SIA Informationssicherheitsmanagementsystem

Ziel dieses Dokuments:
Präsentation des Informationssicherheitsmanagementsystems von SIA.

1-CMS-2010-005-05
13. Oktober 2017

Das vorliegende Dokument ist Eigentum von SIA SpA. Alle Rechte vorbehalten.

Sein Inhalt darf ohne Einverständnis von SIA nicht vervielfältigt oder verbreitet werden.

ZUSAMMENFASSUNG

Alle Rechte vorbehalten

1. GRUNDSÄTZE DER INFORMATIONSSICHERHEIT

1.1 Einführung

SIA betrachtet Informationssicherheit als einen primären Aspekt des Schutzes seines Geschäfts und seiner Kunden.

Der Ruf des Unternehmens stützt sich auf seine physischen Vermögenswerte, wertvollen Informationen und Personalressourcen, und deswegen ist es von fundamentaler Bedeutung für seinen Fortbestand, dass ein Gerüst aus Sicherheitsrichtlinien den Schutz der Geschäftsprozesse und Informationen vor einer großen Bandbreite von Bedrohungen gewährleistet und den Einfluss solcher Bedrohungen auf die Kontinuität des Betriebs minimiert.

Die Haltung der SIA Security trägt außerdem zu weiter gefassten Sicherheitszielen bei, darunter zur Stärkung der Widerstandsfähigkeit des Finanz-Ökosystems als Ganzem gegen Bedrohungen aus dem Cyberspace, womit Erwartungen von Behörden, Aufsichts- und Regulierungsstellen und Kunden entsprochen wird.

1.2 Grundsatzerklärung

Verwaltungsrat und Geschäftsleitung unterstützen die effektive Verwaltung und Kontrolle der Informationssicherheit, indem sie:

- Eine Kultur der Informationssicherheit schaffen, die ein effektives Informationssicherheitsprogramm und die Rolle aller Arbeitnehmer beim Schutz der Dienstleistungen und Informationen, Systeme und Infrastruktur des Unternehmens fördern;
- Aufgaben und Verantwortlichkeiten in der Informationssicherheit im ganzen Unternehmen klar definieren und kommunizieren;
- Adäquate Ressourcen zur effektiven Förderung des Informationssicherheitsprogramms bereitstellen;
- ISO/IEC 27001 zum Referenzstandard für ihr Informationssicherheitsmanagementsystem machen.

Diese Grundsätze sowie damit verbundene Verfahren, die die zu befolgenden Anweisungen ausführlich beschreiben, gelten für alle Funktionen und Arbeitnehmer von SIA sowie alle Dritten, die unternehmenseigene Einrichtungen, Geräte und Systeme der Informations- und Kommunikationstechnik nutzen oder Zugang zu unternehmenseigenen Informationen haben oder diese aufbewahren oder beaufsichtigen.

Die Grundsätze der Informationssicherheit werden regelmäßig oder im Falle von wesentlichen Änderungen überprüft, um ihre fortgesetzte Eignung, Angemessenheit und Effizienz zu gewährleisten.

1.3 Ziele

Die Hauptziele des Informationssicherheitssystems von SIA sind:

- die Gewährleistung eines angemessenen Informationsschutzes hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit;
- der Schutz der Interessen von Kunden, Arbeitnehmern und Dritten;
- die Einhaltung der maßgeblichen Gesetze und Verordnungen zu Datenverarbeitung und Datenschutz sicherzustellen;
- die Sicherstellung von Standardrichtlinien zum Informationsschutz und des Managements damit verbundener Risiken;
- die effektive Reaktion auf die wachsenden Bedrohungen für das Informationssystem im Cyberspace.

Alle Rechte vorbehalten

Sie stellen die Grundlage für die Schaffung, Einführung, das Funktionieren, die Überwachung, Überprüfung, Wartung und dauernde Verbesserung eines wirkungsvollen Informationssicherheitsmanagementsystems dar, das nach dem ISO/IEC 27001-Standard konzipiert wurde.

1.4 Rollen und Verantwortlichkeiten

SIA fördert eine digitale Kultur, die sich der Sicherheits- und Datenschutzrisiken bewusst ist.

Eine Sicherheitskultur trägt zur Effizienz des Informationssicherheitsprogramms bei. Das Informationssicherheitsprogramm ist umso wirkungsvoller, wenn sicherheitsbezogene Prozesse fest in der Kultur von SIA verankert sind.

Zum Aufbau einer Sicherheitskultur ist das Informationssicherheitsmanagementsystem wie folgt organisiert:

- Der Einzelne

  Die Sicherheitsgrundsätze von SIA gelten für alle Arbeitnehmer sowie Dritten, die unternehmenseigene Einrichtungen, Geräte und Systeme der Informations- und Kommunikationstechnik nutzen oder Zugang zu unternehmenseigenen Informationen haben oder diese aufbewahren oder beaufsichtigen. Sie sind verantwortlich dafür, sich Verhaltensmaßnahmen zu eigen zu machen, die im Einklang mit dem Verhaltenskodex, den Sicherheitsrichtlinien, der Gesetzgebung und der geltenden Verträge stehen, unter besonderer Bezugnahme auf die Vertraulichkeitsbestimmungen und den Schutz personenbezogener Daten nach geltendem Recht.

