Agile ISMS

Know-how to go: ISMS-Automatisierung – Agil. Sicher. Effizient.

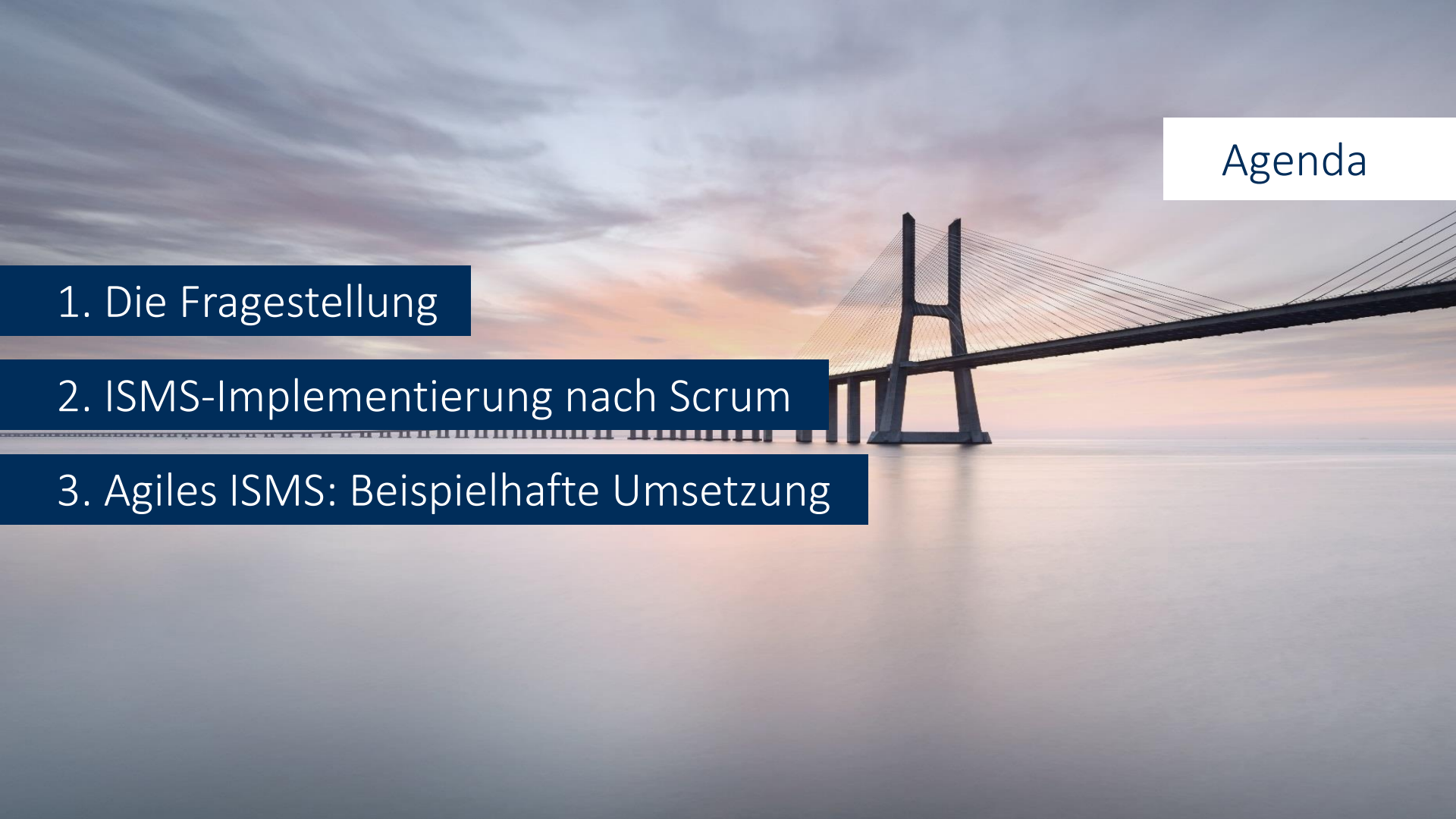
HiSolutions AG

Rengbar Hardam

Rengbar Hardam
Consultant

- Themenschwerpunkte: ISMS-Implementierung (ISO 27001, BSI IT-Grundschutz, Grundschutz++), Audits, agile Sicherheitsstrategien
- Beratung von großen Organisationen bis Start-ups bei maßgeschneiderten Sicherheitslösungen
- M. Sc. Wirtschaftsinformatik
- BSI IT-Grundschutz-Praktiker, BSI BCM-Praktiker
- ISO27001:2022 Lead Auditor
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a BSIG
- Interessen: KI-Einsatz zur Optimierung von Sicherheitsprozessen

