Cassini I Guiding ahead

Gemeinsam statt einsam!

Mit Outsourcing-Partnern Sicherheit managen

Inna Thies I Cassini Consulting

cassini GUIDING AHEAD

Referentin

Inna Thies
Senior Consultant
Cassini Consulting

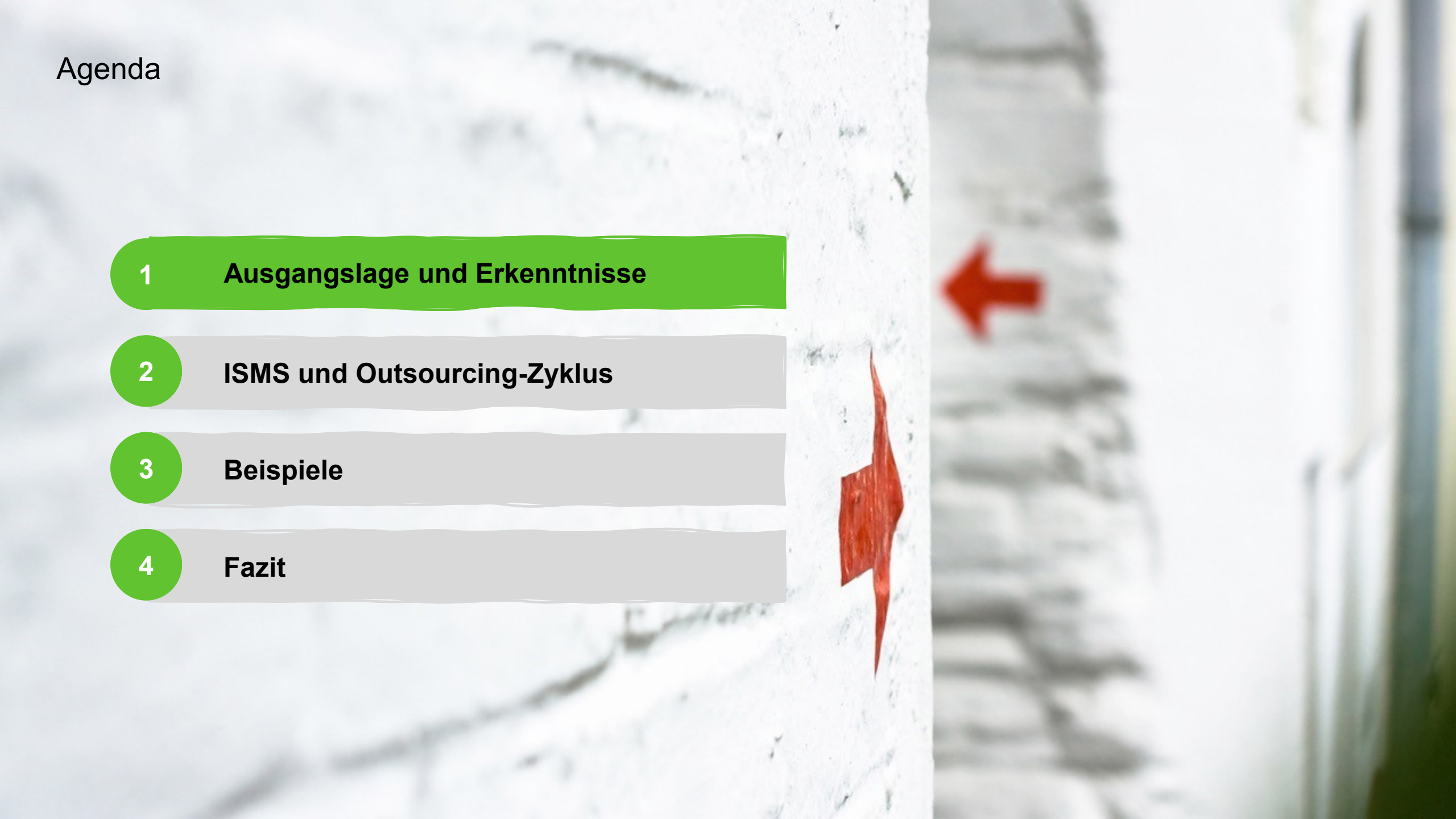
- Management- und Organisationsberaterin
- Zertifizierte BSI Grundschutz Praktikerin

Cassini Consulting ist eine Management- und Technologie-Beratung mit 250 Beraterinnen und Beratern.

