Wirtschaftsgrundschutz

Vorstellung und Einführung

Prof. Timo Kob

HISOLUTIONS

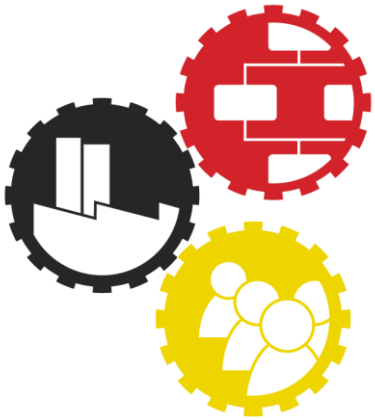
© HiSolutions 2017 | Wirtschaftsgrundschutz

Das Ziel: Ein Paradoxon auflösen!

- Für das – vermeintlich – neue Angriffsziel IT gibt es seit 20 Jahren ein erfolgreiches Hilfsmittel: Den IT-Grundschutz des BSI

- Für die „klassischen“ Angriffsziele wie Mensch, Infrastrukturen und Prozesse gibt es dies nicht

- Ziel war es, diese Lücke zu schließen!



© HiSolutions 2017 | Wirtschaftsgrundschutz

Die Projektpartner

ASW Bundesverband

- Bundesverband für Sicherheitsverantwortliche in der Wirtschaft und Verantwortliche in der Sicherheitswirtschaft
- Scharnier zwischen Wirtschaft und Behörden.
- Bringt so Staat, Wirtschaft und Anbieter zusammen

HISOLUTIONS

- Beratungsspezialist für Informationssicherheit und Wirtschaftsschutz
- Führender Experte für den IT-Grundschutz und Rahmenvertragspartner des BSI

Herausgeber der Ergebnisse:

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Verfassungsschutz

ASW Bundesverband

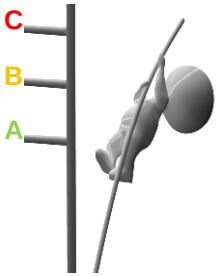
HISOLUTIONS

© HiSolutions 2017 | Wirtschaftsgrundschutz

Generisches Vorgehensmodell

1.
Bausteine sichten und vorauswählen

2.
Anhand von Kontrollfragen individuelle Relevanz der Bausteine verifizieren



3.
Individuelle „Messlatte“ festlegen

4.
Aus gewählten Bausteinen und auf Basis der „Messlatte“ geeignete Maßnahmen auswählen

5.
Prüfen, ob spezielle individuelle Risiken (auch hier bereits Vorschläge in Bausteinen enthalten) zusätzliche Maßnahmen erforderlich machen.

6.
Ausgewählte Maßnahmen zu Sicherheitskonzept zusammenstellen, ggf. konkretisieren/ anpassen-> BASIS-Konzept fertigstellen.

© HiSolutions 2017 | Wirtschaftsgrundschutz

Ebene 1: Standards

„Best Practices“ für

- Ziele
- Rollen
- Prozesse
- Themen
- Dokumentationen

um Wirtschaftsschutz dauerhaft zu managen.

© HiSolutions 2017 | Wirtschaftsgrundschutz

Ebene 2: Bausteine

„Best Practices“ um konkrete Sicherheitsprobleme zu lösen (oder um Vorschläge der Standards zu konkretisieren).

- Hilfe durch Kontrollfragen, ob Baustein für den Leser relevant
- Kurze Einführung in das Thema
- Beschreibung der Bedrohungslage als Basis für individuelle Risikoanalysen
- Priorisierte Maßnahmen
- Gesamtlänge ca. 20 Seiten, Verweise auf vertiefende Literatur

© HiSolutions 2017 | Wirtschaftsgrundschutz

Aufbau und Struktur des Wirtschaftsgrundschutzes

- Alle Bestandteile des Wirtschaftsgrundschutzes sind hierarchisch nach **Modulen** bzw. **Schichten** geordnet