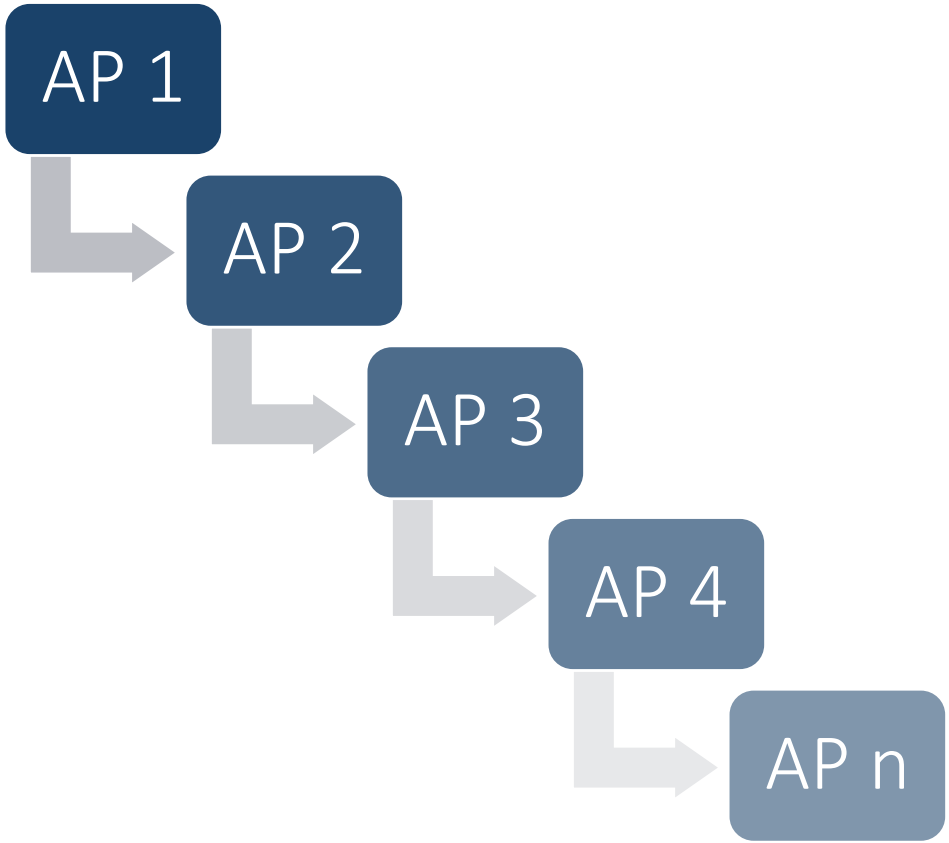
Agenda



1. Die Fragestellung
2. ISMS-Implementierung nach Scrum
3. Agiles ISMS: Beispielhafte Umsetzung

1. Die Fragestellung

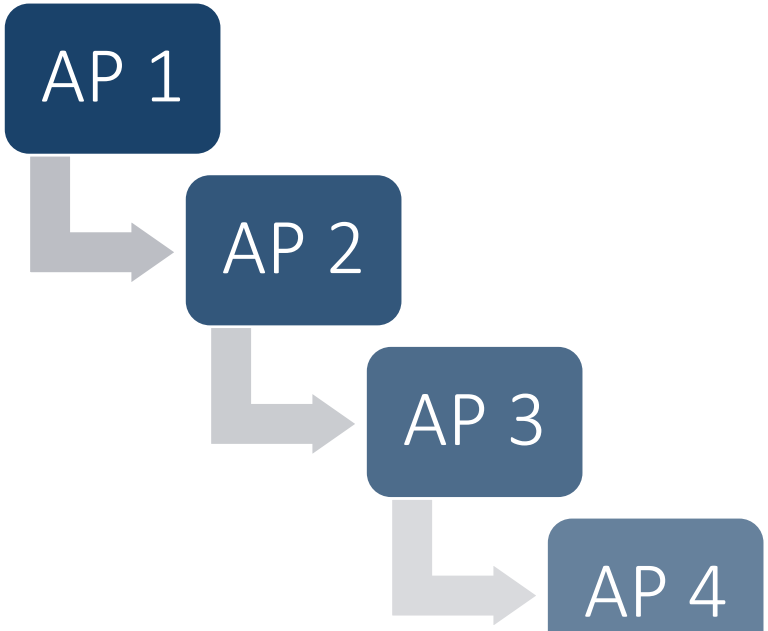
„Wir benötigen die ISO-27001-Zertifizierung dringend. Das Projekt sollte schnellstmöglich gestartet werden.“ – Oberste Leitung



Projektmanagement-Methode

Wasserfall-Modell

Der vollständige, sequenzielle Plan mit allen Arbeitspaketen, Meilensteinen und Deadlines für das gesamte Projekt ist vorab fixiert.



Projektmanagement-Methode

Wasserfall-Modell

Agile Sicherheit

Agile Sicherheit

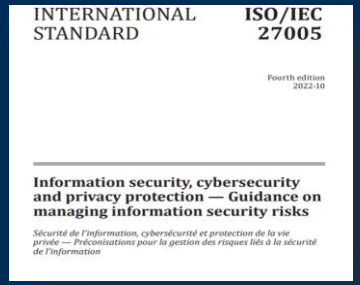
Entwicklung eines Blueprints für die Implementierung von ISO/IEC 27001:2022 mit Scrum

Agile Sicherheit

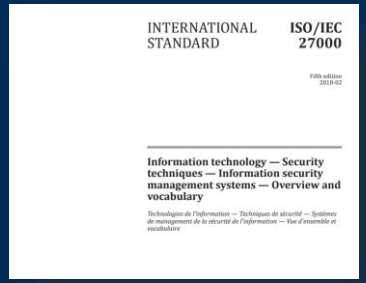
Entwicklung eines Blueprints für die Implementierung von ISO/IEC 27001:2022 mit Scrum

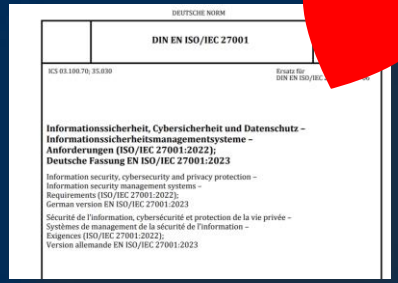
2. ISMS-Implementierung nach Scrum

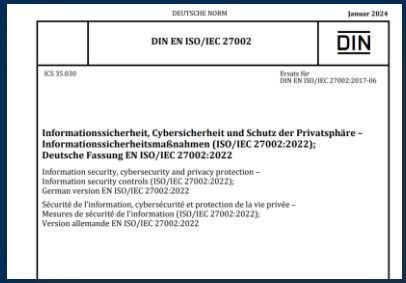
ISO/IEC 27000er: Das Regelwerk für Informationssicherheit