Die Unternehmen agieren unterschiedlich beim Informationssicherheitsmanagement im Rahmen der Outsourcing Beziehungen

Agenda

1. **Ausgangslage und Erkenntnisse**
2. **ISMS und Outsourcing-Zyklus**
3. **Beispiele**
4. **Fazit**



Informationssicherheitsmanagementsysteme hinken der IT-Entwicklung hinterher

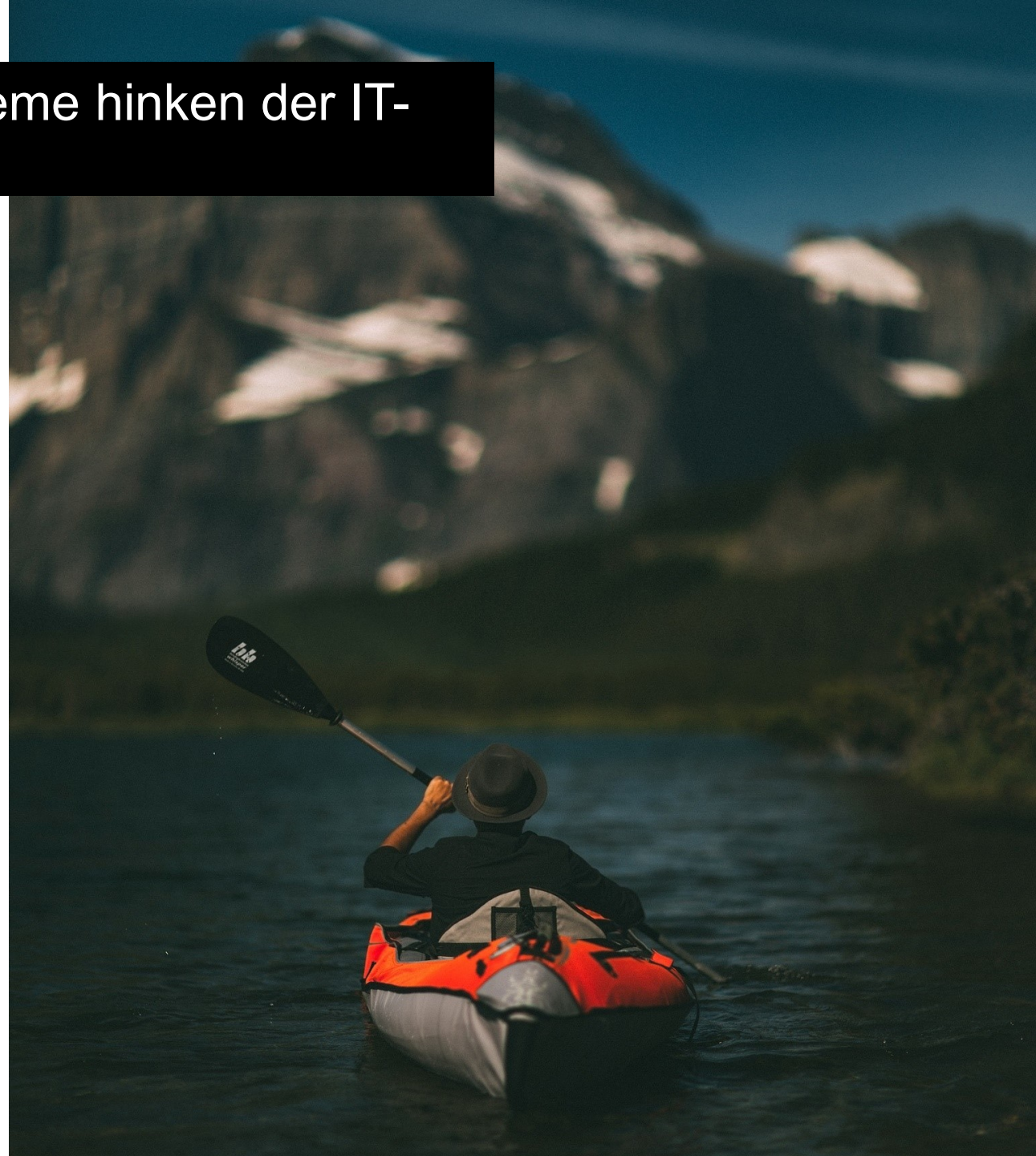
- Die Informationssicherheit …
  - wird oft "alleine" gemacht
  - wird „on top" und als "one last thing" betrachtet