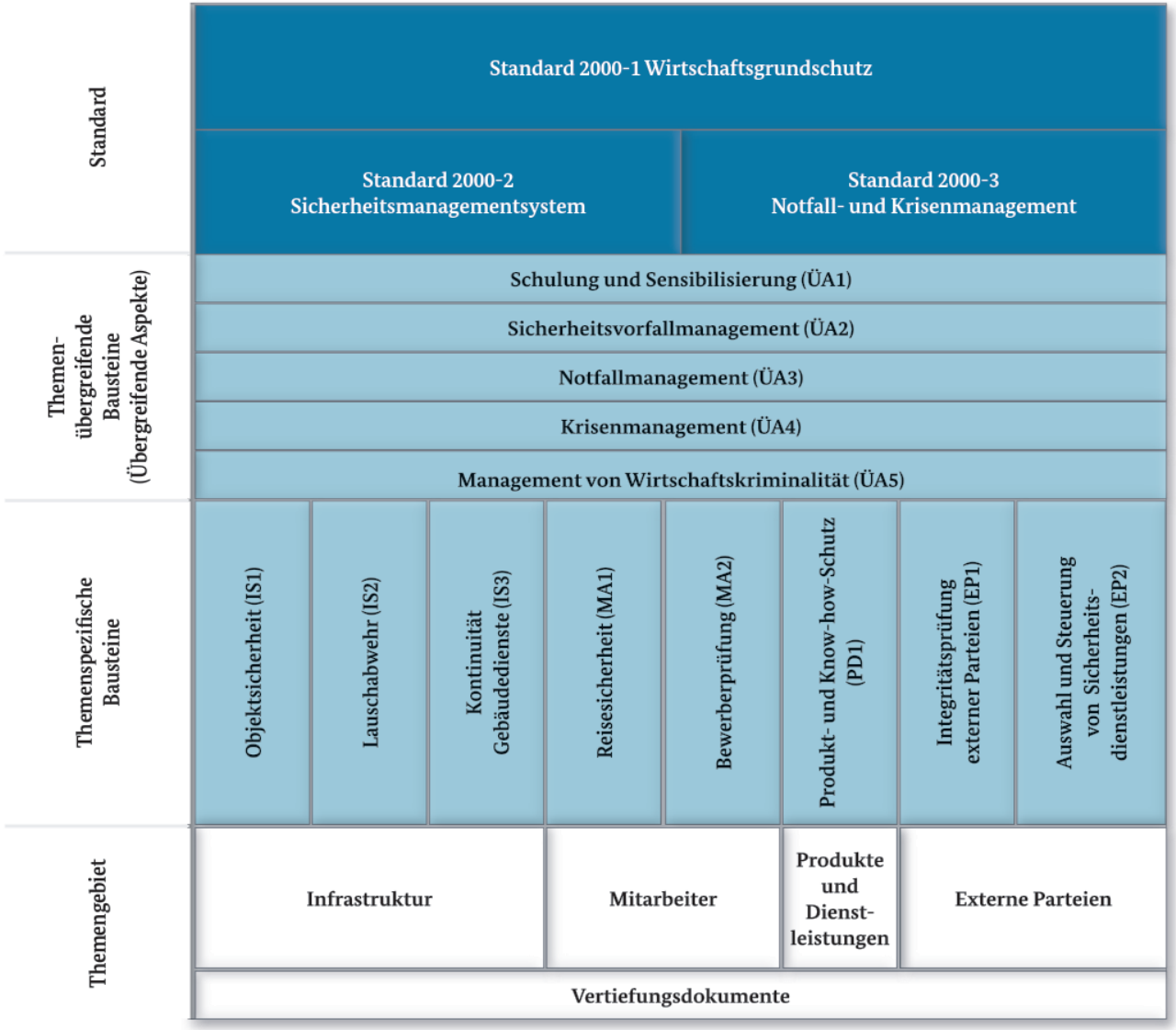
- Durch das **Schichtenmodell** werden Komplexität reduziert und Redundanzen vermieden

- Die Bausteine werden in folgende **Kataloge** gruppiert
  - Schicht 1: Übergreifende Aspekte (ÜA)
  - Schicht 2: Infrastruktur (IS)
  - Schicht 3: Mitarbeiter (MA)
  - Schicht 4: Produkte und Dienstleistungen (PD)
  - Schicht 5: Externe Parteien (EP)

- Die **Rahmenbedingungen** werden im übergeordneten Standard **2000-1** geregelt

© HiSolutions 2017 | Wirtschaftsgrundschutz

Überblick der Gesamtstruktur der enthaltenen Dokumente



© HiSolutions 2017 | Wirtschaftsgrundschutz

Überblick der Inhalte des Standards 2000-1 (Wirtschaftsgrundschutz)

