

Umstellung auf ISO 27001:2013 Praxisbericht

**Workshop GfI Gesellschaft für Informatik
Frankfurt 28. November 2014**

Inhalt

- **Kurzvorstellung VSA GmbH**
- Organisation des ISMS innerhalb der VSA
- Migrationsprojekt ISO 27001:2013



VSA-Unternehmensgruppe

Branchensoftware
für Apotheken

awinta 
SICHER GEWINNT



Rezeptabrechnung
für Apotheken


VSA[®]



Rezeptabrechnung
und Branchen-
software für SoLei

azh



Branchensoftware
für Pflegedienste
und -heime

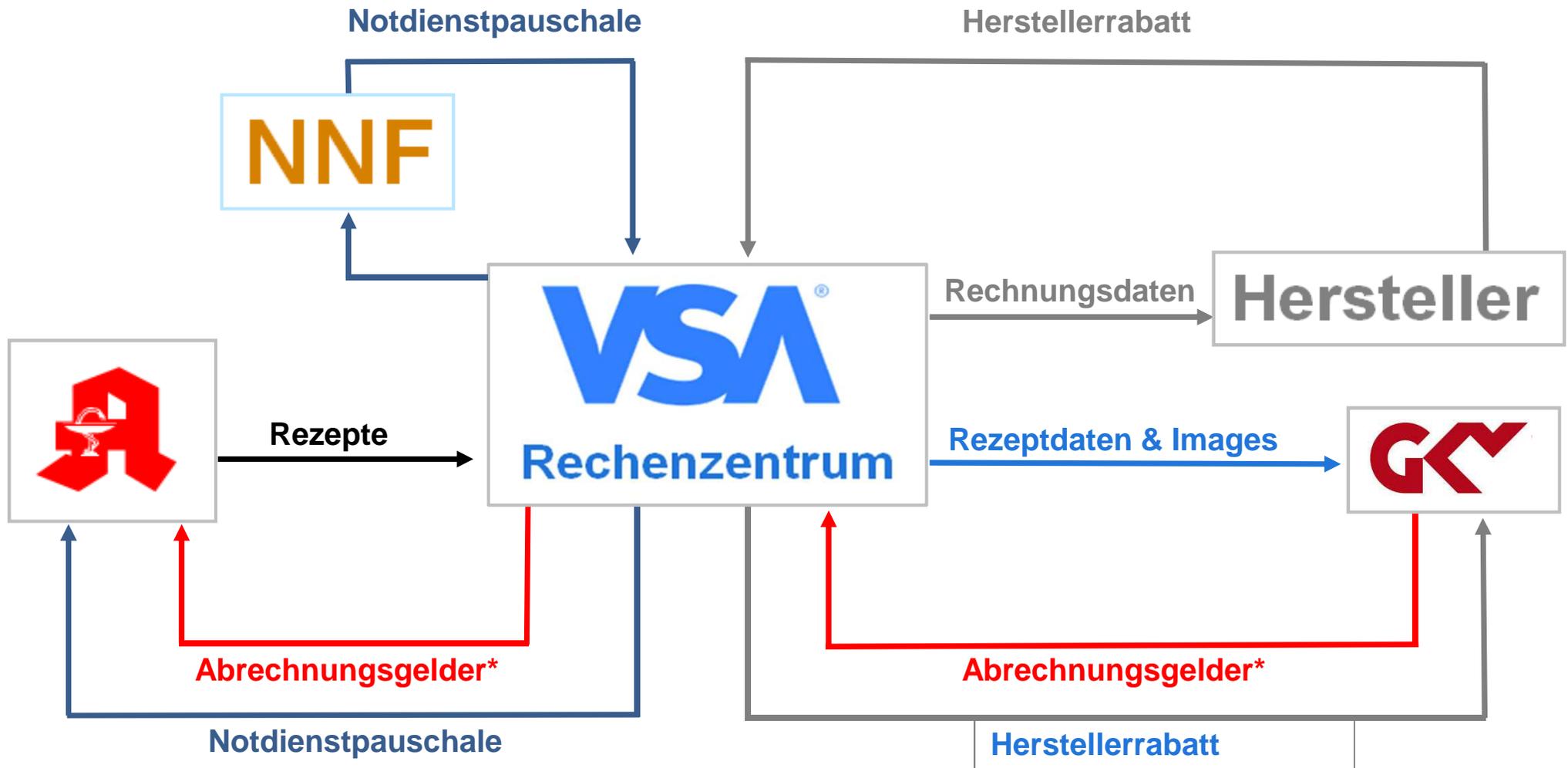

BoS&S



VSA-Unternehmensgruppe



Rezeptabrechnung für Apotheken



* Abrechnungsgelder abzgl. Apothekenabschlag und Herstellerabschlag

ISMS und Zertifizierung

Gründe dafür



Nachweis der Einhaltung von Gesetzen und Verträgen

Zunehmende (IT-)Risiken

Weitergehende Digitalisierung

Anforderungen an Verfügbarkeit und Sicherheit / Integrität

Effizienz

Weiter steigende Komplexität und Datenmengen

Transparenz

Vertrauen

Qualität

Zunehmende Sensibilisierung im Gesundheitswesen

Vorbildfunktion

Rezeptabrechnung ist unternehmenskritisch

Vorbereitung für absehbare verpflichtende Standards

Differenzierung im Markt



Inhalt

- Kurzvorstellung VSA GmbH
- **Organisation des ISMS innerhalb der VSA**
- Migrationsprojekt ISO 27001:2013

