Security as a Service

Das richtige Know-how und das richtige Mass an Sicherheit sind ausschlaggebende Faktoren für den Erfolg der Informations- und ICT-Sicherheit; daneben gilt es, den aktuellsten Bedrohungen immer angemessen begegnen zu können. In der heutigen Zeit verlangt dies jedoch nach einem grossen Team von Security-Spezialisten, welches sich auch der Bedrohungslage und der Strategie der Unternehmung fortlaufend anpasst.

Aufgaben der Informationssicherheit

Die Security-Verantwortlichen müssen viele verschiedene Aufgaben bewältigen, um erfolgreich zu sein: Die Informationssicherheit einerseits zeichnet sich durch ihren technologieübergreifenden Charakter aus und reicht bis in Organisation, Risk und Compliance, Governance sowie in Spezialthemen wie bspw. HR und Marketing hinein. Die ICT-Sicherheit andererseits hat einen klaren Technologiefokus und muss nahtlos mit der regelgebenden Informationssicherheit zusammenwirken. Zudem muss ein geschützter Betrieb durch die Einhaltung eines Change-Risk-Managements sichergestellt werden. Und das alles innerhalb von diversen regulatorischen Vorgaben. All diese Funktionen können kaum von einer einzelnen Person wahrgenommen werden. Hierzu benötigt man ein ganzes Team von Security-Spezialisten.

Mit Security as a Service multiplizieren Sie Ihre Investition in Sicherheit, da Sie für die Kosten eines Mitarbeiters ein ganzes Team von hochqualifizierten Security-Experten erhalten.

Häufige Probleme von Inhouse Lösungen

Die Komplexität der Thematik und die daraus resultierenden Anforderungen an interne Mitarbeitende stellt viele Unternehmen oft vor folgende Probleme:

- Abhängigkeit von einer Person (wer übernimmt im Falle von Ferien, Krankheit, Unfall, etc.?)
- Oft kein themenübergreifend umfassendes Spezialistenwissen inhouse (ausser Spezialgebiet der Person)

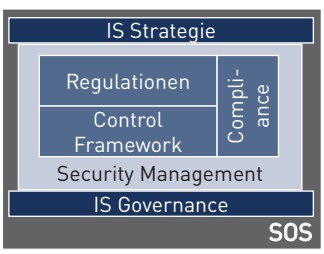
Ihre Geschäftsprozesse können sich verändern. Der Security Service ändert sich automatisch mit.

- Zuzug von Spezialisten notwendig
- Planbarkeit von Ressourcen/Kosten schwierig
- Flexibilität auf 1 Person beschränkt
- Diskussion der hierarchischen Zugehörigkeit des Security Verantwortlichen (Management Level, Salarierung, etc.)
- Kein implizites Benchmarking möglich (keine tiefe Sicht in andere Unternehmen)

SaaS Modelle von ISPIN

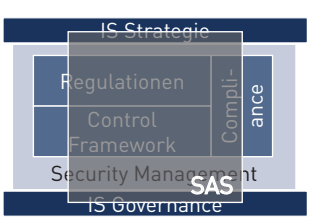
ISPIN bietet diverse Modelle von Security as a Service an, was eine massgeschneiderte Integration in Ihr Unternehmen ermöglicht. Alle SaaS-Modelle erlauben es, das für Ihre Unternehmung passende Control Framework (ISO27002, NIST, BSI,...) und die für Ihre Unternehmung relevanten externen Regulationen und Vorgaben (FINMA RS, GxP, ...) gemäss Ihrem individuellen Schutzbedürfnis umzusetzen.

Security Officer Service (SOS)



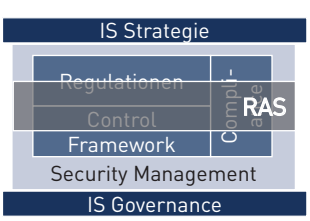
ISPIN stellt einen dedizierten Security Officer zur Verfügung. Dieser übernimmt die Führung der Security und setzt die Verbesserungsprozesse gemäss Security Masterplan um. Zudem ist er Ansprechpartner für alle internen, security-relevanten Themen.

