Rahmenbedingungen IT Governance

OA1004

Group24 AG (group24)

INHALTSVERZEICHNIS

1 DOKUMENTENLENKUNG

1.1 Stammdaten

Referenz-Nummer:	OA1004
Dokumententitel:	Rahmenbedingungen IT Governance
Fachlich Verantwortlicher:	Cihat Dokumaci
Zuständiger Bereich:	Informationssicherheit
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues / Marc Eismann
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	intern

1.2 Änderungsverzeichnis

Version	Datum	Autor	Inhalte der Änderung
0.1	12.09.2022	Sandra Kiemes	Initiale Erstellung
0.2	20.09.2022	Cihat Dokumaci	Anpassung an group24
1.1	27.10.2023	Cihat Dokumaci	Anpassung Regelmäßige Überprüfung des Rechtskatasters

1.3 Reviewnachweis und Freigabe

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues / Marc Eismann	Prüfung Ersterstellung und Freigabe
V1.1	15.11.2023	Marc Eismann	Review 2023

2 EINLEITUNG

Mit dieser Organisationsanweisung werden die Rahmenbedingungen für die IT-Governance der Group24 festgelegt.

Ziel der IT-Governance ist die Erhöhung der Wettbewerbsfähigkeit und Sicherheit durch Ausrichtung und Konsolidierung der Leistungen von Informationsverarbeitung.

- Strategische Ausrichtung mit Fokus auf Unternehmenslösungen
- Nutzengenerierung mit Optimierung der Ausgaben und Bewertung des Nutzens der IT
- Risikomanagement, das sich auf den Schutz des IT-Assets bezieht, unter Berücksichtigung von Disaster Recovery (Wiederanlauf nach Katastrophen) und Fortführung der Unternehmensprozesse im Krisenfall
- Management von Ressourcen, Optimierung von Wissen und Infrastruktur

Teilziele der IT-Governance sind in Anlehnung an COBIT (Control Objectives for Information and Related Technology) als dem international anerkannten de facto-Standard:

- Effektiver Einsatz von Informationsverarbeitung in der Group24
- Effizienz im Geschäftsbetrieb sowie der Projektleitung und -durchführung
- Einhaltung der IT-Compliance
- Gewährleistung der IT-Sicherheit
- Optimaler Einsatz der IT-Ressourcen
- Controlling

Die IT-Governance umfasst die Richtlinien der Group24, die sich sowohl aus Gesetzen, Kundenverträgen, internen und weiteren externen Standards ergeben.

Die erste Gruppe umfasst rechtliche Vorgaben, die entweder gesetzliche Regelungen oder auf gesetzlicher Grundlage erlassene Vorschriften abbilden. Hierzu gehören u.a. Gesetze, Rechtsverordnungen, Rechtsprechungen oder Verwaltungsvorschriften, die sich auf den betrieblichen Einsatz von IT auswirken.

Bei Verträgen, die ein Unternehmen mit Kunden, Lieferanten und weiteren Partnern abschließt, kann zwischen allgemeinen und IT-spezifischen Verträgen unterschieden werden. Der Vertragsgegenstand der allgemeinen Verträge konzentriert sich nicht ausdrücklich auf die IT. Diese Verträge können jedoch IT-relevante Vereinbarungen enthalten. Bei den IT-spezifischen Verträgen bezieht sich hingegen der Vertragsgegenstand direkt auf die Erbringung von IT-Leistungen.

Zu den internen Regelwerken gehören vor allem Richtlinien, Standards und Verfahrensanweisungen, die unternehmensinterne Festlegungen bezüglich der IT enthalten.

Zur Gruppe der externen Regelwerke gehören überwiegend Normen und Standards, die für die Group24 maßgebend sind und quartalsweise auf Aktualität überprüft werden.