Einleitung

- Präambel
- Aufbau und Funktionsweise Wirtschaftsgrundschutz

Grundlagen

- Sicherheitsmanagementsystem im Allgemeinen
- Themenfelder
- Festlegungen (Schutzgut, Strategie, Konzepte, Organisation)

SiMS

- Führungs- und Steuerungsprozesse
- Übergreifende Prozesse

Schulung

- Schulung, Training
- Sensibilisierung
- Kommunikation

© HiSolutions 2017 | Wirtschaftsgrundschutz

Überblick der Inhalte des Standards 2000-2 (Sicherheitsmanagementsystem)

Einleitung

- Präambel
- Einordnung des Dokuments

SiMS

- Ziele und Aufgaben
- Organisation, Rollen, Gremien

Prozesse

- Führungsprozesse, Steuerungsprozesse, Berichts- und Kontrollprozesse der Themenfelder
- PDCA-Zyklus

Anhang

- Glossar
- Aufbau und Verwendung Bausteine und Maßnahmen
- Gefährdungskatalog
- Referenztabellen

© HiSolutions 2017 | Wirtschaftsgrundschutz

Überblick der Inhalte des Standards 2000-3 (Notfall- und Krisenmanagementsystem)

Einleitung	▪ Präambel ▪ Einordnung des Dokuments
Anfor-derungen	▪ Organisatorische Grundlagen ▪ Anforderungen an eine Reaktionsorganisation
Notfall Management	▪ Ziel und Auftrag, Organisation, Dokumentation ▪ Eskalation
Krisen Management	▪ Ziel und Auftrag, Organisation, Dokumentation ▪ Methodische Grundlagen
Krisen-kommunikation	▪ Rolle, Interessengruppen, Dokumentation ▪ Kommunikationsmittel und –materialien
Übung	▪ Übungsarten ▪ Übungsvorgehen
Infrastruktur	▪ Anforderungen an eine Infrastruktur

© HiSolutions 2017 | Wirtschaftsgrundschutz

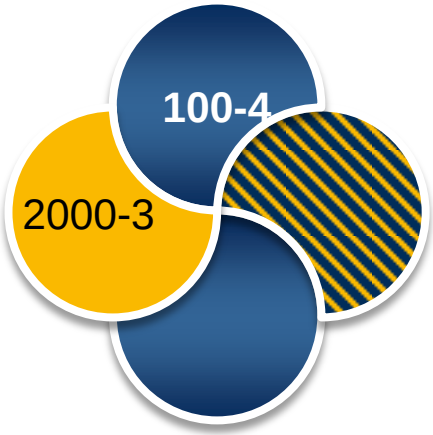
Abgrenzung Wirtschaftsgrundschutz und BSI 100-4

Business Continuity Procedures
„Planung der Geschäftsfortführung“

Strategien, Strukturen und Pläne, um einen definierten Notbetrieb der kritischen Prozesse zu ermöglichen

Emergency Response
“Betriebl. Notfallplanung“

Schutz von Leib und Leben der Mitarbeiter und der (physischen) Vermögenswerte der Institution sowie Schadensbegrenzung (auch: Eingrenzung der Auswirkungen auf Umwelt / Umfeld der Institution)



Crisis Management
„Notfall-/Krisenbewältigung“

Effektive Reaktion auf Notfälle / Krisen, inkl. Meldung, Alarmierung und Eskalation, ggf. Aktivierung von BAO, Krisenmanagement (Stabs-arbeit etc.), Krisenkommunikation

IT Continuity / Disaster Recovery
“IT-Notfallmanagement“

Notfallpläne und –maßnahmen zur Reaktion auf Netzwerk / Technologie-Incidents und zum Wiederanlauf von IT-Ressourcen/Anwendungen.