Security Advisory Service (SAS)



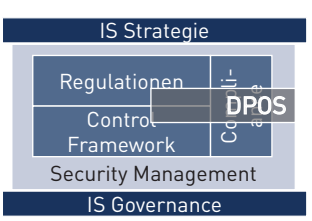
Der bereits vorhandene interne Security Officer erhält beim Security Advisory Service von ISPIN die Unterstützung, die er für die Erfüllung seiner Funktion benötigt. Je nach Themengebiet stellt ISPIN zusätzlich ausgewiesene Fachspezialisten bereit.

Risk Assessment Service (RAS)



Der Risk Assessment Service ermöglicht es Ihnen, mit Unterstützung von ISPIN-Fachspezialisten Ihre Change-Projekte auf Risiken zu beurteilen. Sie erhalten eine transparente Übersicht über alle Risiken, welche durch Changes hinzugefügt werden.

Data Protection Officer Service (DPOS)



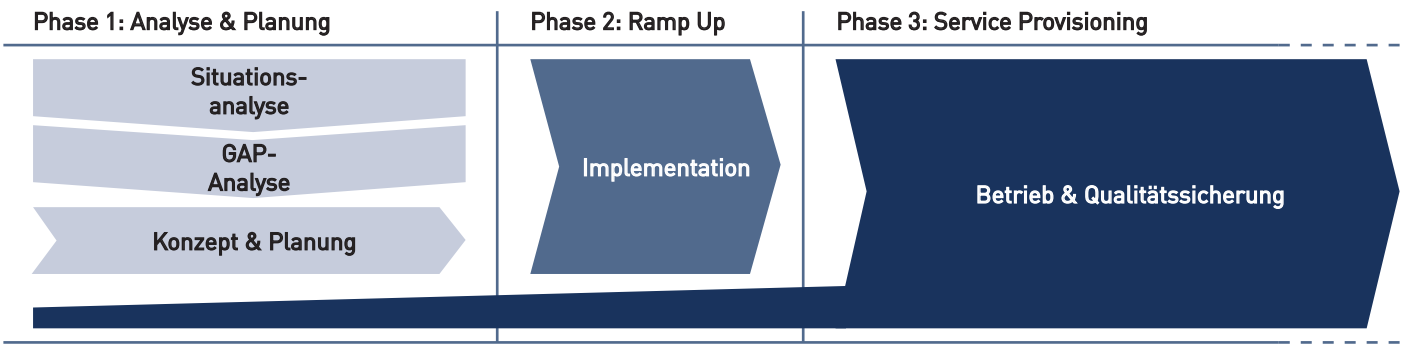
Beim Data Protection Officer Service stellt ein ISPIN-Fachspezialist die Einhaltung des Datenschutzgesetzes und im Finanzumfeld des Bankgeheimnisses in Ihrer Unternehmung sicher.

ISPIN AG ZURICH
swiss made security.

