ISACA Switzerland Chapter

Nr. 01 | März 2023 | www.isaca.ch

NEWSLETTER

Neue Ausgabe von ISO 2001
Insbesondere bei den Kontrollen im Anhang A gibt es substantielle Änderungen **Seite 67**

Vielfalt an Normen und Standards
Verschaffen Sie sich einen Überblick über die riesige Vielfalt an Normen und Standards **Seite 69**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 71**

Aktuell: ISO 27001:2022

Im Oktober 2022 war es nach neun Jahren so weit, die ISO 27001:2022 wurde veröffentlicht. Vorneweg, es hat sich inhaltlich nicht sehr viel geändert. Eine grosse Tragweite haben aber die elf neuen Controls in Anhang A. Zeit also, genauer auf die Norm einzugehen.

Von Andreas Wisler

Lange mussten wir auf die neue Ausgabe warten, nach neun Jahren wurde Ende Oktober die neue Ausgabe herausgegeben. Bislang ist diese nur in Englisch verfügbar (https://www.iso.org/standard/82875.html). Mit der deutschen Übersetzung ist in ca. einem Jahr zu rechnen. Der Aufbau entspricht nun dem aus anderen ISO-Normen gewohnten Bild. Sei es ISO 9001 (Qualitätsmanagement), ISO 22301 (Business Continuity) oder weiteren, die Struktur ist nun identisch. Die Kapitel 9.2 (Internal Audit) und 9.3 (Management Review) haben Unterkapitel erhalten. Die Kapitel 10.1 (Neu: Continual improvement) und 10.2 (Neu: Nonconformity and corrective action) haben ihre Positionen gewechselt.

Aufgefallen ist, dass durchgängig «International Standard» durch «document» ersetzt wurde. Die Definitionen von Begriffen sind schon länger in ISO 27000 enthalten und können kostenlos unter https://www.iso.org/obp abgefragt werden.

Änderungen

Nachfolgend wird auf die geänderten Text-Passagen eingegangen (Hinweis: Deutsche Übersetzungen sind vom Autor. Diese können von der zukünftigen offiziellen Version abweichen):

- Im Kapitel 4.2 (Understanding the needs and expectations of interested parties / Verstehen der Erfordernisse und Erwartungen interessierter Parteien) wurde ein weiterer Punkt ergänzt: Die Organisation muss festlegen, welche dieser Anforderungen durch das Informationssicherheits-Managementsystem (ISMS) erfüllt werden sollen.
- Im Kapitel 4.4 (ISMS) wurde der bestehende Satz mit dem fetten Teil ergänzt: «Die Organisation muss in Übereinstimmung mit den Anforderungen dieses Dokuments ein ISMS einrichten, umsetzen, aufrechterhalten und kontinuierlich verbessern, **einschliesslich der erforderlichen Prozesse und ihrer Wechselwirkungen.»**
- In Kapitel 5.1 (Leadership and commitment / Führung und Verpflichtung) kam eine Fussnote dazu, die erläutert, dass der Begriff «Business» weit ausgelegt werden kann, um Aktivitäten zu bezeichnen, die die für den Zweck der Organisation von zentraler Bedeutung sind.
- Viele Berater und Auditoren sind über die Fussnote 2 in Kapitel 6.1.3 (Information security risk treatment / Informationssicherheitsrisikobehandlung) froh. «Anhang A enthält eine Liste der möglichen Informationssicherheitskontrollen.» In vielen Audits gab es Diskussionen, ob nun alle Kontrollen umgesetzt werden müssen oder nicht. Diese sind zwar mit dem zusätzlichen Wort «möglichen» noch nicht ganz vom Tisch, aber es zeigt, dass hier Spielraum vorhanden ist.
- Das Erstellen einer SoA (Statement of Applicability / Erklärung zur Anwendbarkeit) wurde bereits mit dem Technical Corrigendium 2 im Dezember 2015 korrigiert und nun nochmals bestätigt.
- Im Kapitel 6.2 (Information security objectives and planning to achieve

them / Informationssicherheitsziele und Planung zu deren Erreichung) wurde zu den Informationssicherheitszielen «überwacht» und «als dokumentierte Informationen verfügbar sein» ergänzt.