© HiSolutions 2017 | Wirtschaftsgrundschutz

Überblick der allgemeinen Bausteinstruktur

Einleitung
- Relevanzentscheidung
- Einordnung des Themas

Beschreibung
- Definitionen und Merkmale
- Ein- und Abgrenzungen

Gefährdungs-lage
- Beschreiben und Aufzeigen der Gefährdungen
- Liste der relevanten Gefährdungen

Maßnahmen
- Ablaufdiagramm
- Maßnahmenliste (mit Kategorie A, B, C)

Anhang
- Links und Hinweise auf Quellen und weitere relevante Dokumente
- Zusammenfassung der wichtigsten Thesen
- Themen- und Maßnahmenübersicht

Vertiefung
- vertiefende Dokumente zum Thema

© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: Sicherheitsmanagement nach WSGS 2000-2

Sicherheitsorganisation

- Aufbau der Sicherheitsorganisation
- Rollen
- Sicherheitsgremien

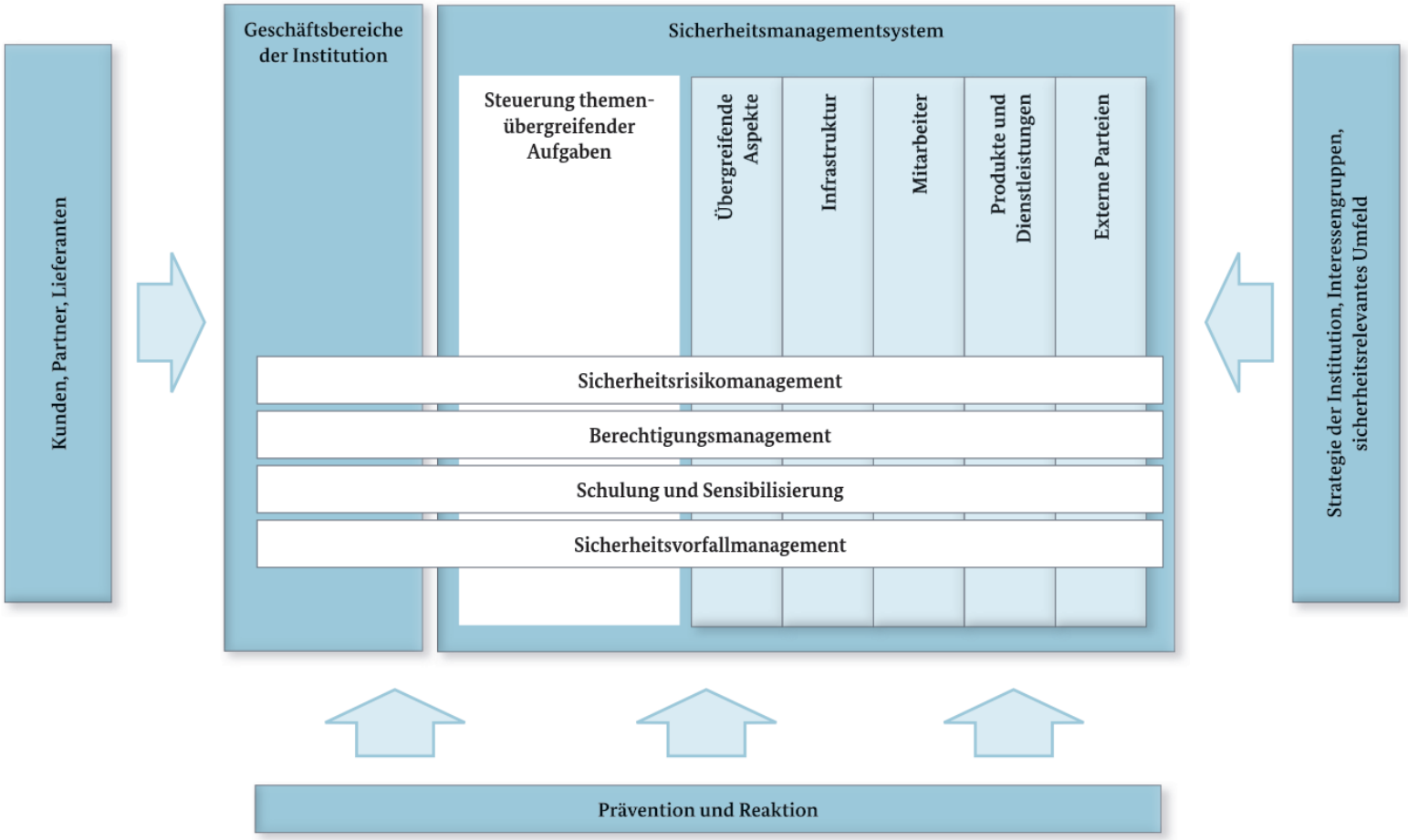
WSGS
2000-1
2000-2

Sicherheitsprozesse

- Kontext
- Führung
- Berichts-/Kontrollprozesse
- Themenübergreifende Prozesse
- Sicherheitsrelevante Themengebiete
- Umsetzung/Wirksamkeit prüfen
- Anpassung/Weiterentwicklung von Sicherheitsmaßnahmen