- Geschäftsleitung

  Entsprechend ihrem Zuständigkeitsbereich - betrieblich oder technisch - sorgt die Geschäftsleitung als Verantwortliche für die Integration von Sicherheitsgrundsätzen sowie des Sicherheitsprogramms in die einzelnen Geschäftsbereiche, betrieblichen Prozesse, Supportfunktionen und das Drittunternehmen-Managementprogramm von SIA.

  Es ist auch ihre Aufgabe, Lieferanten und Berater, die im Auftrag des Unternehmens tätig sind, über die für die Informationsverarbeitung erforderlichen Informationsschutzrichtlinien und -verfahren zu informieren.

- Cybersicherheitsteam

  Wir haben ein engagiertes Team für Cybersicherheitsmanagement aufgestellt, um einen dynamischen, informations- und erkenntnisgestützten sicherheitstechnischen Ansatz in der Betriebsabteilung zu realisieren.

  In die Zuständigkeit der Funktion Cybersicherheit fallen alle der folgenden Aufgaben: die direkte Verwaltung und Steuerung der wichtigsten Sicherheitslösungen, die Schaffung von technischen Verfahren, die verschiedene Aspekte der Cybersicherheit abdecken, die zuverlässige Identifizierung, Abwehr und Reaktion auf Cyberangriffe durch Sicherheitsanalysen und -kontrollen, interne wie externe Instrumente und Informationsressourcen, ein zuverlässiges Sicherheitsmonitoring und die Durchführung von Sicherheitsprüfungen und Sicherheitsrisikobewertungen sowie die Erstellung der Sicherheitskonzepte für Projekte und Initiativen.

  Innerhalb der Cybersicherheit spielt das SIA CERT eine wesentliche Rolle bei der Verwaltung cybersicherheitsbezogener Ereignisse und der Einrichtung von Methoden zum Informationsaustausch zwischen den anerkannten Akteuren des Finanzökosystems.

- Sicherheitsbeauftragte

SIA S.p.A. ist für den Inhalt des vorliegenden Dokuments verantwortlich
Klassifizierung: Öffentlich
Alle Rechte vorbehalten

Für jede Hauptabteilung (d.h. jeden Bereich, Service-Bereich usw.) fungiert der oder die Sicherheitsbeauftragte als:

- Anlaufstelle in Sicherheitsfragen
- Unterstützung der zentralen Cybersicherheitsfunktion bei der Erkennung und Bewertung von Sicherheitsrisiken und -schwachstellen und den entsprechenden Abhilfemaßnahmen
- Unterstützung bei der Festlegung der Zugriffkriterien für die verschiedenen SIA-Levels und die Kommunikation an die an ihrer Umsetzung beteiligten Funktionen
- Mitglieder des Risiko- und Sicherheitsteams, die sich über den Status von Risiken, aufkommenden Bedrohungen, Maßnahmenpläne und Compliance in Sicherheitsfragen austauschen und diese Themen diskutieren.

- Risikokontrolle

  Eine Organisationseinheit für Cybersicherheitskontrolle wurde innerhalb der Risikokontrollabteilung, das heißt, innerhalb des Strategies, Risk, Finance & Control Department, geschaffen, die an den CEO berichtet.

  Diese Struktur gewährleistet, dass die Cybersicherheitskontrolle von den IT und Business Service Lines getrennt ist und dass Sicherheitsrisiken in einem integrierten Ansatz gemeinsam mit anderen Risiko- und Kontrollrichtlinien, d.h. Risikomanagement, Compliance und Betriebskontinuität, gesteuert werden.

- Risikoausschuss

  Der Risikoausschuss besteht aus den wichtigsten Spitzen- und Managementfunktionen.

  Regelmäßige Updates zu Cyberrisiken, Veränderungen in der Risikolandschaft und wesentliche Maßnahmen zur Risikoeindämmung werden vor diesem Hintergrund vorgestellt, damit der Vorstand etwaige Abweichungen von den Unternehmenszielen beurteilen kann.

Alle Rechte vorbehalten

2. INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM

Die Effizienz des Informationssicherheitsprogramms von SIA beruht auf:

- der Anwendung systematischer Risikobewertungsverfahren;
- der Durchführung situationsbezogener Sensibilisierungsmaßnahmen wie Risikoaufklärung und Informationsaustausch, da dies adaptive Risikomanagementverfahren sind;
- der Auswahl, Konzeption und Umsetzung von Maßnahmen zur Minderung von Sicherheitsrisiken;
- der Gewährleistung und Überprüfung der Effektivität der Sicherheitskontrollen;
- der Zweckdienlichkeit der Kontrollen und Effizienz des Informationsschutzsystems, und dessen dauerhafte Instandhaltung und Verbesserung mit Blick auf sich entwickelnde Bedrohungen im geschäftlichen, technologischen oder normativen Kontext.