- Ein neues Kapitel ist die 6.3: «Planung von Änderungen». Darin wird verlangt: «Wenn die Organisation feststellt, dass Änderungen am ISMS notwendig sind, müssen die Änderungen geplant durchgeführt werden.» Eigentlich selbstverständlich, aber nun auch als Muss-Anforderung enthalten.
- Das Kapitel 7.4 (Communication / Kommunikation) wurden die Punkte d) und e) als «wie kommuniziert wird» zusammengefasst.
- Einige Modifikationen hat das Kapitel 8.1 (Operational planning and control / Betriebliche Planung und Steuerung) erfahren. Es wird verlangt, dass zur Steuerung Kriterien für die Prozesse festgelegt und Kontrollen in Übereinstimmung mit diesen durchgeführt werden. Weiter müssen Dokumentationen so verfügbar sein, dass damit ein Nachweis über die korrekte Funktionsweise der Prozesse möglich ist. Auch wird auf extern bezogene Prozesse hingewiesen: «Extern bereitgestellte Prozesse, Produkte oder Dienstleistungen müssen kontrolliert werden.»
- Im Kapitel 9.1 (Monitoring, measurement, analysis and evaluation / Überwachung, Messung, Analyse und Bewertung) wurden die Sätze umgestellt, um den Lesefluss zu verbessern. Neu dazu gekommen ist, dass zum Nachweis der Ergebnisse dokumentierte Informationen verfügbar sein müssen.
- Das Kapitel 9.2 (Internal audit / Internes Audit) wurde komplett neu unterteilt. Es hat nun die Kapitel 9.2.1 (General / Allgemein) und 9.2.2 (Internal audit programme / Internes Auditprogramm). Inhaltlich hat sich aber nichts geändert.
- Analoges gilt auch für das Kapitel 9.3 (Management review / Managementbewertung). Es ist unterteilt in 9.3.1 (General / Allgemein), 9.3.2 (Management review inputs / Inhalte Managementbewertung) und 9.3.3 (Management review results / Resultate Managementbericht). Dazu gekommen ist in 9.3.2, dass auch Änderungen der Bedürfnisse und Erwartungen der interessierten Parteien, die für das ISMS relevant sind, behandelt werden.
- Wie bereits erwähnt, haben die Kapitel 10.1 und 10.2 ihre Positionen gewechselt. Inhaltlich hat sich aber nichts geändert.

Massnahmen-Gliederung

Die grosse Änderung ist im Anhang A zu finden: Information security controls reference, in der deutschen Ausgabe «Referenzmassnahmenziele und -massnahmen» genannt. Die Struktur wurde komplett neu aufgebaut. Anstelle von 114 sind es «nur» noch 93. Und dies, obschon elf neue dazu gekommen sind und nur eines gestrichen wurde. Einige der Massnahmen wurden sinnvollerweise zusammengefasst. Die dazu gehörende ISO 27002 wurde bereits Mitte Februar 2022 veröffentlicht. Ein Entwurf der deutschen Ausgabe wurde im August den interessierten Personen zur Verfügung gestellt.

Die Massnahmen werden in folgende Kategorien eingeteilt:

- Menschen (Kapitel 8, 34 Anforderungen), wenn sie einzelne Menschen betreffen;
- Physisch (Kapitel 7, 14 Anforderungen), wenn sie physische Objekte betreffen;