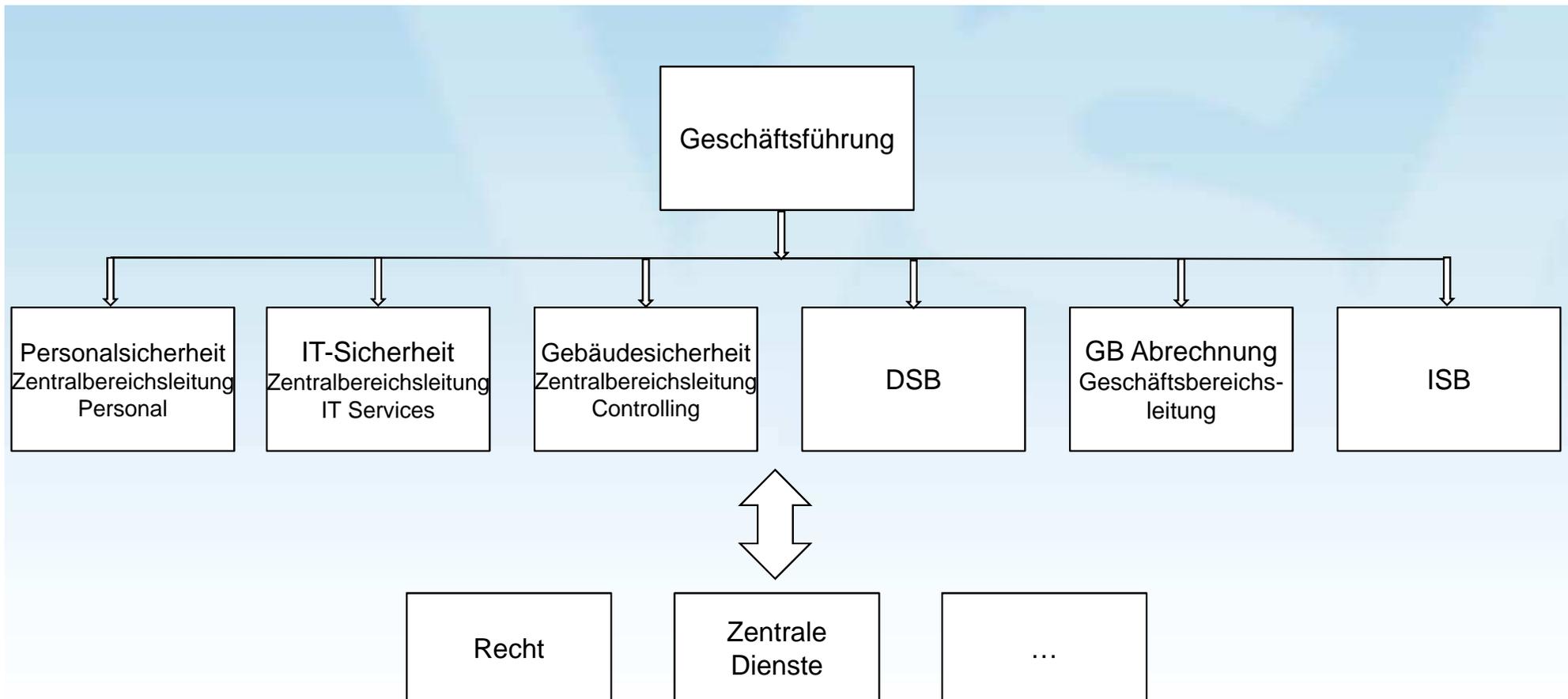


Anwendungsbereich des ISMS

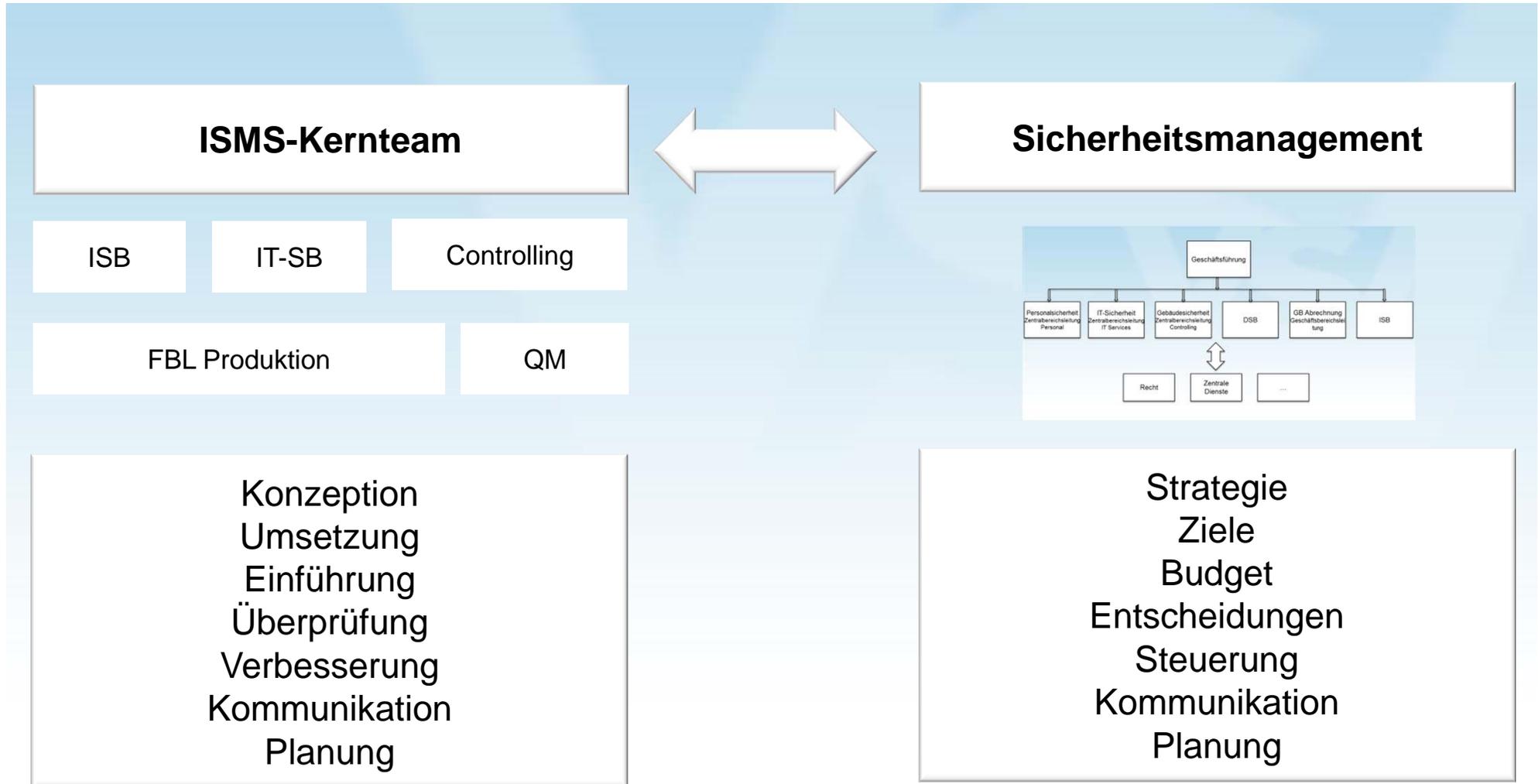
- [...] ist die Erbringung von Abrechnungsdienstleistungen für Apotheken.