2.1 Risikoerkennung, -prüfung und -bewertung

Um angemessenen Schutz zu bieten, werden ausgehend von einem risikobasierten Ansatz und unter Gewährleistung der Anwendung von aktuell vorhandenen Best Practices zur Sicherung der Einhaltung der maßgeblichen gesetzlichen Datenverarbeitungsbestimmungen Anforderungen festgelegt, Kontrollen eingeführt, Wartungen, Prüfungen und Verbesserungen durchgeführt.

Der risikobasierte Ansatz definiert sich durch Methoden und Instrumente, die zur Erkennung, Einschätzung und Handhabung von Informationssicherheits- und Cybersicherheitsrisiken geeignet sind.

Maßnahmen zur Handhabung werden im Rahmen des Plans zum Umgang mit Sicherheitsrisiken (Security Risk Treatment Plan) überwacht, und in der Anwendbarkeitserklärung ist die Liste der im Kontext von SIA anwendbaren Kontrollen festgelegt.

Ein systematischer Ansatz im Informationssicherheitsrisikomanagement ist eine Säule des Enterprise Risk Management Frameworks, indem er eine integrierte Sicht auf alle operativen Risiken bietet, die das Geschäft und die internen Dienste betreffen, und eine Sicherheitsorganisation festlegt, die den Anforderungen der Geschäfts- und Risikozielsetzungen bei SIA genügt. Unter den Informations- und Cybersicherheitsrisiken unterscheidet man das betriebliche Risiko, das als Ausfall- oder Verlustrisiko infolge inadäquater oder fehlgeschlagener Verfahren, menschlicher oder Systemfehler definiert ist.

2.2 Aufklärung und Informiertheit über Risiken

Zusätzlich zum risikobasierten Ansatz diktieren uns die bedeutenden und häufigen Veränderungen in Geschäfts- und technischen Szenarien sowie die zunehmende Raffinesse der kriminellen Praktiken eine adaptive Sicherheitshaltung, die akute Bedrohungen entdeckt und in der Lage ist, darauf effektiv zu reagieren.

Die Informationsbeschaffung und Aufklärung über Risiken bietet diese Vorteile und trägt dazu bei, dass im risikobasierten Ansatz stets aktuelle Risikoszenarien berücksichtigt werden.

Das SIA CERT beschäftigt sich intensiv mit den Fragen der Sammlung und Analyse von Informationen über Bedrohungen aus dem Cyberbereich im Kontext situativer Sensibilität und dessen, wie es die Organisation dabei unterstützen kann, ihr eigenes Informationsumfeld proaktiv zu verteidigen.

2.3 Informationssicherheitsschulungen und Sensibilisierung

SIA betrachtet die Informationssicherheitskultur als Schlüsselwert unseres Unternehmens, und daher wird sie in einem ständigen Schulungs- und Informationsprozess weiterentwickelt.

Alle Rechte vorbehalten

SIA setzt sein Sensibilisierungsprogramm durch Multimedia-Schulungen, Tests und Übungen, die Teilnahme an speziellen Trainingskursen sowie jeglichen anderen Initiativen um, die der Verbreitung der Kenntnisse über und Sensibilität für Sicherheitsaspekte im Unternehmen dienlich sein können.

Alle Mitarbeiter nehmen in regelmäßigen Abständen an Schulungen zur Sensibilisierung für die Informationssicherheit teil, die ihren täglichen Aufgaben und ihrer jeweiligen Funktion innerhalb der Informationssicherheit entsprechen.

2.4 Richtlinien zur Informationssicherheit und Betriebskontinuität

SIA hat einen Dokumentensatz zu Sicherheitsthemen festgelegt, der die Sicherheitsgrundsätze sowie die Richtlinien und Verfahren zur Sicherheit und Betriebskontinuität umfasst.
Die Formalisierung der sicherheitsbezogenen Formerfordernisse und die Erstellung der entsprechenden Dokumentation auf mehreren Ebenen erlauben die Definition und die Bezeichnung von Kontrollen und Steuerungsmechanismen für einzelne Arbeitstätigkeiten.

Richtlinien zur Sicherheit und Betriebskontinuität werden gemäß ISO/IEC 27001 Anlage A Kontrollen, PCI DSS Anforderungen, Datenschutzverordnungen und sonstigen maßgeblichen branchenspezifischen Best Practices gestaltet. Diese Richtlinien werden mit Blick auf die Ergebnisse der Risikobewertung, Anpassungen der Gesetze und Standards sowie der Weiterentwicklung der Technologie- und Risikolandschaft regelmäßig überarbeitet.