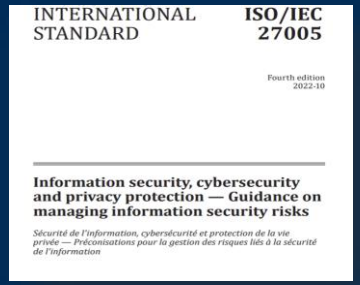


ISO/IEC 27000er: Das Regelwerk für Informationssicherheit

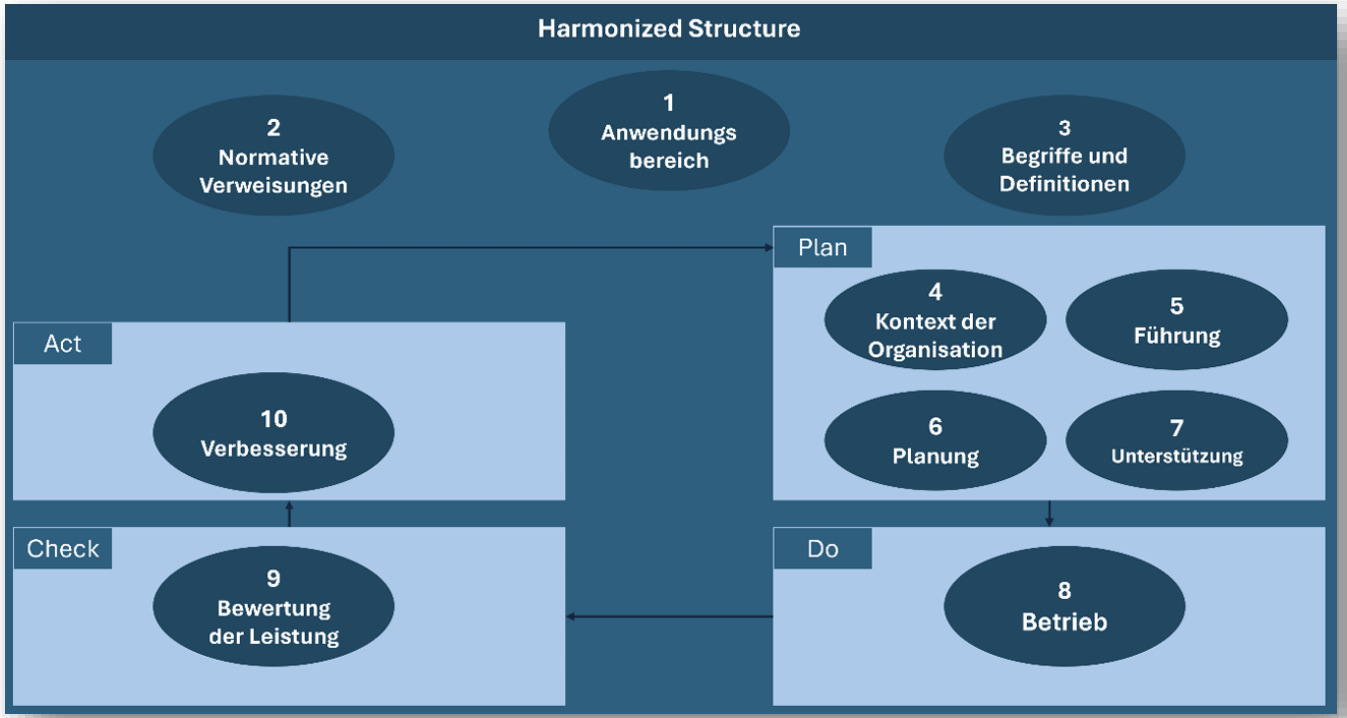




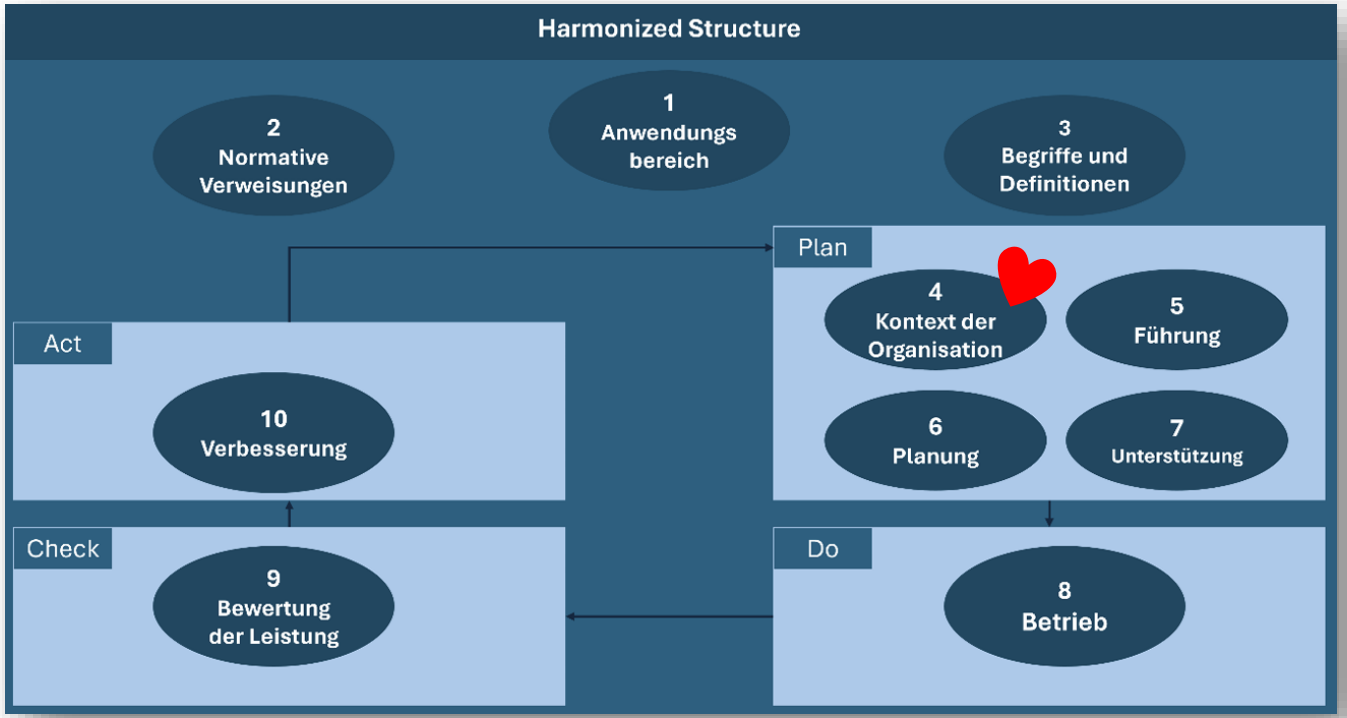




