



ISPIN
Swiss made Security.

Success Story Alternative Bank ABS

Alternative Bank ABS – Revision in 20 Minuten

Der jährliche Besuch der Rechnungsprüfer ist im Allgemeinen nicht sehr beliebt. Das bei der Alternativen Bank ABS implementierte Information Security Management System bringt die Rechnungsprüfer auf den richtigen Weg.

Die Alternative Bank ABS mit Sitz in Olten (Schweiz) folgt einer alternativen Finanzpolitik, die auf ethischen Prinzipien statt auf Gewinnmaximierung basiert. Die Tatsache, dass dieses Prinzip auch wirtschaftlich funktioniert, wird durch die Geschäftsberichte auf der Website belegt. Das Hauptsegment dieser besonderen Bank sind zinsspannenbasierte Aktivitäten, während das Servicegeschäft noch ausgebaut wird. Die Bank hat mehr als 50 Mitarbeiter



und verfügt über Vertretungen und Kontaktstellen in Lausanne, Genf, Zürich und Bellinzona. Die Alternative Bank ABS betont ihre Transparenz – so ist im Geschäftsbericht jeder Kreditnehmer mit Namen und Kredithöhe verzeichnet. Entsprechend werden auch Risiken offen kommuniziert, was ein ISMS mit allgemein anerkannten Prinzipien erforderlich macht. Sicherheitsbezogene Themen und Status müssen für Management und Rechnungsprüfer transparent dargestellt werden. Mit der Einführung eines Information Security Managements können fest formulierte Anforderungen an die Informations-

Marc Gerber, Leiter Informatik, Alternative Bank ABS:

«Es begann mit einer Voranfrage für die Entwicklung eines ISMS. ISPIN AG zeigte uns die Möglichkeiten auf und legte uns die die aktuellen Normen optimaler Verfahren wie ISO 27001, BSI-Norm und CobIT vor. Wir zogen ein Serviceprogramm zum Aufbau und Management des ISMS in Betracht. Dabei hatten wir die Wahl zwischen einem programmgestützten Verfahren zur Prozessmodellierung, der Verwendung einer Tabellenkalkulation oder der Auswertung durch spezielle Drittanwendungen.

ISPIN hat es gut verstanden, die Massnahmen präzise und einfach zu formulieren.

Anhand dieser Analyse haben wir im darauf folgenden Jahr die Umsetzung des ISMS in Auftrag gegeben. In ISPIN sehen wir zur Unterstützung bei allen Lösungen den richtigen Partner.»

Fazit

«ISPIN konnte kurzfristig in enger Zusammenarbeit mit der Alternativen Bank ABS einen nachhaltigen Mehrwert schaffen, ohne dabei das knappe Budget zu überziehen.

Mittlerweile verwendet die Alternative Bank ABS eine von ISPIN entwickelte webgestützte Anwendung, die die Tabellenkalkulation ersetzt. Die anfängliche Sorge der Alternativen Bank ABS hinsichtlich zu grosser, abstrakter Implementierungsvorschläge konnte dank offener Kooperation sehr schnell zerstreut werden.

Mit Hilfe des webbasierten Tools hat die Alternative Bank ABS nun begonnen, ihren Mitarbeitern sicherheitsrelevante Themen bewusst zu machen. Gleichzeitig bietet das Intranet ein Dokumentensammlung zu diesem Thema.»

sicherheit hinsichtlich ihrer Einhaltung (einschliesslich empfohlener Massnahmen) definiert werden.

Das Projekt ISMS

Folgende Bedingungen mussten zu Beginn des Projekts berücksichtigt werden:

– So einfach wie möglich

Basierend auf den vielen teils abstrakten Modellen muss das ISMS für die Alternative Bank ABS exakte Aktionen enthalten und Sollmassnahmen ausklammern.

– Kosten

Der Nutzen des Projekts muss offensichtlich sein, da die Bank nicht Monate für Berateraufträge und komplexe Tools aufwenden will.

Anwendung und Handhabung des ISMS müssen auch für Mitarbeiter aus anderen Bereichen einfach sein.

Ebenso muss ein mögliches Tool eine intuitive Handhabung gewährleisten – ohne grossen Lernaufwand.

– Anwenderbewusstheit

Das ISMS ist nicht das einzige Projekt der IT-Abteilung. Es muss das Bewusstsein der Mitarbeiter hinsichtlich Informationssicherheit schärfen und eine Informationsplattform zu sicherheitsrelevanten Themen bieten.

Vorgehensweise

Zur Entwicklung des Information Security Managements sind folgende Schritte erforderlich:

1. Definition des Umfangs

Grösse und Umfang des ISMS wurden entsprechend den Anforderungen der ABS und basierend auf der Ausgangsanalyse von 2004 definiert – unter der Verantwortung der Alternativen Bank ABS.

