Services › Erstellen von zeitgesteuerten Programm- oder Prozesstarts (cron bzw. AT) › Änderungen an Systemdateien, die den IT-Systemstatus, Systemverhalten, Systemsicherheit beeinflussen (z.B. Änderungen an Systemdateien, Log-Daten, Konfigurationen, Parameter, Workflows, Berechtigungen, Authentifizierung)	**X**	**X**	
PRT-01-06	**Protokollierung von System-Fehler** Fehler müssen protokolliert und analysiert werden, und es sollten entsprechende Maßnahmen ergriffen werden. Die zu beachtenden Bereiche sind: a) Systemalarme und Fehler wie: › Konsolen-Alarme und Meldungen; › Ausnahmen im Systemprotokoll; › Alarme des Netzmanagements;	**X**	**X**	

Sachgebiet **Fehler! Verweisquelle konnte nicht gefunden werden.**

Teilgebiet **Fehler! Verweisquelle konnte nicht gefunden werden.**

Titel **Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
	b) Änderungen oder der Versuch von Änderungen an den Sicherheitseinstellungen des Systems oder an dessen Sicherheitsmaßnahmen. Die Analysemaßnahmen sollen mindestens nachfolgende Maßnahmen umfassen: a) Überprüfung von Fehlerprotokollen, um sicherzustellen, dass die Fehler in befriedigender Art und Weise behoben wurden; c) Kontrolle der Fehlerbehebungsmaßnahmen, um sicherzustellen, dass die Maßnahmen nicht kompromittieren und dass die getroffenen Aktivitäten zur Fehlerbehebung zulässig sind. Fehlerprotokolle werden im Rahmen vom Event Management Prozessen analysiert und ausgewertet.			
PRT-01-07	**Zeitsynchronisation** Die Uhren aller wichtigen informationsverarbeitenden Systeme einer Organisation oder eines Sicherheitsbereichs müssen auf eine vereinbarte, genaue Referenzzeit, synchronisiert werden. Wenn Computer oder Kommunikationsgeräte eine Echtzeituhr besitzen, sollte diese auf einen vereinbarten Standard, z. B. Coordinated Universal Time (UTC) oder die Lokalzeit, gesetzt werden. Da interne Uhren dafür bekannt sind, mit der Zeit abzuweichen, sollte eine Vorgehensweise festgelegt sein, wie Abweichungen zur Referenzzeit festgestellt und gegebenenfalls korrigiert werden. Die korrekte Interpretation des Datums/Zeitformates ist wesentlich um sicherzustellen, dass Zeitstempel die korrekte Zeit darstellten. Lokale Besonderheiten (z. B. Sommerzeit) sollten auch beachtet werden. Eine Funkuhr, die das Zeitsignal einer regionalen Atomuhr bezieht, kann als Referenzzeit zur Synchronisation aller Serveruhren mittels Network Time Protocol (NTP) genutzt werden.	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-01-08	**Übertragung von Protokollinformationen** Die Protokollinformationen müssen zeitnah und automatisiert an einen „Zentralen Protokollserver“ übertragen werden.	X	X	X