Zudem sind spezifische Kontrollen in SIA-interne Prozesse und Verfahren wie die Identitäts- und Zugriffsverwaltung, den Serviceentwicklungslebenszyklus, das Änderungs-, Service-, Schwachstellen- und Störfallmanagement eingebettet.

Richtlinien zur Sicherheit und Betriebskontinuität liefern Kriterien, Anforderungen und Kontrollen, die dazu dienen, den Zielen der Informationssicherheitsgrundsätze Wirksamkeit zu verleihen.

2.4.1 Organisationssicherheit

Menschen sind ein Erfolgsfaktor für den Aufbau einer effektiven Informationssicherheit im Unternehmen.

Kriterien und Kontrollen werden festgelegt, um das menschliche Risiko zu kontrollieren, das durch fehlendes Wissen und fehlende Sensibilität hinsichtlich Sicherheit und Betriebskontinuität sowie durch innovative Arbeitsmethoden (z.B. Telearbeit) entsteht, und um betrügerisches Verhalten zu verhindern.

Die für die Personalverwaltung zuständigen Unternehmensfunktionen müssen diese Kriterien bei der Einführung von Arbeitsmethoden, den Rollen, Schulungen, Arbeitsinstrumenten und Mitarbeiterbewertung während ihres gesamten Lebenszyklus anwenden.

Die Richtlinien umfassen allgemeine Regeln zu:

- Personalauswahl und -beschaffung
- Rollen und Verantwortlichkeiten in den Bereichen Sicherheit und Betriebskontinuität
- Schulungen und Sensibilisierung in den Bereichen Sicherheit und Betriebskontinuität
- Identitäts- und Zugriffsverwaltungssystem
- Disziplinarsystem

Alle Rechte vorbehalten

2.4.2 Informationssystementwicklung

Sicherheit ist das Ergebnis eines auf fortwährende Verbesserung ausgerichteten Prozesses und ist als solches über den gesamten Lebenszyklus der Informationssysteme zu berücksichtigen und zu verfolgen.

Angemessene Sicherheitskontrollen müssen eingerichtet werden, um Themen der Informationssicherheit und Betriebskontinuität bei der Zusammenstellung von Anforderungen für neue Maßnahmen und bei ihrer Machbarkeitsbewertung einzubeziehen, um sicherzustellen, dass die verbundenen Risiken bereits in den Anfangsphasen erkannt und behandelt werden, und nicht erst nach Ausarbeitung der Lösungen.

Bezüglich Dritter, die an der Informationssystemakquise, dem Entwicklungs- und Wartungsprozess beteiligt sind, müssen Informationssicherheitsanforderungen in jeden Vertrag oder jede Service-Level-Vereinbarung aufgenommen werden.

Das Dokument enthält unter anderem Richtlinien zu:

- der Anforderungsdefinition für Informationssicherheit und Betriebskontinuität
- Prinzipien für Sichere Entwicklung und Engineering
- die ausgelagerte Entwicklung von Informationssystemen

2.4.3 Informationssystemverwaltung

Effektive Sicherheitslevels lassen sich durch gewissenhafte Routineverwaltung der Informationssysteme erreichen.

Angemessene Sicherheitskontrollen müssen eingerichtet werden, um die gesicherte Funktion der Informationssysteme zu gewährleisten und die Risiken im Zusammenhang mit vorsätzlichen und zufälligen Bedrohungen wie Datenverlust, Änderungen an Systemen, Netzwerken und Anwendungen, Erschöpfung von Systemressourcen, Einführung von Schadcodes, die Erkennung und Verwaltung ausnutzbarer Schwachstellen abzufedern.

Diese Richtlinien müssen von den unternehmensinternen Funktionen angewendet werden, die für das Management und die Überprüfung der korrekten Entwicklung und Wartung von Systemen, Netzwerken und Anwendungen zuständig sind.

Diese Richtlinien umfassen allgemeine Regeln zu:

- Änderungsmanagement
- Protokollierung und Monitoring
- Datenbackups
- IT-Ressourcentrennung
- Schutz vor Malware
- Handhabung technischer Schwachstellen und Sicherheitstests
- Konfigurationsmanagement
- Entsorgung von IT-Geräten
- Verschlüsselung, digitales Zertifikatsmanagement und -kontrolle

Alle Rechte vorbehalten

2.4.4 Zugriffskontrolle

Eines der Sicherheitsziele ist, die Vertraulichkeit zu gewährleisten, das heißt, dass ausschließlich autorisierte Benutzer von der Eigenschaft der Information Kenntnis haben dürfen.

Spezielle Richtlinien geben Kontrollen zum Umgang mit den Risiken im Zusammenhang mit dem unbefugten Zugriff auf Informationen an; diese Risiken können IT-Betrugsfälle aufgrund von Datendiebstahl nach sich ziehen.