Gruppe	Regelwerk	Inhalt
Rechtliche Vorgaben	Datenschutz-Grundverordnung (EU-DSGVO)	• Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. • Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. • Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.
	Bundesdatenschutzgesetz (BDSG)	Das BDSG regelt die Erhebung, Verarbeitung und Nutzung von Daten natürlicher Personen. Ziel ist es, den Missbrauch personenbezogener Daten zu verhindern. Speziell die Anlage zu § 9 enthält hierfür spezifische organisatorische und technische Vorgaben.
	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)	Die GoBS präzisieren die handelsrechtlichen Grundsätze ordnungsmäßiger Buchführung beim Einsatz von IT-Systemen zur Unterstützung der manuellen Buchführung.
	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)	Die GDPdU regeln die Aufbewahrung digitaler Unterlagen. Hierbei werden handelsrechtliche Vorgaben hinsichtlich der digitalen Aufbewahrung von Geschäftsunterlagen, Buchungsbelegen und Rechnungen konkretisiert.
	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	Das KonTraG ergänzt die Anforderungen des Handelsgesetzbuches und des Aktiengesetzes zur Verbesserung der Corporate Governance in deutschen Unternehmen. Das KonTraG erweitert die Haftung von Vorstand, Aufsichtsrat und Wirtschaftsprüfern und erfordert die Einführung eines Risikofrüherkennungssystems.
Verträge	IT-spezifische Verträge	IT-spezifische Verträge sind Verträge für IT-Leistungen, wie z.B. Hosting, Entwicklung oder Wartung.
	Allgemeine Verträge	Allgemeine Verträge sind Verträge, die IT-relevante Regelungen beinhalten, wie z.B. Geheimhaltungsvereinbarungen oder Vereinbarungen über den Austausch und die Aufbewahrung von Informationen.
Interne Regelwerke	Informationssicherheits-Leitlinie inklusive Sicherheitsrichtlinien	Interne Vorgaben zum Umgang mit Informationen und Informationsverarbeitetenden Systemen.
Externe Regelwerke	IDW PS 330 und RS FAIT 1	Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) fördert und unterstützt die Arbeit der Wirtschaftsprüfer bzw. Wirtschaftsprüfungsgesellschaften. IDW PS 330 ist ein Prüfungsstandard, der Anforderungen an die Durchführung von Abschlussprüfungen beim Einsatz von

		IT enthält. IDW FAIT 1 ist eine Stellungnahme zu den Grundsätzen ordnungsmäßiger Buchführung, die die Anforderungen der §§ 238, 239 und 257 HGB für die IT-gestützte Führung der Handelsbücher konkretisiert.
	IT Infrastructure Library (ITIL)	ITIL ist ein international anerkannter Standard für eine mögliche Umsetzung eines IT Service Managements. ITIL enthält eine Sammlung von Best Practices (Prozesse, Methoden, Vorgehensweisen oder Praktiken), die sich in der Praxis bewährt haben.
	ISO 27001	ISO 27001 ist eine international anerkannte Norm für IT-Sicherheit. Die Norm enthält eine Reihe spezifizierter Anforderungen für die Herstellung, Planung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines Informationssicherheits-Managementsystems.

3 PROZESS MANAGEMENT

Ziel der Prozessdokumentationen ist es, die für die Serviceerbringung relevanten Prozesse der Group24 zu beschreiben, um Prozessbeteiligte und alle an weitergehenden Informationen interessierte Personen oder Personengruppen mit den notwendigen Informationen auszustatten. Ziel ist es sicherzustellen, dass alle prozessrelevanten Punkte erfasst sind und ein gemeinsames Verständnis über Leistungen und Tätigkeiten sowie die Übergabepunkte oder Schnittstellen besteht.

Die Prozessdokumentationen richten sich nach dem ITIL Service Lifecycle in der Version 3 (2011).

Jede Lebenszyklusphase gliedert sich in weitere Prozesse, die jeweils derjenigen Phase zugeordnet sind, in der die Prozesse hauptsächlich oder besonders stark auftreten. Auch wenn diese Prozesse einer Phase zugeordnet sind, so beinhalten die meisten Prozesse Aktivitäten in mehreren Phasen des Servicelebenszyklus.

