ISO 27001 & IKS in der Praxis

Ansatz eines Integrierten Managementsystems (IMS) zur Reduzierung von Aufwänden

Know-how to go – ISMS-Zertifizierung

HiSolutions AG

Marius Wiersch

Marius Wiersch

Managing Consultant & Team Manager

Fachliche Schwerpunkte:

- Kritische Infrastrukturen nach IT-SiG, BSIG und BSI-Kritis-Verordnung
- Beratung zur Informationssicherheit nach ISO 27001 und IT-Grundschutz
- Einführung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001 und IT-Grundschutz
- Integration der IDW PS 951 und ISAE 3402 Standards in ISMS

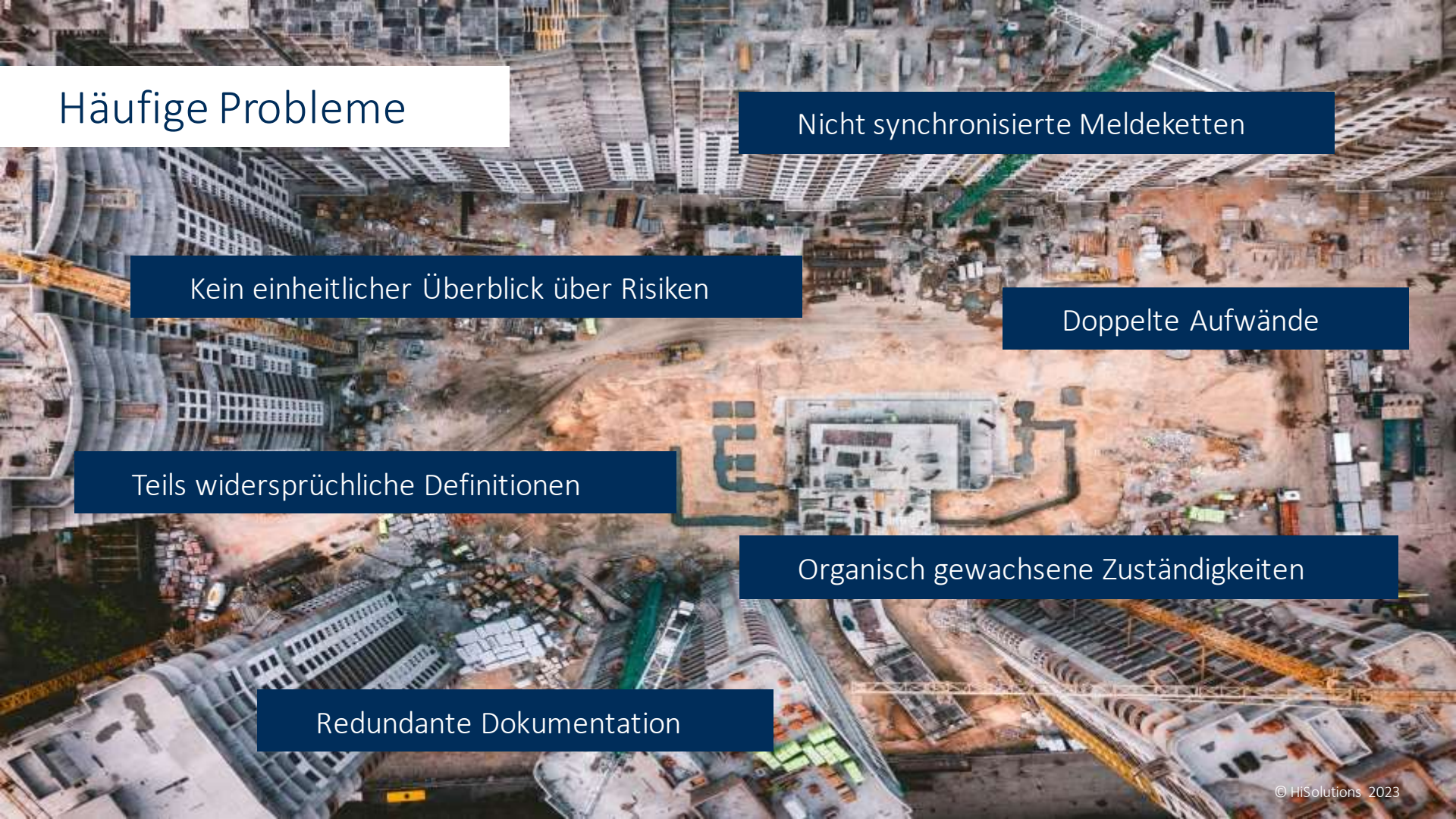
Spezielle Qualifikationen:

