

IT-Governance

(IT-Prozesse steuern, beurteilen und verbessern)

- Drei Fragen an Verwaltungsrat und Geschäftsleitung
- Steuerung der IT auf drei Ebenen
- Der Provida-Ansatz bei der Prüfung von IT-Systemen
- Kurz- bzw. Erstbeurteilung der IT
- Beispiel: Ablauf einer Prüfung im IT-Bereich

Drei Fragen an Verwaltungsrat und Geschäftsleitung

IT: Der Lebensnerv
des Unternehmens.

Die Informations- und Kommunikationstechnologie (nachfolgend als ICT oder - kurz - IT bezeichnet) ist der Lebensnerv vieler Unternehmen. Gemessen an der Bedeutung dieses Bereiches für den Erfolg des Unternehmens wird der Steuerung der IT-Ressourcen durch die Führungsorgane häufig zuwenig Rechnung getragen.

Falls Sie, als Verwaltungsrat oder Mitglied der Geschäftsleitung, die folgenden drei Kontrollfragen überzeugt mit «Ja» beantworten können, zählen Sie zu jenen Führungsverantwortlichen, die sich schon angemessen mit dem Thema «IT-Steuerung» auseinandergesetzt haben.

1. Hat der Verwaltungsrat die strategische Ausrichtung der IT (Zielvorgaben), die Beurteilungs- und Messkriterien sowie den Steuerungsprozess in einem Informatikkonzept schriftlich festgehalten?
2. Werden die definierten Prozesse innerhalb der IT-Fachabteilung im Sinne der IT-Governance gelebt und sind sie dokumentiert?
3. Wird der Verwaltungsrat mindestens einmal jährlich von der IT-Fachabteilung über den Zustand der IT, allfällige Risiken, die umgesetzten Massnahmen und die Ziele im Bereich der Weiterentwicklung informiert?

Perfekte IT ist
unbezahlbar.

Die «perfekt funktionierende IT» ist kein anzustrebender Zustand, weil die Kosten dafür nicht bezahlt werden könnten. Wie in anderen Unternehmensbereichen auch soll der Ressourceneinsatz in der IT optimiert erfolgen. Oberstes Ziel der IT ist die Verfügbarkeit der Systemressourcen und die optimale Unterstützung der Unternehmensaktivitäten.

Aufgrund der Komplexität des IT-Bereiches sind Verwaltungsrat und Geschäftsleitung oft nicht in der Lage, konkrete Ziele vorzugeben oder Aussagen der Fachabteilung zu verifizieren. Trotzdem tragen diese Organe aufgrund der grossen Bedeutung dieses Bereiches für den Betrieb und das investierte Kapital eine besondere Verantwortung. Diese kann nicht delegiert werden, sondern muss durch wirksame Steuerungs- und Überwachungsinstrumente angemessen wahrgenommen werden.

Wir bringen Licht in
die «Black Box» IT.

Die Spezialisten der Provida vermitteln Ihnen die nötige Sicherheit im Umgang mit den IT-Ressourcen und unterstützen Sie bei der Aufgabe, die Steuerung des IT-Bereiches zu gewährleisten. Dies erhöht den wirtschaftlichen Nutzen Ihrer IT und stellt die Einhaltung gesetzlicher und regulatorischer Vorgaben sicher. Wir helfen Ihnen, Licht in die «Black Box» IT zu bringen. Gerne zeigen wir Ihnen auf, mit welchen einfachen Instrumenten wir in der Lage sind, Ihnen, Ihren IT-Mitarbeitern und natürlich auch den IT-Anwendern einen nachhaltigen Nutzen zu vermitteln.

