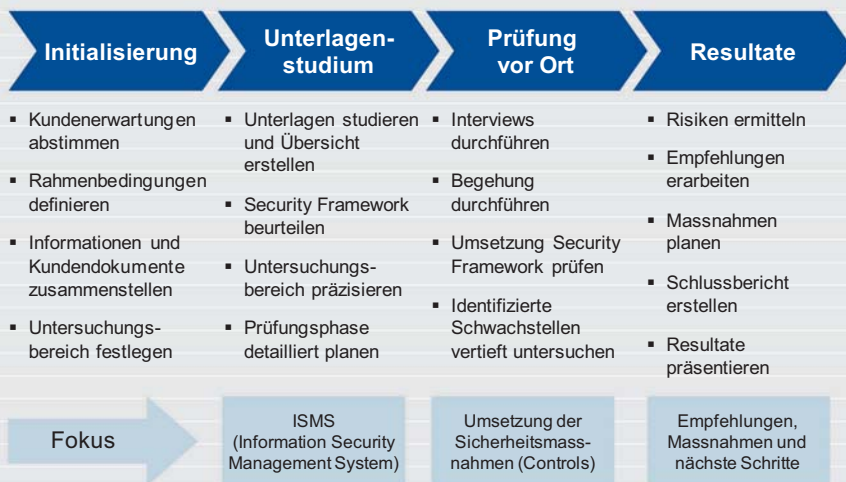


Durch unabhängige Aussensicht Schwachstellen erkennen und bewerten

Die fortschreitende Automatisierung von Geschäftsprozessen macht Unternehmen zunehmend abhängig von der Informationstechnologie. Verarbeitete Informationen sind angemessen zu schützen, da der Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit zu erheblichen Image-/Finanzschäden führen kann. Damit es nicht soweit kommt, muss der Sicherheitsbeauftragte im Unternehmen über den Zustand der IT-Landschaft im Bild sein.

Der Bericht des externen Auditors bringt hierfür die wichtige, unabhängige Aussensicht ein. Erfahrungsgemäss werden damit Schwachstellen und Risiken entdeckt die andernfalls, teils wegen "Betriebsblindheit", verborgen bleiben würden.

Erfahrungswerte des Auditors erlauben zusätzlich zur Bewertung gegenüber ‚Best Practices‘ (z.B. ISO27001/02) eine objektive Aussage im Branchenvergleich. Die Definition und Priorisierung von Massnahmenvorschlägen durch den Auditor zeigt konkret das Vorgehen für Verbesserungen auf. Die nachfolgende Grafik zeigt das Vorgehen von AWK in einem Audit.



Kann sich Ihre IT sehen lassen?

Die Investitionen zum Schutz von Informationen haben in den letzten Jahren laufend zugenommen. Getrieben von Compliance-Anforderungen hat die Einführung von Kontrollsystemen, IT-Governance-Frameworks und Key Performance Indicators zu einer Professionalisierung geführt. Die regelmässigen, unabhängigen Prüfungen werden dadurch jedoch nicht ersetzt. Denn die Servicequalität sowie die Aussagekraft von Kontrollmechanismen erodiert auf Grund von Nachlässigkeit, Ignoranz oder Überoptimierung. Gerade in turbulenten Zeiten mit massivem Spardruck kann sich diese Entwicklung beschleunigen. Audits sind das richtige Mittel, um die dadurch entstehenden Schwachstellen zu identifizieren.



Thomas Diem
CISA

Senior Consultant

Unsere Dienstleistungen

Klar strukturierte, nachvollziehbare Vorgehensweise und Arbeitsergebnisse:

- Dokumentieren der Schwachstellen
- Einschätzung des Risikopotenzials der Schwachstellen
- Massnahmenvorschläge zur Behebung von Schwachstellen
- Objektive Darstellung des Gesamteindrucks in einem Management Summary

Professionelles Audit-Team:

- Zertifizierte Auditoren: CISA, CISM (ISACA); ISO Lead Auditor (ISO)
- Versierte Auditoren mit langjähriger Erfahrung im Bereich Informationssicherheit

Bewertung nach Good Practice:

- Objektive Bewertung; frei von Interessenbindungen
- Basierend auf anerkannten Normen und Standards

Optionen:

- Einführende Business Impact Analyse zur Gewichtung der Audit Ergebnisse
- ISO27001 Kurzassessment
- Masterplanung für die Bereinigung der Schwachstellen inkl. zeitlichem Ablauf, Priorisierung und geschätztem Aufwand

Unsere Kunden

Die AWK Group hat u. a. bei den folgenden Unternehmen und Organisationen bereits erfolgreich IT-Audits durchgeführt:

- Aargauische Kantonalbank
- AEK Energie
- Bulgarian Telecommunications Company
- Bundesamt für Statistik
- Elektrizitätsgesellschaft Laufenburg
- Kanton Schaffhausen
- Kanton Schwyz
- Orange Communications
- Schweizerische Bundesbahnen SBB
- Stadt Zürich
- Swisscom
- Swisspower

Untersuchungsgebiet und Nachforschungstiefe beeinflussen den Auditaufwand.

Das Untersuchungsgebiet kann die gesamte Informatik inklusive Organisation, Prozesse und Infrastruktur umfassen oder sich auf einzelne geschäftskritische Fachapplikationen und Schlüsselkomponenten der IT-Infrastruktur konzentrieren. Gerne unterstützen wir Sie bei der Festlegung des Untersuchungsgebiets zum Beispiel mit einer einführenden Business Impact Analyse.

Die Wahl der sinnvollen Nachforschungstiefe ergibt sich aus dem Kundenbedürfnis und der Maturität der IT. AWK empfiehlt einen Top-Down-Ansatz und bewertet hierzu die Ist-Situation basierend auf der vorhandenen Dokumentation (Weisungen, Prozesse, Organisation, Spezifikationen). Davon ausgehend kann die Fokussierung des Audits sowie die sinnvolle Nachforschungstiefe gemeinsam mit dem Kunden festgelegt werden.