

Corporate Governance

Gute Gründe, zu vertrauen.



Ihr Mehrwert

Die Anforderungen an Corporate Governance und Compliance steigen permanent und können sich zu einer echten Belastung für Unternehmen entwickeln. Das muss nicht sein – mit den richtigen Partnern profitieren Sie von anspruchsvollen Compliance-Vorgaben: Durch mehr Transparenz, Sicherheit und klare Entscheidungsstrukturen für Ihr Unternehmen, sowie durch ein Qualitätssiegel, das Sie deutlich von Ihren Mitbewerbern abhebt.

Ihre Vorteile

- » Sie steigern die Qualität Ihrer Leistung, ohne entsprechende Ressourcen aufbauen zu müssen.
- » Ihre IT-Organisation kann sich voll auf die kontinuierliche Verbesserung Ihrer Geschäftsprozesse konzentrieren und schafft damit Effizienzgewinne.
- » Durch Ihre umfassende Corporate Governance positionieren Sie sich im Markt als zuverlässiger Partner.

Vertrauen ist gut, Zertifizierungen sind besser.

Um Zukunftsfähigkeit und Vertrauenswürdigkeit von Unternehmen auch in wirtschaftlich turbulenten Zeiten nachhaltig zu sichern, werden zunehmend gesetzliche Vorschriften, Richtlinien oder Standards entwickelt. Diese Regelungen stammen teils von Politik und Verbänden, teils kommen sie aus den Unternehmen selbst. Dann bilden sie als Corporate Governance sozusagen die Verfassung des Unternehmens.

Die Umsetzung dieser Vorgaben ist oft mit großem Aufwand für die Unternehmen verbunden. Diese Bemühungen zahlen sich jedoch aus: Denn Unternehmen, die sich intensiv mit ihrer Corporate Governance befassen, schaffen eine solide Basis für ihren Erfolg, genießen höheres Ansehen in der Öffentlichkeit und mehr Vertrauen bei ihren relevanten Zielgruppen.

Die Umsetzung der Richtlinien und Gesetze in Form einer Corporate Governance betrifft alle Geschäftsprozesse und die unterstützenden IT-Systeme. Deshalb ist Corporate Governance auch ein wichtiges Thema beim IT-Outsourcing: Bereiche, die das Unternehmen auslagert,

werden oft nicht selbst geprüft. Es gelten die Prüfungsergebnisse des Outsourcing-Partners auch für das Unternehmen. Dadurch haben Unternehmen gerade im IT-Bereich die Möglichkeit, durch höchste Sicherheits- und Qualitätsstandards zu überzeugen, ohne dass ihre IT-Abteilung zahlreiche Ressourcen für diese Thematik bereitstellen muss. Stattdessen kann sie sich voll auf ihr Kerngeschäft, die optimale Unterstützung der Geschäftsprozesse, konzentrieren und damit weitere Wettbewerbsvorteile für das Unternehmen schaffen.

Rechtliche Rahmenbedingungen für Compliance und IT-Outsourcing

Für die Einhaltung von Compliance beim IT-Outsourcing sind Gesetze, Richtlinien, Standards, Referenzmodelle und innerbetriebliche Vorgaben relevant. Auf letztere gehen wir hier nicht ein, weil sie sehr individuell ausfallen können. Aber selbstverständlich berücksichtigen wir sie als Ihr Outsourcing-Partner. Nachfolgend finden Sie eine Übersicht der wichtigsten Compliance-Vorgaben sowie deren Umsetzung bei FI-TS.

Gesetzliche Regelungen

Gesetz zu Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

KonTraG ist ein Artikelgesetz, das die bestehenden Gesetze, insbesondere HGB und AktG, ergänzt. Es verpflichtet die Geschäftsführung dazu, ein Kontrollsystem zu installieren, das Entwicklungen, die die Existenz des Unternehmens bedrohen können, frühzeitig erkennt. Auch die Outsourcing-Partner müssen in das Risiko-Management-System (RMS) eingebunden sein.

Als Ihr IT-Partner sorgen wir dafür, dass wir Ihre RMS-Vorgaben konsequent befolgen und arrangieren für Sie regelmäßige Kontrollen.

Das Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz wurde im Jahr 2001 an die EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr angepasst.

Ziel der EU-Richtlinie ist ein einheitliches Datenschutzniveau in allen EU-Mitgliedsstaaten. Mit der BDSG-Novelle II (1.9.2009) wurden die Anforderungen an die Auftragsdatenverarbeitung in §11 BDSG konkretisiert. Die datenschutzrechtliche Ausgestaltung bildet das wesentliche Element in Outsourcing-Projekten, um personenbezogene Daten (im Auftrag) zu verarbeiten. Mit der Neufassung des §11 BDSG sind konkrete Vorgaben an die Auftragserteilung gestellt, die in einem nicht abschließenden 10-Punkte-Katalog aufgeführt werden.

