Trust in, and value from, information systems

Switzerland Chapter

Nr. 01 | März 2014 | www.isaca.ch

NEWSLETTER

Datenschutz
Verantwortungen und Massnahmen im Zusammenhang mit personenbezogenen Daten. **Seite 67**

IT-Strategiep als Instrument der IT-Governance
Gliederung und Entwicklung des Strategieprozesses **Seite 70**

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

Welcher Schutz ist wichtig für unsere Daten?

Die Sicherheit der Daten ist ein wichtiges Thema: Verantwortungen und Massnahmen im Zusammenhang mit personenbezogenen Daten.

Von Davide Vazzari

Die Einhaltung der Datenschutzgesetze interessiert immer mehr.

Unternehmen müssen dafür sorgen, dass ihre Daten rechtmässig bearbeitet und geschützt werden. Ein Datenverlust oder eine Datenmisshandlung stellen ein Fehlerrisiko sowie ein potentieller Bruch des Datenschutzrechtes dar, deren Konsequenzen eine Geldstrafe und einen Reputationsschaden beinhalten. In diesem Kontext spielen Unternehmensprozesse und IT-Systeme eine wichtige Rolle, indem sie eine rechtmässige Bearbeitung der Daten definieren und angemessene Kontrollen sicherstellen. Der Artikel beginnt mit einer Kurzübersicht zum Datenschutzrecht und den hauptsächlichen gesetzlichen Anforderungen im Bereich der personenbezogenen Daten. Im zweiten Teil des Artikels werden wir auf die Rolle des Internen Kontrollsystems (IKS) im Zusammenhang mit der Sicherheit von Daten und der Einhaltung des Datenschutzgesetzes eingehen. Der angewendete Ansatz basiert auf dem COBIT-Modell und ist auf die Enabler der Organisationsziele im Zusammenhang mit Datenschutzrecht fokussiert. Obwohl jede Organisation ihre eigene Besonderheit hat, die die Governance und das Management von Organisationen beeinflussen, kann man bestimmte Enabler identifizieren.

Der Artikel beinhaltet somit eine Anwendung des COBIT-Modelles im Bereich des Datenschutzrechtes mit konkreten Beispielen über eine mögliche Strategie zur Minderung der Risiken im Zusammenhang mit personenbezogenen Daten.

Datenschutzrecht in Europa

Zum Datenschutzrecht gehören alle Gesetze, Verordnungen und Gerichtsentscheide, die dem Schutz der Privatsphäre dienen, das Recht auf informationelle Selbstbestimmung ausgestalten oder den Umgang mit personenbezogenen Daten regeln. Ein zentraler Begriff des Datenschutzrechtes sind die «personenbezogenen oder persönliche Daten». Personenbezogene Daten sind sämtliche Informationen, die einer bestimmten oder bestimmbaren Person zugeordnet werden können, zum Beispiel Namen, Adressen, Bankkonto, bzw. sensible Daten beispielweise

medizinische Daten, politische Ansichten oder Rassenzugehörigkeit.

Personendaten dürfen nur rechtmässig bearbeitet werden, wenn man die Zustimmung der betroffenen Person oder andere legitimierte Gründe hat.

Das Datenschutzrecht hat sich international durchgesetzt und reiht sich in den Rahmen des globalen Informationsaustausches ein. Unterschiedliche Ansätze in der Umsetzung der nationalen Datenschutzgesetze führen zu Unterschieden zwischen den Ländern, die die Implementierung der Massnahmen komplizieren, insbesondere bei den Unternehmen, die in verschiedenen Ländern tätig sind, aber auch bei mittelständischen Unternehmen, die über begrenzte Ressourcen verfügen.

In Europa und in der Schweiz stammen die geltenden Datenschutzgesetze aus den 90iger Jahren, das heisst aus Zeiten, wo die Ausdehnung der elektronischen Datenverarbeitung und die Umsetzung des europäischen Binnenmarkts neue Regelungen im Rahmen des Informationsaustausches erforderten[1]. In der Schweiz wurde das Bundesgesetz über den Datenschutz im Juni 1992 in Kraft gesetzt[2].

