Informationssicherheit und Business Continuity Management Richtlinie und Programm

Das Fundament für Resilienz und Stabilität

Stand: 15.04.2026
Version: 1.0
Bereich: 210101

Inhalt

		Seite
1.	Überblick IKT-Risikomanagementsystem	3
2.	Aufbauorganisation und Verantwortlichkeiten	3
3.	Bedrohungsanalyse und Sicherheitsvorgaben	4
4.	Notfallvorsorge	5
5.	Management der IKT- und Sicherheitsrisiken	5
6.	Vorfalls-, Notfall- und Krisenmanagement	6
7.	Security Awareness	7
8.	Kontinuierlicher Verbesserungsprozess (KVP) und Messung	7
9.	Berichterstattung	8

Informationssicherheit und BCM

1. Überblick IKT-Risikomanagementsystem

Das IKT-Risikomanagement der Deka-Gruppe basiert auf einem umfassenden, hierarchisch strukturierten Rahmenwerk zur Sicherstellung der digitalen operativen Resilienz (**DOR**). Das Rahmenwerk wird von der schriftlich fixierten Ordnung (sfO), welche vom Leitungsorgan freigeben ist, begleitet. Es integriert die Managementsysteme für Informationssicherheit (**ISMS**) und Business Continuity Management (**BCMS**) und orientiert sich an der DORA-Verordnung. Ergänzend hierzu gibt es die Strategie zur digitalen operationalen Resilienz. Das IKT-Risikomanagementsystem umfasst die Identifikation, Bewertung und Steuerung von IKT- und Sicherheitsrisiken.

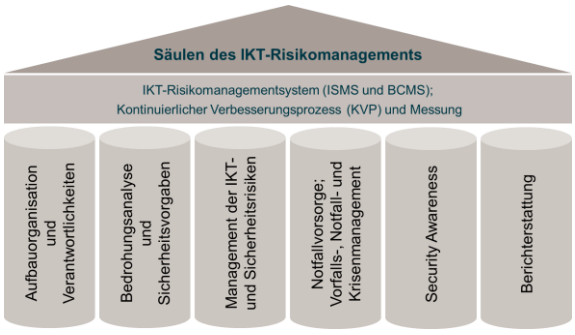
Ziel ist der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie die Kontinuität kritischer Geschäftsprozesse.

Das Rahmenwerk umfasst drei Ebenen: Grundsätze und Ziele, Aufbauorganisation und Maßnahmenkataloge sowie operative Anweisungen.

Ein risikobasierter Ansatz bewertet die Kritikalität von Prozessen und Systemen, um Schutzmaßnahmen zu priorisieren. Regelmäßige Überprüfungen der Sicherheitsvorgaben gewährleisten die Anpassung an Bedrohungen und regulatorische Anforderungen.

Governance-Strukturen sichern die Reaktionsfähigkeit auf Störungen wie Cyberangriffe oder technische Ausfälle. Sensibilisierung von Mitarbeitenden und Drittdienstleistern stärkt das Sicherheitsbewusstsein.

Das IKT-Risikomanagement wird im Folgenden in 8 Abschnitten beschrieben[1], welche als Säulen des IKT-Risikomanagements bzw. des IKT-Risikomanagementsystems gesehen werden können.



2. Aufbauorganisation und Verantwortlichkeiten

Die Aufbauorganisation des IKT-Risikomanagements der Deka-Gruppe ist klar strukturiert, um eine effektive Steuerung und Überwachung von IKT- und Sicherheitsrisiken zu gewährleisten. Die Gesamtverantwortung liegt beim Leitungsorgan, welches die strategische Ziele und Vorgaben festlegt sowie deren Umsetzung überwacht. Ein unabhängiger Beauftragter für digitale operationale Resilienz (DOR) koordiniert die operative Umsetzung und berichtet regelmäßig über den Status der Resilienzmaßnahmen.

Ziel:
Sicherstellung einer klar definierten und wirksamen Organisationsstruktur sowie eindeutiger Verantwortlichkeiten zur effektiven Steuerung, Überwachung und Umsetzung des IKT-Risikomanagements in der Deka-Gruppe.

