

Anwendergruppen und Markt für die **GAP View** Audit Management Software

Eine Reihe von nationalen und europäischen Gesetzen, Richtlinien sowie branchenspezifischen Regelungen verpflichten Behörden, Unternehmen und sonstige öffentliche oder private Organisationen zur Umsetzung geeigneter IT-Sicherheitsmaßnahmen in Form eines ISMS mit dem Ziel, die Widerstandsfähigkeit der genannten Institutionen gegenüber Cyber-Angriffen zu erhöhen.

Sicherheitsstandards und ihre Wirksamkeit

In Deutschland haben sich vor allem die Norm **ISO/IEC 27001** mit ihren fach- und branchenspezifischen Subnormen, die **BSI-Standards** sowie einige weitere Standards, die insbesondere für KMU geeignet sind, etabliert. **Alle** genannten Sicherheitsstandards schreiben eine regelmäßige Überprüfung ihrer Wirksamkeit und Angemessenheit durch **entsprechende Audits und IS-Revisionen** vor.

1. Anwendergruppe: Behörden

Im Rahmen der Umsetzung der „Cyber-Sicherheitsstrategie für Deutschland 2016“ und des „Umsetzungsplans Bund 2017“ sind die Behörden dazu verpflichtet, mittel- und langfristig Informationssicherheit auf hohem Niveau zu etablieren. Ein wichtiger Bestandteil der Umsetzung ist die regelmäßige Überprüfung der eingeführten Informationssicherheitsmaßnahmen im Rahmen von internen und externen IS-Revisionen. Die entsprechenden Anforderungen dafür sind im BSI IT-Grundschutz-Baustein DER.3.1 „Audits und Revisionen“ festgelegt. Die Methodik dieser Überprüfung ist im „Leitfaden für die Informationssicherheitsrevision auf Basis von IT-Grundschutz“ des BSI definiert. Die GAP View bildet alle Anforderungen des Leitfadens zur Planung, Durchführung und Auswertung von BSI-IS-Revisionen (IS-Querschnitts-, IS-Partial- und IS-Kurzrevision) einschließlich der vorgegebenen Form der Berichterstattung ab. Somit ist sie ein ideales Werkzeug für Informationssicherheits- und Datenschutzbeauftragte sowie für interne IS-Revisoren und das interne IS-Revisionsteam. Weitere Themen die mit GAP View abgedeckt werden können sind, u.a. interne Datenschutzaudits [siehe CON.2 Datenschutz] und Lieferantenaudits [siehe ISO 27001, A.5.19-22 v.1.0

Lieferantenbeziehung] oder [OPS.2.3 Nutzung von Outsourcing].

2. Anwendergruppe: Kritische Infrastrukturen

Die Etablierung eines ISMS ist für Kritische Infrastrukturen (KRITIS) keine freiwillige Maßnahme, sondern eine gesetzliche Pflicht [siehe u. a. BSIG, IT-SiG]. Betreiber kritischer Infrastrukturen sind demnach verpflichtet, „angemessene organisatorische und technische Vorkehrungen zu treffen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ zu vermeiden. Ein ISMS (z. B. nach ISO/IEC 27001, BSI IT-Grundschutz oder B3S) ist ein zentraler Baustein zur Erfüllung dieser Anforderungen. Die Angemessenheit der Maßnahmen muss regelmäßig durch interne und externe Audits sowie IS-Revisionen nachgewiesen werden. Mithilfe von GAP View können langfristige Auditprogramme und interne Audits/IS-Revisionen gemäß den genannten Standards geplant, umgesetzt und als Nachweis der Angemessenheit dokumentiert werden [siehe ISO/IEC 27001 NK 9.2 Internes Audit] oder [ITGS DER 3.1 „Audits und Revisionen“].

3. Anwendergruppe: Konzerne und mittelständische Unternehmen

Ein ISMS ist für Konzerne und den Mittelstand nicht flächendeckend gesetzlich vorgeschrieben, wird in vielen Kontexten jedoch indirekt verpflichtend oder ist faktisch unumgänglich. Einerseits gibt es Gesetze, die für ISMS relevant sind, wie die DSGVO (Verpflichtung zu angemessenen technischen und organisatorischen Maßnahmen), HGB § 91 Abs. 2 (Risikofrüherkennungssystem) und AktG § 93 (Sorgfaltspflichten). Andererseits können hohe IT-Abhängigkeit, Zuliefererabhängigkeit für KRITIS-Betriebe oder Behörden oder branchenbedingte Verpflichtungen (Autoindustrie) ausschlaggebend sein. Mit GAP View lassen sich langfristige Auditprogramme, interne Audits und Lieferantenaudits organisieren.

