Softwaregestütztes Prüfungsmanagement

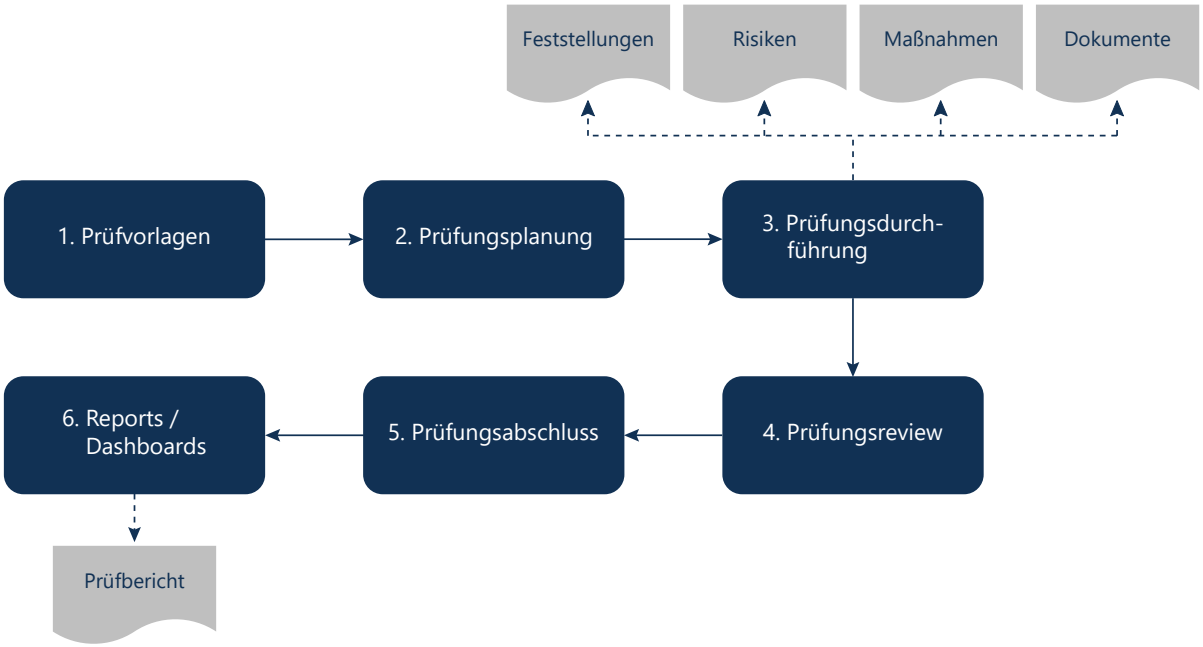
Ein Leitfaden zur Abbildung des Prüfungsmanagements mit ibi systems iris

Fast jedes Unternehmen unterliegt gewissen regulatorischen Anforderungen und muss sicherstellen, diese zu erfüllen. Unabhängig davon, ob es sich dabei um einzelne Sicherheits- oder Compliance-Audits handelt oder ein komplettes internes Kontrollsystem betrieben werden soll, kann Ihnen eine Software hierbei bei der Planung, Durchführung und Verwaltung der Prüfungen behilflich sein. ibi systems iris unterstützt zu Beginn des Kontrollprozesses, führt durch den Prozess und stellt die Ergebnisse zum Abschluss dar. In der Folge kann jederzeit eingesehen werden, welche Regularien bereits eingehalten werden oder wo es noch Nachbesserungsbedarf gibt. Die Software bietet die Möglichkeit, direkt bei der Prüfungsdurchführung Feststellungen, Risiken, Maßnahmen, Dokumente oder Kommentare zu definieren.

- Optimierung der Abläufe
- Steigerung der Qualität
- Ganzheitlicher Ansatz

Softwaregestütztes Prüfungsmanagement

Im Folgenden wird zuerst ein Überblick über den Prozess des Prüfungsmanagements in ibi systems iris gegeben. Danach wird genauer auf die einzelnen Schritte zur Abbildung des softwaregestützten Prüfungsmanagements eingegangen.



Überblick zum Prozess

Als Basis des Prüfungsmanagements dienen Prüfvorlagen. Diese Vorlagen können in der Software erzeugt werden oder aber per Import zur Verfügung gestellt werden. Aus einer Prüfvorlage werden tatsächliche Prüfungen abgeleitet, geplant, durchgeführt und ausgewertet. Softwaregestützte (optionale) Reviews und der (optionale) Prüfungsabschluss runden den Prozess ab. Im Anschluss daran können mithilfe von Reports und Dashboards die Prüfungsergebnisse ausgewertet und dargestellt werden.