30.2 ZUSÄTZLICHE ANFORDERUNGEN FÜR SYSTEMGRUPPE

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-02-01	**HTTP- und FTP-Proxysysteme** Zusätzlich zu den Anforderungen aus Kapitel 4.1müssen HTTP- und FTP-Proxysysteme mindestens die folgenden Protokollmeldungen schreiben: › Aufgerufene URL › Übertragenes Datenvolumen je Verbindung › IP Adresse und/oder Hostname des Quellsystems › Benutzerkennung desjenigen Benutzers, der die URL aufgerufen hat › User Agent (Browser ID) › Fehlgeschlagene Anmeldungen › Abgelehnte Verbindungen bzw. blockierte URL Aufrufe › SSL Interception Status (ja/nein) **Als Proxysysteme im Sinne dieses Kapitels gelten:** › Alle Proxysysteme, die den Zugriff auf Systeme im Internet kontrollieren › Alle Reverse Proxy Systeme und SSL VPN Gateways, die den Zugriff auf Systeme der KfW kontrollieren	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-02-02	**SMTP-Proxysysteme** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen SMTP-Proxysysteme mindestens die folgenden Protokollmeldungen schreiben: › Mailadresse von Sender und Empfänger › Akzeptierte und Blockierte SMTP Kommandos › Übertragenes Datenvolumen je Verbindung › IP Adresse und/oder Hostname des Quellsystems	X	X	
PRT-02-03	**DNS-Proxysysteme** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen DNS-Proxysysteme mindestens die folgenden Protokollmeldungen schreiben: › IP Adresse und/oder Hostname des anfragenden Systems › Angefragten DNS Namen und ausgelieferte Antwort-IP › Erlaubte und abgelehnte DNS-Zonentransfers	X	X	
PRT-02-04	**Firewalls** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen Firewalls mindestens die folgenden Protokollmeldungen schreiben: › Akzeptierte Verbindungen mit Quelladresse, Zieladresse, Quellport und Zielport › Abgelehnte Verbindungen mit Quelladresse, Zieladresse, Quellport und Zielport Einzelne Verbindungstypen (z.B. ausgehende NTP Pakete oder Verbindungen die bereits anderweitig (z.B. am Proxy) protokolliert werden) können begründet ausgenommen werden.	X	X	
PRT-02-05	**VPN Gateways** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen VPN Gateways mindestens die folgenden Protokollmeldungen schreiben: › Akzeptierte VPN-Verbindungen mit Quelladresse, Zieladresse,	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
	Quellport und Zielport › Abgelehnte VPN-Verbindungen mit Quelladresse, Zieladresse, Quellport und Zielport › Authentifizerungsdetails für jede Verbindung › Ergebnisse von Sicherheitsprüfungen der VPN-Gegenstelle (wie z.B. Hostchecker) › Sicherheitsrelevante Informationen der VPN Gegenstelle (z.B. verwendete Verschlüsselungs- oder Authentifizierungsverfahren)			
PRT-02-06	**IPS Systeme** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen IPS Systeme mindestens die folgenden Protokollmeldungen schreiben: › Akzeptierte Verbindungen mit Quelladresse, Zieladresse, Quellport und Zielport, Signaturnamen, Datenübertragunsprotokoll › Abgelehnte Verbindungen mit Quelladresse, Zieladresse, Quellport und Zielport, Signaturnamen, Datenübertragunsprotokoll › Detailinformationen zum Ereignis (z.B. URL, Dateiname, sonstige Rahmenparameter)	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-02-07	**Antivirus-Systeme** Zusätzlich zu den Anforderungen aus Kapitel4.1 müssen Antivirus-Systeme mindestens die folgenden Protokollmeldungen schreiben: › Fundort der Malware › Durchgeführte Aktion (gelöscht, in Quarantäne verschoben, keine) mit Fehlercode (Erfolg / Fehlschlag) › Signaturstand und Version der AV Engine › Datum des letzten erfolgreichen Signaturupdates › Fehlerzustände die eine unvollständige Funktion der AV Engine anzeigen (AV Inaktiv, Datebankfehler, etc.) Antivirus Systeme im Sinne dieses Abschnitts sind alle Antivirussysteme, die auf Servern und Workstations installiert sind, sowie alle Antivirussysteme, die auf Proxysystemen eingesetzt werden.	**X**	**X**	
PRT-02-8	**Applikationen nur bei Schutzbedarf bei Integrität oder Vertraulichkeit von 3 (Hoch) und 4 (Sehr hoch)** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen alle relevante Applikationen mindestens Protokollmeldungen schreiben, die es ermöglichen, die jeweilige Aktion innerhalb der Anwendung mit allen relevanten Parametern nachzuvollziehen.	**X**	**X**	
PRT-02-9	**Web-Applikationen** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen Web-Applikationen mindestens folgende Protokollmeldungen schreiben: › Erfolgreiche und erfolglose Anmeldeversuche an der Webanwendung oder dem Web-Service › fehlgeschlagene Autorisierungsversuche beim Zugriff auf Ressourcen (zum Beispiel Datenbankzugriffe) und Funktionen der Webanwendung oder des Web-Service › fehlgeschlagene Validierung von Ein- und Ausgabedaten › fehlgeschlagene XML -Schema-Validierungen › XML -Parser-Fehler › aufgetretene Fehler (zum Beispiel Exceptions) › Änderungen von Berechtigungen für Benutzer oder	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
	Benutzergruppen der Webanwendung oder des Web-Service (zum Beispiel Zugriffsrechte, Änderung an der Web-Service-Policy) › Änderungen an Benutzerkonten (zum Beispiel Passwortänderung) › Löschvorgänge der Webanwendung (zum Beispiel Beiträge) › erkannte Manipulationsversuche und unerwartete Änderungen (zum Beispiel Anmeldeversuche mit ungültigen oder abgelaufenen Session- ID s) › administrative Funktionsaufrufe und Änderungen an der Konfiguration (zum Beispiel Abruf von Benutzerdaten, Aktivierung und Deaktivierung der Protokollierung) › Starten und Stoppen von Diensten › Produktionsübernahme (Deployment) neuer oder bestehender Web-Services			
PRT-02-10	**Datenbanken** Zusätzlich zu den Anforderungen aus Kapitel 4.1 müssen Datenbanken mindestens Protokollmeldungen schreiben, › alle connects, d.h. Logins/Logouts in die Datenbank › alle Aktionen, für die das dba, dbo, sys, sysadmin oder ähnliches-Privileg erforderlich ist › alle Aktionen, bei denen eine "...does not exist"-Fehlermeldung entsteht Für kritische Datenbankobjekte (wie z.B. Usertabellen, Berechtigungstabellen, Tabellen mit Zahlungsaufträgen, etc.) muss bei Erzeugungen und Veränderungen jeweils unterschieden werden, ob die Aktion Erfolg hatte oder nicht.	**X**	**X**	
PRT-02-11	**Netzwerkgeräte** Zusätzlich zu den Anforderungen aus Kapitel 4.1müssen Netzwerkgeräte die Metadaten (Zieladresse, Quelladresse, Ports, Datenmenge, etc.) aller Verbindungen im Netz der KfW protokollieren.	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

