



Sicherheits- und Risikomanagement Anforderungen durchgängig analysieren und zeitgemäß umsetzen

Themenbereich: Sicherheit

Messe-Stand: SI03

Fragen beantwortet
Ihnen Ihre zuständige
Kundenberatung

Aktuelle gesetzliche und regulatorische Anforderungen – beispielsweise aus 5. MaRisk Novelle und BAIT – werden durchgängig analysiert und in einem Gesamtsystem ganzheitlich verfolgt.

Durchgängig

Ein umfassendes Informationssicherheitsmanagementsystem (ISMS) in Kombination mit einem vernetzten Risikomanagement und einem regelmäßig erprobten Notfallmanagement bietet unseren Kunden einen guten Schutz ihrer Daten:

- Regelmäßige Überprüfungen, Audits und Sicherheitstests kontrollieren die Wirksamkeit der implementierten Maßnahmen.
- Externe Zertifizierungen und Prüfungen bestätigen unseren Kunden die Angemessenheit der implementierten Schutzmaßnahmen.
- Die zahlreich durchgeführten Notfallübungen helfen die definierten Notfallvorsorgemaßnahmen ständig zu überprüfen und fortzuschreiben, um unseren Kunden im Fall eines Falles schnellstmöglich eine Geschäftsfortführung zu ermöglichen.
- Ein unternehmensweit etabliertes Risikomanagement hilft Risiken frühzeitig zu erkennen und angemessen zu steuern. Es unterstützt unsere Kunden bei ihrem eigenen Risikomanagement.

Verzahnt

Die Managementsysteme zur Informationssicherheit, dem Risiko- und Business Continuity Management leiten sich direkt aus der Geschäftsstrategie der Finanz Informatik ab. Die etablierten Prozesse wirken mit allen Unternehmensbereichen der FI zusammen.

Zeitgemäß

Zur Steigerung der Transparenz hinsichtlich des implementierten Schutzniveaus enthält der Produktkatalog der Finanz Informatik konkrete Informationen zu Referenzmaßnahmen.

Bitte umdrehen >>



Seite 02

- Die Finanz Informatik betreibt ein nach internationalem Standard ISO27001:2013 zertifiziertes ISMS. Zur Implementierung des ISMS werden zusätzlich die im Rahmenwerk »Sicherer IT Betrieb« (derzeit SITB V.16) der SIZ GmbH enthaltenen Konzepte herangezogen.
- Ein erweitertes Informationsrisikomanagement ermöglicht eine bankaufsichts-konforme Überwachung und Steuerung von Informationssicherheitsrisiken im Unternehmen sowie eine erhöhte Transparenz für unsere Kunden.
- COBIT 5 for Risk steigert die Risikotransparenz durch systematische Analysemethoden zur frühzeitigen Erkennung von IT-Risiken.
- Mit dem BCM-Prozess werden die jeweils geltenden Anforderungen aus den MaRisk und aus den SIZ-Konzepten des »Sicheren IT-Betriebs« umgesetzt. Die Ausgestaltung orientiert sich am ISO-Standard 22301:2012.

Die schriftlich fixierte Ordnung der Finanz Informatik ermöglicht durchgängig und zeitgemäß eine Verknüpfung der Schutzanforderungen aus der jeweiligen Stufe.

Fragen beantwortet
Ihnen Ihre zuständige
Kundenberatung.