- ISO/IEC 27001 Lead Auditor
- Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG
- Auditor für ISO/IEC 27001 EnWG gemäß IT-Sicherheitskatalog nach § 11 Abs. 1a Energiewirtschaftsgesetz
- Auditor für Energieerzeugungsanlagen nach EnWG § 11 Abs. 1b
- ISO/IEC 22301 Lead Auditor
- BSI IT-Grundschutz-Praktiker
- Foundation Examination TISAX® Assessment

In heutigen Unternehmen wachsen die Managementsysteme stetig

In heutigen Unternehmen wachsen die Managementsysteme stetig

Häufige Probleme



- Nicht synchronisierte Meldeketten
- Kein einheitlicher Überblick über Risiken
- Doppelte Aufwände
- Teils widersprüchliche Definitionen
- Organisch gewachsene Zuständigkeiten
- Redundante Dokumentation

Die Lösung

Harmonisierung der Anforderungen in ein Integriertes Managementsystem

Ein Integriertes Managementsystem soll Synergieeffekte auf allen Ebenen nutzen

Ein Integriertes Managementsystem soll Synergieeffekte auf allen Ebenen nutzen

Ein IMS ist…

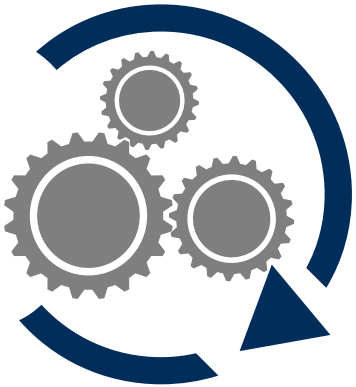
… ein zentrales Mittel der ganzheitlichen Unternehmensführung

… eine standardisierte Struktur von Methoden und Instrumenten zur Einhaltung von Anforderungen aus unterschiedlichen Bereichen

… eine konsistente Prozesslandschaft unter Berücksichtigung verschiedener Anforderungen

Ein Integriertes Managementsystem vereint eine Vielzahl von Vorteilen

- Gemeinsame Organisationsstrukturen
- Schlankes und ressourcenschonendes Management
- Reduzierung von Kosten
- Nutzung von Synergien (z. B. Schulung & Sensibilisierung)
- Einheitliches Reporting und Management Reviews



- Geringerer Dokumentationsauswand
- Einheitliche Begriffe und Definitionen
- Möglichkeit der gemeinsamen Zertifizierung
- Vermeidung von Doppelaufwänden
- Zentrales Risikomanagement

Umsetzung eines IMS

1. Aufnahme der Anforderungen der zu integrierenden Systeme

2. Schaffung formaler Organisationsstrukturen

3. Ausgestaltung der Unternehmensprozesse

4. Erweiterung der Unternehmensprozesse

Praxisbeispiel: ISO 27001 Annex A & IKS

PDCA-Zyklus: ISMS

Grundlagen schaffen

- Geltungsbereich, Ziele und Zweck
- Interested Parties
- Top-Management-Unterstützung
- Ressourcen
- Awareness & Kommunikation