30.3 ANFORDERUNGEN AN DIE SPEICHERUNG VON PROTOKOLLINFORMATIONEN

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-03-01	**Speicherfristen** Kontroll- und Überwachungsunterlagen sind systematisch und für sachkundige Dritte nachvollziehbar abzufassen und grundsätzlich fünf Jahre aufzubewahren. Die Aktualität und Vollständigkeit der Aktenführung ist sicherzustellen. Sofern weitere gesetzliche Anforderung eine davon abweichende Aufbewahrung der Logdaten erfordern, muss dies entsprechend umgesetzt werden.	X	X	X
PRT-03-02	**Verfahren zum Löschen** Das Verfahren zum Löschen der Protokolldaten muss beschrieben sein. Es müssen dabei auch die Protokolldaten in die Löschung einbezogen werden, die auf Datensicherungsmedien oder bei einem Auftragsdatenverarbeiter gespeichert sind.	X	X	X
PRT-03-03	**Zentraler Protokollserver** Die Speicherung von Protokolldaten von Applikationen und IT-Technologien und IT System Plattformen muss soweit technisch möglich auf zentralen Protokollservern erfolgen. Der Zugriff auf diese ist entsprechend zu regeln, ebenso die üblichen Mechanismen zur Datensicherheit und Datenübertragung.	X	X	X
PRT-03-04	**Schutz von Protokollinformationen** Die Ablage der Log-Daten muss in einer gesicherten Umgebung erfolgen. Protokollierungseinrichtungen und Informationen aus Protokollen müssen vor Verfälschung und unbefugtem Zugang geschützt werden. Der Zugriff auf die Protokoll-Daten muss auf einen kleinen Personenkreis	X	X	

Kürzel	Anforderung	Schutzziel		
		V	I	V
	beschränkt bleiben. System-Administratoren dürfen nicht berechtigt sein, Aufzeichnungen ihrer eigenen Aktivitäten zu löschen oder das Aufzeichnen zu deaktivieren. Systemprotokolle enthalten oft eine große Menge an Informationen, wobei ein Großteil keine Relevanz für die Sicherheitsüberwachung hat. Um wichtige Ereignisse für die Sicherheitsüberwachung zu identifizieren, sollte man diese Daten automatisch in einen zweiten Protokollsatz kopieren und angemessene System- oder Revisionswerkzeuge zur Analyse und Vereinfachung des Vorgehens benutzen. Die kopierten Protokollsätze unterliegen den gleichen Anforderungen wie der originale Protokollsatz.			