Der Zugriff auf Unternehmensinformationen und Informationssysteme muss über die Authentifizierung und das Authentifizierungsverfahren kontrolliert werden, aufgrund der Prinzipien für die korrekte Zuweisung von Zugriffsprivilegien, Sicherheitsregeln zur Identifikation und Authentifizierung von Benutzerprofilen und Systemen, die auf die Informationen zugreifen, und Methoden zur Definition von Zugriffsprivilegien und -rechten.

Alle internen und externen Mitarbeiter sind rechenschaftspflichtig für die Gewährleistung des Schutzes ihrer eigenen Anmeldedaten zur Autorisation.

Die Richtlinien umfassen allgemeine Regeln zu:

- Benutzer- und Systemzugriff hinsichtlich der Identifizierung, Authentifizierung und Autorisierung
- Verantwortlichkeiten der Benutzer für angemessenen Schutz
- Zugriff auf Netzwerkdienste und Netzwerkkontrollen
- Fernzugriff

2.4.5 Klassifizierung von Informationen

Informationen sind ein entscheidender Vermögenswert für jedes Unternehmen. Deshalb bedürfen Informationen eines angemessenen Schutzes, angesichts des Wertes, der ihnen vom Unternehmen selbst direkt oder indirekt zugeschrieben wird (Bewertung von Kunden, Regulierungsstellen oder Dritten). Unternehmensinformationen müssen stets auf Basis ihrer Sensibilität und Relevanz klassifiziert werden.

Kriterien zur Klassifizierung von Informationen werden festgelegt, um die Risiken im Zusammenhang mit der Missachtung der regulatorischen Pflichten bezüglich der Nichtbeachtung der anwendbaren Vorschriften und kritischen Punkten hinsichtlich der unbefugten Offenlegung oder Abänderung derselben auszuschalten und zu handhaben.

Die Klassifizierung ist ein zwingendes Erfordernis für die Durchführung des Risikobewertungsverfahrens.

Informationen muss ein Eigentumsstatus zugeordnet werden, damit gewährleistet ist, dass im Informationsklassifizierungsverfahren bestimmte Personen rechenschaftspflichtig bzw. verantwortlich für Informationen sind. Anforderungen an die Speicherung von Informationen sind bei Bedarf zu identifizieren. Die Klassifizierung von Informationen ist in regelmäßigen Abständen zu überprüfen.

Das Dokument enthält unter anderem Richtlinien zu:

- Informationsklassifizierungskriterien
- Dokumentenklassifizierung und -verwaltung

2.4.6 Physische Sicherheit

Informationssicherheit wird erreicht, indem der Schutz der gesamten physischen Infrastrukturen (wie Rechenzentren, Werke, IT-Ausrüstung und -Geräte) gewährleistet wird, die für das Funktionieren der Informationssysteme erforderlich sind.

Alle Rechte vorbehalten

Richtlinien sind vorhanden, um den Schutz der Informationssysteme vor unerlaubten physischen Zugriffen sowie Beschädigungen und Beeinträchtigungen von Verarbeitungsräumen und -geräten zu garantieren, um Verlust, Manipulation, Diebstahl oder Beeinträchtigung der Informationswerte, Betriebsunterbrechungen zu verhindern und Gesundheit und Sicherheit in den Arbeitsumgebungen zu gewährleisten.

Es gibt speziell zugeordnete Unternehmensfunktionen, die für die Verwaltung der Rechenzentren, der Unternehmensräume und des Unternehmensgeländes sowie der dazugehörigen Ausstattung in umfassender Zusammenarbeit mit der Sicherheits- und Betriebskontinuitätsfunktion zuständig sind.

Die Richtlinien umfassen allgemeine Regeln zu:

- Physische Bereichsklassifikation und Zuständigkeitsaufteilung
- Sicherheit des physischen Zugangs und der Umgebung
- Schutz von Standorten vor Naturkatastrophen und externen Bedrohungen
- Schutz der Arbeitsumgebungen

2.4.7 Sicherheitszwischenfallmanagement

Ein fundierter und effektiver Ansatz in der Unternehmenssicherheitspolitik wird durch die Entwicklung von Fähigkeiten und Instrumenten zur Bestätigung und Handhabung von Vorfällen erreicht, die eine Gefahr für Systeme und Informationssicherheit darstellen.

Es bedarf eines strukturierten Zwischenfallmanagementverfahrens, das alle nötigen Schutzmaßnahmen definiert, durch die eine rasche, effektive und systematische Reaktion auf tatsächliche und vermutete Informationssicherheitszwischenfälle gewährleistet ist.

Am Verfahren beteiligte Stellen sind: der Zuständige für das Zwischenfallmanagementverfahren, die am Zwischenfall- und Problemmanagementverfahren beteiligten technischen Strukturen, Ansprechpartner für Kunden und Behörden, die für das Sicherheits- und Betriebskontinuitätsmanagement verantwortlichen Funktionen, jeder Arbeitnehmer, der mögliche Sicherheitszwischenfälle meldet.