Umsetzen & Betreiben

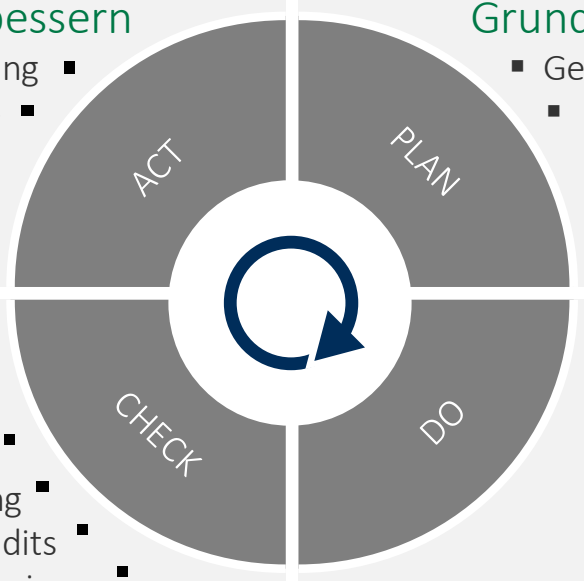
- Schutzbedarfsanalysen
- Information Security Risk Management
- Mindestvorgaben an die Informationssicherheit (2nd Line)
- Sicherheitsvorgaben (1st Line)

Überwachen & Überprüfen

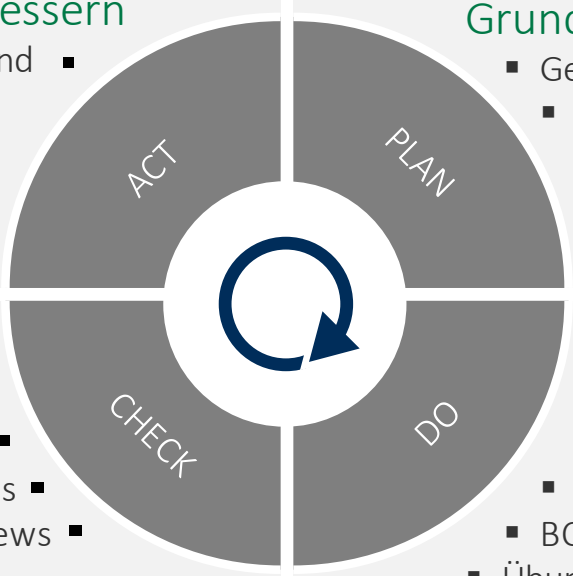
- Leistungsüberwachung
- Messung
- Bewertung
- Interne Audits
- Management Reviews

Aufrechterhalten & Verbessern

- Konformitätsprüfung
- Korrektur- und Verbesserungsmaßnahmen
- Kontinuierlicher Verbesserungsprozess



PDCA-Zyklus: BCM



Grundlagen schaffen

- Geltungsbereich, Ziele und Zweck
- Interested Parties
- Top Management Unterstützung
- Ressourcen
- Awareness & Kommunikation

Umsetzen & Betreiben

- Business Impact Analyse
- BCM-Risiko-Analyse
- BC-Strategie
- BC-Verfahren
- Übungen und Test/reale Notfälle