NEUE KONTROLLEN

Titel	Anforderung
5.7 Bedrohungsintelligenz (Englisch Threat intelligence)	Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten (Englisch Information security for use of cloud services)	Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.
5.30 IKT-Bereitschaft für Business Continuity (Englisch ICT readiness for business continuity)	Die IKT-Bereitschaft sollte auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.
7.4 Physische Sicherheitsüberwachung (Englisch Physical security monitoring)	Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.
8.9 Konfigurationsmanagement (Englisch Configuration management)	Konfigurationen, einschliesslich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.
8.10 Löschung von Informationen (Englisch Information deletion)	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.
8.11 Datenmaskierung (Englisch Data masking)	Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.
8.12 Verhinderung von Datenlecks (Englisch Data leakage prevention)	Massnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.
8.16 Überwachung von Aktivitäten (Englisch Monitoring activities)	Netzwerke, Systeme und Anwendungen sollten auf anormales Verhalten überwacht und geeignete Massnahmen ergriffen werden, um potenzielle Informationssicherheitsvorfälle zu bewerten.
8.23 Webfilterung (Englisch Web filtering)	Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.
8.28 Sicheres Coding (Englisch Secure coding)	Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.

- Technologisch (Kapitel 6, 8 Anforderungen), wenn sie die Technik betreffen;
- ansonsten werden sie als organisatorisch (Kapitel 5, 37 Anforderungen) eingestuft.

Neue Massnahmen

Die Tabelle auf der vorherigen Seite beschreibt kurz die elf neuen Kontrollen.

Wie geht es nun weiter?

Eine erste Zertifizierung nach der neuen ISO 27001:2022 ist in einigen Ländern bereits seit November möglich. Die Schweizerische Akkreditierungsstelle SAS (https://www.sas.admin.ch/) hat angekündigt, dass sie ein halbes Jahr benötigt, um die Anforderungen an die Zertifizierungsstellen fertig zu stellen. Gemäss Abklärungen führen die Zertifizierungsstellen ab April 2023 Zertifizierungen nach der neuen Norm durch.

Die letzte Möglichkeit für eine Erst- oder Rezertifizierung nach der alten ISO 27001:2013 (Englische Ausgabe) bzw. 2017 (Deutsche Ausgabe) ist 18 Monate, bzw. April 2024. Hinweis: damit sind nicht die Aufrechterhaltungs-Audits gemeint.

Bestehende Zertifizierungen haben eine Gültigkeit von 3 Jahren, d.h. max. bis Oktober 2025. Bis dahin müssen alle Informationssicherheitsmanagementsysteme (ISMS) auf die neue Norm angepasst sein.

Fazit

Die neue Ausgabe der ISO 27001:2022 hat vor allem kosmetische Änderungen erfahren. Einige Klarstellungen sind vorhanden, aber ein Wechsel benötigt keinen riesigen Aufwand. Dieser versteckt sich in den angepassten Massnahmen. Vor allem die elf zusätzlichen Kontrollen bescheren einiges an Aufwand. Auch wenn noch drei Jahre Zeit bis zum Wechsel bleiben, sollte sich jedes bereits zertifizierte Unternehmen damit auseinandersetzen und einen Projektplan zur Migration erstellen, damit nicht am Ende doch noch ein (unnötiger) Zeitdruck entsteht.

DER AUTOR

Andreas Wisler ist Inhaber der Firma goSecurity AG (https://goSecurity.ch). Er ist CISA, CDPSE, ISO 22301, 27001 sowie der erste Schweizer ISO 27701 Lead Auditor. Seit über 20 Jahren ist er im IT-Sicherheitsbereich tätig und unterstützt Firmen beim Aufbau eines ISMS und der Erlangung des ISO 27001 Zertifikats. Alle zwei Wochen veröffentlicht er den Podcast «Angriffslustig», zu abonnieren unter https://angriffslustig.ch.

Den Überblick behalten ist schwierig

Eine schier unglaubliche Vielfalt an Normen und Standards

Peter R. Bitterli, CISA, CISM, CGEIT, CRISC, CDPSE

Wenn ich den obigen Artikel von Andreas Wisler zur Aktualisierung von ISO27001/2 lese, werde ich ganz nostalgisch: Ich mag mich noch gut erinnern an den damals visionären DTI Code of Practice for Information Security Management, der anfangs der 90er erstmals veröffentlicht und dann 1995 fast wortwörtlich in den British Standard BS7799 umgewandelt wurde. Damals war die Welt der Informationssicherheits-Standards noch einfach: In meiner Erinnerung gab es BS7799 und sonst nichts. Daraus wurden dann mit der Zeit eine Serie mit immer mehr Standards – unterdessen sind es wohl rund 40, wobei sich teils mehrere zum selben Thema äussern.