Neu hat die Europäische Kommission eine Revision der Regelungen bezüglich Datenschutzrechten geplant, die eine Verschärfung der Rechenschaftspflicht sowie eine Harmonisierung der Regelungen in den 27 EU Staaten beinhalten soll. Die aktuelle EU-Richtlinie zum Datenschutz wird voraussichtlich revidiert[3].

Im Hinblick auf die EU-Richtlinie über Datenschutzrecht und die geplante Revision der Richtlinien kann man die folgenden Aspekte erwähnen:

- Datenschutzrecht trifft alle Organisationen, die Datenbanken mit persönlichen Informationen anlegen, d.h. von grossen multinationalen bis zu mittelständischen Unternehmen.

- Die extraterritoriale Wirkung der EU-Vorschriften bedeutet, dass die Vorschriften auch gelten, wenn eine Organisation keinen Sitz in der EU hat.

- Die Übermittlung personenbezogener Daten in die EU-Staaten oder ausserhalb der EU unterliegt bestimmten Bedingungen; besonders ausserhalb der EU darf eine solche Übermittlung nur erfolgen, wenn ein angemessenes Schutzniveau im Land des Empfängers oder innerhalb der empfangenden internationalen Organisation gewährleistet ist und diese Übermittlung ausschliesslich die Wahrnehmung von Aufgaben ermöglichen soll.

- Bei schweren Verletzungen des Schutzes von personenbezogenen Daten muss die zuständige Behörde innerhalb 24 Stunden benachrichtigt werden.

- Die kommende EU-Datenschutzrichtlinie sieht höhere Geldstrafen vor, die nach Schwere des Verstosses zwischen 0,5 und 2,0 Prozent des Umsatzes sein können.

Obwohl der Gesetzgeber darauf verzichtet, bestimmte einzelne Maßnahmen zwingend vorzuschreiben, verlangen Datenschutzgesetze neben der Benennung eines Datenschutzbeauftragten auch die Einführung von organisatorischen und technischen Massnahmen, die den Datenschutz sicherstellen, was die Geschäftsprozesse und IT-Systeme sowie das Risikomanagement von Unternehmen beeinflusst.

Datenschutz und Internes Kontrollsystem

Jede Organisation muss ihre eigenen Geschäftsinformationen sicherstellen und die gesetzlichen Anforderungen und Vorschriften erfüllen. Dafür muss ein wirksames Internes Kontrollsystem (IKS) mit entsprechenden Massnahmen zum Datenschutz implementiert sein. Im Rahmen des Datenschutzrechtes ist die Organisation verantwortlich für die Implementierung und Aufrechterhaltung von angemessenen Kontrollen über die Sammlung, die Bearbeitung und die Sicherheit der personenbezogenen Daten.

Das Enterprise Risk Management Framework (ERM) beschreibt das Interne Kontrollsystem als einen integrierten Prozess, der verschiedene Kontrollelemente enthält. Dazu gehören die Unternehmenskultur, die Struktur, Richtlinien, Kontrolltätigkeiten und die Überwachung.

Das COBIT Modell hat einen ähnlichen integrierten Ansatz. Dieses Modell zeigt nämlich eine unternehmensweite, durchgängige Perspektive der Governance und des Managements von Information (und zugehörige Technologien), in der Organisationsziele zu IT-bezogenen Zielen kaskadieren[4].

Für die Implementierung einer effektiven Governance verfügt die Organisation über «Enabler», die relevante Ressourcen für die Implementierung der Governance und des Managements von Unternehmensinformationen darstellen.

Das COBIT Rahmenwerk beschreibt die folgenden sieben Enabler-Kategorien:

1. Prinzipien, Richtlinien und Rahmenwerke
2. Prozesse
3. Organisationsstruktur
4. Kultur, Ethik und Verhalten
5. Informationen
6. Services, Infrastruktur und Anwendungen
7. Mitarbeiter, Fähigkeiten und Kompetenzen

Die erste Kategorie zeigt die erwünschten Verhalten, die man in täglichen Tätigkeiten erwartet. Im Rahmen des Datenschutzrechtes beinhalten diese Enabler allgemeine Erwartungen. Prozesse beschreiben ausführliche Aktivitäten und erwartete Ergebnisse, die zur Erreichung allgemeiner datenschutzbezogener Ziele beitragen. Ein Beispiel sind die IT-Prozeduren für die Datensicherheit, die Zutritts-, Zugangs- und Zugriffskontrolle definieren.