Das Leitungsorgan trägt die oberste Verantwortung für die Steuerung und Überwachung des IKT-Risikomanagements. Es genehmigt die Leitlinie zum IKT-Risikomanagement, überwacht deren Umsetzung und wird regelmäßig über die Angemessenheit und Wirksamkeit informiert. Zudem benennt es unabhängige Beauftragte, darunter den Informationssicherheitsbeauftragten (**ISB**), den Business Continuity Management Beauftragten (**BCMB**) und den DOR-Beauftragten, die für die operative Umsetzung von Sicherheits- und Kontinuitätsmaßnahmen zuständig sind. Das Leitungsorgan stellt sicher, dass Informationssicherheit, Notfallvorsorge und Krisenmanagement effektiv umgesetzt werden und fundierte Entscheidungen auf Basis aktueller Risikoberichte getroffen werden können.

Der Beauftragte für digitale operationale Resilienz (DOR) übernimmt eine zentrale Rolle in der Überwachung und Koordination der Resilienzmaßnahmen. Zu seinen Aufgaben gehören die Überprüfung der Einhaltung von Sicherheitsstandards, die Durchführung von Risikobewertungen zur Identifikation von Schwachstellen sowie die Empfehlung geeigneter Maßnahmen zur Risikominderung. Er unterstützt die erste Verteidigungslinie bei der Umsetzung der Sicherheitsvorgaben, führt unabhängige Kontrollen durch und sorgt für eine transparente Berichterstattung an das Leitungsorgan. Darüber hinaus trägt er zur Einhaltung regulatorischer Vorgaben bei, schützt die Organisation vor Sicherheitsvorfällen und fördert eine robuste Sicherheitskultur.

Die Beauftragten agieren unabhängig und berichten regelmäßig an das Leitungsorgan über die Wirksamkeit und Angemessenheit des IKT-Risikomanagements. Sie arbeiten eng mit operativen Einheiten und zentralen Funktionen zusammen, um die Einhaltung der Sicherheitsvorgaben sicherzustellen und kontinuierliche Verbesserungen zu ermöglichen.

Die Organisation folgt dem 3-Lines-of-Defense-Modell, das eine klare Trennung von Verantwortlichkeiten sicherstellt:

[1] Die Inhalte dieses Dokuments und der jeweiligen Abschnitte sind ein Extrakt der freigegeben sfO

- 1st Line: Operative Einheiten setzen Sicherheitsvorgaben und Maßnahmen um.
- 2nd Line: Zentrale Funktionen überwachen die Einhaltung der Vorgaben und unterstützen die operative Umsetzung inkl. Ansiedlung der o.g. Beauftragten Personen.
- 3rd Line: Die interne Revision prüft unabhängig die Wirksamkeit des IKT-Risikomanagements.

Mitarbeitende der Deka-Gruppe sind verpflichtet, Sicherheitsvorgaben einzuhalten und an Schulungen sowie Sensibilisierungsmaßnahmen teilzunehmen, um ein hohes Maß an Sicherheitsbewusstsein zu gewährleisten. Externe Dienstleister, die in die Geschäftsprozesse eingebunden sind, werden in das IKT-Risikomanagement integriert und müssen die festgelegten Sicherheitsanforderungen erfüllen.

3. Bedrohungsanalyse und Sicherheitsvorgaben

Der Abschnitt "Bedrohungsanalyse und Sicherheitsvorgaben" im IKT-Risikomanagement der Deka-Gruppe beschreibt Maßnahmen und Standards zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen der Organisation und ihrer Kunden. Diese Vorgaben basieren auf gesetzlichen und regulatorischen Anforderungen, insbesondere aus dem Digital Operational Resilience Act (**DORA**), dem Kreditwesengesetz (**KWG**) und den Mindestanforderungen an das Risikomanagement (**MaRisk**), und dienen der Stärkung der digitalen Resilienz.

Ziel:
Stärkung der digitalen Resilienz durch die Umsetzung angemessener und aktueller Sicherheitsvorgaben sowie kontinuierliche Anpassung und Überwachung von Schutzmaßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen.

