IT-Sicherheit im Fokus des Gesetzgebers

Banken, Versicherungen und Finanzdienstleister

Bundesinnenminister Thomas de Maizière stellte im August 2014 den Entwurf für ein **neues IT-Sicherheitsgesetz** vor. Ziel sei es, dass "branchenweite Standards für die IT-Sicherheit in den Bereichen der Wirtschaft eingeführt werden, **die für das Wohl unserer Gesellschaft von elementarer Bedeutung sind**".

*Zu den wichtigen und elementaren Branchen zählen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie das **Finanz- und Versicherungswesen**.*

Kernpunkte sind eine gesetzliche **Meldepflicht für IT-Sicherheitsvorfälle** sowie die **Einhaltung von IT-Mindeststandards** in der Wirtschaft und eine **regelmäßige Nachweispflicht**, die Anforderungen an **IT-Sicherheit** zu erfüllen.

Sind Sie vorbereitet? Wir können helfen!

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) überprüft die Umsetzung der Mindestanforderungen an das Risikomanagement (MaRisk) regelmäßig im Rahmen der Jahresabschlussprüfung, in den vergangenen Jahren auch vermehrt in Form von **Sonderprüfungen** (§44 Abs. 1 KWG).

Laut MaRisk müssen Prozesse etabliert und technische sowie organisatorische Maßnahmen umgesetzt werden, um einen sicheren und anforderungskonformen Betrieb von IT Systemen in Kreditinstituten herzustellen. Thematische Schwerpunkte sind vor allem IT-Sicherheit, IT-Risikomanagement, die zugehörigen IT-Prozesse und ein effektives Notfallkonzept.

ISIS12 – Die Lösung für MaRisk und IT-Sicherheitsgesetz

- AT 2.2 Tz. 1 Regelmäßige Risikoinventur
- AT 3 Tz. 1 Gesamtverantwortung der Geschäftsleitung
- AT 4.2 Tz. 1 Geschäftsstrategie / IT-Strategie
- AT 4.2 Tz. 2 Risikostrategie
- AT 4.3 Internes Kontrollsystem
- AT 5 Organisationsrichtlinien
- AT 6 Dokumentation
- AT 7.2 Tz. 2 Informationssicherheit nach gängigen Standards
- AT 7.2 Tz. 3 Prozesse f. Implementierung u. Anpassung von IT-Systemen
- AT 7.3 Notfallkonzept
- AT 8.2 Änderung betrieblicher Prozesse und Strukturen
- AT 9 Outsourcing
- BTO Tz. 9 Funktionstrennung bei IT-Unterstützung
- BTR 4 Tz. 2 Mind.

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

powered by: ISIS12 Informationssicherheit für den Mittelstand — apsec applied security

IT-Sicherheit im Fokus des Gesetzgebers

Banken, Versicherungen und Finanzdienstleister

Stärken kombinieren und Vorhandenes nutzen

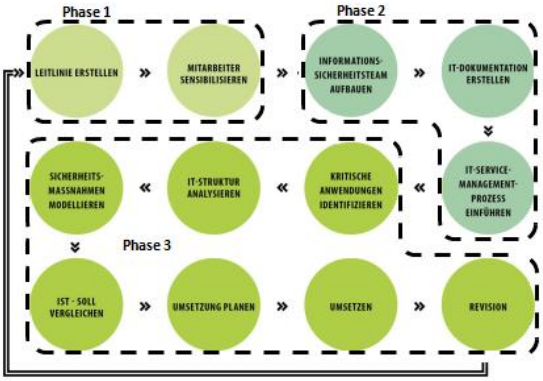
Der besondere Vorteil von ISIS12 in Bezug auf den Einsatz bei Banken, Sparkassen, Volks- und Raiffeisenbank sowie Finanzdienstleistern entsteht dabei durch die **konzeptionelle Verbindung der Stärken verschiedener Rahmenwerke**.