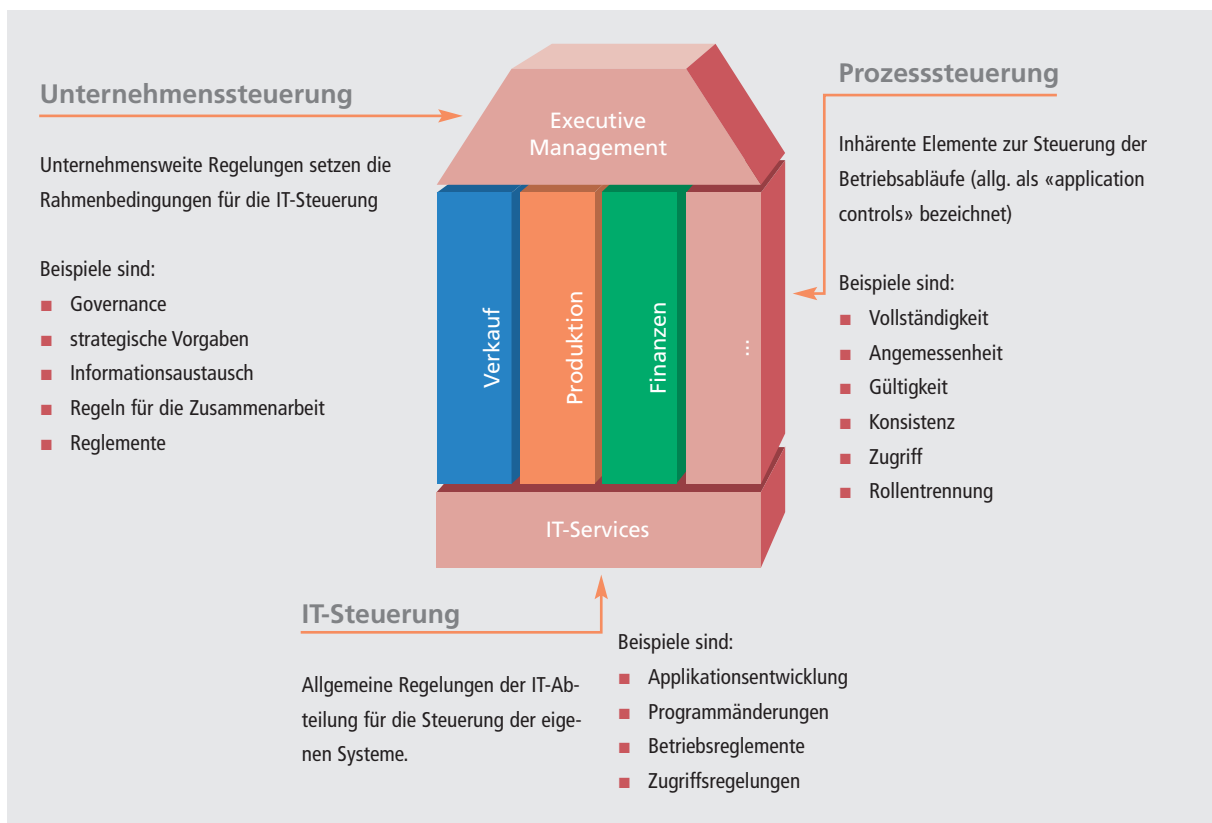
Steuerung der IT auf drei Ebenen

Von Verwaltungsrat und Geschäftsleitung wird heute erwartet, dass sie die IT im Unternehmen so organisiert, steuert und beaufsichtigt, dass die Unternehmensziele zweckgerichtet, effizient und legal erreicht werden können. Das «IT Governance Institute» unterscheidet drei Ebenen der Steuerung und Überwachung von IT-Ressourcen:

Drei Ebenen der Steuerung und Überwachung.

1. die strategische Ausrichtung der IT am Geschäftszweck als Aufgabe der Unternehmenssteuerung,
2. die Verwendung der Informationstechnologie in den Geschäftsprozessen (Prozesssteuerung) und
3. die Steuerung der IT-bezogenen Geschäftsrisiken (IT-Steuerung).

Diese Unterscheidung deckt sich mit den Standards des «Public Company Accounting Oversight Board», das die Einhaltung des Sarbanes-Oxley-Gesetzes (SOX) in den USA überwacht und dessen Vorschriften in einer globalisierten Wirtschaft auch für schweizerische Unternehmen immer wichtiger werden.



Spezifisches Instrument für jede Stufe.

Auf jeder dieser drei Stufen steht den Führungsorganen der Unternehmen ein spezifisches Instrument zur Steuerung und Überwachung der IT-Ressourcen zur Verfügung:

■ Stufe: Unternehmenssteuerung

Auf Stufe der Unternehmensführung verlangen die Regeln der «Corporate Governance» ein ausgebautes Risikomanagement für das gesamte Unternehmen. Auch IT-Risiken müssen durch das Risikomanagement systematisch bewirtschaftet werden. COSO¹ als klassisches Instrument des Risikomanagement bietet hier wesentliche Unterstützung (vgl. dazu die Provida-Broschüre «Implementierung und Prüfung von Riskmanagement und internem Kontrollsystem»).