2. Auswahl von Kontrollmechanismen und Massnahmen

Basis für den Massnahmenkatalog der Alternativen Bank ABS bilden hauptsächlich die Anforderungen aus BSI-Norm, CobIT, bankenspezifische Anforderungen und gesetzliche Bestimmungen. Kontrollmechanismen aus ISO 27001 wur-



Beispielbewertung «Laufzeitanalyse», geordnet nach Themen

den bewusst nicht berücksichtigt, da diese Norm keine detaillierten Implementierungsanweisungen enthält.

ISO 27001 behandelt hauptsächlich den Aufbau eines Information Security Managements und die organisatorischen Aspekte. Die BSI-Norm beschreibt detailliert standardisierte Sicherheitsmassnahmen, die sich auf nahezu alle Informationssysteme anwenden lassen, ohne der ISO 27001 zu widersprechen.

Beim Aufbau des Fragebogens war es wichtig, dass die Anforderungen der Alternativen Bank ABS nachvollziehbar sind, darauf reagiert werden kann und sie in kürzester Zeit implementiert werden können – auch ohne umfassende Kenntnis von Sicherheitsbelangen und -bereichen. Nicht das «Was» ist wichtig, sondern das «Wie». «ISPIN hat es gut verstanden, die Massnahmen präzise und einfach zu formulieren», bestätigt Marc Gerber.

Die Beurteilung des aktuellen Sicherheitsstatus basierte auf der Beschreibung von sicherheitsrelevanten Anforderungen (Massnahmenkategorien) für die Schutzstufe – definiert für die Alternative Bank ABS.

Die sicherheitsrelevanten Anforderungen wurden dem Rang (Menschen, Anwendungen, Systeme, Netzwerk, Gebäude) und folgenden Fachgebieten zugeordnet:

- Zugangsschutz
- Zugriffsschutz
- Geschäftsfortgang (Katastrophenplan)
- Backup
- Sicheres Systemmanagement
- Einhaltung und Gesetz
- Training & Bewusstmachung



3. Dokumentieren der Vorschriften und Massnahmen

In einem gemeinsamen Workshop wurden die Anforderungen gemäss definierten Leistungskriterien bewertet.

Wo interne Dokumente bereits existierten und die Anforderungen abdecken konnten, wurden sie entsprechend eingebunden und auf sie verwiesen.

Wo die Anforderungen nicht durch bestehende Vorschriften oder Dokumente abgedeckt werden konnten, wurden geeignete Massnahmen definiert und möglichst umgehend implementiert.

Bei noch nicht implementierten Massnahmen wurden Verantwortung und Zeitrahmen sowie Priorität definiert.

4. Kommunikations- und Berichtswesen – ISMS lebt!

Anhand einer grafischen Analyse (Bewertungsgrafik) kann der aktuelle Sicherheitsstatus kommuniziert werden. Die Bewertungsgrafik liefert einen Hauptzugangspunkt für das Intranet im Sicherheitsbereich. «Die Strukturierung der Anforderungen anhand von Rängen oder Themen erlaubt uns, schnell aufzuzeigen, wo welche Informationen zu welchem IT-System oder Thema verfügbar sind und welche Anforderungen erforderlich sind», erläutert Marc Gerber. So können Mitarbeiter z. B. einfach auf sicherheitsrelevante Anforderungen für ein Mail-System zugreifen. Zusätzlich erfährt der Mitarbeiter, auf welcher Norm die Anforderung basiert (BSI, CobiT, bankenspezifische Anforderungen) und welche Massnahmen bereits ergriffen wurden. Das standardisierte Information Security Managementsystem «lebt», und die Mitarbeiter werden auf spezifische Sicherheitsthemen aufmerksam gemacht. Die Struktur des ISMS kann jederzeit an interne Änderungen angepasst werden und ist ausbaufähig.

Swiss made Security.

Die Schweiz steht für Qualität, Neutralität, Stabilität und Kompetenz. Entsprechend diesen Attributen bieten wir nutzbringende, sinnvolle Lösungen im Bereich Informationssicherheit und Datenschutz. Unser umfassendes Leistungsangebot ermöglicht es Ihnen, sämtliche Sicherheitslösungen aus einer Hand zu erhalten. Als Spezialist für einfache Lösungen verlieren wir nie die Sicht auf das Ganze. Dass ISPIN ein vertrauenswürdiger Partner ist, der für Qualität und Kompetenz steht, bestätigen die über 140 langjährigen Geschäftsbeziehungen.



Wissenstransfer ist wichtig. Aus diesem Grund engagieren sich die Mitarbeiter der ISPIN AG in diversen Verbänden und bei Fachtagungen. Dazu gehören ISSA, Symposium on Privacy und Security, Datenschutzforum oder Infosurance. Dank dieser Verbände und Tagungen bleibt das erlangte Wissen nicht bei einer einzelnen Person, sondern wird veröffentlicht und schriftlich sowie mündlich weitergegeben.

**Wir schützen
vertrauliche Informationen.**



ISPIN AG
Grindelstrasse 15
CH-8303 Bassersdorf
Tel. +41 44 838 31 11
Fax +41 44 838 31 12
E-Mail: info@ispin.ch
www.ispin.ch