Gründe für den Security Service von ISPIN

- **Steigende Compliance Anforderungen**: Die externen Anforderungen zwingen Unternehmen in Compliance zu investieren. Obwohl oft nur eine Teilzeistelle nötig wäre, um die Funktion aufrecht zu erhalten, muss eine Vollzeitstelle dafür eingesetzt werden.
- **Benchmarking**: Aufgrund der breiten Erfahrung von ISPIN können wir Ihnen ein Benchmarking mit anderen Unternehmen in der gleichen Branche zur Verfügung stellen.
- **Steigende Komplexität**: Die steigende Komplexität der Cyber-Bedrohungen führt zu einem exponentiellen Wachstum an benötigtem Spezialisten-Personal. Wir können Ihnen die richtige Person für Ihre Situation zur Verfügung stellen.
- **Haftungsrisiken**: Diverse Regulationen setzen Unternehmen immer mehr Haftungsrisiken aus, falls Sorgfaltspflichten nicht eingehalten werden. Mit unserer Erfahrung können wir sicherstellen, dass Security und Compliance richtig umgesetzt werden.
- **Kostentransparenz**: Sie wissen aufgrund des Fixpreises immer, wieviel Sie der Service kostet.
- **Image**: Den Namen seiner Unternehmung wegen eines erfolgreichen Hacker-Angriffes in der Presse zu lesen, führt oft zu Reputationsproblemen und kann einen direkten Einfluss auf Ihren Umsatz haben.
- **Steigende Anforderungen an Know-how**: Security-Spezialisten müssen immer am Ball bleiben, die Anforderungen an ihre Ausbildung steigen stetig. Wir halten unsere Security-Experten in Sachen Sicherheit auf dem neuesten Wissensstand.
- **Planungssicherheit**: Ihre Geschäftsstrategie kann sich ändern, der Security Service von ISPIN ändert sich automatisch mit. Die damit verbundene Planungssicherheit verhindert versteckte Kosten.
- **Professioneller Partner mit höchstem Sicherheitslevel**: ISPIN hat über 15 Jahre Erfahrung im Bereich Cyber Security und verfügt über hochqualifizierte Mitarbeitende.
- **Personelle Unabhängigkeit**: Sie müssen sich nicht um Rekrutierung, Mitarbeiterförderung, Karriereplanung, Ausfall durch Krankheit oder Unfall und alle anderen personellen Herausforderungen kümmern. Wir machen das für Sie!

Phasen des Security as a Service



Der Einstieg in ein SaaS beginnt mit der **Analyse & Planungs-Phase.** Wir analysieren die aktuelle Situation der Informationssicherheit in Ihrer Unternehmung. Dies wird, je nach SaaS-Modell in unterschiedlicher Tiefe und Breite, basierend auf einem etablierten Analyseprozess durchgeführt. Eine GAP-Analyse zeigt auf, wo die Lücken in Bezug auf Ihren Sicherheitsbedarf und Ihren regulatorischen Vorgaben liegen.

Diese beiden Resultate fliessen in unseren Security-Masterplan ein, welcher die Strategie und den Plan für die Umsetzung der Security-Massnahmen über die nächsten Jahre definiert. Dieser Masterplan wird in enger Zusammenarbeit mit Ihnen erarbeitet und von Ihrer Unternehmensführung abgesegnet. Die Freigabe stellt den ersten grossen Meilenstein dar, der den Start der zweiten Phase, der Ramp Up-Phase initiiert.

Bereits ab dem ersten Tag des SaaS Services, übernimmt ISPIN Tagesthemen und unterstützt Sie in Ihren Security-Aktivitäten.

In der **Ramp Up-Phase** beginnen die dedizierten ISPIN-Spezialisten sich in Ihre Unternehmung zu integrieren und den Service, je nach gewähltem Modell, hochzufahren. Die nötige Governance wird aufgebaut, Prozesse definiert und etabliert; dies alles mit transparentem Monitoring und Reporting und in enger Zusammenarbeit mit Ihnen. Arbeitsabläufe werden optimiert und so angepasst, dass sie optimal in Ihre internen Abläufe und in Ihre individuelle Unternehmenskultur passen. Erst nach erfolgter Freigabe, dem zweiten wichtigen Meilenstein in unserer Zusammenarbeit, erreichen wir die dritte Phase, die Betriebs- und Qualitätssicherungs-Phase.

In der **Betriebs- und Qualitätssicherungs-Phase** läuft der Security Service in Ihrer Unternehmen. Durch regelmässige Qualitätsmessungen und im regelmässigen Kontakt mit Ihnen stellen wir sicher, dass unsere Leistungen Ihren Ansprüchen vollumfäglich gerecht werden.

Kontaktieren Sie uns.

Gerne stellen wir eine massgeschneiderte Offerte für Sie zusammen.
Kontaktieren Sie uns für mehr Informationen und Referenzauskünfte.

Craig Fletcher, CCO
+41 44 838 31 11
craig.fletcher@ispin.ch