Die Bedürfnisse beschränken sich aber nicht nur auf eine angemessene Informations-/IT-Sicherheit: Relativ früh gab es Bestrebungen, Risiken im Bereich der Rechnungsabschlüsse durch den Einsatz entsprechender Gesetze, Standards und Normen zu reduzieren (z.B. Sarbanes-Oxley Act, SOC1 und SOC2, Basel II/III, Gramm-Leach Bliley Act). Aktuell erscheint gefühlt fast im Sekundentakt irgendein neuer Cyber- und andere Sicherheitsstandard: NIST CSF, CIS, NY CRR 500, usw. um nur einige zu nennen – viele davon mit einem vorgegebenen Set an je vielleicht 100 oder auch mehr Kontrollen (im Kasten sind ein paar der in der Schweiz bekannteren dieser Standards aufgeführt).

Ein einzelnes Unternehmen hat meist die Möglichkeit, sich auf einen dieser Standards zu fokussieren. Von einem Provider wird aber erwartet, dass er sämtliche Kontrollen/Sicherheitsmassnahmen aus allen passenden Standards implementiert hat und dies auch bestätigen kann. Entsprechend schmücken viele Provider

ihre Webseite mit einer Sammlung von Zertifikaten und/oder Attestierungen.

Wenn man das Ganze etwas genauer betrachtet, merkt man rasch, dass es zwischen den verschiedenen Standards zu einem bestimmten Thema wie z.B. Cyber Security nicht allzu grosse Unterschiede gibt. Das ist nicht wirklich erstaunlich, weil alle themenspezifischen Standards mehr oder weniger dieselben Risiken abdecken und damit in der Regel auch sehr ähnliche Sicherheitsmassnahmen (Kontrollen) aufführen. Als Unternehmen sollte man sich daher wohl auf den einen (z.B.) Cyber Security-Standard fokussieren, der für die meisten Stakeholder passend ist.

Bohrt man bezüglich Standard-Vielfalt noch etwas tiefer, stellt man fest, dass auch viele Standards aus höchst unterschiedlichen Fachbereichen sehr ähnliche Kontrollen aufweisen. Zum «Change Management» findet sich z.B. im Service Management-Standard ITIL eine Kontrolle, aber auch bei ISO27001, BSI 200, NIST 800 oder «sogar» im Schweizer Revisionshandbuch. Fast identische Kontrollen in unterschiedlichsten Standards lassen sich für enorm viele Themen finden (z.B. Incident Management, Business Continuity Management, Schutz der Privatsphäre, …).

Für unsere eigene Arbeit setzen wir seit Jahren ein minimalistisches Tool ein mit «allen» relevanten Kontrollen aus dem Handbuch für Wirtschaftsprüfer, aus dem uralten Vorgehensmodell IT-Risikoanalyse für KMU-Prüfer, aus dem IKT-Minimalstandard des Bundes (= NIST 800), aus ISA 315 revised, aus den beiden kürzlich aktualisierten FINMA-Rundschreiben 18/3 und 23/1 (vormals 08/21) und auch aus ISO27001 (aktuelle Version 2022). Je nachdem, auf welcher Abstraktionsebene man die Kontrollen auflistet, gibt es auf der Inputseite wohl rund 500 Kontrollen aus den hier aufgeführten Standards und Normen – auf der Outputseite aber nur rund 80, wovon weniger als die Hälfte wirklich relevant sind. Stark vereinfacht ausgedrückt heisst das:

1. Es gibt Überlappungen zwischen den verschiedenen Standards (eliminiert schon mal einen sehr grossen Teil der offensichtlich redundanten Sicherheitsmassnahmen).
2. Nur wenige der in den Standards aufgeführten Kontrollen sind für die Mehrheit der Stakeholder von Bedeutung, so dass sie (mindestens in einem Provider-Bericht) auch weggelassen werden können.