Darüber hinaus haben alle Arbeitnehmer und externen Vertragspartner die Pflicht, jegliche tatsächlichen oder vermuteten Informationssicherheitszwischenfälle unverzüglich zu melden.

Das Dokument enthält unter anderem Richtlinien zu:

- Cybersicher-Zwischenfallmanagementprozess
- Verantwortlichkeiten der Arbeitnehmer beim Störungsmanagementprozess
- Aufklärungs- und Informationsmöglichkeiten über Cyberrisiken

2.4.8 Lieferantenverwaltung

Gewöhnlich konzentrieren sich versuchte Angriffe auf größere und strukturiertere Unternehmen auf die schwächsten Glieder der Kette, was in unserem Fall die Lieferanten sein dürften.

In den hierfür geltenden Richtlinien werden Vorschläge für die Definition von Maßnahmen und Vereinbarungen mit dem Lieferanten unterbreitet, damit nicht die gesamte Sicherheits- und Betriebskontinuitätsebene geschwächt wird, und damit folglich Lieferanten zum Faktor werden können, der zur Erreichung der Geschäftsziele beiträgt.

Diese Richtlinien gelten für alle Unternehmensfunktionen, die für die Auswahl und Verwaltung von Lieferantenbeziehungen Verantwortung tragen.

Alle Rechte vorbehalten

2.4.9 Betriebskontinuität

Aufgrund der zunehmenden Komplexität der Finanzdienstleistungen und ihrer unterstützenden Infrastrukturen, der intensiven Nutzung von Informationstechnologien sowie der Erwartungen von Kunden und Aufsichtsbehörden ist es für Organisationen wie SIA unerlässlich, dass sie ihre Maßnahmen und Bemühungen zur Gewährleistung eines adäquaten Levels der Betriebskontinuität konsolidieren.

Die Realisierung eines Betriebskontinuitätsmanagementsystems und verbundener Aktivitäten (z.B. die Erstellung von Kontinuitätsplänen, die Performance von Text- Sensibilisierungsmaßnahmen) gestatten die Definition von Rollen, Instrumenten, Verfahren und Fertigkeiten zur Bewältigung von Risikoszenarien, deren Folge wäre, dass Büros und/oder Geräteräume in den Dienstversorgungsstandorten infolge von Naturereignissen oder menschlichem Handeln nicht zur Verfügung stehen, oder auch, dass kein Personal verfügbar ist.

Diese Richtlinien müssen von den Mitarbeitern von Abteilungen/Bereichen mit einer Rolle im Betriebskontinuitätsmanagementsystem angewendet werden, und von Unternehmensfunktionen, die an der Definition und Verwaltung von Disaster Recovery Infrastrukturen, an der Steuerung der externen Kommunikation und der Beschaffung von Waren und Dienstleistungen beteiligt sind.

2.4.10 Compliance in Sicherheitsaspekten

Im Rahmen der Integration mit der Compliance Governance des Unternehmens berücksichtigt das Informationssicherheitskontrollsystem die gesetzlichen Anforderungen und branchenspezifischen Bestimmungen (zum Beispiel den Datenschutzkodex (Privacy Code) [4], PCI-DSS [6]) zum Schutz und zur Verarbeitung von Informationen.

Die entsprechenden Richtlinien zielen darauf ab, Verstöße gegen das Gesetz, Regelungen, Bestimmungen oder vertragliche Pflichtklauseln bezüglich aller betroffenen Informations- und Sicherheitsanforderungen zu vermeiden.

Alle relevanten gesetzlichen, regulatorischen, vertraglichen und betrieblichen Anforderungen und Standards, die für die Informationen und Informationssysteme von SIA maßgeblich sind und sich auf die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen auswirken, müssen identifiziert, dokumentiert und an ICT kommuniziert werden.

Die Richtlinien sind von den Mitarbeitern anzuwenden, die für die Bestimmung der Anforderungen im Zusammenhang mit Gesetzen, Vorschriften und Standards, die Beachtung der sich daraus ableitenden Pflichten und Kontrollen und die Aufrechterhaltung des Compliance-Levels verantwortlich sind.

2.5 Effizienz des Informationssicherheitsmanagementsystems

Das Informationssicherheitsprogramm wird regelmäßig überarbeitet, um die kontinuierliche Steigerung der Effizienz des Programms sicherzustellen.

Die Überarbeitungen betreffen die Veränderungen im Kontext der Umgebung, in der das Programm funktioniert, hinsichtlich Entwicklungen bei den Gefahren, der technologischen, regulatorischen oder geschäftlichen Landschaft, sowie bei den Erwartungen von Interessengruppen an die Sicherheitshaltung von SIA. Es werden Schlüsse aus Erfahrungen und Auditergebnissen und anderen Indikatoren für Verbesserungsmöglichkeiten gezogen und daraufhin entsprechende Anpassungen am Programm vorgenommen.

