Public Group Information Security Policy

Inhalt

Inhalt 1

A. Zweck dieses Dokuments 2

B. Geltungsbereich dieses Dokuments 2

C. Zuständigkeit für dieses Dokument 3

D. Ziele des Informationssicherheits- und des Business Continuity Managements 3

E. Ausrichtung des Informationssicherheitsmanagementsystems und Business Continuity Managementsystems (ISMS und BCMS) 3

F. Governance-Modell des ISMS und des BCMS (Three Lines of Defense-Modell) 4

G. Rollen und Verantwortlichkeiten der Informationssicherheit und des Business Continuity Management 5

H. Change history and other notes 5

A. Zweck dieses Dokuments

Informationen sowie die kontinuierliche Verfügbarkeit der Produkte und Services sind für die Unternehmenstätigkeit der CompuGroup Medical SE & Co. KGaA (CGM) von entscheidender Bedeutung und nehmen hierbei eine wesentliche Rolle ein. Diese Policy definiert die Vorschriften und Anforderungen, die für den sicheren und zuverlässigen Umgang mit Informationen und die Sicherstellung des Geschäftsbetriebs erforderlich sind. Wenn Informationen unbeabsichtigt offengelegt oder kompromittiert werden oder nicht verfügbar sind, ist die CGM und ihre Kunden einem hohen Sicherheitsrisiko ausgesetzt.

CGM ist entscheidend auf das kontinuierliche Vertrauen der Kunden und Partner angewiesen. Dieses Vertrauen ist dank der jahrelangen Bemühungen aller Mitarbeiter der CGM entstanden. Dieser Wettbewerbsvorteil muss geschützt werden, denn dessen Verlust könnte für die CGM schwerwiegende Folgen haben und die Reputation des Unternehmens empfindlich beeinträchtigen. Deshalb ist der Schutz von Informationen und die Sicherstellung eines kontinuierlichen Geschäftsbetriebs von großer Bedeutung.

Aus diesen Gründen hat der Vorstand der CGM beschlossen, ein konzernweites Informationssicherheitsmanagement-System (ISMS) und ein konzernweites Business Continuity Management System (BCMS) einzuführen, aufrechtzuerhalten und zu verbessern. Diese Policy und deren konsequente Anwendung hat das Ziel Gefährdungen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationswerten vorzubeugen, die durch den unsachgemäßen Gebrauch von Informationen entstehen können, einschließlich Betrug und Veruntreuung, Industriespionage und Sabotage, Mängel und Nichtverfügbarkeit der internen und von unseren Kunden verwendeten IT-Systeme. Zudem sollen zeitkritische Prozesse und Ressourcen abgesichert und auch in Notfällen oder Krisen auf einem definierten Niveau verfügbar sein.

Das ISMS und das BCMS richten sich an den internationalen Standards ISO/IEC 27001 bzw. ISO/IEC 22301 aus und sind keine autarken Managementsysteme, sondern haben Schnittstellen sowohl untereinander als auch zu anderen Disziplinen, z. B. dem Enterprise Risk Management, dem Datenschutz (vgl. Kap. 4.6) oder dem Qualitätsmanagement.

Diese Policy legt überdies die notwendigen Mindestmaßnahmen fest, um gegen rechtliche Vorwürfe wie Fahrlässigkeit, Verletzung der treuhänderischen Pflicht oder Verstöße gegen die Datenschutzbestimmungen vorzubeugen. Die Policy definiert Grundregeln, mit denen jeder bei CGM, Lieferanten und Partnern vertraut sein und diese konsequent befolgen muss..

B. Geltungsbereich dieses Dokuments

Diese Policy zu Informationssicherheitsmanagement (ISM) und Business Continuity Management (BCM) ist für jeden Mitarbeiter und alle Tochtergesellschaften der CGM verpflichtend. Externe Mitarbeiter, Lieferanten und Partner sind im angemessenen Maße entweder vertraglich auf die Einhaltung zu verpflichten oder haben über eigene adäquate ISM- und BCM-Standards zu verfügen.