1. Prüfvorlagen

Durch Prüfvorlagen besteht die Möglichkeit, gewisse Prüftemplates einmalig zu erstellen und diese beliebig oft abzuleiten und zu verwenden. Dadurch entsteht nur ein geringer Pflegeaufwand und zusätzlich können übergreifende Auswertungen über alle abgeleiteten Prüfungen einer Prüf-

vorlage erstellt werden. Eine Prüfvorlage kann, wie gewünscht, in mehrere Prüfblöcke mit Kontrollen geschachtelt und aufgebaut werden. Bei jeder einzelnen Kontrolle kann konfiguriert werden, welcher Ergebnistyp genutzt werden soll.

Beispielhafte Ergebnistypen in ibi systems iris:

- Auswahlmenü (Reifegrad, Ampel etc.)
- Schutzbedarf
- Ja/Nein
- Prozent
- Text
- Benutzer
- Organisationseinheit

Des Weiteren können Prüfvorlagen dupliziert werden. Beispielsweise kann diese Funktion genutzt werden, wenn eine neuere, überarbeitete Version einer Prüfvorlage erschienen ist und diese auf Basis der bisherigen Prüfvorlage in der Software zur Verfügung gestellt werden soll. Dies hat den Vorteil, dass beide Prüfvorlagen revisionssicher in der Software enthalten bleiben und der Ersteller der neuen Prüfvorlage erspart sich einen Großteil des Zeitaufwandes, da die bisherige Vorlage als Basis dient.

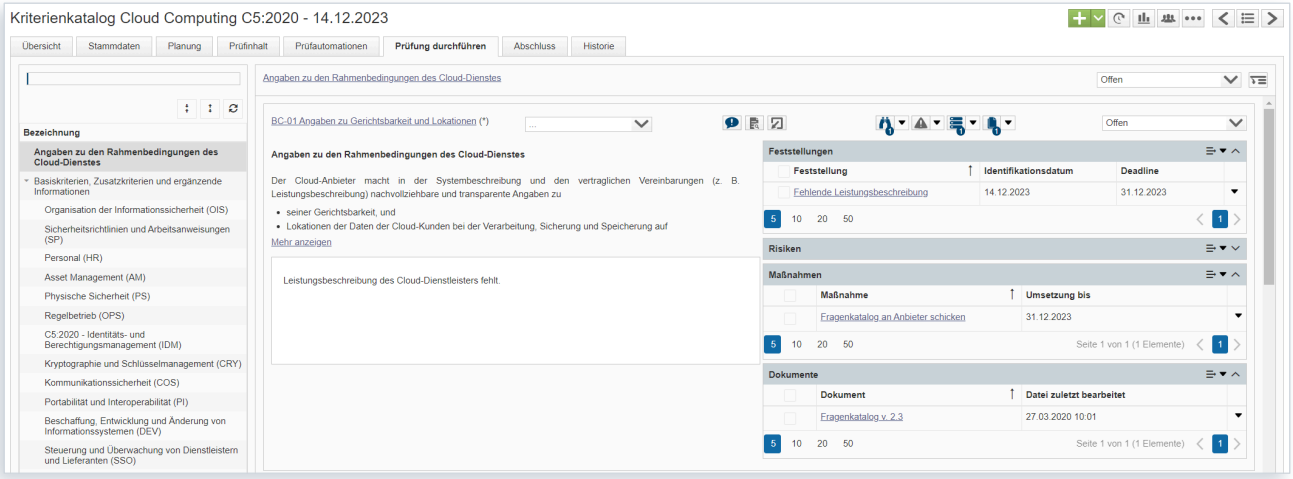
2. Prüfungsplanung

Nach der Erstellung einer Prüfung kann diese umfangreich geplant werden. Zu Beginn der Planung wird ein Prüfzeitraum definiert und entschieden, ob die Prüfung ausschließlich in diesem Prüfzeitraum sichtbar sein soll. Anschließend kann entschieden werden, welche Personen die Prüfung durchführen, reviewen und abschließen dürfen. Die Definition des Prüfzeitraums und der beteiligten Personen kann entweder für die gesamte Prüfung oder aber für jeden einzelnen Prüfblock vorgenommen werden.