© HiSolutions 2017 | Wirtschaftsgrundschutz

Aufbauorganisation - Sicherheitsmanagement



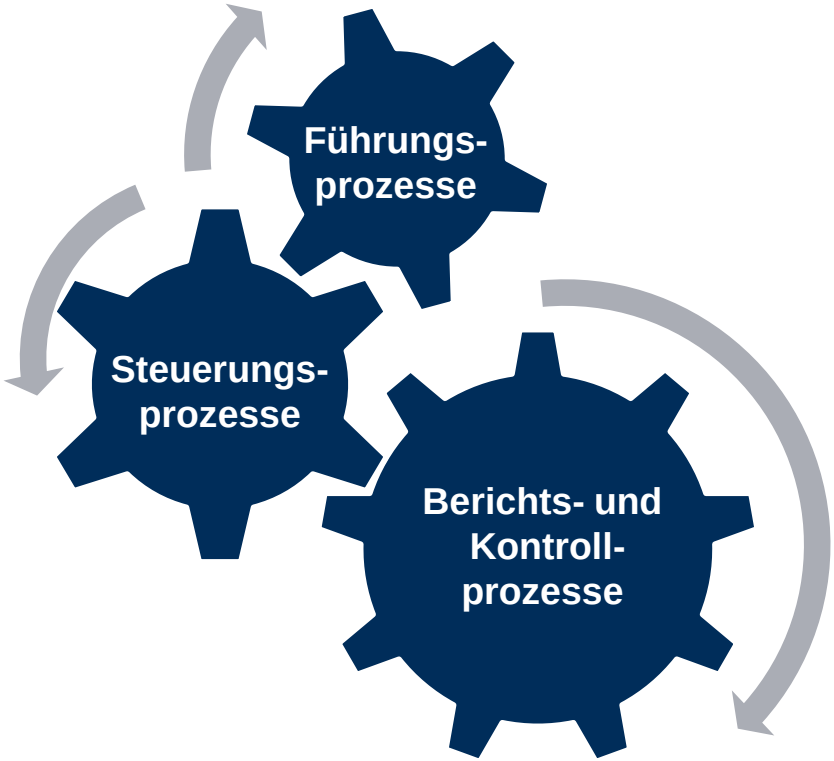
Aufbauorganisation aus dem WSGS (2016)

© HiSolutions 2017 | Wirtschaftsgrundschutz

Die Ablauforganisation des Sicherheitsmanagements orientiert sich an gängigen Normen.

© HiSolutions 2017 | Wirtschaftsgrundschutz

Prozessmodell im Wirtschaftsgrundschutz



- Der **wesentliche Führungsprozess** des Sicherheitsmanagementsystems ist hierbei das **Sicherheits-risikomanagement**.

- Die Sicherheitsorganisation definiert zentral die Methodik und wesentliche Aspekte des Sicherheits-risikomanagements.

© HiSolutions 2017 | Wirtschaftsgrundschutz

Prozessmodell im Wirtschaftsgrundschutz: **Führungsprozesse**

Mit den Führungsprozessen sorgt die Sicherheitsorganisation für:

- die Ausrichtung, also das Erstellen einer an den individuellen Kontext der Institution angepassten **Sicherheitsstrategie**
- das **Definieren** geeigneter **Prozesse**
- das Erstellen von **Regelwerken** (Richtlinien, Prozessbeschreibungen usw.)
- die **Einbindung** der **Leitung** der Institution
- das **Bereitstellen** angemessener **Ressourcen**, sowohl personell und technisch als auch monetär

© HiSolutions 2017 | Wirtschaftsgrundschutz

Prozessmodell im Wirtschaftsgrundschutz: **Steuerungsprozesse**

Die **Sicherheitsorganisation steuert die sicherheitsrelevanten Themengebiete**, die ggf. auch in einem nachrangigen Managementsystem beschrieben sind, mit den Steuerungsprozessen.