Diese Policy gilt nicht nur für elektronisch verarbeitete und gespeicherte Daten, sondern auch für gesprochenes Wort und in Papierform vorliegende Informationen.

Weitere Detailregelungen zu organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind grundsätzlich in separaten Richtlinien zum ISM und BCM geregelt.

C. Zuständigkeit für dieses Dokument

Der CISO (Chief Information Security Officer) legt die Inhalte der Policy fest und kommuniziert diese innerhalb der CGM. Verantwortlich für die kontinuierliche Pflege und Weiterentwicklung dieser Policy ist der Information Security Manager.

Auf Ebene der Segmente, Divisionen, Business Areas, Business Units und Functional Units sind die jeweiligen Linien-Manager für die Umsetzung und Einhaltung dieser Policy verantwortlich. Diese gewährleisten, dass alle Mitarbeiter eine angemessene Schulung zur Informationssicherheit und dem Business Continuity Management erhalten.

Alle internen und externen Mitarbeiter sind verpflichtet, diese Policy zu befolgen.

D. Ziele des Informationssicherheits- und des Business Continuity Managements

Die Erfüllung von vertraglichen Vereinbarungen mit Kunden und Dienstleistern, die Einhaltung der gesetzlichen Vorschriften sowie die damit verbundenen Tätigkeiten stehen im Mittelpunkt der täglichen Arbeit der CGM. Ziel des ISM ist es, dass jede Art von Information, egal ob diese elektronisch gespeichert oder übertragen, auf Papier gedruckt, geschrieben oder in einem Gespräch übermittelt wird, immer angemessen geschützt und gespeichert wird.

Die grundlegenden Werte und Schutzziele der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit stehen dabei im Mittelpunkt.

Das übergeordnete Ziel des BCM ist die Fortführung der zeitkritischen Geschäftsprozesse der CGM und die Verfügbarkeit von Ressourcen (Gebäude und Infrastruktur, IT, Personal, Dienstleister) auch bei Eintritt einer Notfall- oder Krisensituation zu gewährleisten.

Das Hauptziel dieser Policy ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen auf allen Ebenen der Verarbeitung sicherzustellen und Schadensfälle mit hohen finanziellen Auswirkungen, Reputationsverlusten oder regulatorischen Verstößen zu vermeiden.

E. Ausrichtung des Informationssicherheitsmanagementsystems und Business Continuity Managementsystems (ISMS und BCMS)

Informationssicherheit und Business Continuity sind kein einmaliges Projekt, sondern erfordern ein zielgerichtetes und sich kontinuierlich verbesserndes Managementsystem, das sich an die stetig verändernden Rahmenbedingungen der CGM anpasst.

Kern dieser kombinierten Managementsysteme ist demnach der PDCA-Zyklus, welcher in der folgenden Abbildung grafisch dargestellt wird:

