finanz **informatik**
technologie service

Executive Whitepaper

Gute Gründe, uns zu vertrauen

Governance, Risk & Compliance

Die Einhaltung gesetzlicher und regulatorischer Vorschriften und die konsequente Erfüllung von Richtlinien und Standards hat für FI-TS höchste Priorität. So positioniert sich FI-TS als vertrauenswürdiger Partner in der Finanz-IT-Branche für eine nachhaltige und zukunftsorientierte Zusammenarbeit.

Höchste IT-Qualitätsstandards

Um Zukunftsfähigkeit und Vertrauenswürdigkeit von Unternehmen auch in wirtschaftlich turbulenten Zeiten nachhaltig zu sichern, werden zunehmend gesetzliche und regulatorische Vorschriften, Richtlinien oder Standards entwickelt. Diese Regelungen stammen teils von der Politik und Verbänden, teils kommen sie aus den Unternehmen selbst. Um die verschiedenen Anforderungen effizient und effektiv umzusetzen, hat FI-TS einen Rahmen für Governance, Risk und Compliance (kurz: GRC) aufgebaut.

Governance

Die Summe der verschiedenen Regelungen, die auf Unternehmen wirken, bilden als Governance sozusagen die Verfassung der Unternehmen. Die Umsetzung dieser Vorgaben und Regelungen wird in den einzelnen Unternehmen zu Corporate Governance und ist oft mit großem Aufwand 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.

Risk

Risikomanagement in einem Unternehmen umfasst neben Risikobeurteilung und Risikobewältigung auch die Risikoüberprüfung, Risikoüberwachung und Risikokommunikation. Als fortlaufender Prozess kommt Risikomanagement in der gesamten Organisation zur Anwendung und wird kontinuierlich weiter entwickelt. FI-TS bietet Ihnen als Ihr Weiterverlagerungspartner ein Risikomanagementsystem (RMS), mit dem Risiken systematisch aufgedeckt und bewertet, überwacht und kommuniziert werden. Es entspricht den aktuellen gesetzlichen Vorgaben und regulatorischen Anforderungen (z. B. Gesetz zu Kontrolle und Transparenz im Unternehmensbereich – KonTraG). Weiterhin sind bei FI-TS geeignete Organisationsstrukturen und Werkzeuge etabliert, um Risiken für FI-TS und seine Kunden erfolgreich zu managen.

Compliance

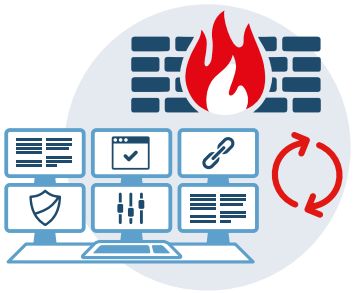
Die Umsetzung der Richtlinien und Gesetze im Rahmen einer „Corporate Governance“ betrifft alle Geschäftsprozesse und die unterstützenden IT-Systeme. Um dies alles regelgerecht einzuhalten spricht man von „Compliance“ – Durchführung und Nachhalten von Vorgaben und Regelungen. Deshalb ist Corporate Governance auch ein wichtiges Thema bei der Weiterverlagerung der IT. Bereiche, die ein Unternehmen weiterverlagert, werden oft nicht selbst geprüft. Unternehmen, die ihre IT an FI-TS weiterverlagert haben, können sich auf die Umsetzung anhand von Prüfergebnissen beziehen und somit durch höchste Sicherheits- und Qualitätsstandards am Markt überzeugen, ohne dass ihre IT-Abteilung zahlreiche Ressourcen für diese Thematik bereitstellen muss. Stattdessen kann sich das Unternehmen voll auf sein Kerngeschäft, nämlich auf die optimale Unterstützung der Geschäftsprozesse, konzentrieren und damit weitere Wettbewerbsvorteile für sich schaffen.

Basis der Umsetzung: Three-Lines-of-Defense (TLoD)

Die Aufbauorganisation im Finanzdienstleistungsbereich folgt dem weitverbreiteten Modell der „Three-Lines-of-Defense“. Dieses Modell erlaubt ein systematisches Herangehen an Risiken im Unternehmen. Die drei zusammenhängenden Verteidigungslinien werden wie folgt untergliedert:

Die **FIRST Line of Defense** bilden die operativen Einheiten, die Services unter Beachtung geeigneter Kontrollen erbringen (wie z. B. Firewall, Operation Control etc.).

Die **SECOND Line of Defense** geben Richtlinien vor, die im Compliance Management, im Datenschutz, im Informationssicherheitsmanagement und im Risikomanagement verankert sind. Die regelmäßige Überprüfung der Einhaltung dieser Richtlinien findet durch das Audit Management statt.



Die **THIRD Line of Defense** ist die Interne Revision, welche regelmäßig überprüft, ob die erste und zweite Verteidigungslinie ordnungsgemäß arbeiten und angemessen zusammenwirken.

