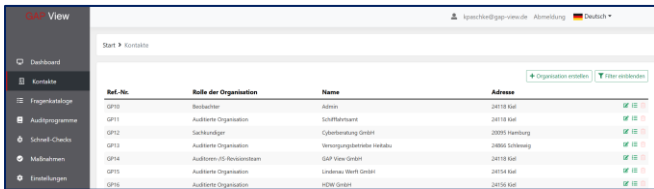


Audit und IS-Revisionsprozess mit GAP View Software (Zusammenfassung)

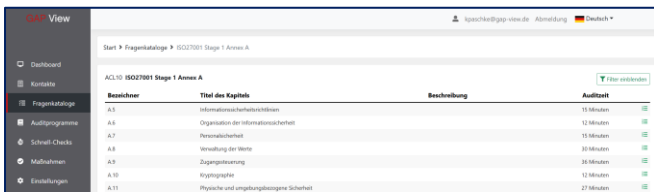
Die Gap View Audit Management Software bildet die Vorgaben der ISO 19011, der ISO/IEC 17021 und des BSI-Leitfadens für IS-Revisionen auf Basis von IT-Grundschutz ab. Die folgende Zusammenfassung erläutert Schritt für Schritt die Planung, Durchführung und Bewertung eines Audits oder einer IS-Revision.

Schritt 1: Die für die Organisation des Audits benötigten Informationen zu allen am Audit beteiligten Institutionen und Personen werden zentral erfasst.



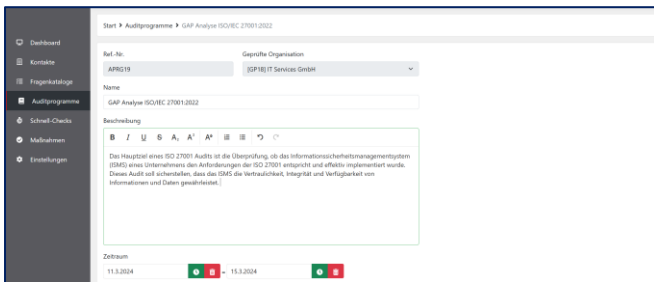
Ref.-No.	Rolle der Organisation	Name	Adresse
GP10	Buchhalter	Adrian	20118 Kiel
GP11	Auditoren Organisation	ISO/IEC 17021	20118 Kiel
GP12	Sachverständiger	Überwachungs GmbH	20095 Hamburg
GP13	Auditoren Organisation	Vertragsgestaltung Institute	20095 Hamburg
GP14	Auditoren-IS-Revisoren	GAP View GmbH	20118 Kiel
GP15	Auditoren Organisation	Lindemann Netz GmbH	20118 Kiel
GP16	Auditoren Organisation	SDW GmbH	20118 Kiel

Schritt 2: Die für die Auditplanung und -durchführung benötigten Fragenkataloge werden entweder importiert (MS Excel-Format) inklusive der geschätzten Auditzeit pro Normkapitel oder manuell erstellt.



Bereich	Titel des Kapitels	Beschreibung	Auditzeit
A.3	Informationssicherheitsrisiken		15 Minuten
A.4	Organisation der Informationssicherheit		12 Minuten
A.7	Personalrichtlinien		15 Minuten
A.8	Spezifikation der Dienste		30 Minuten
A.9	Zugangskontrollen		30 Minuten
A.10	Kryptographie		12 Minuten
A.11	Physische und umgebungsbezogene Sicherheit		27 Minuten

Schritt 3: Ein oder mehrere Auditprogramme werden unter Angabe der beteiligten Personen, der Zeitvorgaben und der Ziele festgelegt [vgl. ISO 27001, NK 9.2 Internes Audit].



Ref.-No.: Geprüfte Organisation
APR019: (GP)BIT Services GmbH

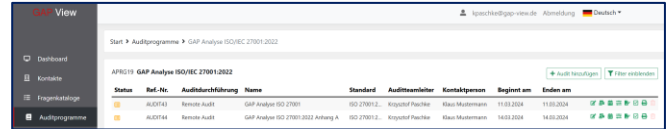
Name: GAP Analyse ISO/IEC 27001:2022

Beschreibung: Das Hauptziel eines ISO 27001 Audits ist die Überprüfung, ob das Informationssicherheitsmanagementsystem (ISMS) eines Unternehmens den Anforderungen der ISO 27001 entspricht und effektiv implementiert wurde. Dieses Audit soll sicherstellen, dass das ISMS die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten gewährleistet.