■ Stufe: Prozesssteuerung

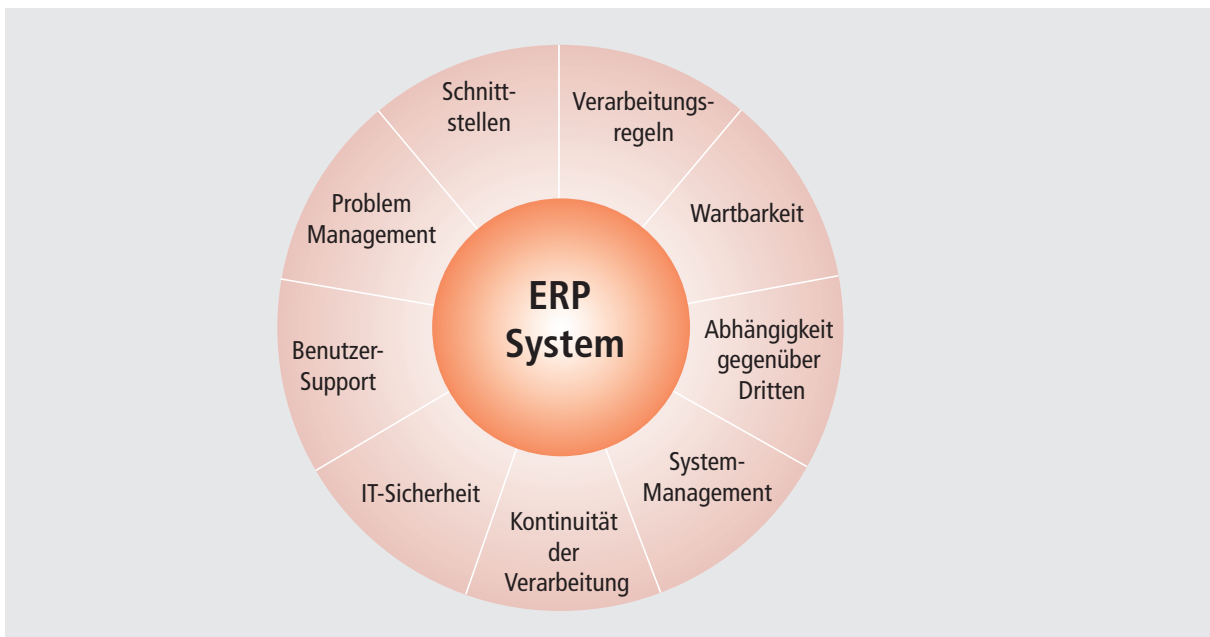
COSO erlaubt auch die Messung und Kontrolle der Risiken, die sich aus den operativen Geschäftsprozessen ergeben. Ein an COSO ausgerichtetes internes Kontrollsystem (IKS) beinhaltet die Gesamtheit aller von der Unternehmensführung angeordneten Vorgänge, Methoden und Massnahmen zur Vermeidung der betrieblichen Gefahren und zur Sicherstellung des ordnungsgemässen Ablaufs der betrieblichen Aktivitäten – insbesondere jenen, mit Auswirkung auf die finanzielle Berichterstattung (weitere Informationen hierzu entnehmen Sie bitte der oben erwähnten Provida-Broschüre).

■ Stufe: IT-Steuerung

Häufig setzt das IKS ein funktionierendes IT-System voraus. Ein Kontoauszug oder eine Bilanz muss sämtliche relevanten Daten aus dem Buchhaltungssystem bereitstellen. Diesem spezifischen Aspekt vermag das COSO-Modell leider nur unzureichend Rechnung zu tragen. Der COBIT-Framework² ergänzt COSO in diesem Bereich durch generell anwendbare Kontrollziele für die spezifischen IT-Prozesse. Die Gesamtheit der IT-Prozesse im COBIT, mit ihrer Ausrichtung auf das Risikomanagement der IT-Ressourcen wird als IT-Governance bezeichnet. In der Regel gehen wir von folgenden primär betroffenen Risikobereichen aus:

¹ COSO = Committee of Sponsoring Organizations of the Treadway Commission

² COBIT = Control Objectives for Information and related Technology.



