

ISO 27001-konforme Informationssicherheits-Audits mit **GAP View Software**

1. Einführung

Etablierte Informationssicherheitsstandards, wie die Norm ISO/IEC 27001 mit ihren fach- und branchenspezifischen Subnormen, die BSI-Standards sowie einige weitere Standards, die insbesondere für KMU geeignet sind, schreiben eine regelmäßige Überprüfung ihrer Wirksamkeit und Angemessenheit durch entsprechende Audits und IS-Revisionen vor.

2. Problemstellung

Zeitvorgaben: Die Aufgabe, eine ISO-konforme Organisation von Audits im Rahmen eines oder mehrerer langfristiger Auditprogramme zu gewährleisten, ist zeitintensiv und erfordert ein hohes Maß an Sorgfalt [vgl. ISO 27001, NK 9.2 Internes Audit]. Die Zeitvorgaben für die Dauer von ISO-Audits, also für die Planung, Durchführung und Bewertung sowie die Erstellung eines Auditberichts, sind knapp bemessen und müssen von internen und/oder externen Auditoren eingehalten werden.

Office Werkzeuge: In der beruflichen Praxis erfolgen Erstellung und Verteilung von Auditplänen sowie Durchführung und Auswertung von Audits weitgehend mit herkömmlichen Office-Werkzeugen (Textverarbeitung und Tabellenkalkulation). Insbesondere bei großen Institutionen mit mehreren Standorten, komplexen IT-Verbänden und einer Vielzahl beteiligter Personen stellt dies den leitenden Auditor vor eine zeitintensive und fehleranfällige Herausforderung.

Fragenkataloge: Die Fragenkataloge als Grundlage der Audits stellen sicher, dass alle relevanten und geplanten Aspekte der Informationssicherheit geprüft werden. Sie erleichtern dem Auditor und den Beteiligten zudem die effiziente Durchführung des Audits. Ihre Erstellung, regelmäßige Aktualisierung und Bereitstellung in gleicher Fassung und mit gleichem Inhalt für alle am Audit teilnehmenden Personen ist jedoch eine fehleranfällige und zeitintensive Aufgabe.

Korrekturmaßnahmen: Die im Audit festgestellten Abweichungen (Nichtkonformitäten) müssen im Rahmen von Korrekturmaßnahmen

angemessen behandelt werden [vgl. ISO 27001, NK 10.2 „Nichtkonformität und Korrekturmaßnahmen“]. In diesen wird festgelegt, welche Maßnahmen ergriffen werden müssen, um die Nichtkonformität zu beheben. Darüber hinaus werden die Verantwortlichkeiten, Prioritäten, der Zeitaufwand und die Fristen für die Umsetzung festgelegt und die Beteiligten über die Umsetzung informiert. Eine regelmäßige Überprüfung des Umsetzungsstandes muss ebenfalls gewährleistet sein. Diese organisatorische Aufgabe ist zeit- und ressourcenintensiv.

3. Lösung

Die Audit Management Software **GAP View** wurde speziell für die effiziente, kontinuierliche Überprüfung der Wirksamkeit, Vollständigkeit und Angemessenheit der implementierten Informationssicherheits- und Datenschutzmaßnahmen mit folgenden Zielen entwickelt:

- Ganzheitliche Unterstützung der internen und externen Auditoren sowie der Informationssicherheits- und Datenschutzbeauftragten bei der langjährigen, normkonformen Organisation von Audits
- Signifikante Optimierung des gesamten Auditprozesses (Ressourcen, Zeit und Kosten)
- Genaue Abbildung der Anforderungen an die Planung und Durchführung von internen und externen Audits nach **ISO 19011** und **ISO/IEC 17021**
- Genaue Abbildung der Vorgaben des BSI Leitfadens für die **IS-Revision auf Basis von IT-Grundschutz** und des Bausteins **DER.3.1 Audits und Revisionen**
- Effektive und effiziente Unterstützung der beteiligten Mitarbeiter und Auditoren während des gesamten Auditprozesses durch den Funktionsumfang, Automatismen, einfache Bedienbarkeit (UI), Cloud- oder On-Prem-Betrieb und die Integration von **OpenAI ChatGPT**, Speech-to-Text
- Unterstützung verschiedener Audit- und Bewertungsmethoden nach ISO und BSI
- Quick- und Expresschecks (Schnelldiagnose bzgl. Umsetzungsstatus von IT-Sicherheits- und Datenschutzmaßnahmen)

- Bereitstellung von themenbezogenen **Audit-Fragenkatalogen (Content)** für ISO-Audits und BSI-IS-Revisionen

4. Softwareeigenschaften

- Zentrales Stammdatenmanagement aller im Auditprogramm beteiligten Institutionen und Personen
- Zentrales Management und einheitliche Bereitstellung der Fragenkataloge für alle Beteiligten, die für die geplanten Audits verwendet werden
- Bereitstellung der herstellereigenen Fragenkataloge für Audits der Informationssicherheits- und Datenschutz-managementsysteme
- Management von mehrjährigen Auditprogrammen [vgl. ISO 27001, NK 9.2.2 Internes Auditprogramm]
- Zentrales Management aller geplanten und durchgeführten Audits mit genauer Zeitplanung (Kalender), Ressourcenzuteilung, Fragenkatalogen, Nachweisen und Ergebnissen
- Zentrales Management aller für ein Audit erforderlichen Dokumentationen und Auditnachweisen (Dateien unterschiedlicher Formate sowie im Audit generierte Fotos)
- Unterstützung aller erforderlichen Prüfmethoden (u.a. Befragung, Begehung, Beobachtung, Aktenanalyse, technische Prüfung, Datenanalyse)
- Unterschiedliche Bewertungsmethoden der Ergebnisse
- Unterstützung von Remote- und Vor-Ort-Audits sowie Self-Assessments
- Zentrales Management der Korrekturmaßnahmenkataloge mit Zuordnung der zuständigen Personen, geschätztem Zeitaufwand, Umsetzungsdatum, Prioritäten und Umsetzungsstatus
- Dashboard (Stand der Umsetzung eines Audits, verbleibende Zeit bis zum Abschluss

es Audits, Bewertung, Stand der Umsetzung von Korrekturmaßnahmen)

- Umfassendes Berichtswesen für die Planung, Durchführung und Bewertung von Audits sowie Korrekturmaßnahmen



5. Anwendungsbeispiele

- Branchenspezifische Sicherheitsaudits u.a. B3S, NIS-2, DORA, TISAX, PCI DSS, C5
- Auditmanagement von ISMS, BCMS und DSMS u.a. ISO/IEC 27001 mit fachspezifischen Normen, ISO/IEC 22301 BSI 200-4, EU-DSGVO und BDSG
- Lieferanten-Audits nach BSI und ISO
- IDW Audits und Revisionen, u.a. Due Diligence (TAX und Legal), IDW PS

Ready for Audit

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