Zeitraum: 11.3.2024 - 11.3.2024

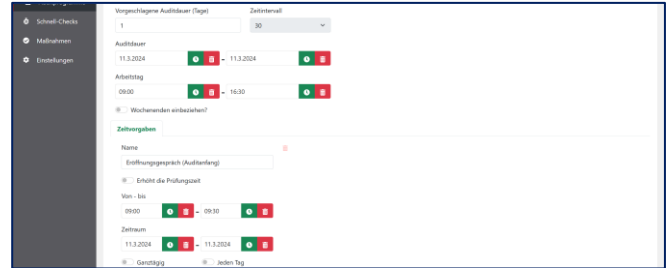
Schritt 4: Es werden ein oder mehrere Audits unter Angabe der beteiligten Personen, der Zeitvorgaben, der Ziele, der verwendeten Fragenkataloge, Bewertungsmethode und der

Ressourcenplanung festgelegt [vgl. ISO 27001, NK 9.2 Internes Audit].



Status	Ref.-No.	Auditdurchführung	Name	Standard	Auditverantwortl.	Kontaktperson	Beginnt am	Endet am
OK	APR019	Internes Audit	GAP Analyse ISO 27001	ISO 27001:2022	Kristofel Paschke	Markus Mottmann	11.03.2024	11.03.2024
OK	APR019	Externes Audit	GAP Analyse ISO 27001:2022 Arteng A	ISO 27001:2022	Kristofel Paschke	Markus Mottmann	14.03.2024	14.03.2024

Die Auditdauer sowie feste Termine wie Besprechungen und Pausen werden festgelegt und automatisch in der Planung berücksichtigt.



Vorgeschlagene Auditdauer (Tage): 1
Zeitraum: 30

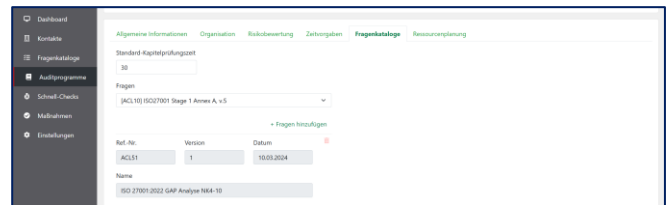
Auditdauer: 11.3.2024 - 11.3.2024

Arbeitszeit: 09:00 - 16:30

Wochenschemen einbehalten?

Zeitraum: 11.3.2024 - 11.3.2024

Die benötigten Fragenkataloge (bei IS-Revision IT-Grundschutzbausteine) werden ausgewählt.



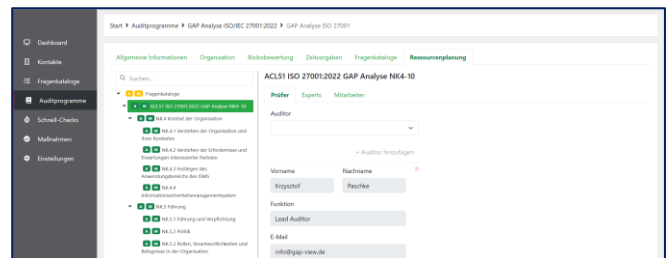
Standard-Kapitelprüfungszustell: IS

Fragen: ICL10 ISO27001 Stage 1 Annex A, v.5

Ref.-No.: ACIS1
Version: 1
Datum: 10.03.2024

Name: ISO 27001:2022 GAP Analyse NKA-10

Die Ressourcen (Auditoren, Mitarbeiter, ggf. externe Experten wie z. B. Forensiker) werden den einzelnen Normkapiteln, in die sie involviert sind, zugeordnet.



ACIS1 ISO 27001:2022 GAP Analyse NKA-10

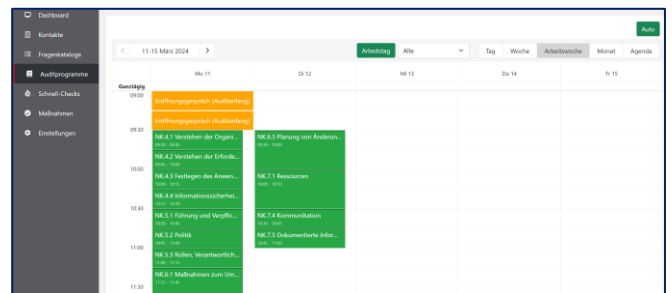
Prüfer: Experts, Mitarbeiter

Auditoren: Kristofel Paschke

Funktion: Lead Auditor

E-Mail: info@gap-view.de

Schritt 5: Ein Prüfplan (Auditplan) kann auf Knopfdruck automatisch generiert werden. Eine manuelle Nachbearbeitung (zum Beispiel Terminänderung oder Dauer der Befragung) ist jederzeit möglich.