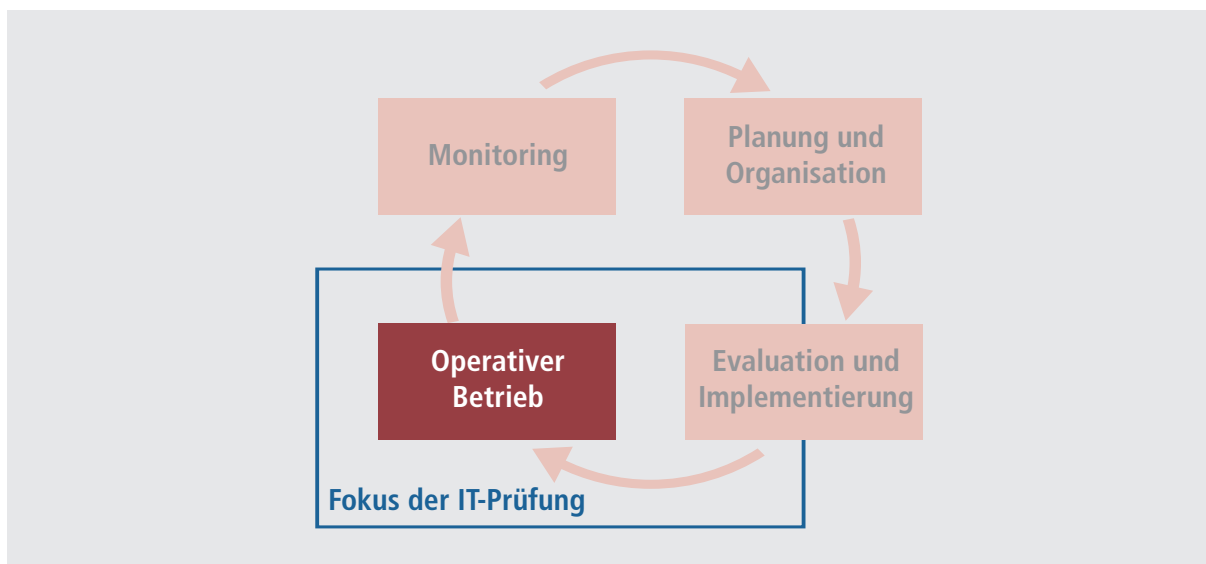
Der Provida-Ansatz bei der Prüfung von IT-Systemen

COBIT integriert als Checkliste in verblüffend einfacher Weise die Sicherheits- respektive Kontrollanforderungen der bekanntesten Standards der Informationstechnologie und ist leicht in ein unternehmensweites IKS integrierbar. Die Vermeidung von Risiken und die Sicherstellung des ordnungsmässigen betrieblichen Ablaufs ist ein zentrales Anliegen. Im Rahmen eines auf die finanzielle Berichterstattung ausgerichteten IKS sollen Kontrollen nur dort erfolgen, wo die betrieblichen Aktivitäten Risiken für die finanzielle Berichterstattung bergen. Als ganzheitliches und umfangreiches Werkzeug der IT-Governance umfasst COBIT natürlich weit mehr Kontrollziele, als für die spezifischen IKS-Kontrollziele im erwähnten Zusammenhang erforderlich sind. Hier kommt der von der Provida eigens für KMU entwickelte IKS-Ansatz zum tragen. Bei einem IT-Audit im Zusammenhang mit der finanziellen Berichterstattung hält sich die Provida deshalb an folgendes bewährtes Vorgehen.

Vermeiden von Risiken und Sicherstellung des ordnungsmässigen betrieblichen Ablaufs ist ein zentrales Anliegen.

Für die Auswahl der relevanten Kontrollziele hat CobiT 34 kritische IT-Prozesse identifiziert und sie in vier Gruppen zusammengefasst, die den IT-Lebenszyklus abbilden (sogenannte «Domänen»). Als praxisorientierte Prüfungs- und Beratungsgesellschaft nutzt die Provida die relevanten Prozesse dieser Domänen zur Konkretisierung des Prüfungszieles und richtet dabei den Focus auf die Einhaltung der gesetzlichen Mindestanforderungen. Unser Vorgehen ist einfach, wirtschaftlich und wirkungsvoll. Kunden, die einen Zusatznutzen wünschen und über die Mindestanforderungen hinausgehen, sind frei, die entsprechenden Aufträge zu formulieren. Der Schwerpunkt eines Prüfungsauftrags ist deshalb abhängig von den gesetzlichen Erfordernissen, den Wünschen des Auftraggebers und dem aktuellen Zustand der IT.