Gerade im Bankensektor, unserem „Heimatmarkt“, handelt es sich um sensible Daten im Sinne des BDSG. Deshalb ist Datenschutz seit Jahren ein wichtiges Thema für uns. Als Ihr Outsourcing-Partner für Auftragsdatenverarbeitung treffen wir gemeinsam mit Ihnen klare Vereinbarungen über Zuständigkeiten und Schutzmaßnahmen, die als BDSG-konforme Grundlage für die Behandlung Ihrer Daten dienen.

Sarbanes-Oxley-Act (SOX)

Der Sarbanes-Oxley-Act (SOX) gilt für alle Unternehmen, deren Wertpapiere in den USA gehandelt werden. Er schreibt effektive interne Kontrollsysteme für das Finanzberichtswesen vor. Im Zusammenhang mit SOX beziehen sich insbesondere zwei Veröffentlichungen auf das Outsourcing: Zum einen macht das Public Company Accounting Oversight Board (PCAOB) deutlich, dass sich Unternehmen nicht der rechtlichen Verpflichtung für ihre IT-Systeme entziehen können, auch wenn sie diese auslagern. Stattdessen müssen sie vom Outsourcing-Partner nachweise fordern, dass er über ein funktionsfähiges Kontrollsystem verfügt.

Zum anderen legt der Prüfungsgrundsatz Nr. 5 des PCAOB in Anlehnung an SAS 70, Absatz 324 „Service Organisationen“ fest, wie eine Prüfung durchzuführen ist, wenn Leistungen von einem Outsourcing-Anbieter bezogen werden, die zum IT-System des auslagernden Unternehmens gehören.

Als Ihr Outsourcing-Partner sorgen wir dafür, dass die bei uns ausgelagerten Bereiche Ihrer IT den Anforderungen Ihres Kontrollsystems entsprechen.

Richtlinien

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

Diese Richtlinie ist eng mit den Grundsätzen ordnungsgemäßer Buchführung verbunden und umfasst u.a. das Recht und die Art des Zugriffs der Finanzbehörden auf digitale Daten und EDV-Systeme, die im Zusammenhang mit der Besteuerung des Unternehmens bei Betriebsprüfungen verwendet werden.

FI-TS berücksichtigt die Anforderungen der GDPdU und damit die gesetzeskonforme Archivierung und Historisierung von Daten der Finanzbuchhaltung oder anderer steuerlich relevanter Systeme.

Basel II

Die vom Basler Ausschuss für Bankenaufsicht Ende Juni 2004 verabschiedete neue Eigenkapitalvereinbarung (Basel II) soll die Sicherheit und Zuverlässigkeit des Finanzsystems stärken, die Wettbewerbsgleichheit erhöhen und die Risiken besser erfassen. Im Hinblick auf Outsourcing wirkt sich Basel II sowohl direkt, als auch indirekt aus. Die direkte Einflussnahme bezieht sich vor allem auf die Behandlung operationeller Risiken. Sie hängen direkt von der IT-Sicherheit ab und sind das zweitgrößte Verlustrisiko für Finanzinstitute. Deshalb sind diese verpflichtet, besondere Vorkehrungen zu treffen, um übermäßige Risiken zu vermeiden, wenn sie geschäftskritische Prozesse auslagern. Auch bleibt die Verantwortung für die Einhaltung gesetzlicher Bestimmungen bei dem auslagernden Unternehmen. Die indirekten Auswirkungen von Basel II zeigen sich bei der Kreditvergabe, denn da das Kreditausfallrisiko verstärkt beachtet wird, rücken auch ausgelagerte, geschäftskritische IT-Prozesse in den Fokus der Risikobetrachtung.

FI-TS räumt dem Risikomanagement einen hohen Stellenwert ein und trägt so dazu bei, dass Ihnen günstige Konditionen offen stehen.

Standards – Buchführung

Grundsätze ordnungsmäßiger Buchführung (GoB) und Grundsätze DV-gestützter Buchführungssysteme (GoBS)

Die GoB sind Standards für die ordnungsgemäße Buchführung und Bilanzierung. Die GoBS wenden diese Standards auf die DV-gestützte Buchführung an. Auch hier ist der Buchführungspflichtige – d.h. das auslagernde Unternehmen – für die Einhaltung der Vorgaben des Standards verantwortlich. Die GoBS verlangen die Einrichtung eines internen Kontrollsystems, das auch die Integration des Outsourcing-Anbieters in den Kontrollprozess umfasst.