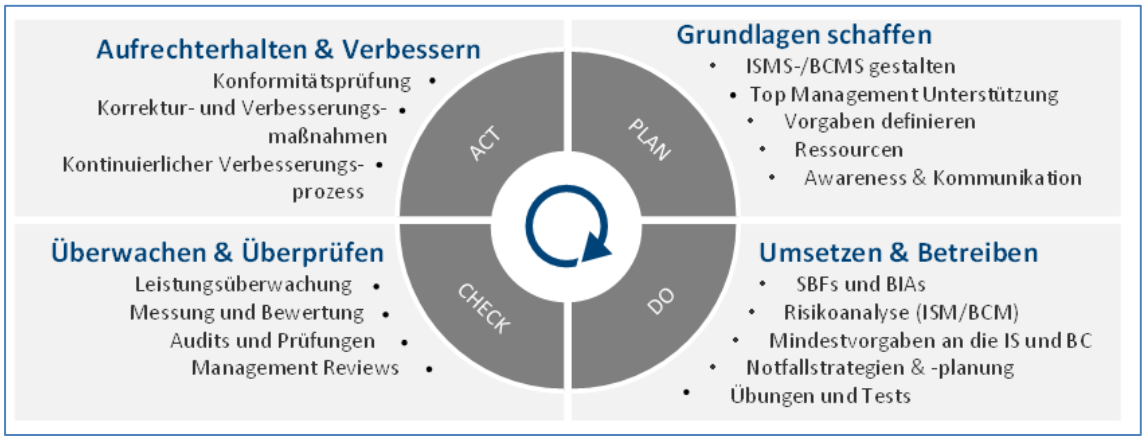

Figure 1 Übersicht der ISMS-/BCMS-Ablauforganisation

Mit Hilfe dieses Zyklus ist es der CGM möglich, die Managementsysteme strukturiert zu initiieren (PLAN), normkonform umzusetzen und zu betreiben (DO), kontinuierlich zu überwachen (CHECK) sowie gezielt kontinuierlich zu verbessern (ACT).

F. Governance-Modell des ISMS und des BCMS (Three Lines of Defense-Modell)

Die nachfolgend beschriebenen Rollen und Verantwortlichkeiten des Governance-Modells des ISMS und des BCMS der CGM sind an das Three Lines of Defense-Modell angelehnt.

Die zugrundeliegende Prämisse dieses Modells ist es, dass unter der Aufsicht und Leitung des CISO drei getrennte Gruppen (Verteidigungslinien) innerhalb der Organisation für eine effektive Verwaltung von Risiken im Bereich ISM und BCM erforderlich sind. Hierdurch werden die Rollen und Verantwortlichkeiten von Stakeholdern, die an den ISMS- und BCMS-Prozessen beteiligt sind, klar definiert.

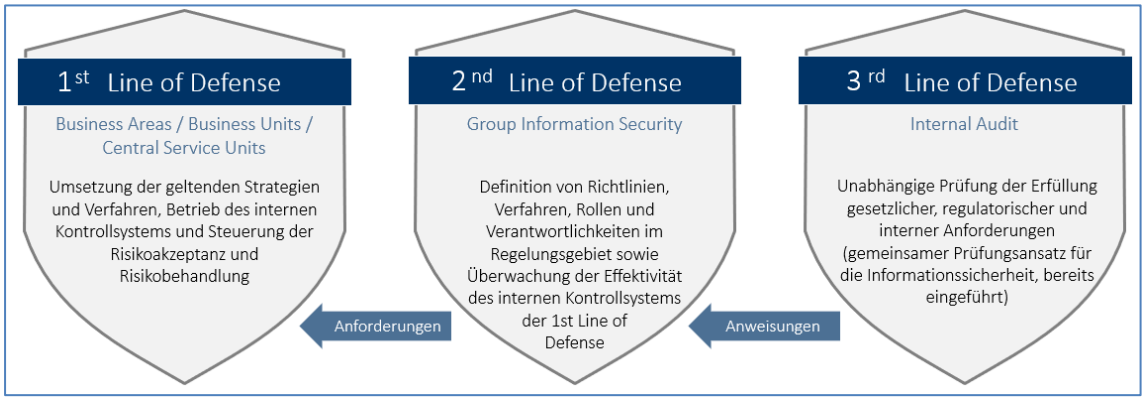

Figure 2 Three Lines of Defense Modell

1st Line of Defense – "Risikoeigentümerschaft"

Die erste Verteidigungslinie („1st Line of Defense“) bilden die Information Security Coordinator der Business Units und Service Units. Diese setzen die Vorgaben und Methodik aus der 2nd Line of Defense in ihrem Zuständigkeitsbereich um. Die 1st Line of Defense ist für die operative Identifikation, Bewertung, Steuerung und Behandlung von Risiken verantwortlich.

2nd Line of Defense – "Risikokontrolle"

Die zweite Verteidigungslinie („2nd Line of Defense“) bildet die Group Information Security innerhalb der CGM unter der Verantwortung des CISO. Die 2nd Line of Defense definiert Vorgaben und stellt

die Nutzung gleicher Methodiken und Verfahren für die Behandlung der Risiken durch die 1st Line of Defense sicher und kontrolliert die korrekte Umsetzung bzw. Anwendung.