Ein zentraler Bestandteil ist das IKT-Risikomanagementsystem (**IKT-RMS**), das einen umfassenden Katalog von Referenzmaßnahmen zur Informationssicherheit und Notfallvorsorge umfasst. Das System wird regelmäßig durch Umweltanalysen überprüft, um sicherzustellen, dass die Maßnahmen den aktuellen Bedrohungslagen und technologischen Entwicklungen entsprechen. Die Kritikalität der Informationswerte wird kontinuierlich analysiert und dokumentiert, um Schutzmaßnahmen bedarfsgerecht anzupassen.
Die Sicherheitsvorgaben umfassen fortschrittliche Sicherheitslösungen und Überwachungsmechanismen zur frühzeitigen Erkennung und Abwehr von Bedrohungen. Ziel ist es, Risiken proaktiv zu identifizieren, Schwachstellen zu beheben und präventive Maßnahmen zu implementieren. Die Vorgaben sind Teil einer umfassenden Sicherheitsstrategie, die präventive und reaktive Maßnahmen integriert. Regelmäßige Überprüfungen und Anpassungen gewährleisten, dass die Organisation aktuellen und zukünftigen Herausforderungen im Bereich Informationssicherheit und digitale Resilienz gewachsen bleibt.

Spezielle Techniken zur Verhinderung von Cyberattacken werden u.a. durch die folgenden technischen Maßnahmen erreicht:

Maßnahme	Beschreibung
Firewall/DMZ	Der Datenaustausch (extern & interner Traffic) wird durch verschiedene Firewalls geleitet.
Intrusion Detection Systems (IDS)	Die beiden wichtigsten IT-Anbieter (Rechenzentren) halten IDS an den wichtigsten Verbindungspunkten zum Internet vor.
Mehrschichtiger Malwareschutz	Dateien, die in die Deka-IT-Systeme gelangen (z.B. per E-Mail oder Internet/Download), werden von mindestens zwei verschiedenen Arten von Malware-Scannern zweier verschiedener Hersteller überprüft.
Security Information & Event Management (SIEM)	Es erfolgt ein Use-Case-basiertes Screening von Sicherheitsereignissen (Netzwerk, Infrastruktur, Systeme, etc.), um Anomalien im Verkehrs- oder Nutzerverhalten zu identifizieren.
Erkennung externer Hardware	Eine Verbindung von externer Hardware mit den Netzwerken der DekaBank wird überwacht und ein SIEM-Ereignis ausgelöst. Darüber hinaus ist die externe Hardware aufgrund der zertifikatsbasierten Autorisierung technisch nicht in der Lage, sich mit den internen Netzwerken zu verbinden.
Schwachstellenüberprüfung	Interne Systeme werden regelmäßig anhand einer Liste bekannter Schwachstellen überprüft, um die Notwendigkeit einer Aktualisierung bzw. eines Patches zu ermitteln.
Client Compliance Check	Alle Clients, die mit internen Netzwerken verbunden sind, werden regelmäßig anhand einer Liste von genehmigten Konfigurationen überprüft, um Anomalien/Schwachstellen zu erkennen sowie Systeme zu identifizieren, die von Angreifern übernommen wurden.
Berechtigungsmanagement	Genehmigung, Vergabe, Einrichtung und Löschung von allen Berechtigungen auf den verschiedenen Technologieebenen erfolgt ausschließlich über dedizierte Prozesse; die eingerichteten Berechtigungen werden regelmäßig auf Minimalprinzip und Funktionstrennung überprüft.
E-Mail	Die E-Mail-Kommunikation unterliegt einem umfangreichen Spamschutz, welcher zudem mittels Filterfunktion mögliche Phishing-mails überprüft.
Penetrationstests	Penetrationstests (automatisierte Tests für gängige Angriffsmuster und manuelle Tests für komplexere Muster) werden regelmäßig durchgeführt, insbesondere für Systeme, die von öffentlichen Netzwerken aus erreichbar sind.

Informationssicherheit und BCM

Zusätzlich gibt es verschiedene Maßnahmen zur Sicherstellung der digitalen operationalen Resilienz. Im Rahmen des Testprogramms der digitalen operationalen Resilienz (DOR-Testprogramm) soll die Umsetzung dieser Maßnahmen überprüft und deren Wirksamkeit bewertet werden. Dazu werden Tests verschiedener Art durchgeführt, die darauf abzielen, potenzielle Schwachstellen und Nichtumsetzungen von Vorgaben zu identifizieren und diese proaktiv zu behandeln.