3. Prüfungsdurchführung

Wizardgestützte Durchführung

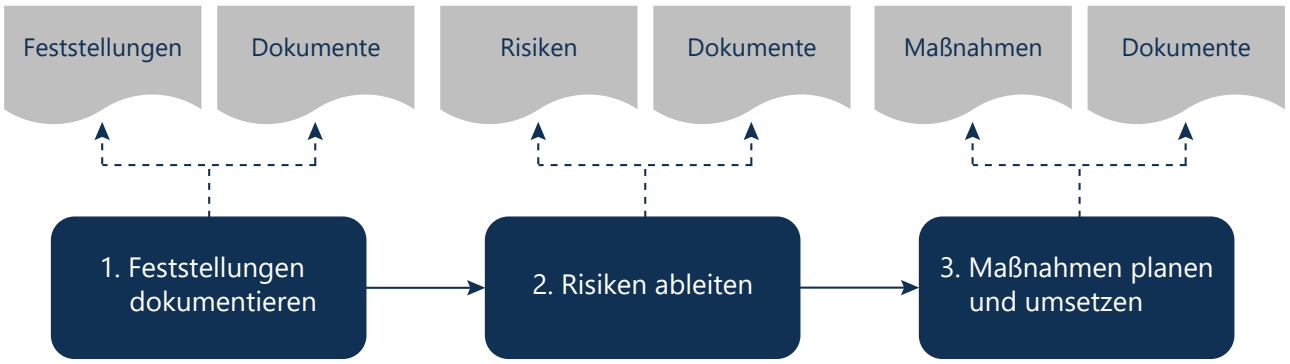
Im Anschluss an die Prüfungsplanung können die ausgewählten Prüfer die Prüfung im angegebenen Prüfzeitraum durchführen. Die Prüfungsdurchführung in der Software ibi systems iris zeigt eine Auflistung aller Prüfblöcke an. Durch diese Navigation kann benutzerfreundlich jederzeit zu anderen Prüfblöcken gewechselt werden. Die Software führt den Prüfer durch jede Kontrolle der Prüfung. Hierbei hat der Prüfer die Möglichkeit, ein Ergebnis, einen Kommentar, Feststellungen, Risiken, Maßnahmen und Dokumente für eine Kontrolle zu definieren. Die Prüfblöcke und Kontrollen werden durch eine Beschreibung näher erläutert und bieten somit dem Prüfungsdurchführenden eine Hilfestellung an.



Hinweis:

Neben der Durchführung direkt in der Software bietet ibi systems iris auch die Option der Offline-Bearbeitung an. Die Prüfungen können exportiert werden, im Excel bearbeitet und anschließend wieder hochgeladen werden. Dies bietet sich sowohl für externe Auditoren als auch interne Kollegen ohne aktiven Zugang zur Software an.

Exemplarische Schritte basierend auf der Prüfungsdurchführung



Feststellungen: In der Prüfungsdurchführung ist es generell möglich, die vier verschiedenen Elemente Feststellungen, Risiken, Maßnahmen und Dokumente zu erstellen bzw. zu verknüpfen. Der hier beschriebene exemplarische Prozess stellt die Dokumentation von Feststellungen (z. B. einer Abweichung oder einer Schwachstelle) direkt in der Prüfungsdurchführung dar. Alle weiteren Schritte werden nicht direkt in der Prüfungsdurchführung bearbeitet.

Risiko ableiten: In ibi systems iris kann aus einer Feststellung direkt ein Risiko abgeleitet werden. Dieses Risiko kann detailliert beschrieben werden. Durch die Ableitung in der Software wird automatisch die Referenz zwischen der Feststellung und des angelegten Risikos erzeugt.

Risikobewertung: Die (abgeleiteten) Risiken können in der Software nun bewertet werden. Hier bietet ibi systems iris verschiedene Bewertungsmethoden an, um die Schadenauswirkung und die Eintrittswahrscheinlichkeit zu bewerten. Beispielsweise kann nach Schutzbedarfsklassen, Schwachstellenkategorien, individuellen Kategorien oder aber standardmäßig nach gewissen Ausprägungen qualitativ oder quantitativ bewertet werden. Es kann sowohl die IST- als auch die SOLL-Bewertung durchgeführt und dokumentiert werden. Zusätzlich kann eine Risikobehandlungsstrategie ausgewählt werden.

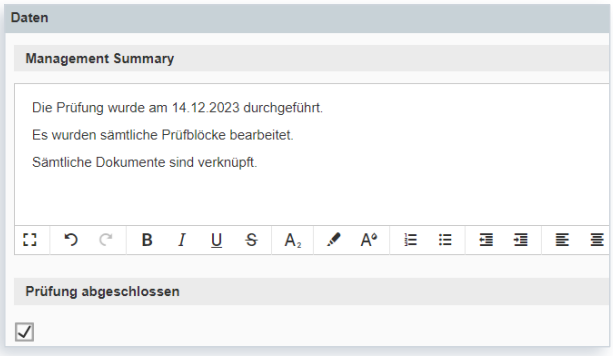
Maßnahmenplanung und Umsetzung: Für den Fall, dass ein Risiko nicht akzeptiert werden kann, da die Kombination aus Schadenauswirkung und Eintrittswahrscheinlichkeit zu hoch ist, können in der Software direkt Maßnahmen zur Risikobehandlung verknüpft werden. Diese Maßnahmen können in den Stammdaten detailliert beschrieben werden. Zusätzlich besteht die Möglichkeit, die Maßnahmenumsetzer zu definieren und somit automatisch von der Software benachrichtigen zu lassen. Als Maßnahmenverantwortlichkeit kann somit jederzeit der Überblick über den Fortschritt der verschiedenen Maßnahmenumsetzungen erhalten bleiben.