3rd Line of Defense – „Risikoabsicherung “

Die dritte Verteidigungslinie („3rd Line of Defense“) stellt die Konzernrevision dar. Diese kontrolliert unabhängig die Vorgaben- und Kontrollmechanismen in der zweiten Verteidigungslinie sowie die Umsetzung und Wirksamkeit der Maßnahmen in der ersten Verteidigungslinie. Für Audits der ersten Verteidigungslinie wird ein gemeinsamer Audit-Ansatz in Zusammenarbeit mit der Group Information Security festgelegt.

G. Rollen und Verantwortlichkeiten der Informationssicherheit und des Business Continuity Management

Bei CGM sind eindeutige Rollen und Verantwortlichkeiten innerhalb der Themenfelder ISM und BCM etabliert. Diese sind in der Abbildung 3 dargestellt und im Folgenden beschrieben. Die konkreten Aufgaben der jeweiligen Rollen sind in den entsprechenden Jobprofilen dokumentiert.

Die Angemessenheit der Organisationsstruktur im ISM und BCM muss jährlich überprüft werden. Dabei müssen Veränderungen der Unternehmensstruktur berücksichtigt werden.

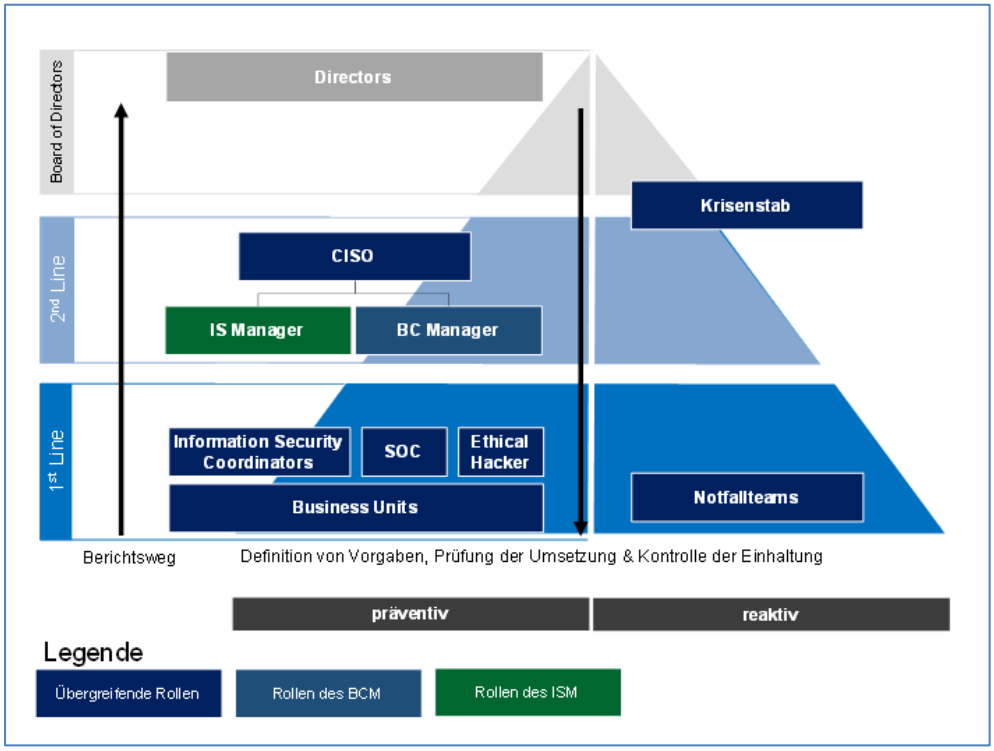

Figure 3 Sicherheitsorganisation der CGM

H. Änderungshistorie

Version	Release Datum	Name des Ersteller / Bearbeiter	Verifizierer	Releaser	Beschreibung der Änderung
1	22.11.2022	Robert Kisner	Jochen Klein	Managing Directors	Initial version
1.2	25.09.2023	Rober Kisner	Jochen Klein	Jochen Klein	Formatting change
1.3	12.11.2024	Mona Mürlebach	Sergiy Baranov	Holger Wess	Formatting changed to new QM template