- Transfer der grundsätzlichen Vorgaben des Sicherheitsmanagements in die Themengebiete
- Prozessuale Grundlage für ein angemessenes, durchgängiges und einheitliches Sicherheitsniveau in der gesamten Institution

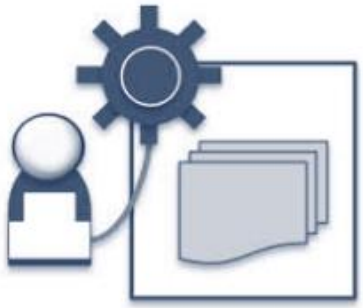
© HiSolutions 2017 | Wirtschaftsgrundschutz

Prozessmodell im Wirtschaftsgrundschutz: **Berichts- und Kontrollprozesse**

Die Berichts- und Kontrollprozesse definieren die:

- **Überwachung** der **Umsetzung** und ggf. der daraus abgeleiteten Verbesserungsmaßnahmen
- **Einbindung** der **Leitung** der Institution mittels des Berichtswesens

Die Sicherheitsorganisation schafft hiermit die **Grundlage** für eine **kontinuierliche Weiterentwicklung** des gesamten Sicherheits-managementsystems.



© HiSolutions 2017 | Wirtschaftsgrundschutz

Ausgestaltung des Sicherheitsmanagementsystems

Kontext	Führung	Berichts- & Kontrollwesen	Themen-übergreifende Prozesse
• Strategie der Institution • Interessengruppen • Sicherheitsrelevantes Umfeld/Gefährdungslage	• Regelwerke • Rollen • Budget, Personal • Einbindung Leitung der Institution • Kontinuierliche Verbesserung	• Revision • Management Review • Berichtswesen	• Sicherheitsrisikomanagement • Sicherheitsvorfallbehandlung • Berechtigungsmanagement • Schulung und Sensibilisierung

Plan: Maßnahmen festlegen	Do: Betreiben	Check: Umsetzung und Wirksamkeit überprüfen	Act: Aktualisieren
• Schutzobjekte • Schutzziele • Schutzkonzepte	• Übergreifende Aspekte • Mitarbeiter • Infrastruktur • Interessengruppen • Wissen & Produkte • Reaktionsmanagement	• Kontrollsystem • Messindikatoren	• Maßnahmen anpassen • Dokumentation aktualisieren

Sicherheitsmanagementsystem aus dem WSGS 2000-2 (2016)

© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: Baustein „Auswahl und Steuerung von Sicherheitsdienstleistungen“

Fakt:

- Institutionen suchen nach Kostenvorteilen
- Flexibilisierungspotenzialen
- Qualitätsdienstleistungen von Spezialisten

Risiko:

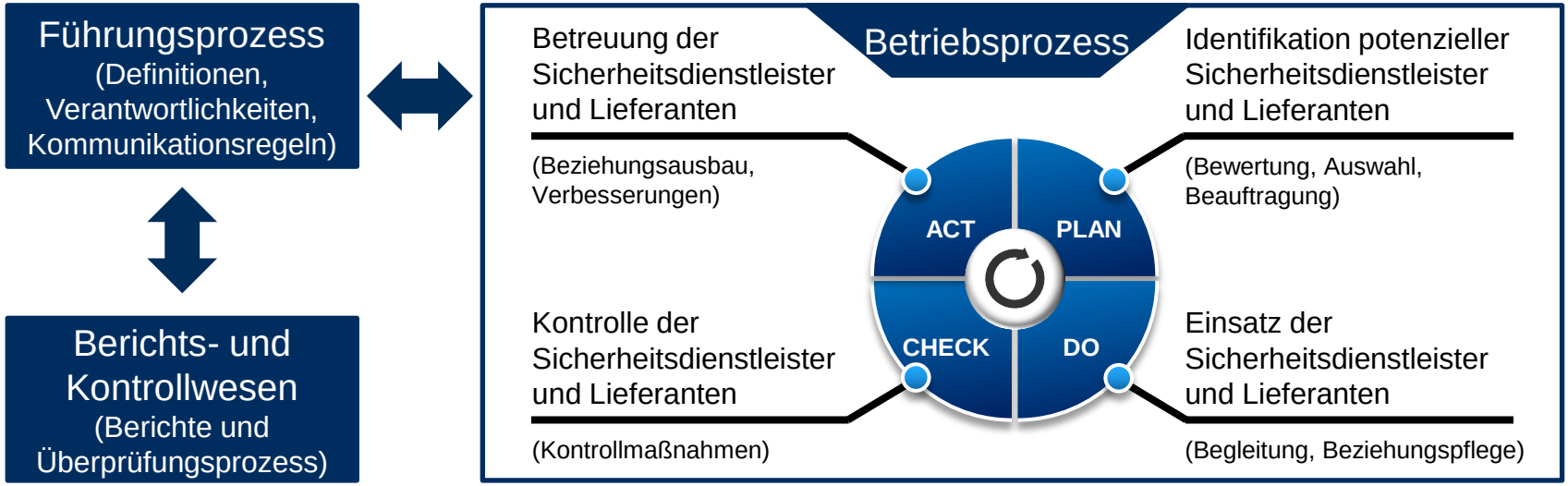
- Auslagerung ≠ Risikobehandlung
- Sicherheitsdienstleister kontrollieren sich selbst
- Wenig Fokus auf eigene Unternehmenswerte