4. Abschluss und Review

In ibi systems iris besteht die Möglichkeit, ein Review durchzuführen. Entweder erzeugt die Software automatisch zufällige Kontrollen für das Review oder die verantwortliche Person wählt manuell Kontrollen aus. Anschließend kann das Prüfungsergebnis angezeigt und dann entschieden werden, ob das Ergebnis korrekt oder nicht korrekt ist.

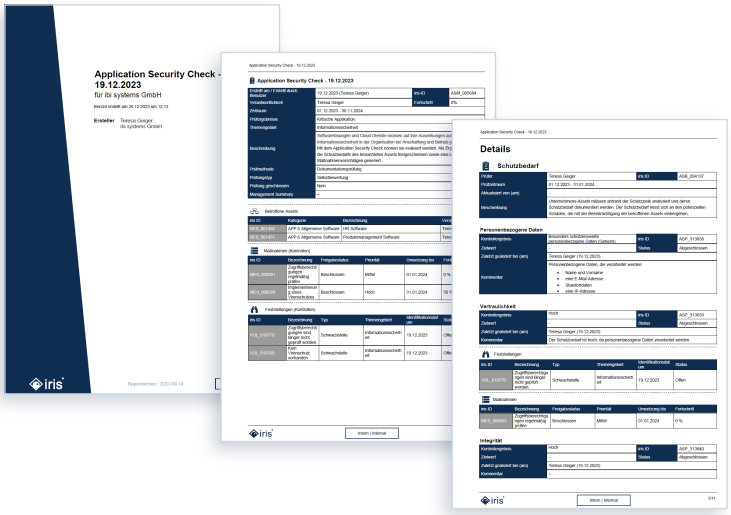
Kontrolle	Ergebnis (review)
BC-03 Angaben zu Wiederanlaufparametern im Notbetrieb	Positiv
COS-01 Technische Schutzmaßnahmen	Negativ
DEV-01 Richtlinien zur Entwicklung/Beschaffung von Informationssystemen	Positiv
IDM-07 Zugriff auf Daten der Cloud-Kunden	Positiv
OIS-05 Kontakt zu relevanten Behörden und Interessenverbänden	Negativ

Sobald die Prüfer die komplette Prüfung durchgeführt und dokumentiert haben, kann die Prüfung abgeschlossen und somit revisionssicher abgelegt werden.

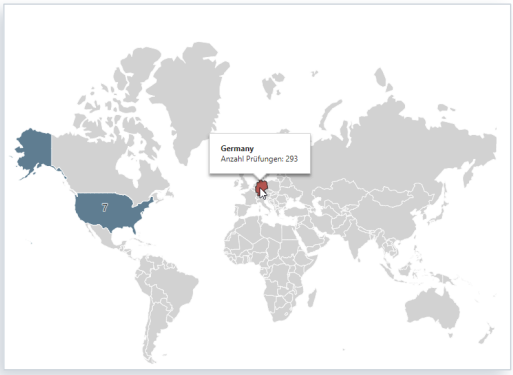


5. Prüfbericht und Auswertung

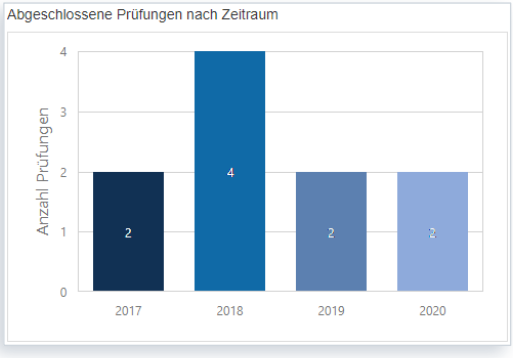
ibi systems iris bietet umfangreiche Standardreports an. Der Standardreport im Prüfungsbereich listet sämtliche Prüfungsergebnisse inkl. aller Kommentare, Feststellungen, Risken, Maßnahmen und Dokumente in einer kompakten und detaillierten Darstellung auf. Zusätzlich besteht die Möglichkeit, eigene Reports zu erzeugen oder bestehende Reports über einen Report Designer in der Software zu modifizieren.