In Einzelfällen (z.B. bei einer verlangten ISO-Zertifizierung) kann es durchaus notwendig sein, dass man jede einzelne Detailmassnahme aus einem bestimmten Standard umsetzt. Aus meiner ganz persönlichen Optik macht es aber wesentlich mehr Sinn, sich als Unternehmen auf die vielleicht 30–50 Kontrollen zu fokussieren, welche den grössten Nutzen bringen – unabhängig davon, ob diese jetzt in einem internen Bericht an die obere Führungsetagen rapportiert oder in einem formalen ISAE3000-Bericht externen Stakeholdern zur Verfügung stellt.

Machen Sie sich fit !

Besuchen Sie die ISACA After Hours Events, die ISACA-Fachtagungen oder die ISACA-Zertifikatsausbildungen. Hier lernen Sie, in der riesigen Fülle an vorhanden Sammlungen von sinnvollen (und weniger sinnvollen) Kontrollen die Gemeinsamkeiten sowie die wirklich wesentlichen Schlüsselkontrollen zu erkennen. Für alle Personen aus dem Umfeld der IT-Revision, der IT- und/oder Informationssicherheit, dem (IT-) Risikomanagement, der IT-Governance und neu auch aus Data Privacy bietet das ISACA Switzerland Chapter eine seriöse Aus- und Weiterbildung in der Form von umfassenden Vertiefungskursen für CISA, CISM, CGEIT, CRISC und CDPSE an, welche den Teilnehmenden sowohl die notwendigen theoretischen Grundlagen (grösstenteils im Rahmen eines strukturierten Selbststudiums ab 1. Februar 2023) als auch die bewährte Berufspraxis (grösstenteils im Präsenzunterricht im Juni) vermitteln. Ausführliche und klar strukturierte Unterlagen mit Fachbüchern, Skript und Fallstudien dienen nicht nur zur Vorbereitung auf die internationale Zertifikatsprüfung, sondern auch als Nachschlagewerk im Berufsalltag (siehe www.itacs-training.ch).

Für Personen, welche sich (ausschliesslich) auf eine der internationalen Zertifikatsprüfungen vorbereiten wollen, gibt es verschiedene Anbieter mit kompakten Prüfungsvorbereitungskursen. Informieren Sie sich bei www.isaca.ch

ÜBERBLICK ÜBER DIE IN DER SCHWEIZ WOHL BEKANNTESTEN «SICHERHEITS»-STANDARDS

Thema Finanzen

- BCBS: Basel III IT Operations Controls
- GLBA: Gramm-Leach Bliley Act
- PCI DSS: Payment Card Industry Data Security Standards
- SOX: Sarbanes-Oxley Act

Thema Sicherheit allgemein & Cyber Security

- BSI: BSI 200-1, 200-2, 200-3: Informationssicherheit
- CIS: Center for Internet Security – Critical Security Controls
- CMMC: Cybersecurity Maturity Model Certification
- ISO270xx: Information Security (40 Standards)
- SOC Service Organization Control 2 Type II

Thema Persönlichkeitsschutz, Datenschutz

- NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information
- NIST 800-53 Security and Privacy Controls for Information Systems and Organizations
- GDPR: General Data Protection Rule
- HIPAA: Healthcare Insurance Portability and Accountability Act
- HITRUST: Healthcare Information Trust Alliance Common Security Framework

Meta-Standard

- COBIT 2019 mit unzähligen nahtlos integrierten «Zusatzpaketen»

DER AUTOR

Peter R. Bitterli, Bprex Group AG; CISA, CISM, CGEIT, CRISC, CDPSE

ISACA After Hours Seminare

Reservieren Sie sich die nächsten Termine:
Die After Hours Seminar des ISACA Switzerland Chapters sind ein beliebter Treffpunkt für Fachspezialisten aus den Bereichen Information Governance, Information Risk Management, Information Security und Information Audit/Assurance. Rund 40 bis 50 Personen besuchen regelmässig diese Anlässe um sich über aktuelle Themen zu informieren und Kontakte zu pflegen.