Dieses Modell der TLoD bildet innerhalb von FI-TS die Basis des GRC-Ansatzes.

Vertrauen ist gut – Zertifizierungen sind besser

Die Überprüfung der Ordnungsmäßigkeit weiterverlagerter Geschäftsprozesse und der damit verbundenen IT ist ein wesentlicher Bestandteil der Auslagerungssteuerung. Neben den vom Auslagerungspartner erstellten Berichten sind Bestätigungen und Zertifikate unabhängiger Dritter dafür ein wertvoller Garant. FI-TS setzt dabei in den verschiedenen Themengebieten auf die folgenden Nachweise:

Rechnungslegung

In der heutigen digitalen Welt stützt sich die Jahresabschlussprüfung von Unternehmen meist in großen Teilen auf die Erkenntnisse der Prüfung der IT-Systeme. Dazu wird häufig der Prüfungsstandard IDW PS 331 „Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“ des Instituts der Wirtschaftsprüfer (IDW) herangezogen.

Internes Kontrollsystem

Das interne Kontrollsystem von FI-TS orientiert sich an COBIT (Control Objectives for Information and Related Technology). Das COBIT-Modell liefert ein generell anwendbares und international akzeptiertes Rahmenwerk, das die in einem IT-Kontrollsystem zu erfüllenden Kontrollziele detailliert festlegt. Der formale Rahmen von COBIT wird dabei ergänzt um die für einen IT-Dienstleister relevanten, regulatorischen Anforderungen, wie den Bankaufsichtlichen Anforderungen an die IT (BAIT) und den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT). Die Bestätigung der Angemessenheit und Wirksamkeit des internen Kontrollsystems erfolgt über die jährliche Prüfung nach IDW PS 951. Um den Aufwand für alle Seiten bei ausgelagerter IT gering zu halten, besteht die Möglichkeit, das interne Kontrollsystem des Dienstleisters zentral durch einen Wirtschaftsprüfer prüfen zu lassen. Daher wird das dienstleistungsbezogene interne Kontrollsystem von FI-TS jährlich durch einen externen Wirtschaftsprüfer auditiert. Die Prüfung und anschließende Bescheinigung nach IDW PS 951 bestätigt die Angemessenheit (Typ I) und Wirksamkeit (Typ II) der internen Kontrollen. Die Prüfung bezieht sich auf die von FI-TS im Auftrag seiner Kunden erbrachten Dienstleistungen in den Bereichen IT-Produktion, Datenbereitstellung und Informationssicherheit.

Informationssicherheit

Bei der Wahl des passenden IT-Weiterverlagerungs-Partners spielt die Sicherheit der ausgelagerten Informationen eine zunehmend zentrale Rolle. Die umfassendsten Aussagen bezüglich Informationssicherheit und Risikomanagement beinhaltet dabei die internationale Norm ISO/IEC 27001. Diese beschreibt die Anforderungen an das Management der Informationssicherheit in Unternehmen. Dabei bezieht sich der Begriff „Informationssicherheit" auf die Sicherheitsgrundwerte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen oder Daten. Damit ist die Norm eine solide Basis für ein effektives Risikomanagementsystem der Informationssicherheit und bietet eine ganze Reihe von Vorteilen wie:

- Identifikation der anwendbaren notwendigen Gesetze
- Schutz geistigen Eigentums
- Datenschutz und Datensicherheit
- Risikomanagement
- Zugriffsschutz
- Regelungen zur Kryptographie

FI-TS ist seit Dezember 2006 nach der Norm ISO/IEC 27001 zertifiziert und belegt damit die Erbringung von IT-Services auf hohem Sicherheitsniveau.

Qualitätsmanagement

Bei FI-TS ist das Qualitätsmanagement im Sinne eines Integrierten Managementsystems im Unternehmen etabliert. Das Qualitätsmanagementsystem von FI-TS wird seit 1998 gemäß DIN EN ISO 9001 regelmäßig überprüft und zertifiziert.

Dieser Standard legt die Anforderungen an ein Qualitätsmanagementsystem fest, welchen eine Organisation – wie zum Beispiel FI-TS – zu genügen hat. Dadurch werden sowohl Kundenerwartungen als auch behördliche Anforderungen erfüllt. Zugleich unterliegt das Qualitätsmanagementsystem bei FI-TS einem stetigen Verbesserungsprozess.

Providermanagement

Ziel des Providermanagements ist es sicherzustellen, dass die regulatorischen Anforderungen der Kunden an FI-TS und seinen Dienstleistern korrekt aufgenommen, weitergegeben und so letztendlich erfüllt werden.

Sowohl die Bewertung der zu beschaffenden Dienstleistungen, die Kontrolle der Leistungserbringung hinsichtlich regulatorischer Anforderungen als auch die Risikoanalyse und -bewertung gehören zu den Kernaufgaben des Providermanagements.