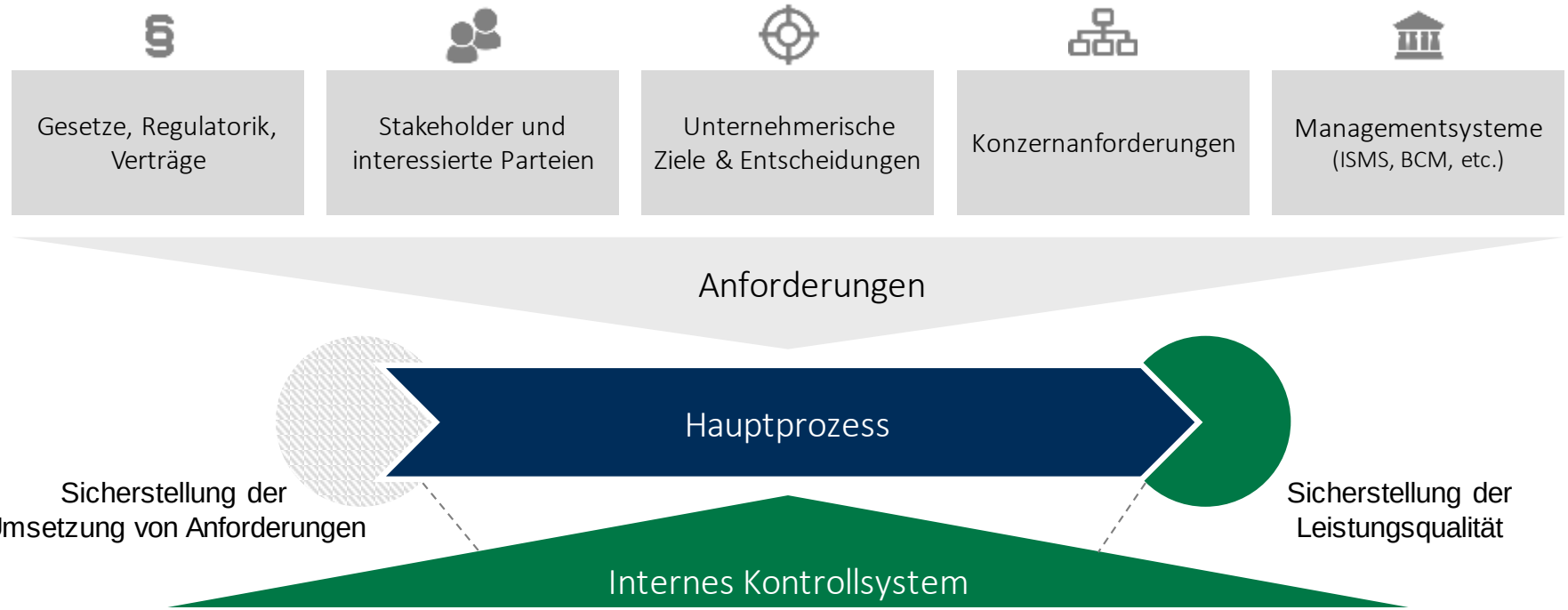
Überwachen & Überprüfen

- Messung
- Bewertung
- Interne Audits
- Management Reviews

Aufrechterhalten & Verbessern

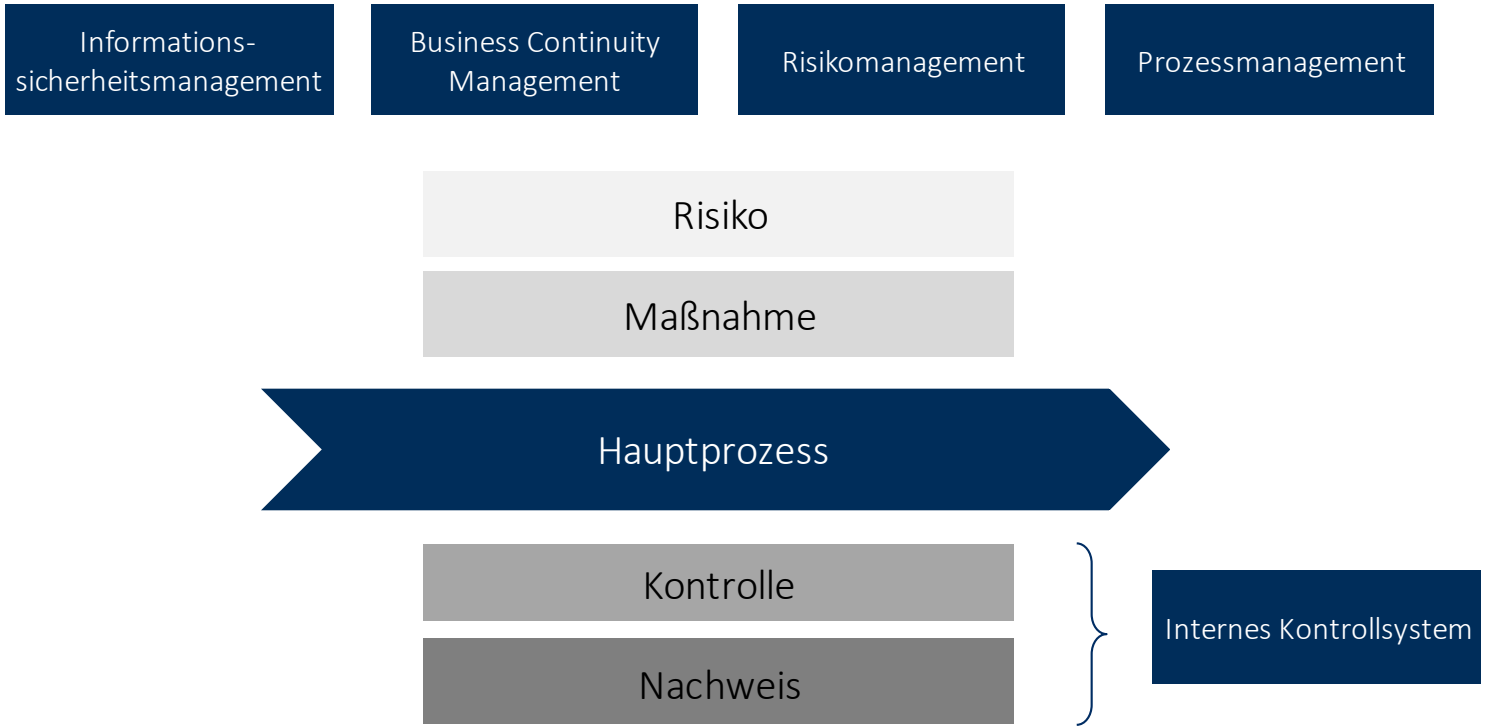