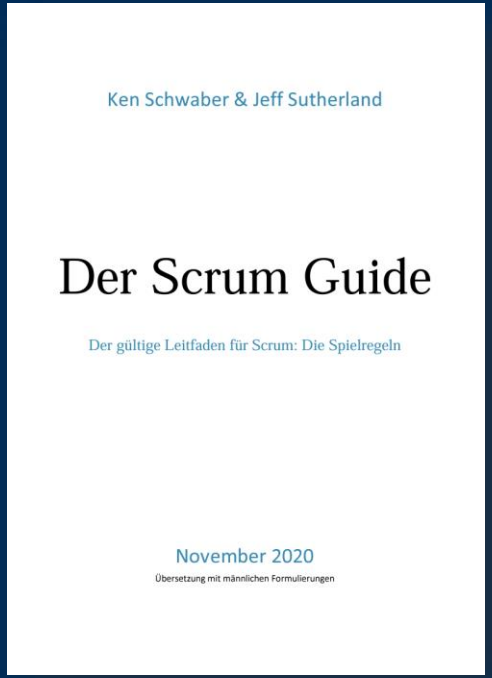
Die ISO-27001-Logik: PDCA-Zyklus der *Harmonized Structure*



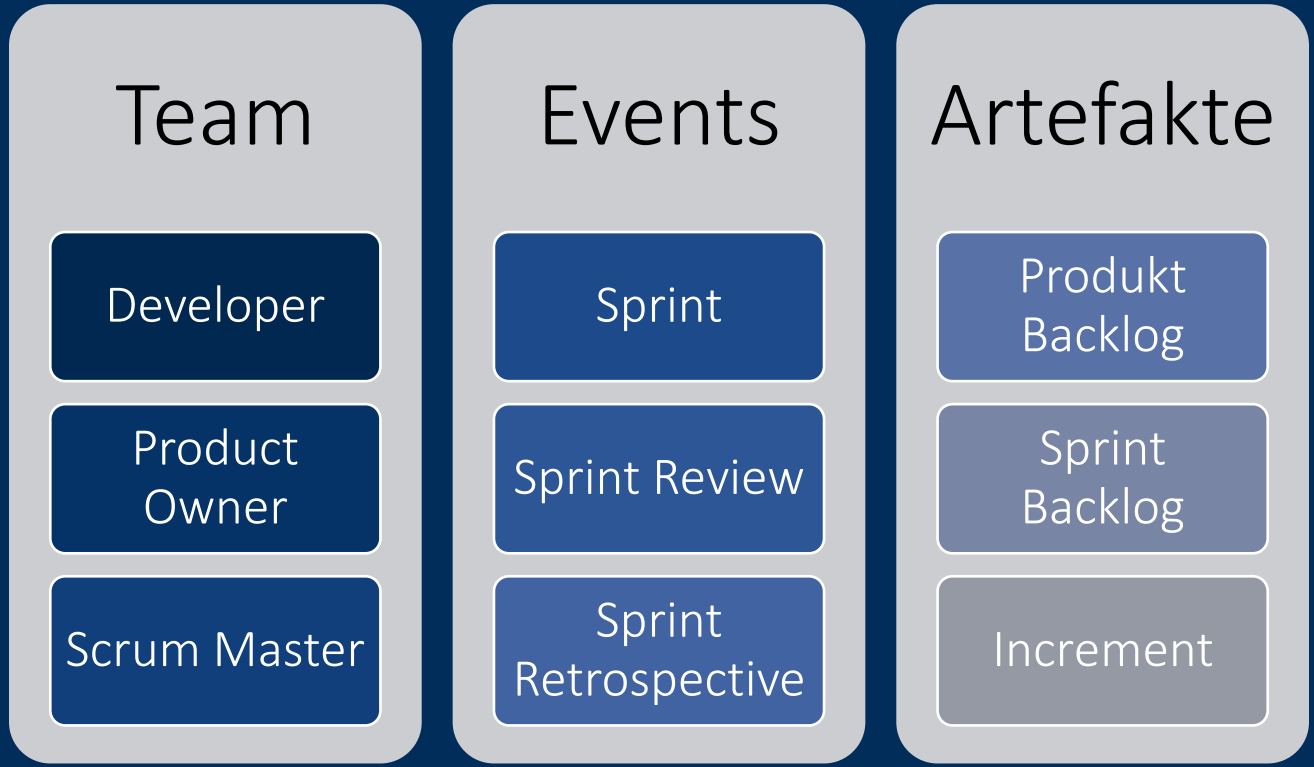
Die ISO-27001-Logik: PDCA-Zyklus der *Harmonized Structure*



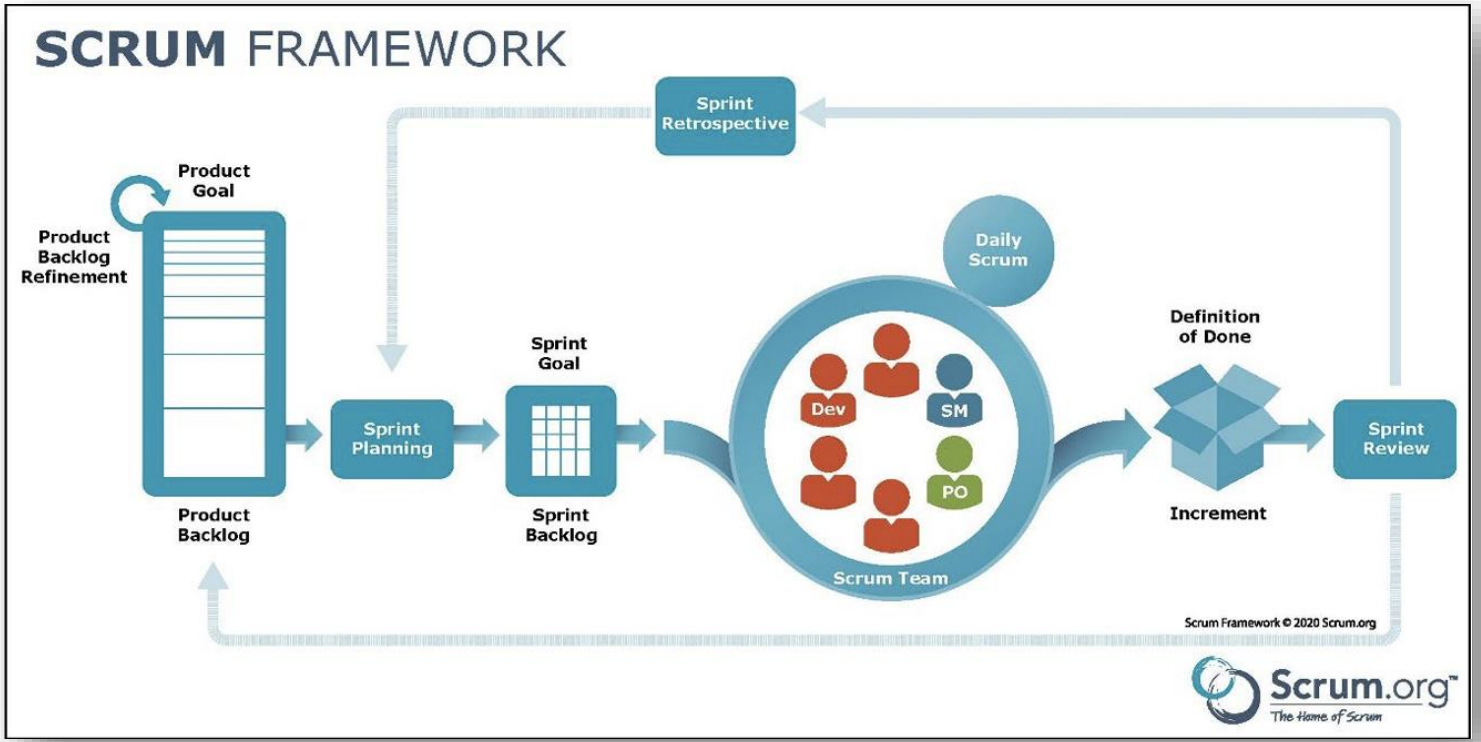
Scrum: Das Fundament. Die offiziellen Spielregeln



Scrum im Überblick: Die drei Säulen des Frameworks



Scrum in Aktion: Der Ablauf vom Backlog zum Increment



3. Agiles ISMS: Beispielhafte Umsetzung

Scrum Master: Mehr als ein Projektleiter (PL)

- Unabhängigkeit der Rolle
- Unterstützung des Scrum-Teams
- Optimierung der Zusammenarbeit mit dem Product Owner
- Coaching des Teams zu agilen Methoden und Prinzipien
- Kein PL, CISO/ISB

ISMS & Scrum: Die Epics im Product Backlog

- **Epic 0**: Initiierung und GAP-Analyse
- **Epic 1**: Etablierung des ISMS-Rahmenwerks
- **Epic 2**: Dokumentation des Managementsystems
- **Epic 3**: Assetmanagement
- **Epic 4**: Risikomanagement
- **Epic 5**: Operationalisierung
- **Epic 6**: Effektivitätsbewertung
- **Epic 7**: Managementbewertung
- ***Epic 8**: Auditmanagement*

Artefakte

Product Backlog

Sprint Backlog

Increment

Epic 1 – Kapitel 4 & 5 der ISO 27001: Die ersten Schritte

- Dokumentation der Anforderungen der interessierten Parteien
- Definition des Anwendungsbereichs des ISMS und entsprechende Dokumentation
- Entwicklung der ISMS-Policy
- Bekenntnisschreiben der obersten Leitung und Verabschiedung der Policy durch das Management

Artefakte

Product Backlog

Sprint Backlog

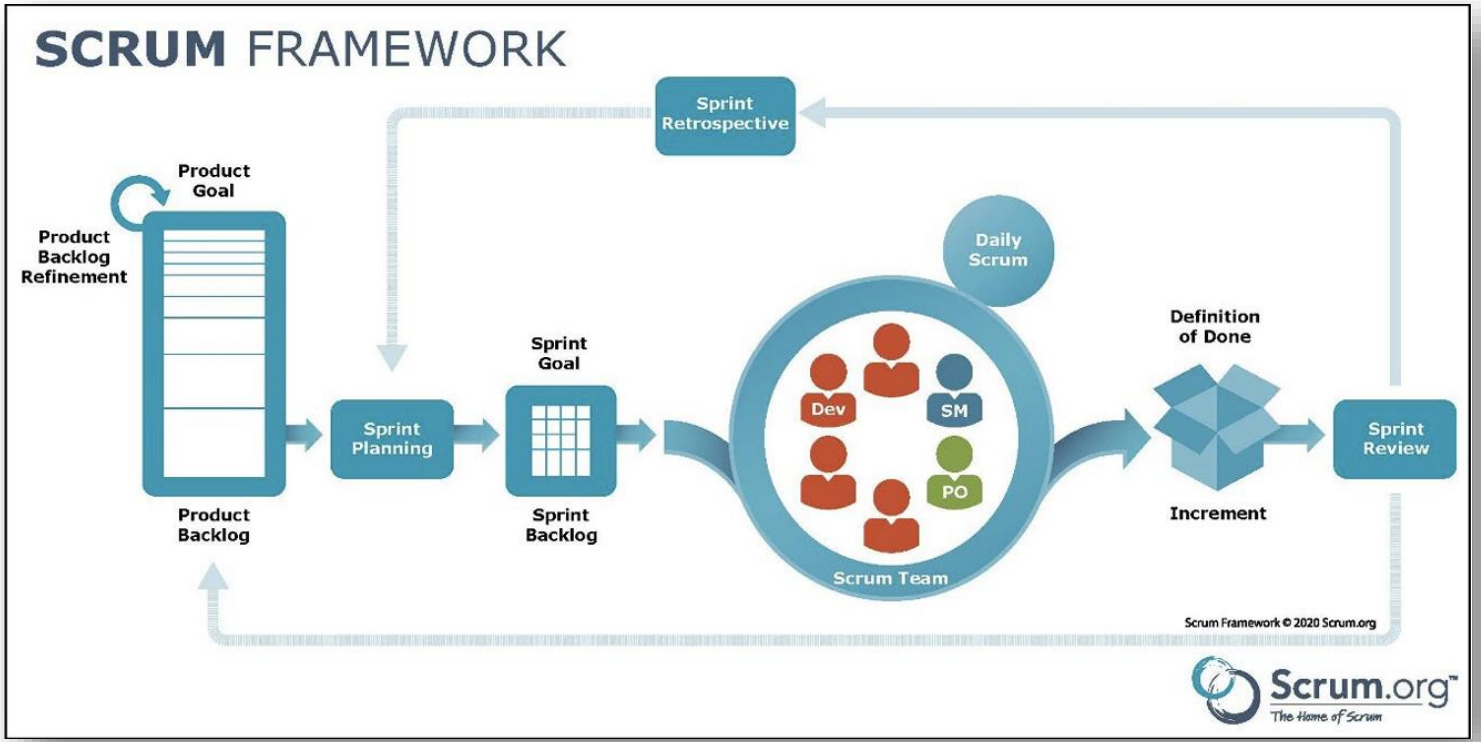
Increment

Abarbeitung Epic 1: Etablierung des ISMS-Frameworks

ID	Epic	Epicname	Task	Beschreibung	Abhängigkeit	Task Owner	Motivation/Begründung
				Einflüsse zu identifizieren, die das ISMS betreffen könnten.			
T106	1	Etablierung des ISMS-Rahmenwerks	Workshop durchführen	Führe den Workshop durch, um die Anforderungen der interessierten Parteien zu diskutieren, zu sammeln und zu dokumentieren.	T104		Sammlung der Anforderungen der interessierten Parteien
T107	1	Etablierung des ISMS-Rahmenwerks	Ergebnisse des Workshops dokumentieren	Halte die Ergebnisse des Workshops fest, einschließlich der und der identifizierten Anforderungen.	T106		Nachvollziehbarkeit der Workshop-Ergebnisse
T108	1	Etablierung des ISMS-Rahmenwerks	Dokumentation der interessierten Parteien finalisieren	Finalisiere das Dokument, das die Anforderungen der interessierten Parteien zusammenfasst.	T107		Abschluss der Anforderungsdokumentation
T109	1	Etablierung des ISMS-Rahmenwerks	Dokumentation der Geschäftsführung zur Verabschiedung vorlegen	Lege das finalisierte Dokument der Geschäftsführung zur Verabschiedung vor.	T108		Einholung der Geschäftsführungs-Freigabe
T110	1	Etablierung des ISMS-Rahmenwerks	Protokoll des Workshops erstellen	Erstelle ein detailliertes Protokoll des Workshops, das auch die Gründe für die Irrelevanz bestimmter Themen nachvollziehbar macht.	T106		Dokumentation der Workshop-Diskussionen und Entscheidungen
T111	1	Scope des ISMS	Überprüfung der Workshop-Teilnehmer	Stelle sicher, dass die Teilnehmer des Workshops "Kontext und interessierte Parteien des ISMS" auch für die Diskussion des ISMS-Scope relevant und angemessen sind.	T110		Relevanz der Teilnehmer für ISMS-Scope sicherstellen
T112	1	Scope des ISMS	Zusätzliche Teilnehmer für Scope-Definition identifizieren	Ermittle, ob zusätzliche Stakeholder für die Scope-Definition benötigt werden, und lade sie gegebenenfalls	T111		Vollständigkeit der Stakeholder für Scope-Definition gewährleisten

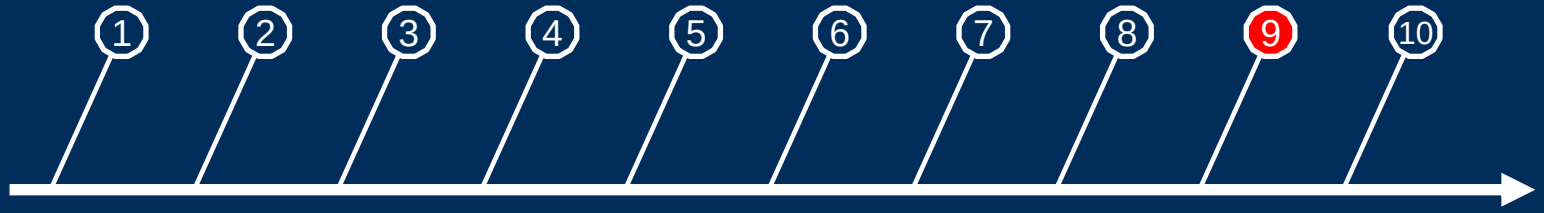
Epic0 | Epic1 | Epic 2 | Epic 3 | Epic 4 | Epic 5 | Epic 6 | Epic 7 | Epic 8

Der Weg zur "Definition of Done": Der Task-Prozess

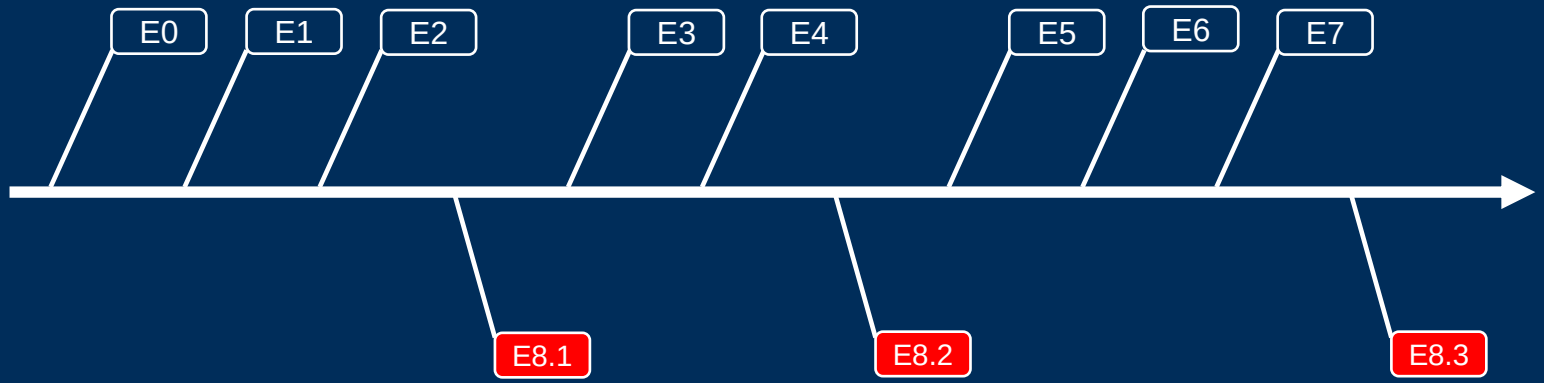


Der agile Weg: Interne Audits als kontinuierlicher Prozess

~~Agil~~



Agil



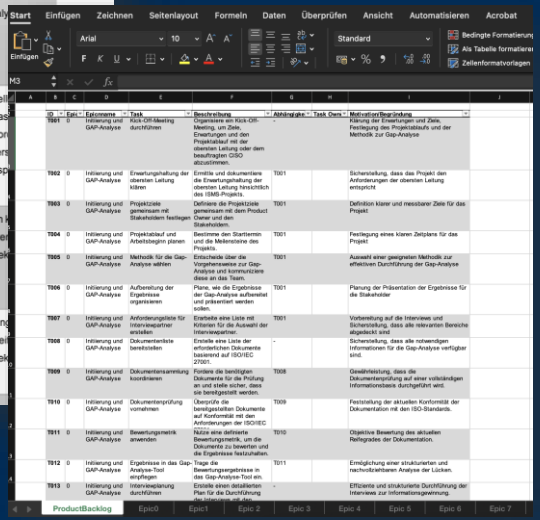
Welche spezifischen Vorteile und Mehrwerte bietet der Einsatz von Scrum im Kontext der ISMS-Implementierung und des fortlaufenden ISMS-Betriebs?

- Aufteilung des internen Audits
  - *Kleinere Audits nach Epics*
  - *Umfassendes internes Audit zum Abschluss der Implementierung*
- Frühzeitige Überprüfung und Korrektur
- Etablierung des kontinuierlichen Verbesserungsprozesses während der Umsetzung
- Förderung der Zusammenarbeit und Kommunikation
- Höhere Transparenz und Sichtbarkeit des Implementierungsfortschritts

Der HiSolutions-ISMS-Blueprint: Das vollständige Product Backlog

Product Backlog

ID	E-pic	Epicname	Task	Beschreibung	Abhängigkeit	Task Owner	Motivation/ Begründung
T001	0	Initiierung und GAP-Analyse	Kick-Off-Meeting durchführen	Organisiere ein Kick-Off-Meeting, um Ziele, Erwartungen und den Projektablauf mit der obersten Leitung oder dem beauftragten CISO abzustimmen.	-		Klärung der Erwartungen und Ziele, Festlegung des Projektablaufs und der Methodik zur Gap-Anal
T002	0	Initiierung und GAP-Analyse	Erwartungshaltung der obersten Leitung klären	Ermittle und dokumentiere die Erwartungshaltung der obersten Leitung hinsichtlich des ISMS-Projekts.	T001		Sicherstell dass das den Anfor der obers tung entsp
T003	0	Initiierung und GAP-Analyse	Projektziele gemeinsam mit Stakeholdern festlegen	Definiere die Projektziele gemeinsam mit dem Product Owner und den Stakeholdern.	T001		Definition messbare das Projek
T004	0	Initiierung und GAP-Analyse	Projektablauf und Arbeitsbeginn planen	Bestimme den Starttermin und die Meilensteine des Projekts.	T001		Festlegu klaren Zei das Projek
T005	0	Initiierung und GAP-Analyse	Methodik für die Gap-Analyse wählen	Entscheide über die Vorgehensweise zur Gap-Analyse und kommuniziere diese an das Team.	T001		Auswahl einer geeigneten Methodik zur effektiven Durchführung der Gap-Analyse
T006	0	Initiierung und GAP-Analyse	Aufbereitung der Ergebnisse organisieren	Plane, wie die Ergebnisse der Gap-Analyse aufbereitet und präsentiert werden sollen.	T001		Planung der Präsentation der Ergebnisse für die Stakeholder
T007	0	Initiierung und GAP-Analyse	Anforderungsliste für Interviewpartner erstellen	Erarbeite eine Liste mit Kriterien für die Auswahl der Interviewpartner.	T001		Vorbereitung auf die Interviews und Sicherstellung, dass alle relevanten Bereiche abgedeckt sind.
T008	0	Initiierung und GAP-Analyse	Dokumentenliste bereitstellen	Erstelle eine Liste der erforderlichen Dokumente basierend auf ISO/IEC 27001.	-		Sicherstellung, dass alle notwendigen Informationen für die Gap-Analyse verfügbar sind.
T009	0	Initiierung und GAP-Analyse	Dokumentensammlung koordinieren	Fordere die benötigten Dokumente für die Prüfung an und stelle sicher, dass sie bereitgestellt werden.	T008		Gewährleistung, dass die Dokumentenprüfung auf einer vollständigen Informationsbasis durchgeführt wird.
T010	0	Initiierung und GAP-Analyse	Dokumentenprüfung vornehmen	Überprüfe die bereitgestellten Dokumente auf Konformität mit den Anforderungen der ISO/IEC	T009		Feststellung der aktuellen Konformität der Dokumentation mit den ISO-Standards.
T011	0	Initiierung und GAP-Analyse	Bewertungsmetrik anwenden	Nutze eine definierte Bewertungsmetrik, um die Dokumente zu bewerten und die Ergebnisse festzuhalten.	T010		Objektive Bewertung des aktuellen Reifegrades der Dokumentation.
T012	0	Initiierung und GAP-Analyse	Ergebnisse in das Gap-Analyse-Tool einpflegen	Trage die Bewertungsergebnisse in das Gap-Analyse-Tool ein.	T011		Ermöglichung einer strukturierten und nachvollziehbaren Analyse der Lücken.
T013	0	Initiierung und GAP-Analyse	Interviewplanung durchführen	Erstelle einen detaillierten Plan für die Durchführung der Interviews zur Informationsgewinnung.	-		Effiziente und strukturierte Durchführung der Interviews zur Informationsgewinnung.



Modellhafte Sprintplanung

Epic	Epicname	Sprint	Task
0	Initiierung und GAP-Analyse	0	**Kick-Off und Projektvorbereitung** • Kick-Off-Meeting durchführen: Organisiere ein Kick-Off-Meeting, um Ziele, Erwartungen und den Projektablauf mit der obersten Leitung oder dem beauftragten CISO abzustimmen. • Erwartungshaltung klären: Ermittle und dokumentiere die Erwartungshaltung der obersten Leitung hinsichtlich des ISMS-Projekts. • Projektziele festlegen: Definiere die Projektziele gemeinsam mit dem Product Owner und den Stakeholdern. • Projektablauf und Arbeitsbeginn planen: Bestimme den Starttermin und die Meilensteine des Projekts. • Methodik für die Gap-Analyse wählen: Entscheide über die Vorgehensweise zur Gap-Analyse und kommuniziere diese an das Team. • Aufbereitung der Ergebnisse organisieren: Plane, wie die Ergebnisse der Gap-Analyse aufbereitet und präsentiert werden sollen. • Anforderungsliste für Interviewpartner erstellen: Erarbeite eine Liste mit Kriterien für die Auswahl der Interviewpartner.
0	Initiierung und GAP-Analyse	1	**Dokumentenprüfung** • Dokumentenliste bereitstellen: Stelle eine Liste der erforderlichen Dokumente basierend auf ISO/IEC 27001 zusammen. • Dokumentensammlung koordinieren: Fordere die benötigten Dokumente für die Prüfung an und stelle sicher, dass sie bereitgestellt werden. • Dokumentenprüfung vornehmen: Überprüfe die bereitgestellten Dokumente auf Konformität mit den Anforderungen der ISO/IEC 27001. • Bewertungsmetrik anwenden: Nutze eine definierte Bewertungsmetrik, um die Dokumente zu bewerten und die Ergebnisse festzuhalten. • Ergebnisse in das Gap-Analyse-Tool einpflegen: Trage die Bewertungsergebnisse in das Gap-Analyse-Tool ein.
0	Initiierung und GAP-Analyse	2	**Durchführung der Interviews** • Interviewplanung durchführen: Erstelle einen detaillierten Plan für die Durchführung der Interviews mit den relevanten Ansprechpartnern. • Interviews führen: Führe die geplanten Interviews durch, um Informationen zur aktuellen ISMS-Situation zu sammeln. • Interviewergebnisse dokumentieren: Halte die Ergebnisse der Interviews fest und bereite sie für die wei-

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com