GAP View GmbH
Audit Management Software

IS-Revision auf Basis von BSI IT-Grundschutz mit GAP View Software

1. Einführung

Ziel einer IS-Revision ist es, das aktuelle Sicherheitsniveau in der Institution festzustellen und Hinweise auf bestehende Sicherheitslücken zu geben und damit die Leitung der Institution, das IS-Management-Team und insbesondere den Informationssicherheitsbeauftragten (ISB) bei der Umsetzung und Optimierung der Informationssicherheit zu unterstützen und zu begleiten.

2. Leitfaden für die IS-Revision auf Basis von IT-Grundschutz

Die Planung, Durchführung und Bewertung von IS-Revisionen ist im BSI-Standard „***Leitfaden für die Informationssicherheitsrevision auf Basis von IT-Grundschutz***“ sowie in verschiedenen Hilfsmitteln in Form von Vorlagen und Musterdokumenten geregelt.

3. Problemstellung

Eine sorgfältige und BSI-konforme Organisation von IS-Revisionen im Rahmen eines langfristigen IS-Verfahrens ist zeit- und ressourcenintensiv. Die Zeitvorgaben für die Dauer von IS-Revisionen nach BSI sind knapp bemessen und müssen vom internen und/oder externen IS-Revisionsteam eingehalten werden. Die Erstellung von IS-Prüfplänen, insbesondere für die IS-Querschnittsrevision bei großen Institutionen mit mehreren Standorten und komplexen IT-Verbünden, mit herkömmlichen Office-Werkzeugen (Textverarbeitung und Tabellenkalkulation) stellt die Verantwortlichen vor eine große Herausforderung. Die Erstellung, Verteilung, regelmäßige Ergänzung und Aktualisierung von Fragenkatalogen/Checklisten stellt für die im Rahmen der IS-Revision vorgesehenen Mitarbeiterbefragungen eine schwierige Aufgabe dar. Eine weitere Herausforderung ist die Organisation von Korrekturmaßnahmen für Abweichungen (Nichtkonformitäten), die bei der IS-Revision festgestellt wurden. Dabei geht es darum, zuständigen und ausführenden Personen zu bestimmen, Prioritäten festzulegen und die Fristen für die Umsetzung zu bestimmen.

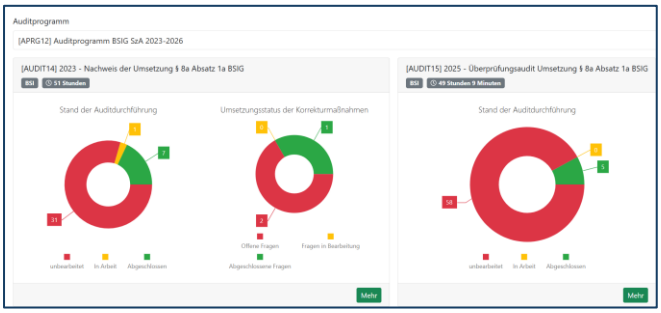
4. Lösung

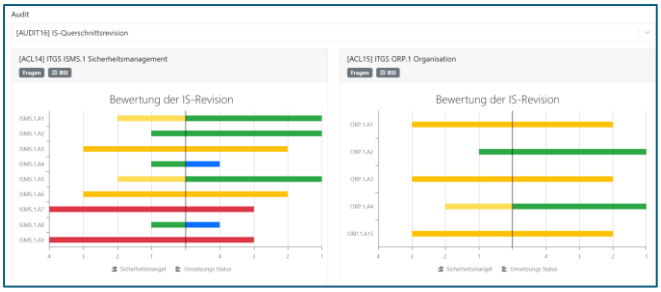
Die **Audit Management Software GAP View** wurde speziell für die kontinuierliche Überprüfung der Wirksamkeit, Vollständigkeit und Angemessenheit der implementierten Informationssicherheitsmaßnahmen unter strikter Berücksichtigung des BSI „Leitfadens für die IS-Revision auf Basis von IT-Grundschutz“ entwickelt. Ziel ist es, alle an einem IS-Revisionsverfahren und den dazugehörigen IS-Revisionen beteiligten Personen, von der Institutsleitung, den Mitgliedern interner und externer IS-Revisionsteams, bis hin zu den Mitarbeiterinnen und Mitarbeitern, ggf. externen Lieferanten und Experten, effizient und effektiv zu unterstützen.