- Korrektur- und Verbesserungsmaßnahmen

Welche Ziele verfolgt das Interne Kontrollsystem?



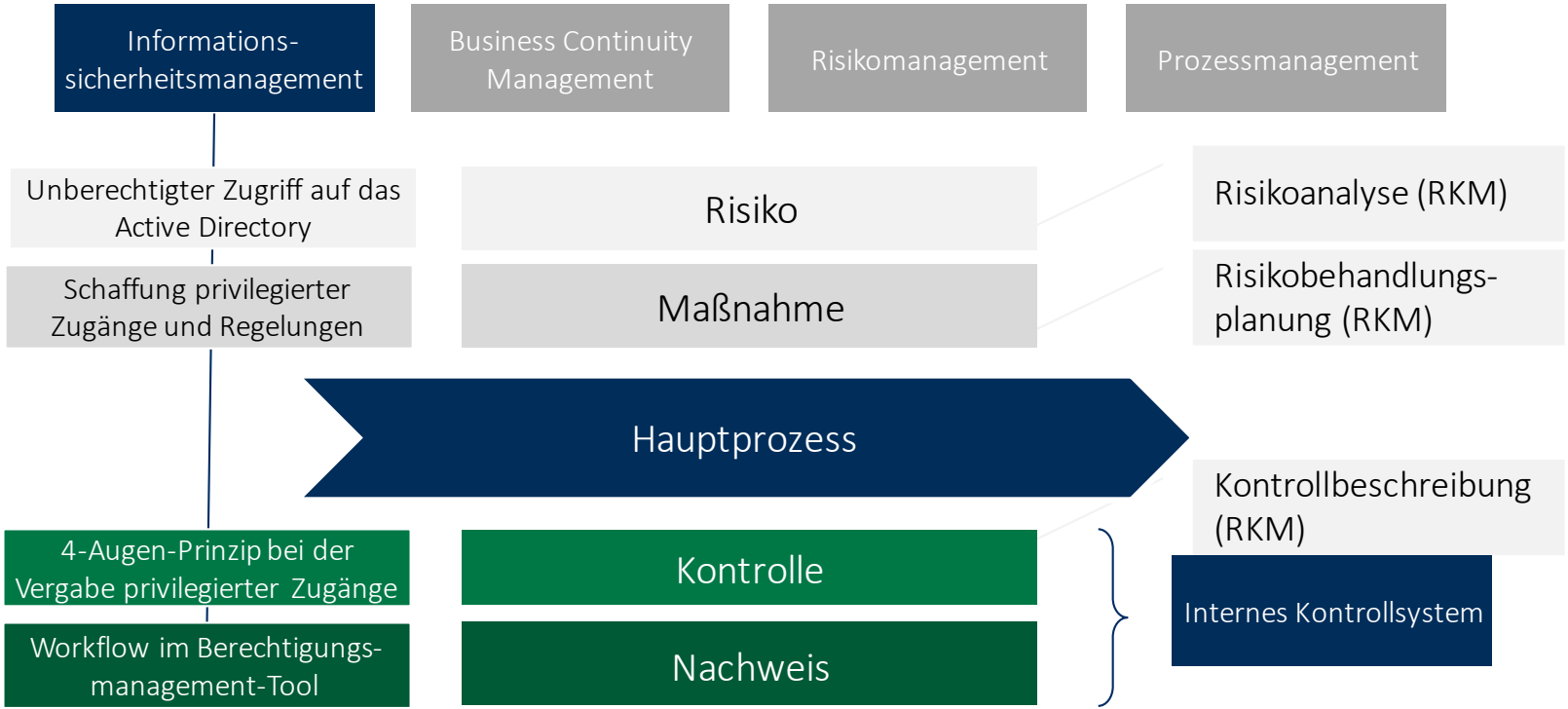
Wie werden die Ziele des Internen Kontrollsystems erreicht?