Management-Attention

- Auftrag von Aufsichtsrat und Geschäftsführung
- Installation des Sicherheitsmanagement-Teams SiMA



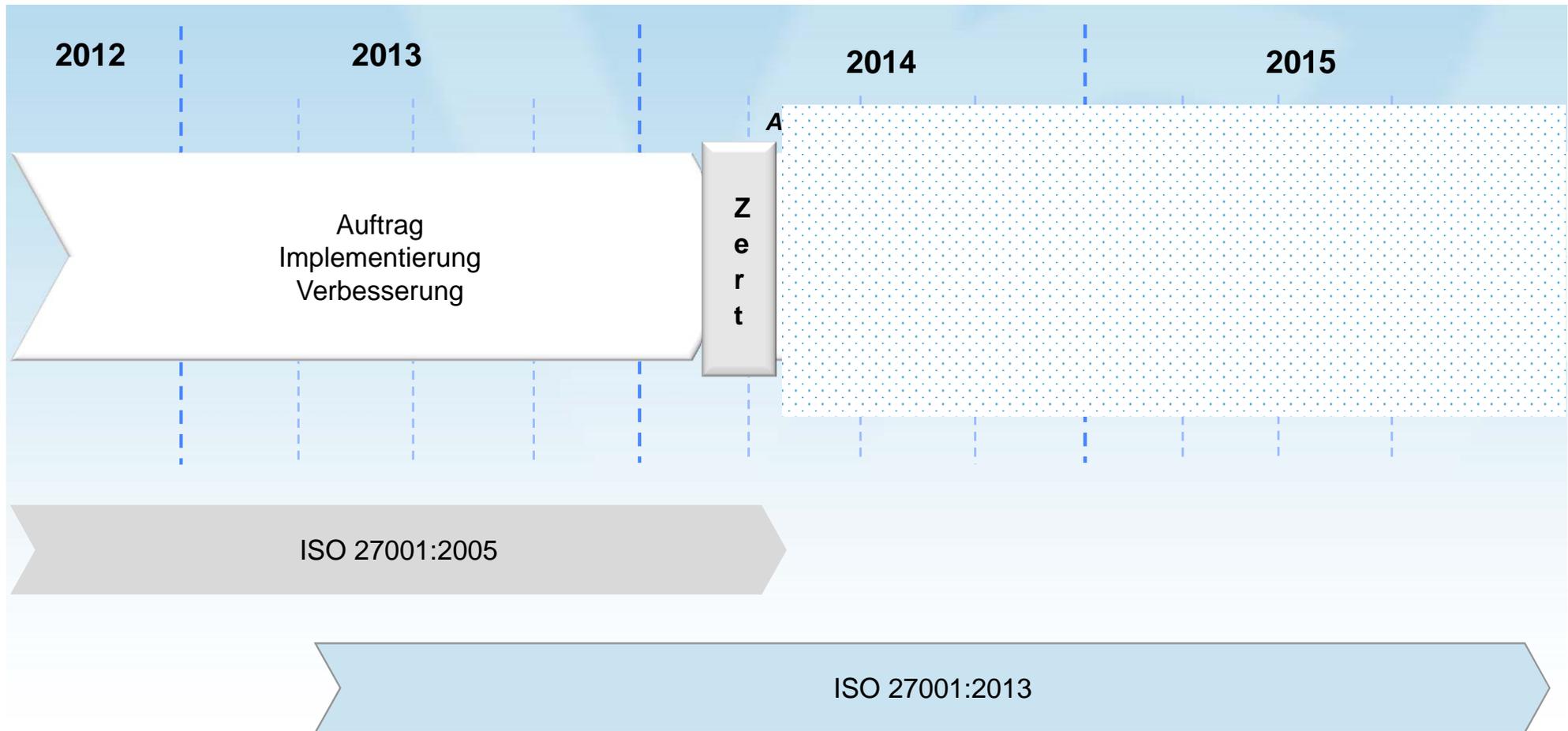
ISMS-Kernteam / SiMa



Inhalt

- Kurzvorstellung VSA GmbH
- Organisation des ISMS innerhalb der VSA
- **Migrationsprojekt ISO 27001:2013**