Des Weiteren können die Prüfungen und Audits über Dashboards in ibi systems iris ausgewertet werden. Durch den Dashboard Designer können neben den Standard-Dashboards, eigene Dashboards direkt in ibi systems iris erzeugt werden. In den Abbildungen sind Teilbereiche aus den Standard-Dashboards ersichtlich. Beispielsweise können die Prüfungen nach Ländern, abgeschlossenen Prüfungen nach Zeitraum oder Prüfungen nach Prüfzeitraum angezeigt werden.



Es kann ein komplettes Dashboard oder Teilbereiche davon aus der Software ibi systems iris als Bild-, PDF- oder Excel-Datei exportiert werden. Somit ist es möglich auf Knopfdruck aus der Software heraus z. B. eine Management-Präsentation anzureichern.

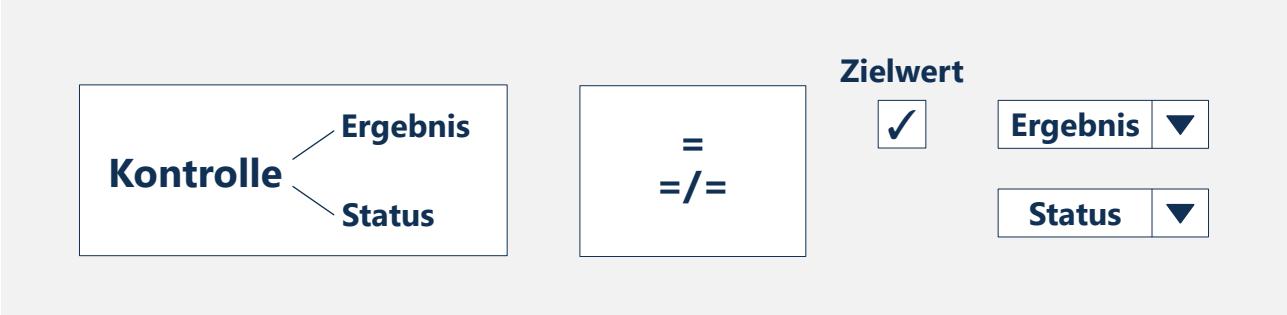


Funktionale Highlights

In diesem Abschnitt wird ein Überblick über die funktionalen Highlights des softwaregestützten Prüfungsmanagements mit ibi systems iris gegeben.

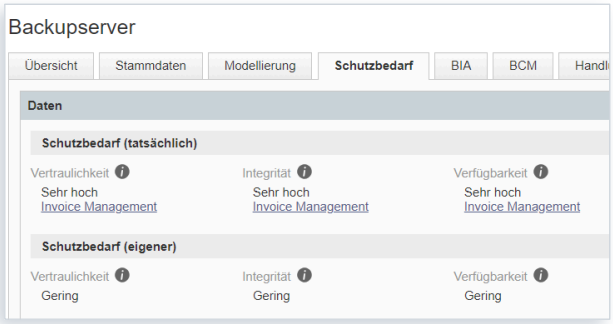
1. Prüfautomationen

Es existieren drei Arten von Automationen in ibi systems iris: Anpassung betroffener Elemente, Maßnahmenempfehlungen sowie dynamische Prüfinhalte. Die Grundlage einer Prüfautomation stellt die Regeldefinition mit beliebig vielen Bedingungen dar. Hier kann beispielsweise angegeben werden, dass bei der Prüfungsdurchführung das Ergebnis einer Kontrolle einen vordefinierten (Ziel-)Wert annimmt oder von ihm abweicht, oder ein definierter Status (nicht) eintreten soll.