4. Notfallvorsorge

Die Notfallvorsorge im IKT-Risikomanagement der Deka-Gruppe ist ein zentraler Bestandteil zur Sicherstellung der digitalen operationalen Resilienz und der Kontinuität von kritischen oder wichtigen Funktionen im Sinne der DORA bzw. zeitkritischer Geschäftsprozesse. Sie umfasst präventive und reaktive Maßnahmen, um die Auswirkungen von Störungen zu minimieren und die Handlungsfähigkeit der Organisation sicherzustellen. Dabei orientiert sie sich an den übergeordneten Zielen des IKT-Risikomanagements sowie an regulatorischen Anforderungen und den spezifischen Bedürfnissen der Deka-Gruppe. Ein Kernaspekt der Notfallvorsorge ist die szenariobasierte Planung, die potenzielle Störungs- und Schadenslagen berücksichtigt. Diese Planung ist geschäftsprozessorientiert und umfasst mögliche Ausfälle in Bereichen wie Standorte, IT-Systeme, Personal und Dienstleistungen. Szenarien werden regelmäßig überprüft und an aktuelle Bedrohungslagen sowie technologische Entwicklungen angepasst.

Ziel:
Aufrechterhaltung der Kontinuität zeitkritischer Geschäftsprozesse und schnelle Wiederherstellung des Normalbetriebs im Falle von Störungen zur Minimierung negativer Auswirkungen und zur Absicherung des Geschäftsbetriebs.

Die Notfallvorsorge beinhaltet die Entwicklung und regelmäßige Überprüfung von (IKT-)Geschäftsfortführungsplänen sowie der erforderlichen Ressourcen. Ergänzend werden jährliche Tests durchgeführt, die unter anderem die Notfall- und Krisenorganisation, technische Notfallausstattungen und die Einbindung von IKT-Drittanbietern umfassen. Ziel ist die Überprüfung der jeweils für die fortlaufende Aufrechterhaltung und schnelle Wiederherstellung von ausgewählten zeitkritischen, kritischen oder wichtigen Funktionen sowie Geschäftsprozessen benötigten Ressourcen. Dabei werden gezielt nur die für den jeweiligen Test relevanten Ressourcen und Prozesse betrachtet..

Abgestimmte Notfallkonzepte regeln Zuständigkeiten, Kommunikationswege und Schutzmaßnahmen, um eine nahtlose Integration externer Dienstleister sicherzustellen.

Die kontinuierliche Überprüfung und Anpassung der Notfallpläne ist essenziell. Szenariobasierte Verfahren definieren Prozesse zur Reaktion und Wiederherstellung von Anwendungen, IT-Infrastrukturen und Geschäftsprozessen. Klare Verantwortlichkeiten und enge Zusammenarbeit zwischen prozessverantwortlichen Organisationseinheiten und IT-Funktionen gewährleisten die Handlungsfähigkeit der Organisation in Notfall- und Krisensituationen.

Die Deka-Gruppe verfügt über eine etablierte Geschäftsfortführungsplanung (**GFP**), die sicherstellt, dass kritische und wichtige Geschäftsfunktionen innerhalb ihrer maximal tolerierbaren Ausfallzeit (**MTPD**) von bis zu drei Arbeitstagen aufrechterhalten bzw. wiederhergestellt werden können. Die Erstellung und Pflege der GFP erfolgt in einem Tool durch die Fachbereiche und wird durch die Rolle des Business Continuity Coordinators (**BCC**) der Fachbereiche koordiniert. Bei Aktivierung eines GFP ist eine standardisierte Notfalldokumentation zu führen und an die Zentrale Kontakt- und Koordinationsstelle (**ZKK**) in der 2nd LoD zu übermitteln. Die Deaktivierung erfolgt nach Wiederherstellung des Normalbetriebs. Zur Sicherstellung der Wirksamkeit werden die (IKT-)Geschäftsfortführungspläne regelmäßig getestet und geübt. Die mehrjährige Testplanung wird jährlich durch ISM & BCM fortgeschrieben, durch den BCMB freigegeben und in der IKT-Risikoberichterstattung adressiert. Erkenntnisse aus Übungen und tatsächlichen Ereignissen (z. B. Abweichungen, Wirksamkeitsdefizite) werden dokumentiert, analysiert und in den IKT-Risikobewertungsprozess zurückgespielt, sodass eine laufende Aktualisierung und Verbesserung der Pläne gewährleistet ist.