Tag	11-13 März 2024	14-15 März 2024
09:00	Einleitungsgespräch (Auditplanung)	Einleitungsgespräch (Auditplanung)
09:30	NK 4.1 Verständnis der Organisationsstruktur	NK 4.3 Planung von Audits
10:00	NK 4.2 Verständnis der Erfordernisse	NK 4.4 Kommunikation
10:30	NK 4.3 Festlegen des Ansatzes	NK 4.5 Dokumentierte Informationen
11:00	NK 4.4 Informationssicherheitsmanagement	NK 4.6 Kommunikation
11:30	NK 4.5 Führung und Verpflichtung	NK 4.7 Kommunikation
	NK 4.6 Politik	NK 4.8 Kommunikation
	NK 4.7 Rollen, Verantwortlichkeiten und Befugnisse	NK 4.9 Kommunikation
	NK 4.8 Maßnahmen zum ISMS	NK 4.10 Kommunikation

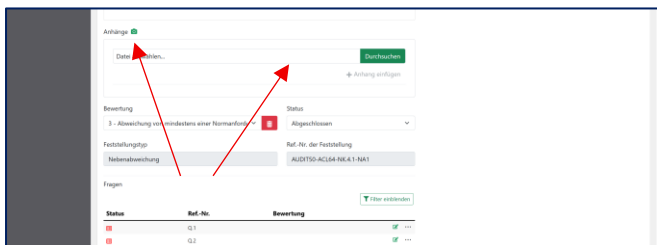
Schritt 6: Den Auditoren steht eine Liste mit Fragen zur Verfügung, die nach den Vorgaben der Planung generiert und sortiert wurde.

Status	Fragen	Ref.-Nr.	Maßnahmeziele	Bewertung
...
...
...
...
...
...

Schritt 7: Die Fragen können den Interviewpartnern gestellt werden. Die Feststellungen können entweder konventionell mit der Tastatur getippt oder mithilfe der „Speech-to-Text“-Funktion eingegeben werden. Die gesprochenen Angaben werden in Text umgewandelt. Darüber hinaus kann die Unterstützung von OpenAI ChatGPT hinzugezogen werden.



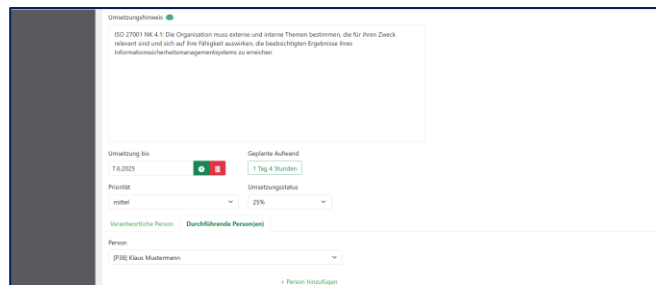
Es können beliebig viele Prüfungsnachweise (audit evidences) als Dateien oder als direkt aus der Software gemachte Fotos eingefügt werden.



Schritt 8: Nach Abschluss des Audits werden alle festgestellten Nichtkonformitäten automatisch in einem Katalog von Korrekturmaßnahmen zusammengefasst.

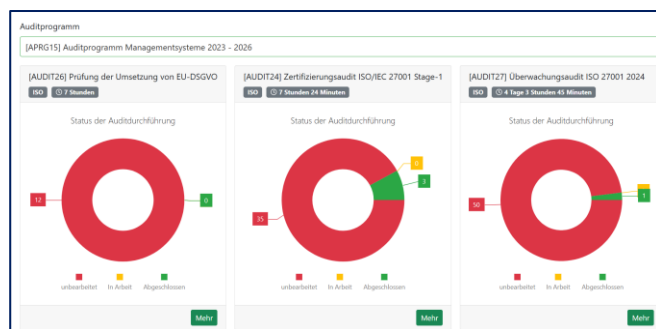
Ref.-Nr.	Bewertung	Anforderung	Verantwortliche Person	Durchführende Person(e)
AUDIT03-AC11-100	Verbesserung	Verstehen der Organisation und ihres Kontextes	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-101	Verbesserung	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-102	Verbesserung	Rezeption	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-103	Verbesserung	Verstehen der Erfordernisse und Erwartungen interessierter Parteien	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-104	Verbesserung	Kompetenz	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-105	Verbesserung	Kompetenz	Klaus Madermann	Lisa Mähler
AUDIT03-AC11-106	Verbesserung	Dokumentierte Informationen	Klaus Madermann	Lisa Mähler

Die einzelnen Korrekturmaßnahmen zeigen die Bewertung und Feststellung des Auditors zu der jeweiligen Norm-Anforderung. Der Informationssicherheits- oder Datenschutzbeauftragte (ISB) bzw. eine andere für das Audit zuständige Person kann einen Umsetzungs-hinweis eintragen. Dieser kann mithilfe von ChatGPT erstellt und ggf. angepasst werden.



Darüber hinaus können die Priorität, der Status der Umsetzung, die durchführenden Personen sowie der Umsetzungszeitraum festgelegt werden.

Schritt 9: Mithilfe eines Dashboards werden der aktuelle Status des Audits sowie die Bewertungen der einzelnen Normkapitel angezeigt.



Ein ausführliches Berichtswesen zur Auditplanung, zu den Ergebnissen und zu den Korrekturmaßnahmen (mit unterschiedlichen Detaillierungsgraden) liefert den Verantwortlichen wichtige Informationen.

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