30.4 ANFORDERUNGEN AN DIE ÜBERWACHUNG SICHERHEITSRELEVANTER EREIGNISSE

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-04-01	**Überwachung sicherheitsrelevanter Ereignisse** Die übergreifende Überwachung und Korrelation verschiedener sicherheitsrelevanter Protokollierungsdaten auf unterschiedlichsten Systemen muss mit einem Security Information and Event Management-Systems (SIEM) erfolgen.	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-04-02	**Use Cases zur Erkennung einer Bedrohungssituation** Sicherheitsrelevante Log-Informationen und andere Informationsquellen (z.B. Threat Intelligence, CERT) zur Erkennung einer Bedrohungssituation müssen zu einem Use Case zusammengeführt werden. Für die konkrete Überwachung müssen Use Cases für die einzelnen Anwendungen, Datenbanken, Systeme, Netzelemente etc. in Abhängigkeit von Schutzbedarf, Bedrohungsituation und Angriffsfläche (z.B. Web-Server, DMZ) festgelegt werden. Grundsätzlich sind für alle Anwendungen mit Vertraulichkeit/Integrität der Stufe 4 (Sehr hoch) und für alle Schutzsysteme (z.B. Firewalls) Use Cases zu erstellen. Darüber hinaus müssen alle IT-Systeme (Großrechner, Server, Datenbanken, Workstations, etc.) über standardisierte Use Cases (z.B. Brute Force) überwacht werden.	X	X	
PRT-04-03	**Schwellwerte für Use Cases** Für Use Cases müssen Schwellwerte (ab wann ein Use Cases als kritisch gilt) festgelegt werden. Die Schwellwerte sind unter Anwendung der Bedrohungssituation und des Schutzbedarfs (V-I-V) der IT-Systeme gemäß RL000081 „IS-Werte- und –Risikomanagement“ festzulegen.	X	X	
PRT-04-04	**Fristen zur Auswertung** Grundsätzlich müssen Use Cases, durch die eine Bedrohungssituation für die KfW automatisiert erkannt wurde, zeitnah (unverzügliches Handeln, ohne schuldhaftes Zögern) unter Wahrung des Prinzips der Verhältnismäßigkeit, d. h. einer Risikoabwägung und im Einklang mit den jeweiligen Dienstvereinbarungen, ausgewertet werden.	X	X	
PRT-04-05	**Einhaltung Dienstvereinbarungen** Die Auswertung der Nutzung informationsverarbeitender Einrichtungen darf nur im Einklang der DV SIEM vereinbarten SIEM-Verfahren stattfinden. Alle Auswertungstätigkeiten im Rahmen der Web-Proxies und E-Mail-Gateways für den Internetverkehr unterliegen weiterhin den Regelungen der DV EMail und Internet.	X	X	
PRT-04-06	**Überwachung der sicherheitsrelevanten Log-Daten ohne Use Cases**	X	X	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Kürzel	Anforderung	Schutzziel		
		V	I	V
	Die sicherheitsrelevanten Log-Daten müssen auch ohne Use Cases anlassbezogen oder stichprobenartig überwacht werden. Das Ziel der Überwachung ist es, die Abweichung vom Normalzustand, sogenannte Anomalien in den Log-Daten zu erkennen.			

30.5 DATENSCHUTZANFORDERUNGEN AN DIE PROTOKOLLIERUNG

Kürzel	Anforderung	Schutzziel		
		V	I	V
PRT-05-01	**Zweckbindung** Alle Protokolldaten dienen allein dem Zweck der Aufrechterhaltung der Informations- und Datensicherheit und dürfen grundsätzlich nicht für eine automatisierte Verhaltens- und Leistungskontrolle der Beschäftigten genutzt werden. Ein ständiger Überwachungsdruck ist auszuschließen. Automatisierte Einzelentscheidungen dürfen nicht getroffen werden.	**X**	**X**	
PRT-05-02	**Erforderlichkeit** Art, Umfang und Dauer der Protokollierung sind auf das zur Erfüllung des Protokollierungszwecks erforderliche Maß zu beschränken. Möglichkeiten zur Anonymisierung und Pseudonymisierung sind auszuschöpfen.	**X**	**X**	
PRT-05-03	**Revisionssicherheit** Protokolldaten dürfen nicht nachträglich verändert werden können. Die Verfügbarkeit ist gegen Verlust zu sichern.	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