Die umfangreichen Maßnahmen der BSI IT-Grundschutzkataloge wurden mit Blick auf die Zielgruppe **reduziert, zusammengefasst und vereinfacht** und ergeben mit den ausgewählten, eher abstrakten, aber strukturierenden Elementen aus der ISO/IEC 2700x einen **klaren, konkret anzuwendenden Leitfaden**.

Die ebenfalls erfolgte Integration der aus der ITIL stammenden IT-Service-Management-Prozesse und der im ISIS12 Vorgehensmodell definierte PDCA-Prozess, führen dann im Ergebnis zu **einem nachhaltigen und dokumentierten Managementansatz** auf strategischer und operativer Ebene.

Damit ist es einem Institut durch die Anwendung des ISIS12-Vorgehensmodells möglich, eine Vielzahl von Anforderungen des **kommenden IT-Sicherheitsgesetzes und der Mindestanforderungen an ein Risikomanagement** (MaRisk) zu adressieren, und durch die Ableitung von BSI IT-Grundschutz, ISO/IEC 2700x und ITIL auf gängige Standards im Bereich der Informationssicherheit zu setzen.

Aufgrund der in aller Regel bereits vorhandenen umfangreichen Regelungen und Dokumentationen in den Instituten zu den einzelnen Bausteinen, kann eine ISIS12 Implementierung auch durch kleine und mittlere Institute mit **akzeptablem Aufwand und Ressourceneinsatz und ohne lange Projektlaufzeiten umgesetzt werden**.



Das ISIS12-Vorgehensmodell wurde in drei Grobphasen aufgeteilt. Vor den eigentlichen operativen Schritten, der Entwicklung der Sicherheitskonzeption (Phase 3), gilt es nach der Initialisierungsphase, zuerst die für den weiteren Verlauf notwendigen Voraussetzungen zu schaffen. Das Vorgehensmodell orientiert sich zwar an der bewährten BSI Grundschutzmethodik, ist aber dennoch ein neuer, für den Mittelstand und Organisationen entwickelter Ansatz.

Zertifizierung macht das verantwortungsbewusste Handeln der Geschäftsleitung nach außen sichtbar

Sobald Sie ISIS12 erfolgreich in Ihrem Institut eingeführt haben und der Schritt 12, die Revision abgeschlossen ist, können Sie sich **von der DQS als Exklusivpartner nach ISIS12 zertifizieren lassen**. Das Zertifikat hat eine Gültigkeit von drei Jahren. In diesen drei Jahren finden zwei Überwachungsaudits statt. Im dritten Jahr kann durch eine Rezertifizierung das Zertifikat neu erteilt werden.

IHR NUTZEN

ISIS12 – **MaRisk konform**

ISIS12 – **Mindeststandard** für ein **Informationssicherheits-Managementsystem** (ISMS)

ISIS12 – **baut auf bestehende Strukturen im Unternehmen auf**

ISIS12 – ist **überschaubar**, **schlank** gehalten und ein **verständlich** beschriebener 12-stufiger Prozess für die Etablierung eines ISMS

ISIS12 - **eigenständiger Betrieb problemlos möglich!**

ISIS12 – **orientiert sich an ISO 27001/BSI Grundschutz** mit einem speziell für den **Mittelstand angepassten**, auf **unternehmenskritische Anwendungen konzentrierten Maßnahmenkatalog** und kann als **Vorstufe zur ISO/IEC27001- bzw. BSI IT-Grundschutz-Zertifizierung** verwendet werden

ISIS12 – enthält **klar formulierte Anweisungen**, auch zur **IT-Dokumentation** und zum **IT-Service Management** (ISMS und IT-SM werden im Managementprozess integriert)

ISIS12 – **beinhaltet Datenschutz- und Notfallmanagement**

ISIS12 – **werbewirksam zertifizierbar** durch die DQS – Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

powered by: ISIS 12 Informationssicherheit für den Mittelstand — apsec applied security