4. Anwendergruppe: KMU

Bei kleinen und mittleren Unternehmen (KMU) haben sich die VdS-Richtlinie 10000 und CISIS12 als Informationssicherheitsstandards etabliert. Auch hier ist die regelmäßige Überprüfung der Wirksamkeit und Angemessenheit der umgesetzten Sicherheitsmaßnahmen fester Bestandteil des ISMS und eine der wichtigsten Aufgaben eines Informations- und Datenschutzbeauftragten. Die einfache Bedienbarkeit und Automatismen von GAP View ermöglichen eine effiziente Planung und Durchführung der erforderlichen Audits – auch bei personellen Engpässen in KMU.

5. Anwendergruppe: IT-Sicherheitsdienstleister

IT-Sicherheitsdienstleister unterstützen Unternehmen jeder Branche und Größe bei der Planung und Umsetzung von Sicherheitskonzepten. Die GAP View kann in allen Projektphasen eingesetzt werden. Mithilfe der GAP-Analyse können die Lücken zwischen den Normanforderungen und dem Ist-Stand ermittelt werden. Dadurch lässt sich der Implementierungsaufwand festlegen. Während der Implementierung eines ISMS kann kontinuierlich ein Soll-Ist-Vergleich durchgeführt werden, um den Fortschritt des Projekts zu überwachen. Nach Abschluss des ISMS-Projekts können im Rahmen eines Auditprogramms regelmäßige interne Audits und Lieferantenaudits geplant und durchgeführt werden. Die mandantenfähige GAP View Software unterstützt ein zentrales Management aller Kundenstammdaten, Fragenkataloge, Auditprogramme inklusive Planung und Ergebnisse der einzelnen Audits sowie Korrekturmaßnahmen und deren Umsetzungsstatus in einer Datenbank. Diese Informationen können den berechtigten Beratern sowie den Ansprechpartnern bei den Kunden über die Cloud bereitgestellt werden.

6. Anwendergruppe: Akkreditierten Auditoren und IS-Revisoren

Akkreditierte ISO 27001 Auditoren und IS-Revisoren sind für die Planung, Durchführung und Nachbereitung von zertifizierungs Audits von Informationssicherheitsmanagementsystemen (ISMS) zuständig. Die mandantenfähige GAP View Software unterstützt ein zentrales Management aller Kundenstammdaten, Fragenkataloge, Auditprogramme inklusive

Planung und Ergebnisse der einzelnen Audits sowie Korrekturmaßnahmen und deren Umsetzungsstatus in einer Datenbank. Diese Informationen können den akkreditierten Auditoren und IS-Revisoren sowie den Ansprechpartnern bei den Kunden über die Cloud bereitgestellt werden. Die Software unterstützt eine interaktive Durchführung der Audits (Interaktion zwischen Auditor und Interviewpartner).

7. Anwendungsbeispiele

- Unterstützung von internen Audits (**First Party Audit**), Lieferantenaudits (**Second Party Audit**) und Zertifizierungsaudits (**Third Party Audit**). [siehe ISO 19011 und ISO 17021]
- Planung, Durchführung und Auswertung von **GAP-Analysen** und **Audits**, u.a. **ISO/IEC 27001** und Subnormen, **B3S**, NIS-2, ISO/IEC 22301 und BSI 200-4, **BSI C5**, VdS 10000, CISIS12
- Planung, Durchführung und Auswertung von **BSI IS-Revisionen** (IS-Querschnittsrevision, IS-Partialrevision, IS-Kurzrevision)
- Prüfung der Umsetzung von Maßnahmen von **Systemen zur Angriffserkennung** (SzA) gemäß § 8a Absatz 1a BSIg bzw. nach § 11 Absatz 1e EnWG
- Auditplanung, Durchführung und Auswertung von branchenspezifischen Sicherheitsstandards, u.a. **DORA**, **TISAX**, PCI DSS
- Organisation von **Datenschutzaudits**
- Organisation von Lieferantenaudits nach ISO/IEC 27001, BSI 200-2
- IDW Audits und Revisionen

Ready for Audit

Marktvolumen

Zielgruppen	Anzahl der Organisationen
Kritische Infrastrukturen (KRITIS)	1.700
Mittelständische und große Unternehmen (NIS-2)	29.000 bis 40.000
Bundesbehörden	965
Beratungsgesellschaften im Bereich Informationssicherheit und Datenschutz	5.000 bis 8.000
Banken und Sparkassen	1458
Versicherungen	506

Ansprechpartner

Wirt.-Inf. (BA) Krzysztof Paschke

GAP View GmbH
Schauenburgerstraße 116, 24118 Kiel
Telefon: +49 160 88 26 100
<https://www.gap-view.de>
kpaschke@gap-view.de