3.1 Dokumentation der Prozessbeschreibungen

Jeder Prozess ist in einem eigenständigen Dokument beschrieben. Zur besseren Übersichtlichkeit sind alle Dokumente mit der gleichen Gliederungsstruktur versehen, wobei es vorkommen kann, dass manche Unterkapitel für einige Prozesse keine zusätzlichen relevanten Informationen enthalten und daher nur mit einem allgemeinen Vermerk versehen werden. Die Ablage erfolgt im Group24 Teams Verzeichnis.

3.2 Kontrollen des Prozess Managements

Die Prozesse werden jährlich durch ein internes Audit geprüft.

4 RISIKO MANAGEMENT

Im Rahmen des Risikomanagements steuert der Risikomanager die Risiken inklusive der IT Risiken (Risiko Owner: ISB) über ihren gesamten Lebenszyklus hinweg.

Wichtige Quellen zur Identifizierung von IT-Risiken sind:

- Nicht umgesetzte Informationssicherheitsmaßnahmen (Sollmaßnahmen)
- Prüfberichte (externe Prüfer, etc.)
- Ergebnisse von Kontrollhandlungen der Informationssicherheit
- Informationssicherheitsvorfälle

Der Prozess ist beschrieben im Prozess P1006_Risk_Management.

4.1 Dokumentation des Risiko Managements

Die Dokumentation der Risiken erfolgt durch den Risiko Manager in der Risikomatrix.

Die Ablage erfolgt im Teams Verzeichnis.

4.2 Kontrollen des Risiko Managements

Die Risikoinventur wird auf jährlicher Basis durch den Risiko Manager durchgeführt und dokumentiert.

5 INFORMATIONSSICHERHEIT

Der Geltungsbereich des IT-Sicherheitsmanagements der Group24 bezieht sich auf alle IT-Dienste und -Systeme, die die Group24 für sich selbst oder für ihre Kunden verantwortlich betreibt.

Die Sicherheitsleitlinie ist eine Richtungsvorgabe für die Umsetzung von Sicherheit in der Group24. Sie ist die Grundlage für alle nachgeordneten Sicherheitsrichtlinien, -konzepte, -vorgaben und -empfehlungen und weiterführenden Organisationsanweisungen.

Ebenso sind die daraus resultierenden Risiken eingebettet in das zentrale Risiko Management der Group24.

5.1 Dokumentation der Informationssicherheit

Die ISMS-Dokumente sind hierarchisch aufgebaut. Alle Dokumente unterliegen der Sicherheitsleitlinie, darunter gibt es die weiteren, oben aufgeführten, Dokumentebenen. Die ISMS-Dokumentenpyramide ist unten grafisch dargestellt.