SIA S.p.A. ist für den Inhalt des vorliegenden Dokuments verantwortlich
Klassifizierung: Öffentlich
Alle Rechte vorbehalten

2.5.1 Sicherheitstests

Sicherheitstests sind ein Bestandteil des Anwendungs- und Systementwicklungslebenszyklus. Dies und die Entwickler von Weiterqualifizierungsmaßnahmen sorgen dafür, dass Sicherheit in den persönlichen Verantwortungsbereich aller Teams rückt, die am Informationssystem-Lebenszyklus beteiligt sind.

Umfassende Sicherheitstests beinhalten unter anderem:

- Schwachstellenanalyse;
- Penetrationstests;
- statische und dynamische Anwendungssicherheitstests;
- Simulationen und Übungen;

wobei beide Teile des Prozesses abgedeckt werden: a) die Konzipierung des IT-Systems und b) der Betrieb des IT-Systems.

Sämtliche Maßnahmen im Rahmen der Sicherheitstests sind Kontrollpunkte, an denen anhand bekannter Cyber-Schwachstellen und Angriffsszenarien gemessen wird, wie gut das Unternehmen gegen Cyberangriffe gerüstet ist.

2.5.2 Messgrößen

Es werden Messgrößen bestimmt, anhand derer das Maß der Umsetzung des Sicherheitsprogramms und seine Effektivität demonstriert werden. Messgrößen dienen der Messung der Umsetzung der Sicherheitsgrundsätze, der Konformität mit dem Informationssicherheitsprogramm, der Zweckdienlichkeit der Erbringung der Sicherheitsdienstleistungen sowie der Auswirkung von Sicherheitsereignissen auf Geschäftsprozesse.

2.5.3 Audits und Prüfungen

Interne Audits und Prüfungen werden durchgeführt, um Informationen darüber zu liefern, wie das Informationssicherheitsmanagementsystem realisiert und aufrechterhalten wird.

2.6 Verhältnis zu externen Stakeholdern

SIA unterhält starke Beziehungen in Bezug auf Sicherheitsangelegenheiten mit Kunden, relevanten Behörden und Sicherheitssachverständigengruppen, sowohl auf nationaler, als auch auf europäischer Ebene, ebenso wie mit Lieferanten und anderen Unternehmen und Tochtergesellschaften der SIA-Gruppe.

- Die Zusammenarbeit ist der Schlüssel zum Management der Beziehungen mit Kunden und relevanten Behörden.

  In der Tat wird bleibt der Informationsfluss hinsichtlich Sicherheitszwischenfällen oder akuten Bedrohungen zwischen SIA und den Kunden ununterbrochen.

  Daneben wurden mit Unterstützung der SIA CERT zuverlässige Kanäle zu wichtigen Kollegen und Geschäftspartnern aufgebaut, über die Informationsaustauschpraktiken im Finanzmarktökosystem zum Einsatz kommen.

  SIA arbeitet aktiv mit Einrichtungen wie ENISA, CNAIPIC (z.B. Italiens nationales Zentrum für Computerkriminalität zum Schutz kritischer Infrastrukturen) und CERTs zusammen und trägt so dazu bei, die kollektive Widerstandfähigkeit einer breiteren Gemeinschaft gegen Cyberkriminalität zu

Alle Rechte vorbehalten

steigern.

- Kontrolle und Überwachung sind Schlüsselfaktoren im Lieferanten- und Drittparteimanagement. SIA verfolgt die folgenden beiden Hauptdirektiven:
  - die Regelung von Sicherheitsanforderungen und -pflichten in Verträgen mit Dritten und Lieferanten;
  - die Ausweitung der Risikomanagementverfahren auch auf die wichtigsten Lieferanten.

- Die Abteilung für Sicherheitskontrolle und Cybersicherheit (Security Governance and Cybersecurity) von SIA hat die Koordination von Sicherheitsfragen unter den Unternehmen und Tochtergesellschaften der SIA-Gruppe inne, um die Verwaltung der Minderung von Sicherheitsrisiken zu harmonisieren und effektiv zu machen.