Organisationsstruktur

Der nächste Enabler, Organisationsstruktur, vermittelt bestimmte Ziele und identifiziert die Ressourcenverantwortlichen für die Erreichung solcher Ziele. Die Organisationsstruktur hat auch mit der Gestaltung der Handlungsbeziehungen zwischen den Organisationseinheiten zu tun, und ist besorgt, dass das ganze System funktioniert.

Die Abbildung 1 zeigt ein Beispiel bezüglich Hauptverantwortlichkeiten im Zusammenhang mit dem Datenschutzrecht.

ABBILDUNG 1: HAUPTVERANTWORTUNG IM ZUSAMMENHANG MIT DATENSCHUTZGESETZEN

CEO	Als Geschäftsleiter verantwortlich für die allgemeine Einhaltung der Datenschutzgesetze.
CIO	Aufbau und Strukturierung der IT-Abteilung und Festlegung der Konformitätsziele.
Datenschutzbeauftragter	Überwachung der Risiken und der Geschäftsauswirkungen von Datenschutzgesetzen, und Implementierung von Richtlinien und Aktivitäten zur Einhaltung der Datenschutzrichtlinien.
IT Manager	Schutz der Dateien.
HR und andere Business Manager	Effektive Überwachung über Behandlung der personenbezogenen Daten.

Abbildung2: Enabler der Governance und Management von personenbezogenen Daten

Kultur, Ethik und Verhalten

In seinen täglichen Tätigkeiten ist jeder Mitarbeiter verantwortlich für die rechtmässige Behandlung der Daten. Da Organisationen ohne Menschen nicht funktionieren können, sind individuelle Kompetenzen und eine ethische Kultur entscheidend. Kultur, Ethik und Verhalten hängen vorrangig von Menschen ab, aber die Organisationen können ein Bewusstsein bei den Mitarbeitenden mittels Datenschutz-Schulungen schaffen. Das Unternehmen kann in einem Verhaltenskodex sowie in anderen Richtlinien seine grundsätzlichen Standards und Erwartungen festlegen, die ein angemessenes ethisches Verhalten unterstützen.

Die heutige Kommunikation führt zu einem schnelleren Datenaustausch und die Mitarbeiter müssen sich bewusst sein, wie vertrauliche Unternehmensinformationen richtig zu behandeln sind und welche Verhalten und Praktiken verboten sind. Das Kopieren von Dateien auf einen USB-Stick oder auf eine externe Festplatte ist eine ernste Gefahrenquelle für den Datenschutz. Ein anderes Risiko ist die Versendung der sensiblen Daten per E-Mail ohne Verschlüsselung.

Informationen

Der fünfte Enabler des COBIT Modelles ist Informationen. Wenn Organisationen mit verschiedenen Daten zu tun haben, braucht man Informationen über diese Daten, um die Daten systematisch und ordnungsgemäss zu behandeln. Zum Beispiel stellt sich die Frage, zu welcher Kategorie die Daten gehören. Daten des Personals brauchen ein höheres Niveau an Sicherheit als andere Bereiche.

Auch für Daten gibt es einen Lebenszyklus. Die aktuellen Aufbewahrungsvorschriften in einem Land geben die minimale Zeit der Archivierung von Geschäftsunterlagen vor. Wenn die Archivierung personenbezogene Daten enthält, fordern die Datenschutzgesetze, dass die Aufbewahrung nicht länger als nötig sein muss.

Beispielsweise dürfen Kundenlisten nur für die Zeit der Geschäftsbeziehungen gespeichert werden, oder wenn eine rechtliche Pflicht es erfordert.

Eine andere wichtige Information besteht in der Klassifizierung der Daten. Jede Organisation kann ein System von Datenkategorien führen, das nach Sensitivität die Dateien klassifizieren kann. Eine ordnungsmässige Klassifizierung ist der erste Schritt für die angemessene Behandlung der Daten. Für jeden Datentyp können verschiedene Sicherheitsniveaus implementiert werden.