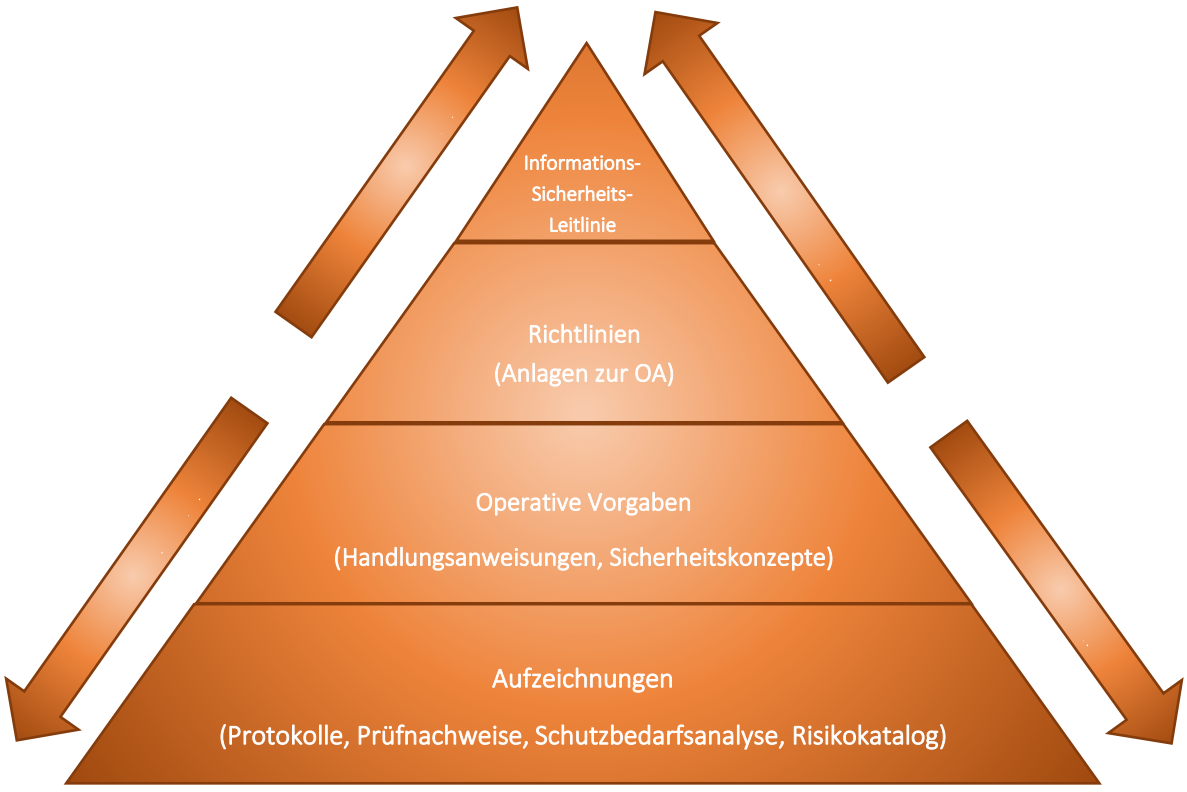

Abbildung 1: Struktur der ISMS-Dokumente

Die Group24 hat Ihr ISMS in Microsoft Teams etabliert und dort für die Mitarbeiter veröffentlicht.

5.2 Kontrollen der Informationssicherheit

Die Informationssicherheit wird zum einen durch die jährliche interne Prüfung des ISMS sowie durch die externen Prüfungen nach ISO27001 geprüft.

6 DATENSCHUTZ

Der Datenschutzbeauftragte der Group24 wird intern gestellt. Der gestellte Datenschutzbeauftragte ist für das Datenschutzmanagement der Group24 zuständig und berät hinsichtlich aller Datenschutz relevanten Themen. Hierunter fallen unter anderem folgende Tätigkeiten:

- Einhaltung der gesetzlichen und kundenspezifischen Datenschutzanforderungen (insbesondere auch bei hohen regulatorischen Compliance-Anforderungen von Finanzdienstleistern)
- Datenschutzkonforme Umsetzung organisatorischer und technologischer Änderungen im IT-Betrieb

6.1 Dokumentation des Datenschutz

Das Datenschutzmanagement ist in der Datenschutz-Leitlinie OA-1001 geregelt und dokumentiert.

6.2 Kontrollen des Datenschutz

Das Datenschutzmanagement der Group24 wird im jährlichen Datenschutzbericht dokumentiert.

7 NOTFALL MANAGEMENT

Es ist Ziel des Notfallmanagements, die Auswirkungen eines Notfallereignisses für die Group24 und ihre Kunden unter Beachtung der Wirtschaftlichkeit sowie der im Folgenden aufgeführten Rahmenbedingungen zu begrenzen.