5. Management der IKT- und Sicherheitsrisiken

Das Management der IKT- und Sicherheitsrisiken ist ein zentraler Bestandteil des operationellen Risikomanagements der Deka-Gruppe. Es zielt darauf ab, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten zu gewährleisten, die digitale operationale Resilienz sicherzustellen und regulatorische Anforderungen zu erfüllen. Gleichzeitig trägt es zur Wahrung des Vertrauens der Stakeholder bei. Es ist in das übergeordnete Management der Non-Financial Risk der Deka-Gruppe eingebettet und folgt dessen grundsätzlichen Methoden und Vorgehensweisen.

Informationssicherheit und BCM

Ziel:
Systematische Identifikation, Bewertung, Steuerung und Nachverfolgung von IKT- und Sicherheitsrisiken zur Sicherstellung der Informationssicherheit und Stabilität der Geschäftsprozesse und zur Einhaltung regulatorischer Anforderungen.

Ein wesentlicher Schwerpunkt der sogenannten IKT-Kontrollfunktion liegt auf der systematischen Identifikation und Bewertung von IKT- und Sicherheitsrisiken. Überwachungsmaßnahmen wie Audits und Self-Assessments sind integrale Bestandteile des IKT-Risikomanagements. Sie dienen der Überprüfung der Einhaltung und Wirksamkeit der Sicherheitsvorgaben sowie der kontinuierlichen Verbesserung der digitalen operationalen Resilienz. Diese Maßnahmen ermöglichen die Bewertung des Umsetzungsgrades der Vorgaben, die Analyse der Risikosituation und die Ableitung notwendiger Anpassungen, um die Sicherheit und Kontinuität der Geschäftsprozesse zu gewährleisten.

Die Bewertung identifizierter Risiken erfolgt anhand standardisierter Kriterien, die potenzielle Auswirkungen und Eintrittswahrscheinlichkeiten quantifizieren und priorisieren. Risiken werden nach ihrem Schweregrad klassifiziert, um fundierte Entscheidungen zur Risikosteuerung zu ermöglichen. Kompetenzregelungen, die auf Risikostufen basieren, legen fest, welche Instanzen berechtigt sind, Risiken zu akzeptieren. Diese Regelungen gewährleisten, dass Entscheidungen auf der jeweils angemessenen Ebene getroffen werden und alle relevanten Stakeholder in den Entscheidungsprozess eingebunden sind.

6. Vorfalls-, Notfall- und Krisenmanagement

Das Vorfalls-, Notfall- und Krisenmanagement der Deka-Gruppe ist ein integraler Bestandteil des IKT-Risikomanagements und gewährleistet die Handlungsfähigkeit der Organisation in kritischen Situationen.

Es umfasst die Identifikation, Bewertung und Bearbeitung von Vorfällen sowie die strukturierte Reaktion auf Notfall- und Krisensituationen.

Ziel:
Sicherstellung der Handlungsfähigkeit und Schadenminimierung der Organisation in Krisen-, Notfall- oder Vorfallssituationen durch strukturierte und koordinierte Prozesse zur schnellen Wiederherstellung eines stabilen Betriebszustands.

Das **Vorfallsmanagement** konzentriert sich auf die Bearbeitung schwerwiegender IKT-bezogener Vorfälle und Sicherheitsvorfälle. Standardisierte Prozesse und Tools ermöglichen die effiziente Erfassung und Klassifikation von Vorfällen. Die Klassifikation erfolgt anhand definierter Kriterien, die Schweregrad und potenzielle Auswirkungen bewerten. Auf dieser Grundlage werden Eskalationen und Maßnahmen eingeleitet. Die Dokumentation der Vorfälle dient der Nachvollziehbarkeit und der kontinuierlichen Verbesserung des Sicherheitsmanagements.