SIA S.p.A. ist für den Inhalt des vorliegenden Dokuments verantwortlich
Klassifizierung: Öffentlich
Alle Rechte vorbehalten

ALLGEMEINE INFORMATIONEN

Definitionen

Akronym/Begriff	Definition
Verfügbarkeit	Eigenschaft, auf Anfrage einer befugten Einheit erreichbar oder zugänglich und nutzbar zu sein
Vertraulichkeit	Eigenschaft, dass Informationen unbefugten Einzelpersonen, Unternehmen oder Prozessen gegenüber nicht verfügbar gemacht oder offengelegt werden
Effizienz/Effektivität	der Umfang, in dem geplante Aktivitäten umgesetzt und geplante Ergebnisse erzielt werden
Informationssicherheit	die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
Integrität	Eigenschaft der Richtigkeit und Vollständigkeit
ISMS	Informationssicherheitsmanagementsystem
Managementsystem/Verwaltungssystem	Mehrere miteinander verbundene oder interagierende Elemente einer Organisation zur Schaffung von Richtlinien und Zielen und Verfahren zur Erreichung dieser Ziele
Risiko	Verunsicherungseffekt in Bezug auf Ziele. Im Kontext der Informationssicherheitsmanagementsysteme lassen sich Informationssicherheitsrisiken als Verunsicherungseffekt in Bezug auf Informationssicherheitsziele beschreiben.
SoA	Anwendbarkeitserklärung (Statement of j)
Bedrohung	die potenzielle Ursache eines unerwünschten Ereignisses, durch das einem System oder einer Organisation Schaden zugefügt werden könnte.

Verweise

[1] ISO/IEC 27000:2016 - Informationstechnologie. Sicherheitstechniken. Informationssicherheitsmanagementsysteme. Übersicht und Wörterverzeichnis

[2] ISO/IEC 27001:2013 - Informationstechnologie. Sicherheitstechniken. Informationssicherheitsmanagementsysteme. Anforderungen

[3] ISO/IEC 27002:2013 - Informationstechnologie. Sicherheitstechniken. Praxisrichtlinien für Informationssicherheitstechniken

[4] ISO 22301:2012 Sicherheit und Schutz des Gemeinwesens - Betriebskontinuitätsmanagementsysteme --- Anforderungen

[5] Verordnung 196/2003 - Gesetz zum Schutz personenbezogener Daten

[6] Verordnung 81/2008 - Konsolidiertes Gesetz zur Sicherheit am Arbeitsplatz

[7] Zahlungskartenbranche - Datensicherheitsstandard (Aktuell gültige Fassung)

[8] 1-CMS-2013-039: SIA - Prozesse und Managementsysteme (Aktuell gültige Fassung)

Alle Rechte vorbehalten

AUFSCHLÜSSELUNG DER ANGABEN AUF DEM UMSCHLAG

Dokumentstatus

Die Unterschriften auf dem Umschlag des vorliegenden Dokuments beziehen sich auf die internen Standards von SIA für die Dokumentationsverwaltung im Unternehmensverwaltungssystem. Sie dienen dazu, die Konfigurationskontrolle zu genehmigen und ihren Bearbeitungsstatus anzuzeigen.

Bitte beachten Sie, dass mit der Unterschrift zur ‚Genehmigung' lediglich die Freigabe zur Weitergabe des Dokuments an die Verteilerliste erteilt wird, dies jedoch in keiner Weise bedeutet, dass das Dokument durch externe Stellen geprüft und/oder angenommen wurde.

Genauer gesagt ist das Dokument als **VERFASST** zu betrachten, wenn es die Unterschrift/en der für seine Erstellung zuständigen Person/en trägt; als **GEPRÜFT,** wenn es die interne Prüfung erfolgreich durchlaufen hat und die Bestätigungsunterschrift/en trägt, mit denen seine Freigabe an das KONFIGURATIONSMANAGEMENT genehmigt wird. Bei einem negativen Prüfergebnis wird das Dokument geändert und erneut geprüft und erhält eine neue Versionsnummer und ein neues Ausstellungsdatum. Das Dokument ist als **GENEHMIGT** zu betrachten, wenn es zusätzlich zu den anderen Unterschriften die Genehmigungsunterschrift trägt.

Der Status eines nicht unterschriebenen Dokuments ist nicht festgelegt. Das Dokument darf somit nicht in Umlauf gebracht werden.

Klassifizierung

Mögliche Klassifizierungen eines Dokuments sind:

- **ÖFFENTLICH**, wenn das Dokument ohne Einschränkung weitergegeben werden darf;
- **INTERN**, wenn das Dokument nur innerhalb von SIA weitergegeben werden darf;
- **VERTRAULICH**, wenn das Dokument nur an eine beschränkte Anzahl von Adressaten weitergegeben werden darf;
- **STRENG VERTRAULICH,** wenn das Dokument nur an eine beschränkte Anzahl von Adressaten weitergegeben werden darf und jedes Exemplar kontrolliert wird;

Anwendungsbereich

Unternehmen in der SIA-Gruppe, für die das Dokument gilt:

SIA-Gruppe wenn das Dokument für alle Tochtergesellschaften der SIA-Gruppe Gültigkeit hat

SIA SPA wenn das Dokument ausschließlich für SIA Gültigkeit hat

…**Liste der Bezeichnungen der Gruppenunternehmen**…**,** wenn das Dokument nur für einige Unternehmen der Gruppe Gültigkeit hat

Alle Rechte vorbehalten