PRT-05-04	**Authentizität von Protokolldaten** Vertraulichkeit, Integrität und Authentizität von Protokolldaten sollen soweit technisch möglich, mit kryptographischen Verfahren zur Verschlüsselung und Signierung nach dem Stand der Technik sichergestellt werden.	**X**	**X**	
PRT-05-05	**Zugang und Zugriff auf Protokolldaten** Protokolldaten dürfen nur Berechtigten zugänglich sein. Zugang und Zugriff auf Protokolldaten sowie deren Weitergabe sind zu dokumentieren. Ein Austausch personenbezogener bzw. -beziehbarer Daten über die Grenzen der EU und des Europäischen Wirtschaftsraums hinweg darf nicht stattfinden.	**X**	**X**	
PRT-05-06	**Auswertung personenbezogener Protokolldaten** Die Auswertung personenbezogener Protokolldaten muss immer unter Beachtung der personalrechtlichen Beteiligungspflichten und unter Einbeziehung des betrieblichen Datenschutzbeauftragten erfolgen.	**X**	**X**	
PRT-05-07	**Die Auswertungen sind zu dokumentieren** Für die Auswertung von personenbezogenen Protokolldaten müssen vorab typische Kategorien geplant werden, in denen Protokolldaten entweder anlassbezogen oder regelmäßig ausgewertet werden. Die Szenarien sind mit dem betrieblichen Datenschutzbeauftragten abzustimmen. Die Szenarien haben das zu erwartende Auskunftsersuchen interner und externer Stellen zu berücksichtigen. Die Vorgehensweise zur Auswertung der Protokolldaten ist zu dokumentieren und die Durchführung ihrerseits zu protokollieren.	**X**	**X**	
PRT-05-08	**Rechte der Betroffenen** Die Rechte der Betroffenen auf Auskunft, Widerspruch, Berichtigung, Sperrung, Löschung sind zu wahren.	**X**	**X**	

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

31 RELEVANTE PROZESSE

Keine relevanten Prozesse

32 RELEVANTE DOKUMENTE

- LL001501 ISMS-Leitlinie
- RL 000081 IS-Werte- und –Risikomanagement
- RL128093 IS-Organisation und Aufgaben
- DV SIEM
- DV002020 DV EMail und Internet

33 ANHANG

Kein Anhang

KfW-
Organisationshandbuch

Richtlinie Nr. RL128091

Sachgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Teilgebiet	**Fehler! Verweisquelle konnte nicht gefunden werden.**
Titel	**Fehler! Verweisquelle konnte nicht gefunden werden.**

Titel Sicherheitsvorgaben für Datensicherung und Wiederherstellung

GELTUNGSBEREICH	VL CO VL IT VL DEG VL X3f
VERANTWORTLICHE OE	COc2
DOKUMENTVERANTWORTLICH	Burghardt, Waldemar
VERTRAULICHKEITSSTUFE	Intern (Stufe 2)
ERSETZT VERÖFFENTLICHUNGSDATUM VOM:	02.11.2017

ÄNDERUNGEN ZUR VORVERSION

Änderungs-datum	**Kapitel**	**Inhalte**
Dez. 2015	alle	Initiale Version
17.01.2017	2	Änderung das Geltungsbereichs auf CO und IT
Jul. 2017	2 3 4	Geltungsbereich angepasst und auf IPEX und DEG ausgeweitet Anpassung auf aktuelle ISO Maßnahmen Einfügen des Wirkens auf die Schutzziele (Vertraulichkeit-Integrität-Verfügbarkeit)
Feb. 2019	alle	Konkretisierung der Vorgaben zu Umsetzung auf Basis der BAIT-Anforderungen

INHALTSVERZEICHNIS

34 KURZBESCHREIBUNG

In dieser IS-Richtlinie werden systematische Sicherheitsmaßnahmen für die Implementierung und Betrieb von Datensicherung (Backup) und Wiederherstellung in der KfW beschrieben.