Das **Notfallmanagement** reagiert auf schwerwiegende Störungen, die die Verfügbarkeit von kritischen oder wichtigen Funktionen sowieGeschäftsprozessen gefährden. Es basiert auf detaillierten Notfallplänen, die regelmäßig überprüft und an aktuelle Anforderungen und Bedrohungslagen angepasst werden. Tests und Übungen überprüfen die Wirksamkeit der Pläne und bereiten die Mitarbeitenden auf ihre Rollen und Verantwortlichkeiten vor.

Das **Krisenmanagement** geht über das Notfallmanagement hinaus und adressiert Szenarien, die die Organisation in ihrer Gesamtheit gefährden können. Es folgt einem klar definierten Prozess, der die Alarmierung, die strukturierte Bewältigung der Krise und die Beendigung des Krisenmanagements umfasst. Die Alarmierung erfolgt über festgelegte Kommunikationswege und Tools, die eine schnelle Benachrichtigung der Krisenstabsmitglieder sicherstellen.

Informationssicherheit und BCM

Der **Krisenstab**, bestehend aus Vertretern verschiedener Fachbereiche, dem BCM-Beauftragten, Vertretern der 2nd Line sowie einem Mitglied des Leitungsorgans koordiniert Maßnahmen und trifft Entscheidungen. Die Krisenbewältigung erfolgt iterativ durch Lagebeurteilung, Maßnahmenentscheidung, Umsetzung und Wirksamkeitskontrolle, um flexibel auf die Situation zu reagieren und die Effektivität der Maßnahmen sicherzustellen.

Ein internes und externes Meldewesen ist etabliert.

Die Verantwortlichkeiten im Krisenmanagement sind klar definiert. Der Leiter des Krisenstabs trägt die Gesamtverantwortung und koordiniert die Aktivitäten. Der BCM-Beauftragte (Business Continuity Management) integriert das Krisenmanagement in das übergeordnete Kontinuitätsmanagement und stellt die Übereinstimmung mit den strategischen Zielen sicher. Das Emergency Response Team (**ERT**) unterstützt die operative Umsetzung und gewährleistet die effektive Durchführung der Maßnahmen.

7. Security Awareness

Awareness ist ein zentraler Bestandteil des IKT-Risikomanagements der Deka-Gruppe und bildet die Grundlage für die Umsetzung von Sicherheitsmaßnahmen und den Schutz vor Risiken.

Ziel:
Ziel des Security Awareness Managements ist es, ein kontinuierliches Sicherheitsbewusstsein bei Mitarbeitenden zu schaffen, Sicherheitsmaßnahmen in die tägliche Arbeit zu integrieren und eine Sicherheitskultur zu etablieren.

Ein Schwerpunkt liegt in der Sensibilisierung der Mitarbeitenden für IKT-Sicherheitsmaßnahmen. Dies umfasst sowohl Wissen als auch eigene Kampagnen zu Bedrohungen wie Cyberangriffe, Phishing oder Datenlecks sowie deren Konsequenzen. Im Hinblick auf DORA wird durch Lerninhalte und proaktiven Kampagnen die Awarenessbereitschaft geschärft sowie die Cyberreife gestärkt.

Neben technischen Aspekten werden organisatorische und prozessuale Maßnahmen zur Risikominderung vermittelt, um Risiken frühzeitig zu erkennen und angemessen zu reagieren.

Zur Förderung des Sicherheitsbewusstseins setzt die Deka-Gruppe auf Schulungen, Workshops und E-Learning-Module, die flexibel und zielgruppenspezifisch gestaltet sind. Awareness-Kampagnen greifen aktuelle Bedrohungen auf und nutzen Kommunikationskanäle wie Newsletter, Intranet und Plakate, um eine breite Zielgruppe zu erreichen.

Die Maßnahmen werden regelmäßig überprüft und angepasst. Feedback- und Evaluationsprozesse bewerten die Wirksamkeit und identifizieren Verbesserungspotenziale. Diese Optimierung stellt sicher, dass die Awareness-Maßnahmen aktuellen Anforderungen entsprechen und die Mitarbeitenden optimal auf ihre Rolle im IKT-Risikomanagement vorbereitet sind und auf dem Laufenden Stand bleiben.