➡ **Hohes Risiko bei falscher Auswahl und unzureichender Steuerung**

Gefährdungen können auf eingebundene Partner der Institution wirken.
Deshalb: Analyse bestehender Gefährdungen

© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: Lebenszyklus des Bausteins



© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: A-Maßnahmen umgehend mit der Bausteineinführung

M 14 Steuern des Sicherheitsdienstleister- und Lieferanteneinsatzes (A)

Unkontrollierte Auslagerung nährt Kontrollverlust, daher:

Permanentes Monitoring durch den internen Auslagerungsverantwortlichen (z.B. Prüfrecht, besser noch Besuchsrecht inkl. Sicherheits-Audit vor Ort)

Mit-Auslagerung der Kontrollfunktion ist untersagt!

Vorbeugende Steuerung

© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: B-Maßnahmen für vollständigen Grundschutz

M 7 Einfordern eines Notfall- und Krisenmanagements von Sicherheitsdienstleistern/Lieferanten (B)

Fehlendes Notfall- und Krisenmanagement betrifft unmittelbar die eigenen Werte, daher:

Durchgängige Notfall- und Krisenmanagementprozesse definieren (z.B. gemeinsame/s Anprechpartnermatrix, -Kommunikation, -Verständnis von Sicherheitsvorfällen)

Zielgerichtete Notfallreaktion gewährleisten (z.B. durchgängige Alamierungs- und Eskalationsprozesse üben, üben, üben)

Durchgängiger Schutz der Unternehmenswerte

© HiSolutions 2017 | Wirtschaftsgrundschutz

Beispiel: C-Maßnahmen als erweiterter Schutz bei hohem Risikopotenzial (z.B. KRITIS Unternehmen)

M 16 Aufbauen und Optimieren eines Beziehungsmanagements (C)

Lose Beziehungen vernachlässigen vorhandenes Optimierungspotenzial zu nutzen, daher:

Feste Integration der Dienstleister in das interne Sicherheitsmanagement (z.B. durch Gemeinsame Verhaltensregeln, Schulungen, Übungen oder Innovationsworkshops)

Etablierung eines gelebten Schnittstellenmanagements zwischen AG und AN (z.B. Vendormanagement mit Handlungsprogramm)

Gemeinsame Kultur erzeugt Identifikation zum Schutz der Werte

Gemeinsame Normen = gemeinsame Umsetzung

© HiSolutions 2017 | Wirtschaftsgrundschutz

Zeitplan und Ausblick

Bestehende Inhalte aus dem Forschungsprojekt werden sukzessive in den nächsten ca. 6 Monaten veröffentlicht.

Neue Inhalte sind auch schon in der Diskussion/Vorbereitung:

- Krisenkommunikation
- Sabotage/Desinformation über soziale Medien
- Compliance
- Begleitung von Delegation/Werksbesichtigungen

© HiSolutions 2017 | Wirtschaftsgrundschutz

Vielen Dank für IhreAufmerksamkeit!

HiSolutions AG
Prof. Timo Kob

Bouchéstraße 12
12435 Berlin
kob@hisolutions.com
www.hisolutions.com
+49 30 533 289 0

© HiSolutions 2017 | Wirtschaftsgrundschutz