Praxisnahe Auditplanung und Durchführung: Begrifflichkeiten für das gemeinsame Verständnis

Erhebungsmanagement	Über das „Werkzeug Erhebungsmanagement“ wird das Erhebungsmanagement aufgerufen. Dort werden Erhebungen angelegt und bearbeitet. Die Übersicht der Erhebungen (geplante, in Arbeit, geschlossene) im Erhebungsmanagement stellen das Auditprogramm dar (und auch die Übersicht der bewerteten Anforderungsprofile).
Erhebungen	Erhebungen sind Audits oder Anforderungsprofile (Sollmaßnahmenkatalog) und werden im Erhebungsmodul erstellt.
Auditprogramm	Das Auditprogramm unterscheidet sich von der Auditplanung dadurch, dass es sich beim Auditprogramm um die Übersicht von einzelnen Audits handelt. Es legt zunächst nur den geplanten Auditgegenstand bzw. Audit Scope für die geplanten Audits sowie die zeitliche Reihenfolge für die Auditierung fest.
Auditplanung	Die Auditplanung beinhaltet die konkreten Rahmenbedingungen für ein im Auditprogramm festgeschriebenes Audit, z.B. verwendetes Auditprofil (Konzeptkategorie oder Anforderungsprofil), Zeiten, Orte, Auditmethoden, Auditor und Ansprechpartner.
Profile (Auditprofil)	Für Erhebungen können die bereitgestellten Profile genutzt werden. Die Auditprofile (SITB-Anforderungen) werden vom SIZ kontinuierlich gepflegt („managed“). Zudem sind die jeweils aktuellen DSGV Anforderungsprofile hinterlegt. Bei Bedarf können auch individuelle Profile hinzugefügt werden.
Anforderung (RQ)	RQ = Requirement. Im SITB sind funktionale (fachliche) Anforderungen sowie Anforderungen bzgl. der Einhaltung gesetzlicher und regulatorischer Vorgaben abgebildet.
Anforderungsgruppen (GR)	GR = Group of Requirement. Mit Version 18 wurden Anforderungen in sogenannten Anforderungsgruppen (GR) zusammengefasst. Eine Anforderungsgruppe enthält eine oder mehrere Anforderungen (RQ) und stellt dazu eine Auditfrage.
Gegenstand	Der „Gegenstand“ umfasst den Umfang (auch „Audit Scope“) oder Schwerpunkt des Audits beispielsweise ein Unternehmensbereich, ein Standort, eine Dienstleistung oder Service. Jedem Gegenstand ist ein „Unternehmen“ zuzuordnen. Dies ist, z. B. die eigene Sparkasse, ein Fachbereich oder ein relevanter Dienstleister der Sparkasse.
Managementsystem-Audit	Im Managementsystem-Audit werden die SITB-Anforderungen typischerweise auf der Ebene der Anforderungsgruppen (GR) betrachtet. Dieser Audit-Typ wird vorrangig zur Überprüfung der Soll-Soll-Umsetzung genutzt, d. h. der Anteil an stichprobenhaften Soll-Ist-Vergleichen ist hier geringer als beispielsweise beim szenariobasierten Audit.
Delta-Audit	Sonderform des Managementsystem-Audits zur Betrachtung von unterjährig geänderten SITB-Anforderungen, Aktivitäten oder Auditfragen des SITB im Rahmen des Release-Managements des SIZ.
Szenariobasiertes Audit	Das szenariobasierte Audit kann genutzt werden, um risikoorientiert (z. B. Schutzbedarf) oder anlassbezogen für die Informationssicherheit wesentliche Aspekte detailliert zu betrachten. Die Audit-Art wird auf der RQ-Ebene (SITB-Anforderungen) durchgeführt. Dabei werden typischerweise die Anforderungsprofile genutzt. Die Anzahl der Stichproben, also die „Soll-Ist-Vergleiche“ der Umsetzung ist höher als im Managementsystem-Audit.

Vertiefendes Audit	Vertiefende Audits eignen sich, um risikoorientiert oder anlassbezogen für die Informationssicherheit wesentliche Sachverhalte auf Umsetzungsebene zu betrachten. Im Gegensatz zu den szenariobasierten Audits basieren diese Audits nicht direkt auf der Betrachtung von SITB-Anforderungen, sondern gehen darüber hinaus und verwenden in der Regel weitere Quellen, z. B. des Bundesamts für Sicherheit in der Informationstechnik oder eigene Checklisten.
Stichproben	Stichproben ermöglichen im Audit (oder Nachgang) einen Soll-Ist-Abgleich mit den Anforderungen sowie die Verifikation der Audit-Antworten. Stichproben können Organisationsrichtlinien, Konzepte, Protokolle, Nachweise im Intranet, technische Tests etc. sein. Stichproben werden unter „Nachweise“ im Erhebungsmodul des Erhebungsmanagements dokumentiert.
Datenbank	Alle Daten zu geplanten und durchgeführten Erhebungen werden in einer Datenbank (Backup) im Verzeichnis \siz_intern\dbBackup gespeichert. Der Dateiname enthält das Datum und den Zeitstempel. Beispiel: data-20200909T120059.tar.gz Achtung: Beim Zurückspielen gehen alle Änderungen in der Erhebung, die nach dem jeweiligen Backup vorgenommen wurden, verloren.
Anforderungsprofile	Anforderungsprofile wurden in der DSGV-Expertenrunde (Regionalverbänden, FI, der SIZ und dem DSV) für (Betreiber-) Szenarien erstellt, z.B. Server oder Clients. Diese berücksichtigen die SITB-Anforderungen. Ein vom Betreiber beantwortetes Anforderungsprofil ist eine Selbstauskunft und kann nicht als Audit gewertet werden, da keine ausreichende Objektivität bzw. Unabhängigkeit unterstellt werden kann, welche die Voraussetzung für ein Audit ist (vgl. ISO 27001). Bereits beantwortete Anforderungsprofile können grundsätzlich ins Erhebungsmanagement importiert werden und als Basis für ein szenariobasiertes Audit herangezogen werden. In einem Auditprogramm sollten auch Audits auf der Ebene von Anforderungsprofilen über einen Zeitraum von einigen Jahren (z. B. drei Jahren) eingeplant werden (vgl. FAQ der DSGV-Expertenrunde „Anforderungsprofile/Sollmaßnahmen“).
Betreiber	Die im Zuge der Anforderungsprofile genannten „Betreiber“ können interne Organisationseinheiten sein, die die Leistung erbringen („Eigenbetrieb“), also die „fachlich verantwortlich“ sind. Betreiber können auch externe Dienstleister („Fremdbetrieb“) sein, die Leistungen für die Sparkasse erbringen. Anforderungsprofile können (sollten) vom Dienstleister ausgefüllt und müssen von der Sparkasse bewertet werden.

Quelle: Deutscher Sparkassenverlag, IT-Consulting (GBIC), Bereich Geschäftsbetrieb (Stand: Okt. 2020)