Unser Vorgehen ist einfach, wirtschaftlich und wirkungsvoll.



Die Domänen werden in mehreren Stufen auf konkrete Kontrollziele heruntergebrochen und von der Provida an die spezifischen Gegebenheiten beim Kunden angepasst, sodass diese von der Kontrollinstanz gemessen und protokolliert werden kann, wie nachfolgender Ausschnitt aus einem Prüfplan für ein Provida IT-Audit zeigt:

COBIT-Referenz	Kontrollziele	mögliche Ansprechpartner	mögliche Unterlagen	Potential (0.3)	Prüfpunkt-ja/nein
A16/A17	Programmänderungswesen / Customizing	IT-Leiter	Ablaufbeschreibung		<input type="checkbox"/>
	• Antragsverfahren	Leiter Programmentwicklung	Testkonzept/-anleitungen		<input type="checkbox"/>
	• Entwicklungsrichtlinien	Organisator	Änderungsanträge		<input type="checkbox"/>
	• Transportverfahren	Key-User	Abnahmeformulare		<input type="checkbox"/>
	• Testing				<input type="checkbox"/>
	• Abnahme				<input type="checkbox"/>
	• Verteilung				<input type="checkbox"/>
	• Dokumentation				<input type="checkbox"/>
	• Putlevel-/Releasekonzept				<input type="checkbox"/>
	• Notfallmässige Änderungen				<input type="checkbox"/>

Dienstleistungen der PROVIDA.

Die Provida unterstützt Sie gerne im Bestreben, die Chancen und Risiken der IT erfolgreich zu managen. Wir bieten Ihnen folgende Dienstleistungen an:

- Beurteilung Ihrer IT-Prozesse hinsichtlich Sicherheit, Verfügbarkeit, Effizienz, Effektivität und Ordnungsmässigkeit. Die Analyse referenziert auf COBIT oder andere Frameworks
- Unterstützung bei der Erarbeitung / Implementierung von Instrumenten zur besseren Steuerung, Kontrolle und Organisation von IT-Ressourcen in folgenden Bereichen:
 - Schaffung von Transparenz über die Risiken der IT und Integration der Erkenntnisse ins unternehmensweite Risikomanagement
 - Strategische Ausrichtung der IT auf die Unternehmensziele
 - Effizienter Einsatz der IT-Ressourcen in den Geschäftsprozessen («process reengineering»)
 - Führung der IT-Abteilung
 - Notfallplanung
 - Abnahme- und Testverfahren im Zusammenhang mit neuen Applikationen und/oder Releasewechslern
 - Entwicklung von Zugriffschutz-Konzepten
- Unterstützung bei der Einführung / Implementierung neuer IT-Systeme hinsichtlich Design und Implementierung interner Kontrollen in Geschäfts- und IT-Prozessen sowie auch hinsichtlich Erreichung der Projektziele
- Co-sourcing der internen Revisionsfunktion im Bereich der IT-Risiken

Massgeschneiderte Konzepte.

Anlässlich einer Besprechung erörtern wir gerne mit Ihnen zusammen die Ausgangslage. Im Anschluss daran unterbreiten wir Ihnen ein massgeschneidertes Konzept für das weitere Vorgehen (inkl. Ressourcenplanung, Kostenschätzung, Vorschlag und Terminplan). Den Umfang (und damit auch die Kosten) bestimmen Sie.

Erstbeurteilung

Viele Unternehmen sind sich der Bedeutung korrekt funktionierender IT-Systeme bewusst und haben entsprechende Aufsichtsinstrumente im Einsatz. Der nachstehende Fragebogen unterstützt Sie dabei, das Risikobewusstsein in Ihrer Unternehmung zu prüfen. Gerne zeigen wir Ihnen den Nutzen und die einfache Handhabung des Fragebogens auf.