Regelungsdokumente wie die IS-Richtlinie konkretisieren die ISMS-Leitlinie und dienen als Grundlage für die operative Umsetzung durch die zuständigen Stellen.

Die IS-Vorgaben stellen keine Lösungen dar, sind aber ausreichend konkret, um auf operativer Ebene (1st Line of Defense) Sicherheitskonzepte entwickeln zu können.

Entstehen in der Praxis Situationen, bei welchen die Vorgaben nicht oder nicht vollständig um-setzbar sind, so sind alternative Lösungen zu entwickeln, die dem angestrebten Sicherheitsni-veau entsprechen.

35 GELTUNGSBEREICH

Bereiche: CO und IT der KfW inklusive der Abteilung X3f der Konzerntochter IPEX und der Abteilung LCc der Konzerntochter DEG.

Der Geltungsbereich dieser Richtlinie bezieht dabei alle Bereiche ein, die Sicherheitsvorgaben dieser Richtlinie operativ umsetzen.

Die Töchter weichen lediglich bei institutsspezifischen Besonderheiten (gesetzliche, vertragliche, externe oder geschäftliche Anforderungen) durch spezifische Anpassungen ab. Die Konzernleit- und -richtlinien erlangen nachfolgend erst nach Freigabe durch die jeweilige Geschäftsführung der Töchter („Ratifizierung“) Gültigkeit in den Einzelinstituten DEG/IPEX.
Den Einzelinstituten bleibt es im Übrigen unbenommen, unter Ausschluss von Widersprüchen mit den konzernweit nach den vorstehenden Maßgaben verabschiedeten und geltenden Regelungen konkretisierende Einzelmaßnahmen (Richtlinien, Arbeitsanweisungen) zu verabschieden.

36 ZIELSETZUNG

Erhaltung der Integrität und der Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen durch entsprechender Sicherungsverfahren.

Die Pflicht zur Datensicherung in Betrieben ergibt sich unter anderem aus:

- MaRisk AT 7.2.1 / AT 7.2.2: Die IT-Systeme und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen.
- BAIT Tz45 / Tz49 / Tz51: Die Geschäftsstrategie gibt Anforderungen an Verfügbarkeit, Lesbarkeit und Aktualität von Kunden- und Geschäftsdaten vor. Datensicherung sichert die Anforderungen bei Änderungen und bei Wiederherstellung nach Störungen.
- HGB / GoBD: IT folgt den gesetzlichen Vorschriften über eine ordnungsgemäße, nachvollziehbare, revisionssichere Buchführung.
- DIN ISO/IEC 27001:2013 Annex A, Control 12.3 sowie DIN ISO/IEC 27002 Control 12.3

Dabei ist die „Datensicherung zur Wiederherstelung“ von der „Datenarchivierung“ zu unterscheiden. Diese Richtlinie konzentriert sich auf die Datensicherung zur Wiederherstelung, die Datenarchivierung ist nicht Bestandteil dieser Richtlinie.

37 VORGABEN ZUR UMSETZUNG

Kürzel	Beschreibung	Schutzziel		
		V	I	V
BU-V_M-01	**Vorgaben zur Datensicherung** Die Vorgaben für die Verfahren zur Datensicherung sind schriftlich in einem Datensicherungskonzept zu dokumentieren. Darin sind die Mindestanforderungen an Umfang, Häufigkeit , Aufbewahrungsdauer und Integrität eines Backups durch die jeweiligen Fachbereiche, abgeleitet aus den Anforderungen der Geschäftsprozesse und Geschäftsfortführungspläne (Notfallpläne), zu definieren.		X	X
BU -V_M-02	**Dokumentation und Aufzeichnungen zu Backup Verfahren** Es sind Verfahren zur Erstellung von Datensicherungen, zur Wiederherstellung und Löschung von Daten festzulegenund zu dokumentieren und zu archivieren.	X		X
BU-V_M-03	**Aufbewahrung von Backups** Backups sind in sicherer Entfernung von den gesicherten Datenquellen zu lagern. Bei gespiegelten Backups ist eine getrennte Aufbewahrung in den jeweiligen RZ-Räumen ausreichend. Die Lagerorte von Backups sind gegen Verlust von Vertraulichkeit, Integrität und Verfügbarkeit abzusichern. Bei der Lagerung sind auch Faktoren wie Zutrittsschutz, Zugriffsschutz, Brandschutz und Klimatisierung zu beachten. Die Lagerorte der Backups (mehrere Versionen eines Backups) sind gleichartig abzusichern.	X	X	X
BU-V_M-04	**Physischer Schutz von Backupmedien** Backups sollten angemessen vor physischen und Umwelteinflüssen geschützt werden. Die Maßnahmen, die für Medien am Hauptstandort gelten, sollten somit auch für die Standorte der Backups gelten.			X
BU-V_M-05	**Applikationsspezifische Tests und Wiederherstellung** Wiederherstellungsprozeduren (Desaster-Recovery) sind zu entwickeln, aufzubauen, zu dokumentieren und zu testen. Wiederherstellungsprozeduren sollten regelmäßig überprüft und getestet werden um sicherzustellen, dass sie funktionieren und in dem zeitlichen Rahmen durchgeführt werden können, der in den		X	