Die Services von FI-TS sind so ausgerichtet, dass die für Ihr Kontrollsystem relevanten Kennzahlen Ihnen auf Wunsch zur Verfügung stehen.

FI-TS liefert höchste Qualitätsstandards für Ihre IT.

Wirtschaftsprüfungsstandards

Die Überprüfung der Ordnungsmäßigkeit ausgelagerter Geschäftsprozesse und der damit verbundenen Unternehmens-IT ist ein wesentlicher Aspekt für auslagernde Unternehmen, die ihre betriebliche Führungsverantwortung wahrnehmen. Um den Aufwand für die Überprüfung überschaubar zu halten, ist die Wahl von Outsourcing-Partnern hilfreich, die die prüfungsrelevanten Anforderungen durch international anerkannte Zertifizierungen belegen.

FI-TS orientiert sich an diesen Vorgaben – beispielsweise SAS 70 oder dem deutschen Pendant IDW PS 951 – um den Prüfungsaufwand für die auslagernden Unternehmen so gering wie möglich zu halten.

- » **SAS 70:** Das Statement of Auditing Standards Nr. 70 gibt Dienstleistern die Möglichkeit, die Funktionsfähigkeit Ihres internen Kontrollsystems IKS mittels Reports nachzuweisen. Der Typ I-Report beschreibt die Existenz und den Aufbau des IKS, der Typ II-Report belegt zusätzlich durch Tests die Wirksamkeit der internen Kontrollen über einen bestimmten Zeitraum hinweg und wird als Nachweis der Übereinstimmung mit Compliance-Anforderungen (z.B. nach SOX Section 404) verlangt.
- » **IDW PS 951:** Der Prüfungsstandard basiert auf den Anforderungen von SAS 70 und berücksichtigt in seinem Regelungsbereich nationale Besonderheiten. In Ergänzung zum IDW Prüfungsstandard „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen (IDW PS 331)“ erläutert dieser Standard die Angemessenheit (IDW PS 951 Typ A) und die Wirksamkeit (IDW PS 951 Typ B) in der Umsetzung der Anforderungen.

FI-TS lässt die wichtigsten Prozesse, darunter Risikomanagement und Problem Management, nach IDW PS 951 auf Basis von COBIT 4.1 prüfen. Der Prüfbericht spiegelt die Standards des SAS 70 Typ 1 und SAS 70 Typ 2 wider.

Standards für die Zertifizierung von IT-Prozessen

Neben den Standards für die ausgelagerte Rechnungslegung spielen auch begleitende Aspekte wie die Informationssicherheit eine zentrale Rolle bei der Wahl des passenden IT-Outsourcing-Partners. Die umfassendsten Aussagen bezüglich Informationssicherheit und Risikomanagement beinhaltet dabei die internationale Norm ISO 27001:2005.

FI-TS ist seit Dezember 2006 nach dieser Norm zertifiziert und belegt damit die Erbringung von IT-Services auf hohem Sicherheitsniveau.

- » **ISO 27001:2005:** Die internationale Norm ISO 27001:2005 beschreibt die Anforderungen an das Management der Informationssicherheit in Unternehmen. Dabei bezieht sich der Begriff „Informationssicherheit“ auf die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen oder Daten. Damit ist die Norm eine solide Basis für ein effektives Risiko-Management-System. Gegenwärtig halten nur 130 Unternehmen in Deutschland das Zertifikat der Informationssicherheit ISO 27001:2005. Unter Compliance-Gesichtspunkten bietet der Standard eine ganze Reihe von Vorteilen:
 - Identifikation der anwendbaren notwendigen Gesetze
 - Schutz geistigen Eigentums
 - Schutz von bedeutenden Datensätzen und Dokumenten (SOX)
 - Datenschutz und Datensicherheit (BDSG)
 - Risikomanagement (SOX, KonTraG)
 - Zugriffsschutz (GoBS, GDPdU, SOX)
 - Regelungen zur Kryptographie (Verschlüsselungstechnik)
- » **ISO 9001:2008:** Der Standard definiert die Anforderungen an das Qualitätsmanagement. Das Qualitätsmanagementsystem von FI-TS ist seit 1998 gemäß ISO 9001 zertifiziert.



IT-Outsourcing: Hochqualifizierte Spezialisten, höchste Qualitätsstandards, maßgeschneiderte Services

Referenzmodelle

CobiT

(Control Objectives for Information and Related Technology)

Das CobiT-Modell liefert ein generell anwendbares und international akzeptiertes Rahmenwerk, das die in einem IT-Kontroll-System zu erfüllenden Kontrollziele detailliert festlegt. Bei der Entwicklung von CobiT waren Wirtschaftsprüfer intensiv beteiligt, so dass die meisten Prüfungspläne an CobiT orientiert sind. Das Modell umfasst die wesentlichen IT-Prozesse und die darin enthaltenen und notwendigen Kontrollen.