Kontrollierte Umsetzung von risikoreduzierenden Maßnahmen

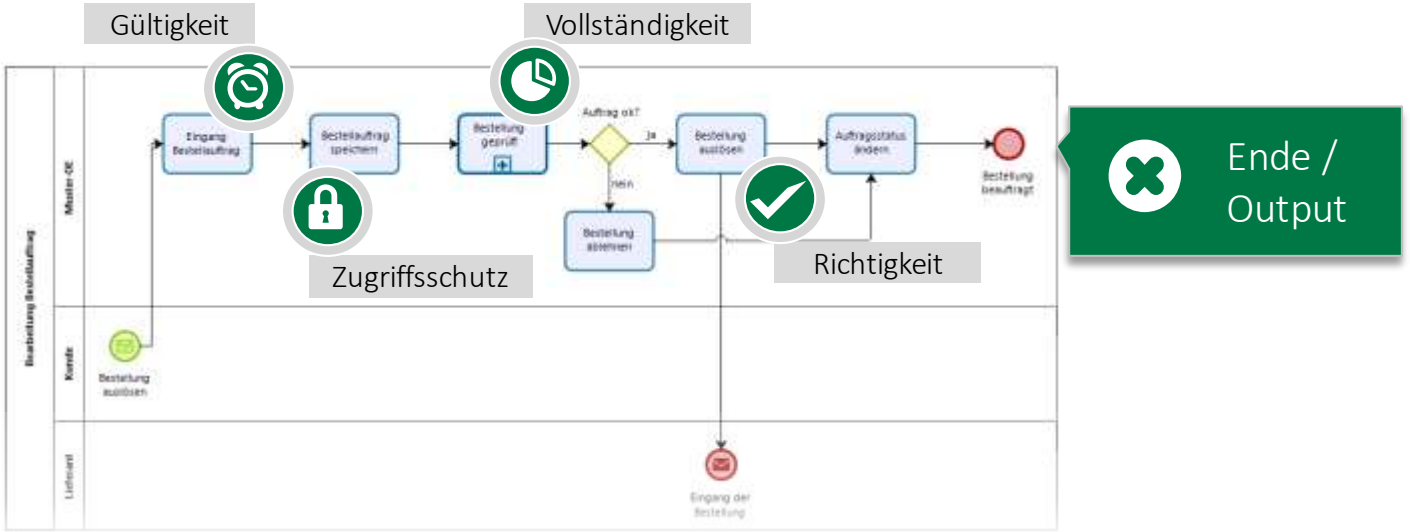


Wie werden die Ziele des Internen Kontrollsystem erreicht?