Services, Infrastruktur und Anwendungen

Der sechste Enabler, Services, Infrastruktur und Anwendungen, umfasst die Infrastruktur und die Technologie, die die Bearbeitung und Speicherung persönlicher Daten sicherstellen.

Angemessene Zugangskontrollen zu einem Rechenzentrum ist ein Beispiel zur physischen Kontrolle, wobei die logische Kontrolle wie zum Beispiel die Einführung von Passwörtern wichtiger ist. Die Wirkung der logischen Kontrolle ist von der angewendeten Technologie abhängig.

Fähigkeiten und Kompetenzen

Obwohl Kultur, Ethik und Verhalten zentrale Voraussetzungen sind, muss die Organisation die notwendige Fähigkeiten und Kompetenzen erwerben und weiterentwickeln. Der Datenschutzbeauftragte spielt diesbezüglich eine wichtige Rolle, denn er ist zuständig für die Überwachung der Risiken und der Geschäftsauswirkungen von Datenschutzgesetzen und er soll die Implementierung von Richtlinien und Aktivitäten steuern und koordinieren. Seine Kompetenzen bestehen darin, über die notwendigen rechtlichen Kenntnisse der Datenschutzgesetze sowie ein allgemeines Verständnis des Geschäftes und der Geschäftsprozesse zu verfügen. Obwohl der Datenschutzbeauftragte eine Beraterrolle inne hat, haben die Mitarbeiter die Pflicht, interne Verfahren zu verstehen und einzuhalten. Dafür wird erwartet, dass Mitarbeiter über die notwendigen Kompetenzen und Erfahrung verfügen.

Mit dritten Parteien muss man in einem schriftlichen Vertrag bestimmte Aspekte festlegen, zum Beispiel:

- Art und Zweck der Nutzung und Verarbeitung von Daten
- technische und organisatorische Massnahmen zur Datensicherheit
- Korrektur, Löschung und Sperrung von Daten
- physischer Ort der Auslagerung von Daten

Die Abbildung 2 illustriert den Zyklus von personenbezogenen Daten zusammen mit den sieben Enablern, die als Unterstützung des Prozesses dienen.

Fazit

Datenschutzrecht ist ein Thema, das die Organisationen in Zukunft immer mehr beschäftigen wird. Die Identifikation von gesetzlichen Anforderungen und die Festlegung von entsprechenden Massnahmen können die rechtlichen Risiken auf ein tragbares Mass reduzieren.

Das Rahmenwerk COBIT bietet einen systematischen Ansatz an, um die zur Erfüllung der Organisationsziele im Zusammenhang mit Datenschutzrecht zu ermöglichen.

DER AUTOR

Davide Vazzari, Dipl. Betriebswirtschaftslehre, CIA, CISA, CFE, Zürich, Switzerland.

Anmerkungen

1) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

2) Bundesgesetz über den Datenschutz, vom 19. Juni 1992.

3) http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

4) COBIT 5, Rahmenwerk für Governance und Management der Unternehmens-IT.

IT-Strategie als Instrument der IT-Governance

Von Markus Baechler

Das Unterfangen, eine IT-Strategie zu entwickeln, entspringt meist einem ganzen Blumenstrauss von Motiven: Eine zielführende mittelfristige IT-Planung zu ermöglichen, Know How und Kräfte zu bündeln, die Basis für durchgängige IT-Prozesse zu schaffen, das IT-Haus mittelfristig neu aufzubauen und besser auf das Geschäft auszurichten oder etwa einen Generationensprung in Hardware, Software und IT-Dienstleistung zu bewältigen.