8. Kontinuierlicher Verbesserungsprozess (KVP) und Messung

Die Deka verpflichtet sich im Rahmen des IKT-Risikomanagements, die Cybersecurity-Maßnahmen kontinuierlich zu verbessern. Der kontinuierliche Verbesserungsprozess (**KVP**) bildet dabei einen zentralen Bestandteil, um die Cyberreife der Organisation laufend zu erhöhen und sowohl aktuellen als auch neuen Bedrohungen wirksam zu begegnen. Regelmäßige Überprüfungen und Anpassungen der Prozesse, einschließlich jährlicher KVP-Workshops und kontinuierlicher Lessons Learned sowie Beobachtung technologischer Entwicklungen, gewährleisten die Integration von Erkenntnissen aus Vorfällen, Audits und Testprogrammen. Die Methodik und Umsetzung orientiert sich am PDCA (Plan-Do-Check-Act)-Zyklus, welcher ein Vorgehen für einen kontinuierlichen Verbesserungsprozess darstellt

Ziel:
Laufende Weiterentwicklung und nachhaltige Steigerung des Reifegrads der Cybersecurity der Organisation durch kontinuierliche Überprüfung, Messung und Optimierung aller relevanten Prozesse, Maßnahmen und Kontrollen.

Zur Sicherstellung der Wirksamkeit der Sicherheitsmaßnahmen werden über alle relevanten Prozesse hinweg geeignete Kontrollen sowie spezifische Kennzahlen eingesetzt. Diese dienen der strukturierten und messbaren Überwachung und unterstützen die kontinuierliche Weiterentwicklung der Cybersecurity. Die Ergebnisse der Kontrollen und Kennzahlen werden im Rahmen des KVP ausgewertet und in weitere Optimierungsmaßnahmen überführt, während Fortschritte und Maßnahmen an relevante Stakeholder kommuniziert und in den laufenden Prozessen berücksichtigt werden.

Informationssicherheit und BCM

9. Berichterstattung

Die Berichterstattung im IKT-Risikomanagement der Deka-Gruppe ist ein zentrales Element zur Sicherstellung von Transparenz über den Status des IKT-Risikomanagementsystems (IKT-RMS) und die aktuelle Risikolage. Quartalsweise Berichte werden an den Vorstand, die Geschäftsführungen der Tochtergesellschaftenund die Bereichsleitungen sowie Management Komitee Risiko (nur Risikostatus) übermittelt. Zusätzlich erhält das Leitungsorgan in seiner Aufsichtsfunktion (Verwaltungsrat/Aufsichtsräte) einen jährlichen Bericht zum Sachstand des IKT-Risikomanagementsystems inkl. Risikostatus. Diese Berichte bieten eine Übersicht über die aktuelle Risikosituation und die Wirksamkeit der umgesetzten Maßnahmen. Sie dienen sowohl der internen Kontrolle als auch der Kommunikation mit externen Stakeholdern, einschließlich der Aufsichtsbehörden.

Ziel:
Schaffung von Transparenz und Informationssicherheit durch regelmäßige, adressatengerechte Berichterstattung zum Status des IKT-Risikomanagements und zur aktuellen Risikolage an interne und externe Stakeholder.

Die regelmäßige Berichterstattung gewährleistet, dass alle relevanten Parteien über Fortschritte im Risikomanagement informiert sind und die Organisation auf neue Herausforderungen schnell und effektiv reagieren kann. Ergänzend zu den regelmäßigen Berichten werden Ad-hoc-Berichte bei besonderen Ereignissen oder Vorfällen erstellt. Hinzu kommen Berichte, welche neben internen auch externe Adressaten haben, u.a. der Bericht zur Überprüfung des IKT-Risikomanagementrahmens. Diese Berichte informieren Stakeholder zeitnah über kritische Entwicklungen, beschreiben die ergriffenen Sofortmaßnahmen und geben eine Einschätzung zur weiteren Vorgehensweise.

DekaBank
Deutsche Girozentrale
Große Gallusstraße 14
60315 Frankfurt am Main
Postfach 11 05 23
60040 Frankfurt

Telefon: (0 69) 7147 - 0
Telefax: (0 69) 7147 - 1376
www.deka.de

Finanzgruppe