Die nächsten Termine sind:

- Dienstag, 04. April 2023
- Dienstag, 06. Juni 2023
- Dienstag, 22. August 2023
- Dienstag, 03. Oktober 2023
- Dienstag, 05. Dezember 2023

Die detaillierten Ausschreibungen aktualisieren wir laufend auf unserer Webseite. Bitte beachten Sie dort auch die aktuellen Hinweise zum Ort der Veranstaltung (Online oder lokal).

ISACA-TRAINING

Anbieter	Datum	Hauptthema – Kurstitel
ACTAGIS Govern your IT, Security & Business www.actagis.ch	20.-23.03.2023	CISA 4-day exam preparation course (Module 2) (E/F)
	20.-22.03.2023	CISM 3-day exam preparation course (Module 2) (E/F)
	20.-22.03.2023	CGEIT 3-day exam preparation course (Module 2) (E/F)
	08.-11.05.2023	CISA 4-day exam preparation course (Module 2) (E/F)
	08.-10.05.2023	CISM 3-day exam preparation course (Module 2) (E/F)
	08.-10.05.2023	CGEIT 3-day exam preparation course (Module 2) (E/F)
	08.-10.05.2023	CRISC 3-day exam preparation course (Module 2) (E/F)
	08.-09.05.2023	COBIT 2019 - 2-day course
glenfis www.glenfis.ch	13.-15.03.2023	CCAK - Certificate of Cloud Auditing Knowledge (D) 3 Tage
	03.-05.07.2023	CCAK - Certificate of Cloud Auditing Knowledge (D) 3 Tage
	27.-28.03.2023	COBIT 2019 Foundation (D) 2 Tage
	19.-20.06.2023	COBIT 2019 Foundation (D) 2 Tage
	25.-26.09.2023	COBIT 2019 Foundation (D) 2 Tage
	05.-06.06.2023	CSX Cybersecurity Fundamentals (D) 2 Tage
	06.-07.11.2023	CSX Cybersecurity Fundamentals (D) 2 Tage
itacs by Peter R. Bitterli training www.itacs-training.ch	01.03.2023	Start Selbststudium CISA, CISM, CGEIT, CRISC, CDPSE (Zertifikatskurse; Details siehe unten)
	22./23.03.2023	COBIT 2019: Intensivkurs – KEIN Foundation-Kurs: 2 Tage
	05.-23.06./26.-29.09.2023	CISA-Vertiefungskurs: 10 Tage Juni, 4 Tage September; Selbststudium berufsbegleitend ab 1.3.23
	05.-23.06./04.-06.10.2023	CISM-Vertiefungskurs: 10 Tage Juni, 3 Tage Oktober; Selbststudium berufsbegleitend ab 1.3.23
	05.-23.06./06.-08.09.2023	CGEIT-Vertiefungskurs: 10 Tage Juni, 3 Tage September; Selbststudium berufsbegleitend ab 1.3.23
	05.-23.06./13.-15.09.2023	CRISC-Vertiefungskurs: 10 Tage Juni, 3 Tage September; Selbststudium berufsbegleitend ab 1.3.23
	05.-27.06./11.-13.10.2023	CDPSE-Vertiefungskurs: 9 Tage Juni, 3 Tage Oktober; Selbststudium berufsbegleitend ab 1.3.23
	13.06.2023	(IT-) Risikomanagement – wirksam und sinnvoll umgesetzt (Kompaktkurs)

IMPRESSUM ISACA NEWS

ISACA Switzerland Chapter

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Sekretariat ISACA Switzerland Chapter, c/o BDO AG, Biberiststrasse 16, 4501 Solothurn
Erscheinungsweise: 4× jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch