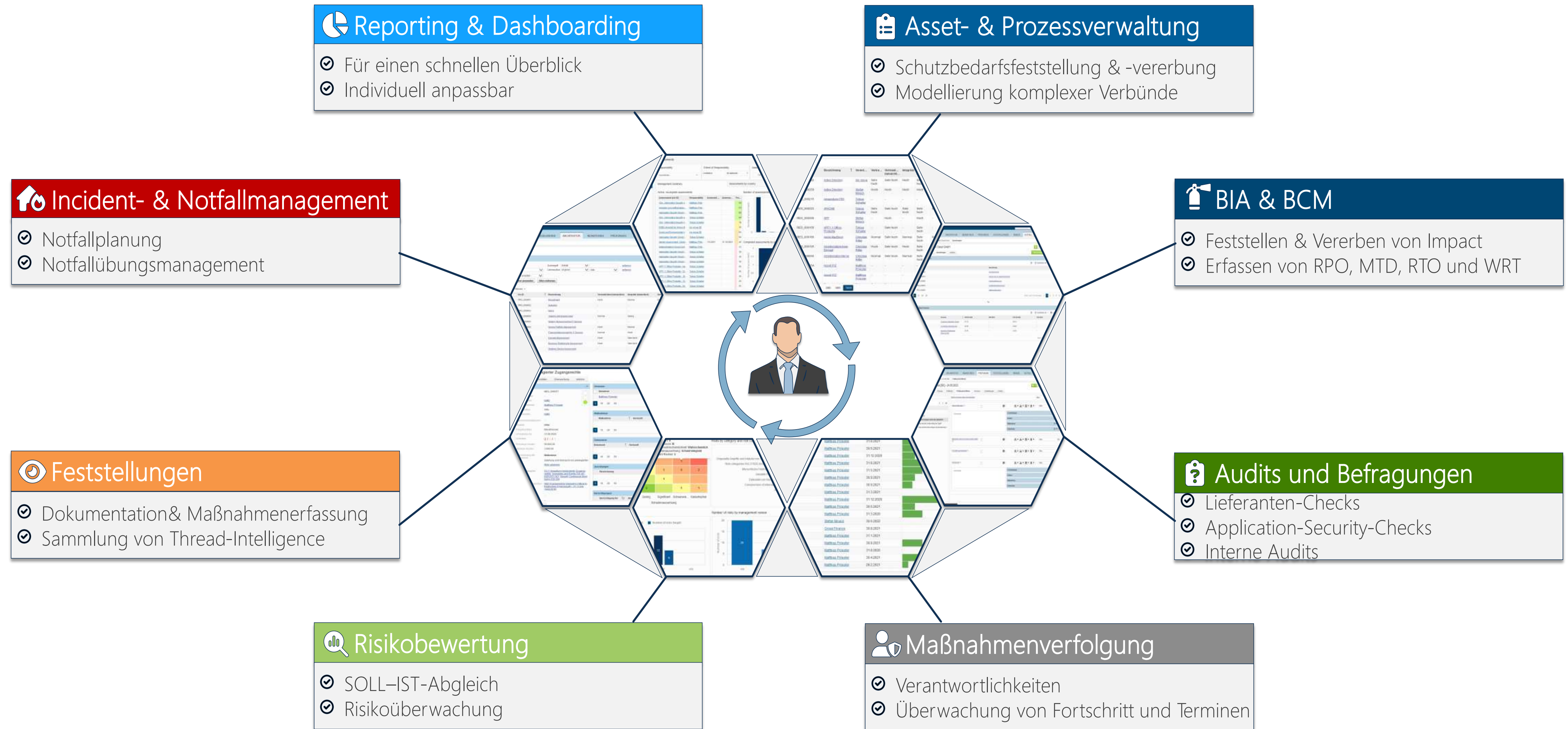


Information Security beyond Compliance

it-sa | Dr. Stefan Wagner

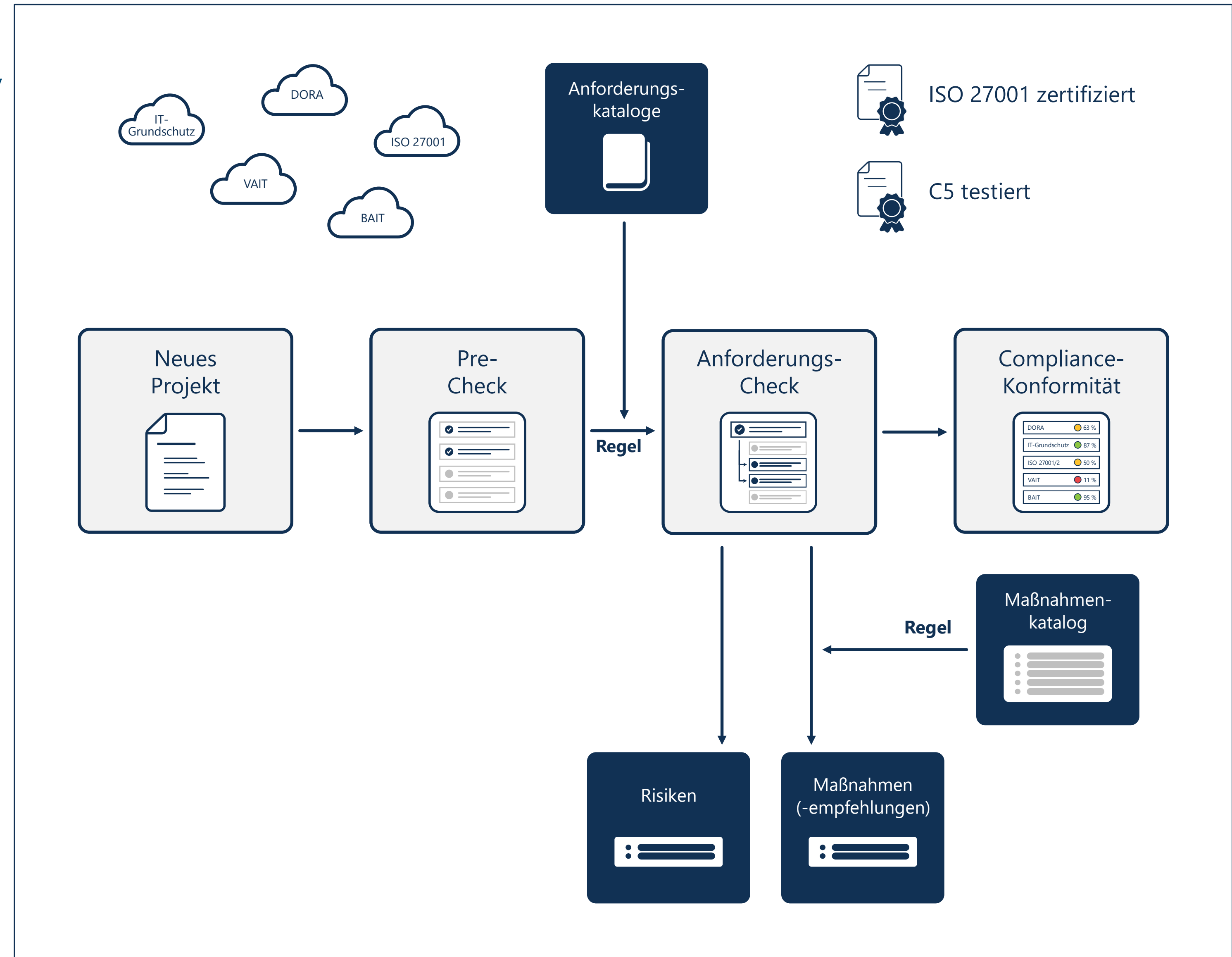


CISO's Universe in ibi systems iris



Lösungsansatz

- Mapping relevanter Anforderungen (NIS, DORA, etc.) in spezifische Anforderungskataloge
 - Externer Service; neuer Lieferant
 - Einkauf Software
 - etc.
- „Pre-Check“ zur Einordnung der anzuwendenden Anforderungskataloge, inkl.
 - Feststellung Schutzbedarf, BIA
 - Datenschutzrelevanz
 - etc.
- „Anforderungs-Check“
 - Compliance-Konformität nach allen gemappten relevanten Anforderungen über alle Projekte
 - Automatisch Maßnahmen
 - Direkte Übersichten zu Risiken



Beispielhafter Anforderungskatalog

KRITIS	Thema	C5:2020	NIST CSF	NIS2*	ISO 27001^	OH SzA
BSI-1	Managementsystem für Informationssicherheit	OIS-01	ID.BE-2 PR.IP-7	30.2.1b	4.1-10.2	P4
BSI-2	Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung	OIS-02	ID.GV-1 ID.BE-3 PR.AT-4 DE.DP-1	30.2.1b	6.2 A.5.1 A.5.2 A.5.4	A1 G1 G2 G3
BSI-3	Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit	OIS-03	ID.GV-2 ID.AM-6	30.1.1	4.3 A.5.3 A.5.4	
BSI-4	Funktionstrennung	OIS-04	PR.AC-4	-	A.5.3	
BSI-5	Asset Inventar	AM-01	ID.AM-1 ID.AM-2	30.2.9c	A.5.9	

Quelle:
<https://www.openkritis.de>

Beispielhafte Kontrolle im Detail

2.1 Informationssicherheitsmanagementsystem (ISMS)		
Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage
1.	<p>Managementsystem für Informationssicherheit</p> <p>Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS), das sich an etablierten Standards orientiert. Bei Anwendung der ISO 2700x-Reihe muss die Erklärung zur Anwendbarkeit (Statement of Applicability) die IT-Prozesse zu Entwicklung und Betrieb der kritischen Dienstleistung umfassen.</p> <p>Die hierzu eingesetzten Grundsätze, Verfahren und Maßnahmen ermöglichen eine nachvollziehbare Lenkung der folgenden Aufgaben und Aktivitäten zur dauerhaften Aufrechterhaltung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse zu Entwicklung und Betrieb der kritischen Dienstleistung und umfasst:</p> <ul style="list-style-type: none"> • die Planung und Durchführung des Vorhabens, • Erfolgskontrolle bzw. Überwachung der Zielerreichung und • Beseitigung von erkannten Mängeln und Schwächen sowie kontinuierliche Verbesserung. 	OIS-01

Quelle:
<https://www.openkritis.de>

Auswertungen nach geprüften Kontrollen

Anforderung	Durchschnittlicher Erfüllungsgrad	Zielwert	Anzahl durchgeführte Kontrollen	Anzahl Ja	Anzahl Teilweise	Anzahl Nein
4 Kontext der Organisation (CHA_023443)	○		0	0	0	0
4.1 Verstehen der Organisation und ihres Kontextes (CHA_023454)	●	100%	100%	3	3	0
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien (CHA_023455)	●	75%	100%	2	1	1
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems (CHA_023456)	●	75%	100%	2	1	1
4.4 Informationssicherheitsmanagementsystem (CHA_023457)	●	75%	100%	2	1	1
5 Führung (CHA_023444)	○		0	0	0	0
5.1 Führung und Verpflichtung (CHA_023458)	●	90%	100%	4	2	0
5.2 Politik (CHA_023459)	●	100%	100%	1	1	0
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation (CHA_023460)	●	100%	100%	1	1	0
6 Planung (CHA_023445)	○		0	0	0	0
6.1 Maßnahmen zum Umgang mit Risiken und Chancen (CHA_023461)	○		100%	0	0	0
6.1.1 Allgemeines (CHA_023477)	●	50%	100%	1	0	1
6.1.2 Informationssicherheitsrisikobeurteilung (CHA_023478)	●	50%	100%	1	0	1
6.1.3 Informationssicherheitsrisikobehandlung (CHA_023479)	○		100%	0	0	0
6.2 Informationssicherheitsziele und Planung zu deren Erreichung (CHA_023462)	●	100%	100%	1	1	0
6.3 Planung von Änderungen (CHA_023463)	●	100%	100%	1	1	0
7 Unterstützung (CHA_023446)	○		0	0	0	0

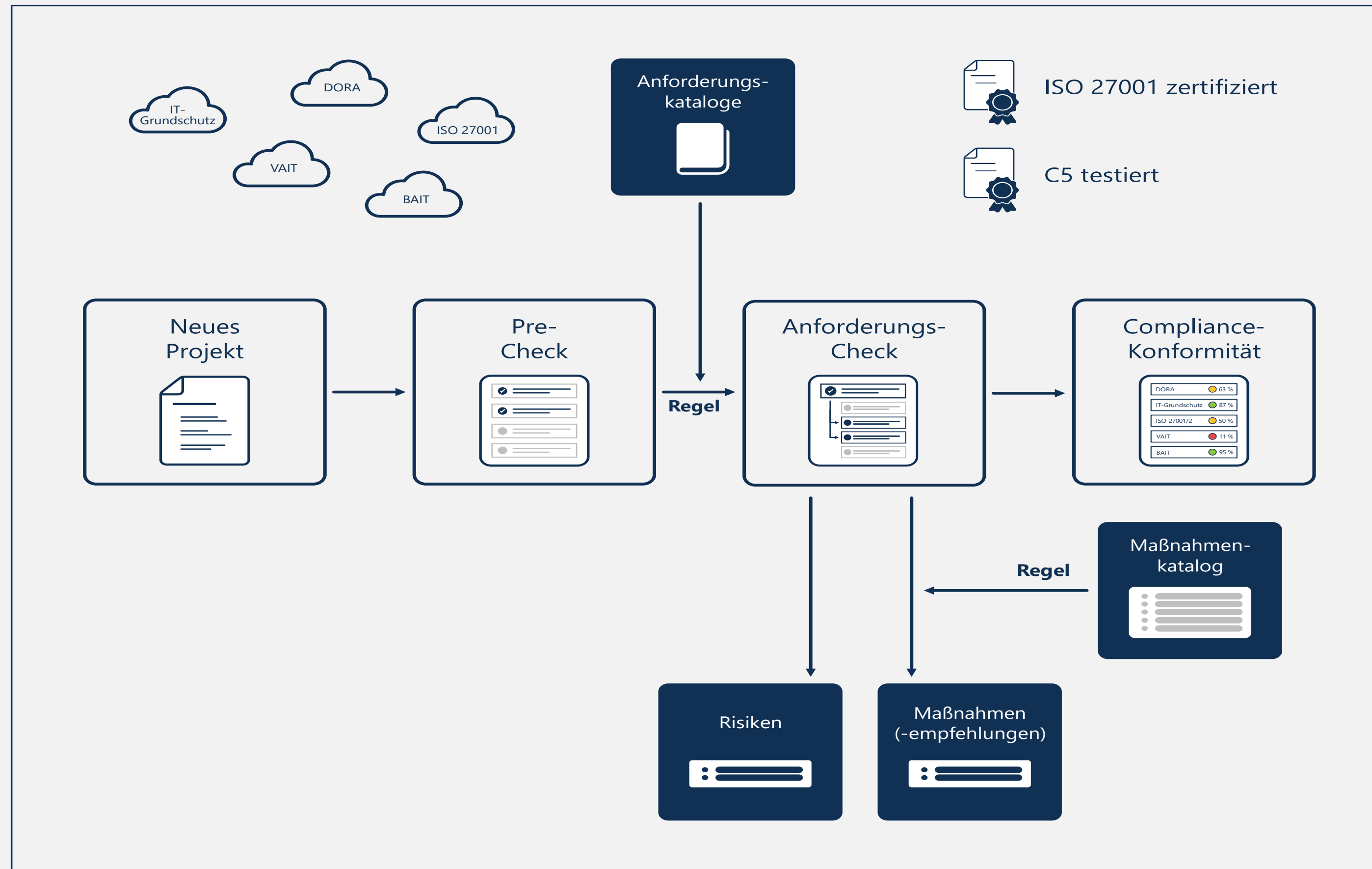
Übersicht der Bewertung der Kontrollen über alle Prüfungen hinweg

Auswertung auf relevante Standards

Assessment (iris ID)	Responsibility	Assessed period from	Assessed period to	Progress
TISAX VDA - Infor...	Konzern AG	1/1/2022	12/31/2022	94
TISAX VDA - Infor...	Konzern AG	1/1/2024	12/31/2024	91
VDA - Information ...				90
TISAX VDA - Infor...	Konzern AG	1/1/2022	12/31/2022	90
Application Securit...	Konzern AG			80
DIN ISO/IEC 2700...	Konzern AG	1/1/2024	12/31/2024	73
Application Securit...	Christian Ritter			50
Internes Regelwerk...	Konzern AG			40
ibi systems iris - Q...	Konzern AG	1/1/2024	1/31/2024	40
Versicherungsaufsi...	Konzern AG			34

Erfüllungsgrade der Standards über alle Prüfungen basierend auf den Mappings und Anforderungskatalogen

Bewährtes Vorgehen



Nutzbarkeit bereits heute durch verfügbare Standard Mappings wie u.a. „OpenKritis“

Compliance erfüllt – Security erhöht

Vielen Dank

Wichtiger Hinweis: Diese Datei ist vertraulich und ausschließlich für von ibi systems GmbH berechnigte Personen und Firmen/Organisationen freigegeben. Wenn Sie diese Datei nicht von ibi systems GmbH erhalten haben, nehmen Sie bitte zur Kenntnis, dass Weitergabe, Kopien, Verteilung und Nutzung unzulässig ist. Falls Sie diese Datei irrtümlich erhalten haben, benachrichtigen Sie ibi systems GmbH bitte unverzüglich telefonisch oder durch eine E-Mail.

Copyright © 2024 ibi systems GmbH. Alle Rechte vorbehalten

Alle Inhalte, Fotos und Grafiken sind urheberrechtlich geschützt. Sämtliche Teile dieses Dokuments dürfen nicht ohne vorherige schriftliche Genehmigung durch die ibi systems GmbH weder ganz noch auszugsweise kopiert, vervielfältigt, verändert oder übertragen werden.

Herausgeber: ibi systems GmbH | Copyright Fotos Siehe Quellenhinweis am jeweiligen Bild in der Präsentation.



Rudolf-Vogt-Straße 6, 93053 Regensburg



+49 941 4629390



Sitz: Regensburg, HRB 13164



Amtsgericht: Regensburg



Dr. Stefan Wagner, Pascal Jonietz