Kürzel	Beschreibung	Schutzziel		
		V	I	V
	Verfahrensanweisungen für Wiederherstellung vorgegeben ist. Backup-Vorkehrungen für einzelne Systeme sind regelmäßig zu prüfen, um sicherzustellen, dass diese den Anforderungen der Pläne zur Sicherstellung des Geschäftsbetriebs (Business Continuity Plans bzw. BCP) genügen. Im Notfall muss das Backup die gesamten Systeminformationen, die Anwendungen und die Informationen beinhalten, um das Gesamtsystem komplett wiederaufsetzen zu können (Desaster Recovery).			
BU-V_M-06	**Verschlüsselung von Backups** Backups von streng vertraulichen Daten (Schutzbedarf „Vertraulichkeit Sehr hoch = 4“) sind durch Verschlüsselung vor unbefugtem Zugriff zu schützen. Die Verschlüsselung hat den Vorgaben der KfW zu entsprechen (RL128097 Absicherung mit Kryptographieverfahren).	X		
BU-V_M-7	**Transport von Backups und Backupmedien** Backup-Medien sind beim Transport außerhalb des RZ und anderen IT-Betreibsräumen zu schützen und der Transport ist zu genehmigen und zu dokumentieren. Werden Backups zum Beispiel vom Rechenzentrum zu einem Tresor über öffentliche Verkehrswege transportiert, sind diese gemäß der Vertraulichkeitsanforderungen der enthaltenen Daten zu schützen. Über den Transport sind Aufzeichnungen wie die Genehmigung, Zweck und Ein-/Auslagerungsprotokolle etc. zu erstellen.	X		
BU-V_M-8	**Beschaffenheit Backup Medien** Backup-Medien sind entsprechend der fachlichen Anforderungen im Hinblick auf die aktuellen technischen Möglichkeiten (Stand der Technik) auszuwählen.			X
BU-V_M-9	**Zugriffschutz für Backups** Die Zugriffe auf Backup Daten und die Durchführung von Restores sind in einem geregelten Verfahren zu dokumentieren.	X		
BU-V_M-10	**Elektronische Übertragung von Backups** Werden Backups über externe Netze übertragen, so sind die Übertragungswege gegen Zugriff von Dritten abzusichern. Die Verschlüsselung hat den Vorgaben der KfW zu entsprechen (RL128097 Absicherung mit Kryptographieverfahren).	X		
BU-V_M-11	**Restore-Tests**		X	X

Kürzel	Beschreibung	Schutzziel		
		V	I	V
	Die Verfahren zur Wiederherstellbarkeit im erforderlichen Zeitraum und zur Lesbarkeit von Datensicherungen sind regelmäßig, mindestens jährlich, im Rahmen einer Stichprobe sowie anlassbezogen zu testen und zu dokumentieren.			
BU-V_M-12	**Löschung von Backups** Nach vorgegebener Aufbewahrungszeit sind Backups zu löschen. Für Datenträger gelten die Vorschriften zur Vernichtung von Daten in der KfW unter Wahrung der Vertraulichkeitsanforderungen.	**X**		

38 RELEVANTE DOKUMENTE

- LL001501 Leitlinie ISMS
- RL128097 Absicherung mit Kryptographieverfahren

39 RELEVEANTE PROZESSE

keine vorhanden