Kontrollierte Umsetzung von risikoreduzierenden Maßnahmen

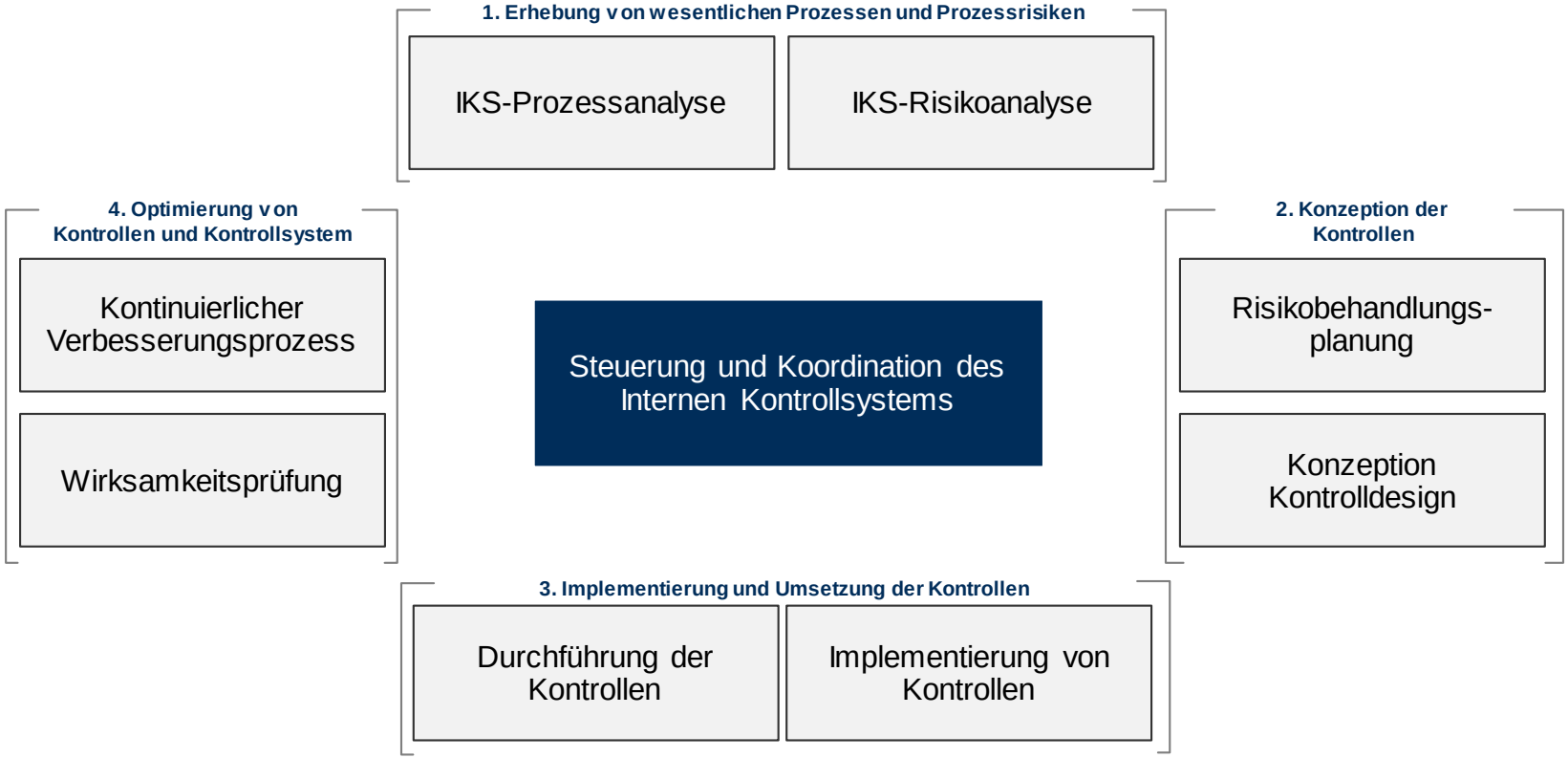


Interne ISMS-Audits durch die Kontrollen eines IKS



Nutzung der IKS-Kontrollen für ISO-27001-Annex-A-Kontrollen

Der IKS-Regelprozess



Beispiel: Access Management

Risiko: Ansammlung von Berechtigungen bei Rollenwechseln

Adressiert von:

- ISO Control 5.18 Access rights
- Cobit 5 DSS05.04
  Managen von Benutzeridentität und logischem Zugriff

Lösung: Erstellung einer IKS-Kontrolle

IKS-Kontrolle 1/3

Kontrollobjekt	Berechtigungen
Kontrollbeschreibung	Bei einer Umorganisation oder Zuordnungsänderung von Mitarbeitern wird durch die jeweilige Führungskraft eine Rezertifizierung durchgeführt.
	HR meldet jegliche Änderungen der Rollen oder Zuordnung an das Accessmanagement.
	Der Verantwortliche zur Kontrolldurchführung prüft die Änderung der Rolle und setzt folgende Maßnahmen um:
	1. sofortiger Entzug jeglicher Berechtigungen bei Beendigung der Zusammenarbeit (gilt für interne und externe MA)
	2. Rezertifizierung von bestehenden Berechtigungen gemeinsam mit der neuen Führungskraft.

IKS-Kontrolle 2/3

Kontrollziel	Es ist sicherzustellen, dass Zugriffsrechte und Berechtigungen basierend auf vordefinierten Rollen und nur für die Bereiche zugeordnet sind, die für die Ausübung der beruflichen Tätigkeiten erforderlich sind.
	Zugriffsrechte werden sofort entzogen oder überarbeitet, wenn sich die Rolle ändert, oder wenn der betreffende Mitarbeiter nicht mehr mit dem Geschäftsprozess betraut ist.