Die Aufrechterhaltung der Informationssicherheit ist in das Business Continuity Management einzubeziehen. Dabei sind die folgenden Punkte zu beachten und zu berücksichtigen:

- Die Anforderungen an die Informationssicherheit sowie das Informationssicherheitsmanagement in Notfallsituationen (einschl. Krisen und Katastrophen) sind festzulegen.
- Zur Aufrechterhaltung der geforderten Informationssicherheit in Notfallsituationen sind geeignete Prozesse, Verfahren und Maßnahmen festzulegen, zu dokumentieren und umzusetzen.
- Die Angemessenheit der festgelegten und umgesetzten Maßnahmen zur Aufrechterhaltung der Informationssicherheit in Notfallsituationen ist regelmäßig zu überprüfen und deren Wirksamkeit zu testen und zu üben.
- Die geforderte Verfügbarkeit informationsverarbeitender Einrichtungen ist durch redundante Architekturen und Komponenten sicherzustellen und zu überprüfen.

7.1 Dokumentation des Notfall Managements

Das Notfallkonzept dient der Umsetzung der Notfallstrategie und beschreibt die Vorgehensweise, um die für das Notfallmanagement gesetzten Ziele zu erreichen. Es beschreibt allgemein etablierte Notfallvorsorge- und Notfallmanagementmaßnahmen der Group24.

7.2 Kontrollen des Notfall Managements

Das Notfallkonzept und die Notfallpläne werden jährlich durch den Notfallmanager geprüft und im Bedarfsfall aktualisiert.

Alle durchgeführten Test werden dokumentiert. Die sich daraus ergebenen Änderungen werden in den Notfallplänen aktualisiert.

8 PROJEKT MANAGEMENT

Die in der Group24 vorgeschriebene Projektmethodik unterliegt einem Rahmenwerk, das als Prozess im Group24 Teams abrufbar ist. Die Kontrolle der Anwendung des Prozesses wird durch das PMO (Projekt Management Office) sichergestellt.

- Alle Projektleiter in einem Einzelgespräch für das Projekt in die Projektmethodik eingewiesen
- monatliche Projektstatusmeeting werden mit allen betroffenen Projektleitern durchgeführt
- alle kritischen Projekte werden durch das PMO an die Management Runde eskaliert.

8.1 Dokumentation der Projekte

Die Standards der Group24 umfassen neben der Projektorganisation und den Dokumentationsrichtlinien Standards, die zum einen die Projekt Richtlinien und zum anderen den Übergang des Projektes in den Betrieb sicherstellt.

Die Dokumentationsrichtlinien umfassen sowohl die interne und externe Kommunikation sowie die Projektplanung und Projektstatus. Die entsprechenden Vorlagen sind in Microsoft Teams der Group24 hinterlegt.

Die Projektdokumentation wird in Microsoft Teams der Group24 verwaltet. Es gibt für Projekte eine vorgegebene Struktur, die der Projektleiter sowie der Vertreter sicherstellen. Es wird pro Projekt eine eigene Microsoft Teams Team erstellt, welches projektspezifische Berechtigungen ermöglicht.

8.2 Kontrollen des Projekt Managements

Das PMO Projekt Management Office verfolgt die Projekte innerhalb der Group24.

9 IT-COMPLIANCE

IT Compliance bezeichnet die Kenntnis und Einhaltung der Vorgaben und Anforderungen an das Unternehmen, die Aufgabe und die Einrichtung entsprechender Prozesse und die Schaffung des Bewusstseins der Mitarbeiter für Regelkonformität, sowie die Kontrolle und die Dokumentation der Einhaltung der relevante Bestimmungen gegenüber internen und externen Adressaten.

9.1 Dokumentation der IT Governance

Die IT Compliance wird in Form des Anweisungswesen der Group24 festgelegt. Die Richtlinien umfassen die notwendigen Rahmenbedingungen für die Vorgaben und Anforderungen im Unternehmen. Diese werden ergänzt um Verfahrensanweisungen.

9.2 Kontrollen der IT Governance

Der jährliche Management Report beinhaltet die Zusammenfassung der Kontrollen und Maßnahmen zur Einhaltung der IT Governance der Group24, die im Anweisungswesen der Group24 festgelegt ist.