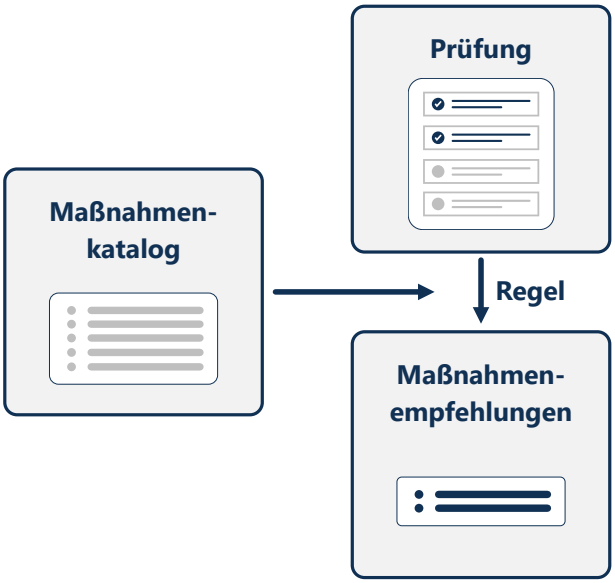
Anpassung betroffener Elemente

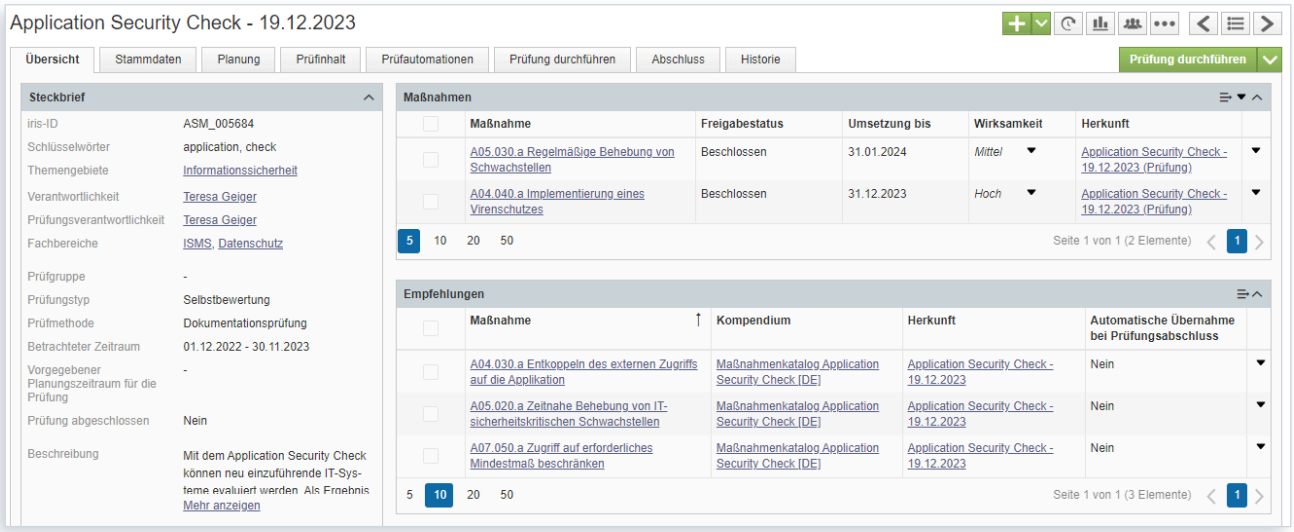
Durch diese Prüfautomation können direkt bei Prüfungsdurchführung Attribute (z. B. der Schutzbedarf) von Prozessen und Assets festgelegt bzw. verändert werden, wenn die definierte Regel zutrifft. Es werden beispielsweise die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit in einer Prüfung abgefragt und eingetragen, direkt mit einem Prüfobjekt verknüpft und somit die Eintragungen in der Prüfung automatisch zum Prüfobjekt weitergegeben.



Maßnahmenempfehlungen

Durch die Funktion der automatisierten Maßnahmenempfehlungen in der Software können mittels der individuellen Regeln gewünschte Maßnahmenempfehlungen je nach eingetragenen Ergebnissen oder Status angezeigt werden. Beispielsweise wird die Entkopplung des externen Zugriffs auf die Applikation als Empfehlung angezeigt, da innerhalb der Prüfungsdurchführung gewisse Fragen bzw. Kontrollen so ausgefüllt wurden, dass es sich um sehr schützenswerte Informationen innerhalb des Prüfobjektes handelt.



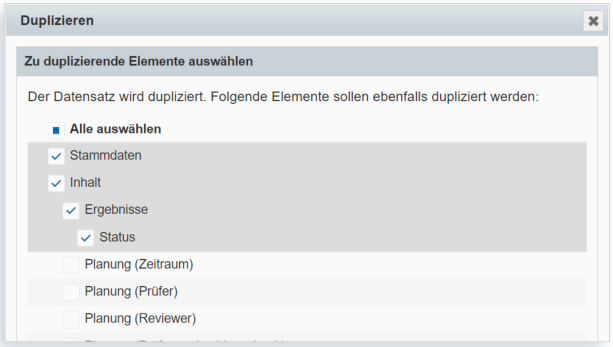


Dynamische Prüfinhalte

Im Rahmen der dynamischen Prüfinhalte können Kontrollen und Prüfblöcke ausgewählt werden, die bei Eintritt einer definierten Automationsregel, wie z. B. einem bestimmten Kontrollergebnis, im Wizard der Prüfungsdurchführung angezeigt werden. Ohne Feuern der Automation sind diese Kontrollen bzw. Prüfblöcke bei der Prüfungsdurchführung für den Prüfer nicht sichtbar.