Wichtig für eine erfolgreiche Strategie-Entwicklung ist die Klarheit bezüglich der Rollenverteilung: Am Tisch sitzen Auftraggeber, Auftragnehmer und geleitet wird der Prozess von einem internen oder externen Moderator. Auftraggeber sind die internen IT-Kunden, d.h. die Geschäftseinheiten. Sie müssen das Gros des Strategie-Entwicklungsteams stellen. Beauftragte zur Umsetzung der Strategie ist die IT, welche Vorschläge zur Umsetzung der Geschäftsstrategie mit IT-Mitteln formuliert und die vorhandenen und erforderlichen Ressourcen für die Umsetzung offenlegt. Dazwischen wirkt im Strategie-Entwicklungsprozess ein Moderator, der eine entscheidende Rolle für das Gelingen des Strategieprozesses erhält: Er muss die Diskussionen und die Diskussionsteilnehmer vorbereiten, den Prozess in operationale Einheiten bzw. Fragestellungen gliedern, welche zu greifbaren Einzelresultaten und Prioritäten führen, aus denen sich schlussendlich die Strategie zusammensetzt und er muss sich in den garantiert auftretenden Interessengegensätzen behaupten und diese so ausbalancieren, dass die resultierende Strategie schliesslich von der Gesamtheit der Unternehmung getragen wird.

Phasen des Strategieprozesses

Der Strategie-Entwicklungsprozess lässt sich grob wie folgt gliedern:

1. Standortbestimmung
Hier werden die Stärken und Schwächen der existierenden IT analysiert. Daraus ergeben sich oft entscheidende Hinweise auf die einzuschlagende Richtung, nicht nur für IT-Leistungen, sondern auch für das IT-Risikomanagement.

2. Formulierung der Zukunftsanforderungen aus Geschäftssicht
In dieser Phase werden, ohne Priorisierung, die Zukunftsanliegen und IT-Anforderungen der Geschäftsbereiche zusammengetragen (Wunschlisten).

3. Definition der Soll-IT-Leistungen
Für eine mittlere Frist von 2-8 Jahren werden die Soll-IT-Leistungen aus Geschäftssicht definiert und priorisiert. Hierbei prallen die unterschiedlichen Interessen einzelner Geschäftsbereiche aufeinander, es können aber auch Synergiepotenzial und wichtige Schnittstellen aufgezeigt werden. Die Priorisierung der Geschäftsanforderungen an die IT ist ein kritischer Schritt im Strategieprozess. Sie ist ein wesentlicher Motor des „Business-IT-Alignements", d.h. der Ausrichtung der IT an den Geschäftsbedürfnissen.

4. Organisation / Ressourcen / Sourcing
Während in der vorigen Phase die zu erbringenden Leistungen definiert wurden, wird hier nach einer effizienten und flexiblen Art und Weise der Erbringung dieser Leistungen gesucht. Dabei stützt man sich idealerweise auf ein Prozess-Framework wie ITIL oder CobIT ab, das die Vollständigkeit, Durchgängigkeit und Führbarkeit der Leistungserbringung gewährleistet.

Diese Phase basiert auf Vorschlägen der IT-Führung, die konfrontiert werden mit den Ressourcen, die das Unternehmen für die erwarteten IT-Leistungen zu erbringen bereit ist.

5. Definition strategischer Vorhaben zur Implementation der IT-Strategie
Um die IT-Strategie umzusetzen, werden ein oder mehrere Projektportfolios definiert, basierend auf der Gap-Analyse zwischen Status Quo und dem Soll-IT-Haus.

6. Finanzierung, Meilensteine, Steuerung
Bei grösseren Umbauten der IT ist oft eine Diskussion der Finanzierungsgrundsätze notwendig. Zur Erhöhung der Kostentransparenz sind die Geschäftseinheiten als Sponsoren ihrer Business-Applikationen in die Verant-

wortung zu ziehen und es ist ein Schlüssel für die Finanzierung der allgemeinen IT-Infrastruktur zu finden. Die Geschäftseinheiten ihrerseits brauchen den Umsetzungszeitplan um ihre Geschäftsprozesse an neue IT-Grundlagen anpassen zu können. Entsprechende, gemischte Steuerungsorgane müssen die Umsetzung überwachen, beurteilen und steuern können.

7. Auswirkungen auf Folgeprozesse

Die IT-Strategie ist Input für andere Steuerungsprozesse wie IT-Architektur, Portfolio- oder Projektmanagement oder auch die IT-Prozesslandschaft. Es ist sicherzustellen, dass diese an der neuen IT-Strategie ausgerichtet werden.