Handlungsfelder

ISO 27001:2005	ISO 27001:2013
0. Introduction	0. Introduction
1. Scope	1. Scope
2. Normative references	2. Normative references
3. Terms and definitions	3. Terms and definitions
4. Information security management system	4. Context of the organization
5. Management responsibility	5. Leadership
6. Internal ISMS audits	6. Planning
7. Management review of the ISMS	7. Support
8. ISMS improvement	8. Operation
Annex A (normativ)	9. Performance Evaluation
Annex B (informativ)	10. Improvement
Annex C (informativ)	Annex A (normativ)

Interessierte Parteien und deren Anforderungen

Risk-Owner

Anpassung der Leistungsbewertung

Handlungsfelder

ISO 27001:2005	ISO 27001:2013	
A.5 Security policy	A.5 Information security policies	
A.6 Organization of information security	A.6 Organization of information security	A.6.1.5. Informationssicherheit im Projektmanagement
A.7 Asset management	A.7 Human resource security	
A.8 Human resources security	A.8 Asset management	
A.9 Physical and environmental security	A.9 Access control	A.12.6.2 Beschränkung von Softwareinstallation
A.10 Communications and operations security	A.10 Cryptography	
A.11 Access control	A.11 Physical and environmental security	
A.12 Information systems access control	A.12 Operations security	A.14.2.1 Leitlinie sichere Entwicklung A.14.2.5 Verfahren zur Systementwicklung A.14.2.6 Sichere Entwicklungsumgebung A.14.2.8 Systemsicherheitsprüfung
A.13 Information security incident management	A.13 Communications security	
A.14 Business continuity management	A.14 System acquisition, development and maintenance	
A.15 Compliance	A.15 Supplier relationships	A.15.1.1 IS-Leitlinie für Lieferantenbeziehungen A.15.1.3 IKT-Lieferkette
	A.16 Information security incident management	
	A.17 Information security aspects of business continuity management	
	A.18 Compliance	

ISCI-Nr.	Thema	Dok.-Name	Beschreibung
Kap. 4.2(a), 4.3(c)			
Kap. 6.1(a, b, c)			
Kap. 6.1			
Kap. 7.4			
Kap. 7.5			
Kap. 8.1			
Kap. 9			
Kap. 10			
A 6.15			
A 14.1.2, 14.1.3			
A 14.2.1, 14.2.5, 14.2.6, 14.2.8			
A 15			
A 16.11, 16.14, 16.15			
A 17.2.1			
A 18.15			
A 8.14			
A 12.7.1			
Kap. 5.1(b)			

Umsetzung der Auditergebnisse aus Zertifizierungsaudit

Gap-Analyse / Workshops

Resultate → Auftragspapier pro Bereich

Erfassung Jira / Tracking

Planung, Termine, Ressourcen, Priorisierung

Umsetzung, Implementierung, Überprüfung, Messung

The screenshot shows the Jira web interface. At the top, there are navigation tabs: 'Startseite', 'Projekte', 'Vorgänge', and 'Vorgang erstellen'. Below this is a search bar with the text 'Suchen' and a 'Speichern unter' button. The search results are filtered for 'ISMS' and show a list of items. The selected item is 'ISMS-86' with the title 'Nr. 17: GAP Analyse, AP-ISMS-4'. The details panel on the right shows the following information:

- Typ: Internes Audit
- Severity: Normal
- Komponente(n): Informationssicherheitsbeauftragter
- Stichwörter: Keine
- Priorität: P5
- Status: (empty)
- Lösung: (empty)

Vielen Dank für Ihre Aufmerksamkeit!

Ihre VSA-Unternehmensgruppe