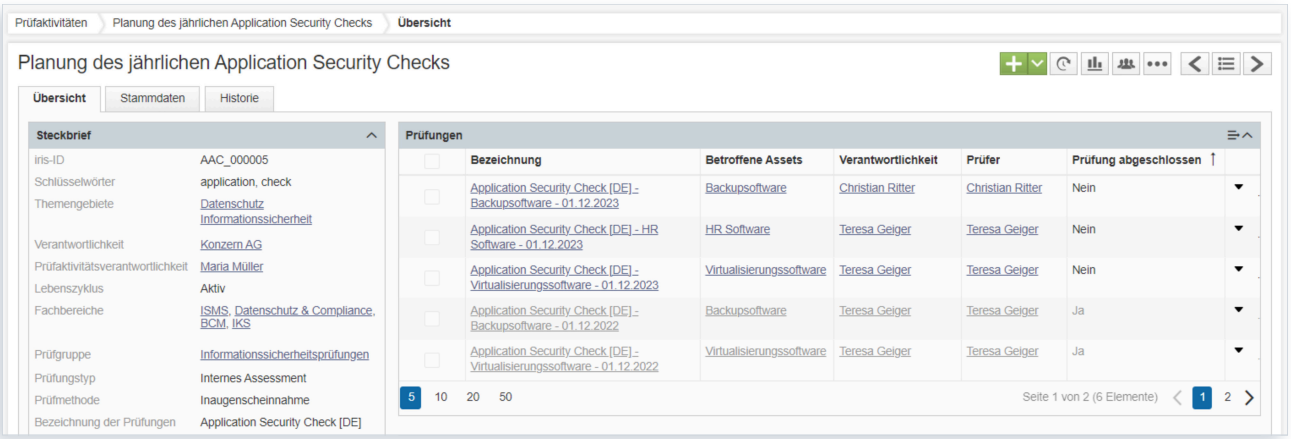
2. Duplizieren von Prüfungen

Ebenso wie bei Prüfvorlagen, können auch Prüfungen selbst dupliziert werden. Somit sind jährliche bzw. wiederkehrende Prüfungen ohne großen Aufwand in der Software erstellbar. Beispielsweise kann die Prüfung des Vorjahrs – inkl. z. B. der Ergebnisse und Dokumente – dupliziert und als Basis für die nächste fällige Prüfung verwendet werden.



3. Prüfaktivitäten

Alternativ gibt es mittels der Prüfaktivitäten die Möglichkeit, anstehende Prüfungen bereits im Voraus zu planen und festzulegen, wann die entsprechenden Prüfungen automatisch erstellt werden sollen. Bei der Planung können sowohl statische als auch dynamische Datensatzinhalte festgelegt werden, die in den erzeugten Prüfungen automatisch belegt werden.



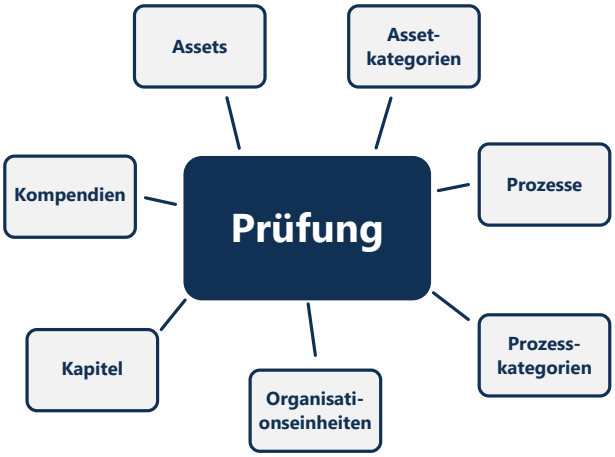
Use Case „Prüfung externer Dienstleister“

Eine ISMS-/GRC-Software sollte einen Großteil der möglichen verschiedenen Abfragearten und -typen berücksichtigen. Ein immens wichtiger Punkt ist diesbezüglich die Prüfungserstellung und Prüfungsplanung. Erst nach erfolgter Erstellung der Prüfung bzw. gut organisierter Prüfungsplanung kann der interne/externe Auditor bzw. Prüfer mit der wirklichen Prüfungsdurchführung starten. Mit der durchgeführten und abgeschlossenen Prüfung ist der Prozess noch nicht beendet. Im Anschluss erwartet jede Behörde oder auch interne Stelle eine vernünftige Auswertung der Prüfung. Deshalb wird in der Software ibi systems iris das Thema Reporting und Dashboarding als sehr bedeutend angesehen.