8. Kommunikation der IT-Strategie

Sowohl Geschäftseinheiten, die IT-Organisation wie auch die einzelnen Mitarbeiter sind von der IT-Strategie betroffen (man denke etwa an ein Outsourcing-Vorhaben). Die gesamte Unternehmung ist daher umfassend über die neue IT-Strategie und ihren groben Umsetzungsplan zu informieren.

IT-Strategie und -Governance

Was hat IT-Strategie mit IT-Governance zu tun? Sehr viel: Die zentralen Anliegen der IT-Governance, nämlich

- die Ausrichtung der IT auf sich wandelnde Geschäftsbedürfnisse,
- die Sicherstellung von Leistung und (Kosten-)Effizienz der IT,
- die Implementation einer Kultur der Dienstleistungsorientierung,
- ein Framework für Aufbau, Kontrolle und Messbarkeit von IT-Prozessen und -Ergebnissen,
- ein IT-Risikomanagement, das ins globale Risikomanagement der Unternehmung integriert ist,

sind Anliegen, die praktisch direkt in den IT-Strategieprozess einfliessen. Der IT-Strategieprozess ist daher immer auch ein Ausgangspunkt nicht nur zur Umsetzung sondern auch zur Weiterentwicklung der IT-Governance eines Unternehmens, insbesondere zur besseren Ausrichtung der IT auf die Anforderungen der Geschäftseinheiten.

Fazit: Um das Führungsteam einer Organisation zusammenzuschweissen, brauchen sie nicht auf einem selbst gebastelten Floss über den Walensee zu rudern. Sie können auch, mit nachhaltigen, effizienzsteigernden Auswirkungen, eine IT-Strategie erarbeiten!

DER AUTOR

Markus Baechler ist Geschäftsführer von iidc (IT Infrastructure Design and Consulting GmbH) und ISACA CRISC. Er berät den Aufbau von IT-Prozessen, IT-Strategie, Riskmanagement und IT-Security und macht Risk Assessments, Audits und Reviews von Projekten und IT-Organisationen. markus.baechler@iidc.ch

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
14.03.2014	CSA-KK	**ISO 27001/2 Self Assessment – effiziente ISMS-Standortbestimmung**
18./19.3.14	LAB-SMA (J)	**Secure Mobile Apps**
20./21.3.14	LAB-SMA (B)	**Secure Mobile Apps**
25.03.2014	AHS	**Vereinsversammlung ISACA Switzerland Chapter**
31.3.-13.5.14	CISA-PV	**CISA-Prüfungsvorbereitungskurs 2014|1**
7.4.-14.5.14	CISM-PV	**CISM-Prüfungsvorbereitungskurs 2014|1**
8./9.4.14	LAB-WAB (J)	**Web Application Security Basics**
10./11.4.14	LAB-WAA (J)	**Web Application Security Advanced**
10.4.-16.5.14	CRISC-PV	**CRISC-Prüfungsvorbereitungskurs 2014|1**
14.4.-15.5.14	CGEIT-PV	**CGEIT-Prüfungsvorbereitungskurs 2014|1**
29.04.2014	AHS	**After Hours Seminar ISACA Switzerland Chapter**
05.05.2014	AWA-KK	**Wirksame Awareness-Kampagnen gestalten und umsetzen**
6./7.5.14	ERM-UF	**Effektives Management von IT-bezogenen Risiken mit COBIT5**
6./7.5.14	LAB-WAB (B)	**Web Application Security Basics**
8./9.5.14	LAB-WAA (B)	**Web Application Security Advanced**
19.05.2014	SAM-VD	**Risikominimierung durch Software Asset- und Lizenz-Management**
20.05.2014	LM5-VD	**Revision von Software Asset Management - Lizenzmodelle**
www.isaca.ch		
17.-19.3.14	COB-FD	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
24.-26.3.14	COB-Assessor	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
16.-18.6.14	COB-FD	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
23.-25.6.14	COB-IG	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
www.glenfis.ch		

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise: 4x 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
Copyright: © Switzerland Chapter der ISACA