Rechenzentren

Die Zuverlässigkeit von Rechenzentren sowie Rechenzentrums-Clustern kann anhand des vom TÜV Informationstechnik GmbH (TÜViT) entwickelten Standards Trusted Site Infrastructure (TSI) bestätigt werden. Dabei ist TSI ein Verfahren zur Prüfung und Zertifizierung der physischen Sicherheit und Verfügbarkeit von Rechenzentren. In den zugrundeliegenden Kriterienkatalog sind Maßnahmenempfehlungen der Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) und einschlägige EN- und DIN-Normen aber auch VDE-Vorschriften und VdS-Publikationen eingeflossen.

Die FI-TS Rechenzentren sowie die Rechenzentrums-Cluster sind nach TSI zertifiziert und werden regelmäßig überprüft.

State-of-the-Art-Technologien – im Einklang mit aufsichtsrechtlichen Vorgaben

Als erfahrener IT-Outsourcing-Partner der Finanz- und Versicherungsbranche sind der präzise Umgang mit strengsten Sicherheits- und Qualitätsrichtlinien sowie das Erfüllen der gesetzlichen Vorgaben für FI-TS selbstverständlich.

Optimiert für die regulatorischen Anforderungen an Banken, Finanzdienstleister und Versicherungen.

FI-TS arbeitet mit allen relevanten Richtlinien und Zertifizierungen für Qualität und Sicherheit. Vom Betrieb der Rechenzentren über unsere Services bis hin zum Projektmanagement:

DIN EN ISO 9001

Qualitätsmanagementsystem

ISO/IEC 27001

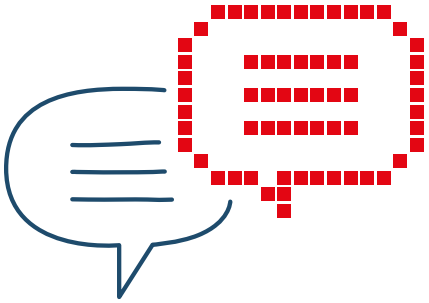
Informationssicherheitsmanagementsystem

Über Finanz Informatik Technologie Service (FI-TS)

Die Finanz Informatik Technologie Service GmbH & Co. KG (FI-TS) ist ein etablierter IT-Partner der Finanzwirtschaft und größter IT-Dienstleister für Landesbanken. Als Tochter der Finanz Informatik (FI) und Teil der Sparkassen-Finanzgruppe unterstützt der IT-Provider private und öffentliche Banken, Versicherungen und Finanzdienstleister mit standardisierten IT-Dienstleistungen.

FI-TS versteht sich als „The Bridge to Digitalization in Financial Industries“. Auf Basis einer integrierenden IT-Service-Plattform mit Leistungen vom klassischen Rechenzentrumsbetrieb bis hin zu Public Cloud-Produkten und Services wie Compliance, Providermanagement, Transition, Transformation, Beratung ermöglicht das Unternehmen seinen Kunden die digitale Transformation. FI-TS bringt langjährige Erfahrungen aus der Finanzbranche in Kundenbeziehungen ein und richtet seine Services an den regulatorischen Anforderungen der Branche aus – „IT made for Banking and Insurance“.

Die hundertprozentige Tochter der Finanz Informatik hat ihre Unternehmenszentrale in Haar bei München. Dort und an den Standorten Hannover, Nürnberg, Offenbach und Stuttgart (Fellbach) arbeiten rund 1.000 Mitarbeiterinnen und Mitarbeiter. Der Umsatz beträgt 400 Millionen Euro (2021).



Ihr Mehrwert

Die Anforderungen an eine umfängliche und effiziente Governance steigen permanent und können sich zu einer echten Belastung für Unternehmen entwickeln. Das muss nicht sein – mit den richtigen Partnern profitieren Sie von einer effektiven Umsetzung der anspruchsvollen gesetzlichen und regulatorischen Vorgaben.

FI-TS bietet mehr Transparenz, Sicherheit und klare Entscheidungsstrukturen für Ihr Unternehmen sowie ein Qualitätssiegel, das Sie deutlich von Ihren Mitbewerbern abhebt.

Wir können langjährige Erfahrung mit durch BaFin[1] oder EZB[2] beaufsichtigte Kunden nachweisen. Erkenntnisse aus Prüfungen der Aufsichten fließen regelmäßig in die Verbesserung der angebotenen Services ein.

[1] BaFin: Bundesanstalt für Finanzdienstleistungsaufsicht

[2] EZB: Europäische Zentralbank

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.

Finanz Informatik Technologie Service

Richard-Reitzner-Allee 8, 85540 Haar
+49 89 94511-0
anfragen@f-i-ts.de
www.f-i-ts.de

finanz **informatik**
technologie service