5. Softwareeigenschaften

- Zentrales Stammdatenmanagement aller im IS-Revisionsverfahren beteiligten Institutionen und Personen
- Zentrales Management und eine einheitliche Bereitstellung aller Fragenkataloge, die für die IS-Revisionen verwendeten werden
- Optionale Bereitstellung der herstellereigenen Fragenkataloge je BSI IT-Grundschutz Baustein inkl. geschätzter Auditbearbeitungszeit
- Management von mehrjährigen Auditprogrammen/IS-Revisionsverfahren,
- Zentrales Management aller geplanten und durchgeführten IS-Revisionen mit genauer Zeitplanung (Kalender), Ressourcenzuteilung, Stichprobendefinition (Baustein-Zielobjekt), Fragenkatalogen, Nachweisen und Ergebnissen
- Zentrales Management aller für eine IS-Revision erforderlichen Dokumentationen (u.a. IS-Revisionshandbuch, Organigramm)
- Unterstützung aller Arten von IS-Revisionen (IS-Kurzrevision, IS-Partialrevision und IS-Querschnittsrevision)
- Unterstützung aller erforderlichen Prüfmethoden (mündliche und schriftliche Befragung, Inaugenscheinnahme, Beobachtung, Aktenanalyse, technische Prüfung, Datenanalyse)

- Zweistufige Bewertung der Ergebnisse (Umsetzungsstatus und Sicherheitsmängel)
- Automatische Generierung von Korrekturmaßnahmenkatalogen (Nichtkonformitäten)
- Zentrales Management der Korrekturmaßnahmenkataloge mit Zuordnung der zuständigen Personen, geschätztem Zeitaufwand, Umsetzungsdatum, Prioritäten und Umsetzungsstatus
- Ausführliches Berichtswesen u.a. IS-Revisionsverfahren, IS-Revisionshandbuch, IS-Prüfplan, IS-Revisionsbericht (unterschiedliche Detaillierungsgrade)
- Dashboard (Stand der Umsetzung einer IS-Revision, verbleibende Zeit bis zum Abschluss der IS-Revision, Bewertung der IS-Revision, Stand der Umsetzung von Korrekturmaßnahmen)





- Unterstützung verschiedener Audit-methoden (Vor-Ort-Audit, Remote-Audit und Self Assessment)
- Unterstützung von ExPress Informations-sicherheits-Checks (EPIC), u.a. Schnell-diagnose zum Umsetzungsstand von IT-Sicherheits- und Datenschutzmaßnahmen

6. Funktionsumfang (Auszug)

- Webbasierte Anwendung
- Betrieb wahlweise in der Cloud-Umgebung oder On-Prem
- Einsatz auf Desktop, Notebook und Tablet,
- Einfache intuitive Bedienung (UI)
- Integration von OpenAI ChatGPT
- Zeitsparende, hoher Automatisierungsgrad der Planung, Durchführung, Auswertung von IS-Revisionen
- Multi-Faktor-Authentifizierung
- Rollenbasiertes Berechtigungskonzept
- Importschnittstelle für Fragenkataloge und Checklisten (MS Excel)
- Importschnittstelle für das BSI IT-Grundschutz-Kompendium (XML)
- Reporting gem. der Anforderungen der BSI und ISO Standards

7. Weitere Anwendungsbeispiele

- Audit Management nach ISO 19011 und ISO/IEC 17021
- Branchenspezifische Sicherheitsaudits u.a. NIS-2, DORA, TISAX, PCI DSS
- 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

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