Nr.	Anforderung	Beurteilung 1–3	Begründung / Erläuterung / Empfehlung
1	Es existiert eine dokumentierte ICT-Strategie. Diese ist vom Verwaltungsrat beschlossen		
2	Ein Mitglied des Verwaltungsrats verfügt über vertiefte Kenntnisse der ICT.		
3	Die ICT-Abteilung informiert den Verwaltungsrat mindestens einmal jährlich über Entwicklungen, Risiken, Ziele und Massnahmen bezüglich der ICT-Strategie		
4	Die Unternehmungskultur und Organisation fördern eine stetige Optimierung von Prozessen und Kontrollen.		
5	Die IKS-relevanten Kontrollziele der Kernprozesse gemäss CobiT sind definiert, dokumentiert und werden gemessen.		
6	Es existiert ein schriftliches Sicherheits- und Berechtigungskonzept. Dieses ist vom Verwaltungsrat abgenommen.		
7	Die wesentlichen Geschäftsprozesse und Kontrollen sind dokumentiert und werden gemäss Dokumentation gelebt.		
8	Es existiert eine leicht verständliche Dokumentation der Systeme, Applikationen und des Netzwerks.		
9	Es existiert eine aktuelle Lizenz- und Vertragsverwaltung.		
10	Es existiert ein Prozess zur Bewilligung und Abwicklung von grösseren ICT-Investitionen (Projektcontrolling).		
11	Die Kosten der ICT sind bekannt und stehen im Einklang mit dem erwarteten Nutzen.		
Auswertung / Gesamt-Beurteilung			(1 = Nein, 2 = Teilweise, 3 = Ja)

Beispiel: Ablauf einer Prüfung im IT-Bereich

Mit einer sorgfältigen Prüfungsplanung steuern Sie die Ziele und Kosten unserer Dienstleistung. In der Regel lässt sich ein IT-Audit in folgende Phasen aufteilen:

Sie steuern die Ziele und Kosten unserer Dienstleistung.

- Vorbereitung:
 - Wahl des Prüfungsschwerpunktes (Domäne gemäss COBIT)
 - Projektplanung (Termine, Verantwortlichkeiten)
 - Definition von Zielen, Grundsätzen und Berichterstattung

- Durchführung:
 - Risikobeurteilung, Prüfungsstrategie und –planung
 - Festlegung der zu prüfenden Kontrollziele gemäss COBIT
 - Analyse und Beurteilung der vorhandener Messresultate
 - Einhalteprüfung und Beurteilung der Kontrollaktivitäten. Daraus wird abgeleitet:
 - Rating
 - Feststellung / Kommentar / Empfehlung

- Dokumentation der Prüfungen und Prüfungsurteil

- Kommunikation mit Unternehmen / Empfehlungen / Management Letter.

Die Provida-Gruppe

Die Zusammenarbeit mit der Provida eröffnet Ihnen eine wirtschaftliche Alternative auf allerhöchstem fachlichen Niveau. Darüber hinaus pflegen wir ein unkompliziertes, direktes und zielorientiertes Vorgehen. Dies wirkt sich positiv auf die Kosten unserer Dienstleistung aus.

Unser Kerngeschäft umfasst neben der Wirtschaftsprüfung und –beratung die Steuer-, Rechts- und Unternehmensberatung sowie Treuhanddienstleistungen. Über unser breites Niederlassungsnetz erhalten Sie Zugang zu bestens ausgewiesenen und praxisorientierten Fachleuten (dipl. Wirtschaftsprüfer, Steuer-, Treuhand-, MWSt- und Sozialversicherungsexperten, Betriebswirtschafter, Finanzierungsspezialisten, Juristen, Rechtsanwälte und IT-Spezialisten).

Als Mitglied der Alliot Group verfügen wir mit 200 Standorten in mehr als 60 Ländern über ein weltweit leistungsstarkes Beziehungsnetz und sind somit in der Lage, unsere Dienstleistungen global anzubieten.

Ansprechpartner Provida

St. Gallen	Hans Mäder, Felix Dittli, Christian Siebert, Kurt Hinder, Manuela Schnyder, Hansjörg Etter, Norbert Bleisch, Schützengasse 12, Postfach 1650, CH-9001 St.Gallen Telefon 071 227 70 70 / Telefax 071 227 70 75
Zürich	Peter Frei, Patrick Weiss Thurgauerstrasse 66, CH-8050 Zürich Telefon 044 307 85 80 / Telefax 044 307 85 85
Frauenfeld	Bernhard Allemann, Roger Bühlmann, Michael Hösli, Arnaud Knobel Bahnhofplatz 68, Postfach 481, CH-8501 Frauenfeld Telefon 052 723 03 80 / Telefax 052 723 03 85
Romanshorn	Walter Schefer, Pascal Strässle, Reto Ringer Neustrasse 2, Postfach 119, CH-8590 Romanshorn Telefon 071 466 71 71 / Telefax 071 466 71 75
E-Mail	vorname.nachname@provida.ch oder info@provida.ch
Internet	www.provida.ch