In diesem Leitfaden wird nun der Anwendungsfall „Prüfung externer Dienstleister“ als Use-Case vorgestellt.

Beispielsweise wurden mit Lieferanten oder sonstigen Dienstleistern gewisse Qualitätsniveaus vereinbart und diese sollen regelmäßig auf Einhaltung überprüft werden. In ibi systems iris ist es möglich, dass diese externen Audits dokumentiert werden oder aber direkt von den externen Dienstleistern nach Freigabe in der Software ausgefüllt werden können. Alternativ bietet ibi systems iris die Möglichkeit, die externen Prüfungen herunterzuladen und offline per E-Mail weiterzuleiten. Die Externen können die Prüfung im Excel ausfüllen und anschließend zurückschicken. Die offline bearbeitete Prüfung kann dann wieder in die Software eingelesen werden.

Für eine Prüfung können beispielsweise die betroffenen Prozesse oder Organisationseinheiten referenziert werden. In dem Anwendungsfall „Prüfung externer Dienstleister“ könnten dies beispielsweise betroffene Prozesse aus der Zusammenarbeit mit einem Lieferanten oder Dienstleister sein. Zusätzlich wäre es möglich, die betroffenen Externen ebenfalls mit der Prüfung direkt in Verbindung zu setzen.



Durch die filterbare und übersichtliche Listenansicht in ibi systems iris kann jederzeit eine Auskunft über den aktuellen Stand verschiedenster Prüfungen bei den externen Dienstleistern gegeben werden. Beispielsweise kann in der Software nach bestimmten Themengebieten oder Bezeichnungen der Prüfung gefiltert werden. Durch den Fortschrittsbalken ist mit einem Blick ersichtlich, inwieweit die Prüfungen bereits durchgeführt wurden.

Bezeichnung	Prüfung abgeschlossen	Verantwortlichkeit	Prüfer	Fortschritt	Fachbereiche
IKS-Prüfung	Nein	Konzern AG	Konzern AG		ISMS, Datenschutz & Compliance, BCM, IKS
ISO 27001 - Statement of Applicability (SoA) - 2022 - en - applicable/not applicable - 27.10.2023	Nein	Konzern AG	Giacomo Pasini		ISMS, Datenschutz & Compliance, BCM, IKS
Revisionsprüfung Identity Management - 06.12.2023	Nein	Konzern AG	Konzern AG, Stefan Wagner		ISMS, Datenschutz & Compliance, BCM, IKS
Application Security Check [DE] - Personalverwaltung	Nein	Christian Ritter	Konzern AG		ISMS, Datenschutz & Compliance, BCM, IKS
ISMS-Check	Nein	Stefan Wagner	Carina Braunmühl, Giacomo Pasini, Stefan Wagner		BCM
Application Security Check [DE] - 23.09.2022	Nein	Stefan Wagner	Stefan Wagner		ISMS, Datenschutz & Compliance, BCM, IKS
Application Security Check [DE] - Virtualisierungsserver2	Nein	Christian Ritter	Konzern AG		ISMS, Datenschutz & Compliance, BCM, IKS
TISAX VDA - Information Security Assessment 2021	Nein	Konzern AG	Carina Braunmühl, Giacomo Pasini, Stefan Wagner		ISMS
DIN EN ISO/IEC 27019:2020 - 28.11.2023	Nein	Konzern AG	Christian Ritter		ISMS, Datenschutz &

Fazit

Mit ibi systems iris kann das komplette Prüfungs- und Auditmanagement systemgestützt dokumentiert, geplant und durchgeführt werden. Durch die Prüfvorlagen werden Templates einmalig erstellt und können mit einem Klick zu einer Prüfung bzw. einem Audit erzeugt werden. Ausgehend von einer Prüfung können direkt weitere Datensätze wie z. B. Risiken, Maßnahmen, Feststellungen oder Dokumente erzeugt oder verknüpft werden.

Durch die vielfältigen Import- und Exportmöglichkeiten in bzw. aus ibi systems iris heraus kann jederzeit mit bestehenden Daten in der Software weitergearbeitet und diese im Nachgang problemlos exportiert werden. So beispielsweise mit der Offline-Bearbeitung von Prüfungen.

Die umfangreichen Reports und Dashboards bieten zu jeder Zeit den vollumfänglichen Überblick über sämtliche Prüfungen aus allen Bereichen. Mit ibi systems iris werden alle Daten mit Bezug zu Prüfungen und Audits an einer zentralen Stelle abgelegt.

Abgerundet wird das Angebot der Software ibi systems iris mit der Option, für Anwender der Software eine Zertifikatsschulung zu absolvieren.