	Durch regelmäßige Überprüfungen wird sichergestellt, dass der Zugriff den derzeitigen Bedrohungen, Risiken, Technologien und Geschäfts-erfordernissen Rechnung trägt.

Vollständigkeit	Richtigkeit
Gültigkeit	Zugriffsschutz

IKS-Kontrolle 3/3

Kontrollzeitpunkt	Präventiv
Kontrolltyp	Plausibilisierung
Automatisierungsgrad	Halbautomatisiert
Kontrollhäufigkeit	Ereignisbezogen
Anzahl durchgeführter Kontrollen	53-250 im Jahr
Nachweise	Auszug aus dem Ticketsystem (Excel) je Führungskraft je Zeile (E-Mail-Antwort mit unterschriebenem Formular der Durchführung); Änderungsmeldung von HR
Status der Kontrolle	Implementiert/dokumentiert
Fehlerbehandlung	Die Führungskräfte stellen im Zuge der Rezertifizierung eine Liste mit Abweichungen zur Korrektur zur Verfügung. Die Korrektur wird dann über das Access Management bearbeitet.

Fazit

- Für ein zertifizierungsreifes internes Auditmanagement gemäß ISO 27001 können vorhandene IKS-Strukturen genutzt werden
- Die IKS-Kontrollen bieten eine permanente Überwachung im Vergleich zu „regelmäßigen“ ISMS-Audits
- Andere ISO-basierte Managementsysteme (QM, BCM) können ebenfalls einfach integriert werden
- Durch die Verknüpfung von Managementsystemen können wirksame Schnittstellen zu anderen Bereichen geschaffen werden
- Die Koordination alleine der Audittätigkeiten schafft freie Ressourcen sowohl in den Managementsystemen als auch in den Fachbereichen

Mit integriertem Management viel managen

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie noch offene Fragen zum Thema Resilienz?