IT Infrastructure Library (ITIL)

ITIL ist ein international anerkanntes Referenzmodell für das IT-Servicemanagement. Es basiert auf einer Sammlung von Best Practices, die den gesamten Lebenszyklus der IT-Services betreffen: Strategie, Design, Überführung, Betrieb und kontinuierliche Verbesserung. Im Rahmen von IT-Outsourcing ist ITIL eine hilfreiche Basis für die Zusammenarbeit, denn Unternehmen und IT-Dienstleister sprechen dann „die gleiche Sprache“ und haben durch die Standardisierung nach ITIL auch Kenntnisse über Art und Aufbau ihrer IT-Prozesse.

ISO/IEC 20000

Die ISO/IEC 20000 ist ein international anerkannter Standard, der die Anforderungen an ein professionelles IT-Service-Management beschreibt. Er spezifiziert die notwendigen Mindestanforderungen

an Prozesse, die Organisationen etablieren müssen, um IT-Services in definierter Qualität bereitstellen und managen zu können. Die Norm richtet sich nach den Prozessbeschreibungen, die durch die IT Infrastructure Library (ITIL) des Office of Government Commerce (OGC) vorgegeben werden, und ergänzt diese.

Die Prozesse bei FI-TS orientieren sich an den Anforderungen der ISO 20000.

Rahmenbedingungen beim IT-Outsourcing

Kostenvorteile sind im Regelfall der Grund für die Auslagerung von IT-Services. Durch die Standardisierung und Zentralisierung von IT-Services erreicht der Outsourcing-Dienstleister über Skaleneffekte Effizienzgewinne, die er an seine Kunden weiter gibt. Dabei ist zu beachten, dass die meisten Outsourcing-Verträge über mehrere Jahre laufen, und dass sich während dieser Vertragslaufzeit die Rahmenbedingungen sowie die Anforderungen des auslagernden Unternehmens mit hoher Wahrscheinlichkeit verändern.

Das wirkt sich auch auf die Wirtschaftlichkeitsbetrachtung aus, die dann von der ursprünglichen Planung abweicht. Damit die Unternehmen maximal von der Auslagerung ihrer IT-Services profitieren ist es deshalb wichtig, den Outsourcing-Vertrag entsprechend flexibel zu gestalten, so dass er sich für beide Vertragsparteien wirtschaftlich sinnvoll an die neuen Anforderungen anpassen lässt.

Über Finanz Informatik Technologie Service (FI-TS)

FI-TS ist ein Tochterunternehmen der Finanz Informatik (FI) und hat sich seit 1994 als einer der führenden IT-Servicepartner der Finanzbranche etabliert. Der Outsourcing-Anbieter überzeugt durch langjährige Erfahrung, Branchenkompetenz, Technologie-Know-how und Beratungsexpertise. Maßgeschneiderte Dienstleistungen optimieren die IT-Kosten, machen Banken und Finanzdienstleister noch effizienter und bieten so konkrete Wettbewerbsvorteile. Die Erfüllung aktueller Governance-Anforderungen sowie die konsequente Umsetzung moderner Sicherheits- und Qualitätsanforderungen sind für FI-TS selbstverständlich. FI-TS beschäftigt in Deutschland am Hauptsitz in Haar

bei München und an den Standorten Hannover, Nürnberg und Offenbach rund 520 Mitarbeiter. Das Unternehmen erwirtschaftet einen Gesamtumsatz von circa 128 Millionen Euro – davon mehr als 70 Prozent non captive. Zu den namhaften Kunden, die sich auf die kompetenten Services von FI-TS verlassen zählen unter anderem BayernLB, Landesbank Hessen-Thüringen, DekaBank, Deutsche Kreditbank, Deutsche WertpapierService Bank, Hauck & Aufhäuser, LBS IT, Sparkassen-Finanzportal und die Bank of Scotland.

IT intelligent nutzen.

Gerne beraten wir Sie ausführlich und stellen mit Ihnen eine auf Ihre Anforderungen abgestimmte Lösung zusammen. Sprechen Sie mit uns.

Finanz Informatik Technologie Service GmbH & Co. KG
Vertrieb · Richard-Reitzner-Allee 8 · 85540 Haar
Telefon +49 89 94511-8393 · Fax +49 89 94511-8952
kundenanfrage@f-i-ts.de · www.f-i-ts.de