→ Es fehlt ganzheitliche Betrachtung der Informationssicherheit im Rahmen des Outsourcings

→ Es herrscht kein partnerschaftliches Verhältnis zwischen Unternehmen und Outsourcing-Dienstleistern

→ Es herrscht oft unklares vertragliches Verhältnis

→ Friktionen und Eskalationen sind in der Praxis nicht die Ausnahme, sondern Normalzustand in Outsourcing-Beziehungen

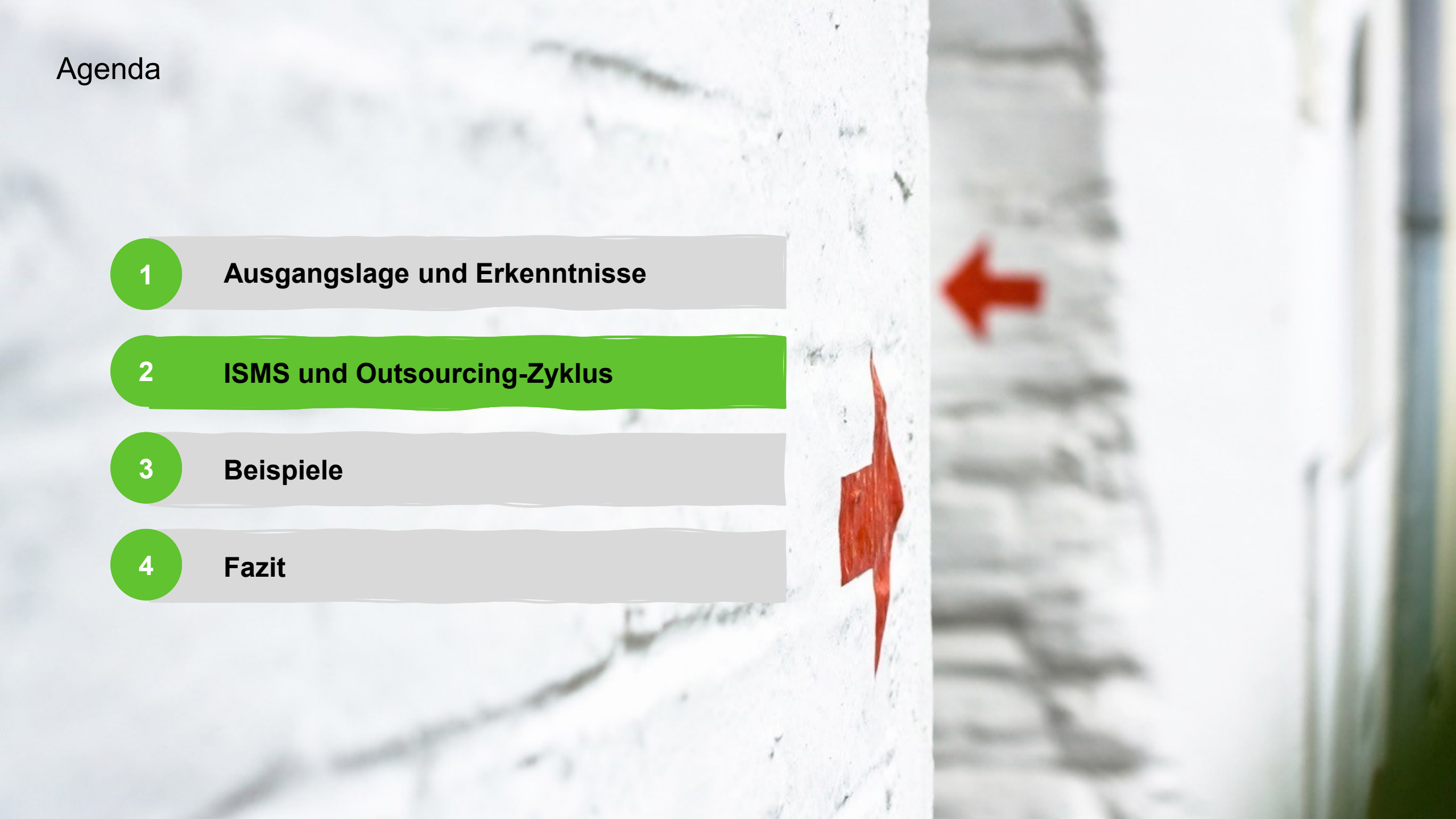


Kunden und Dienstleister müssen mehr der Tatsache die Rechnung tragen, dass sie in einem Boot sitzen

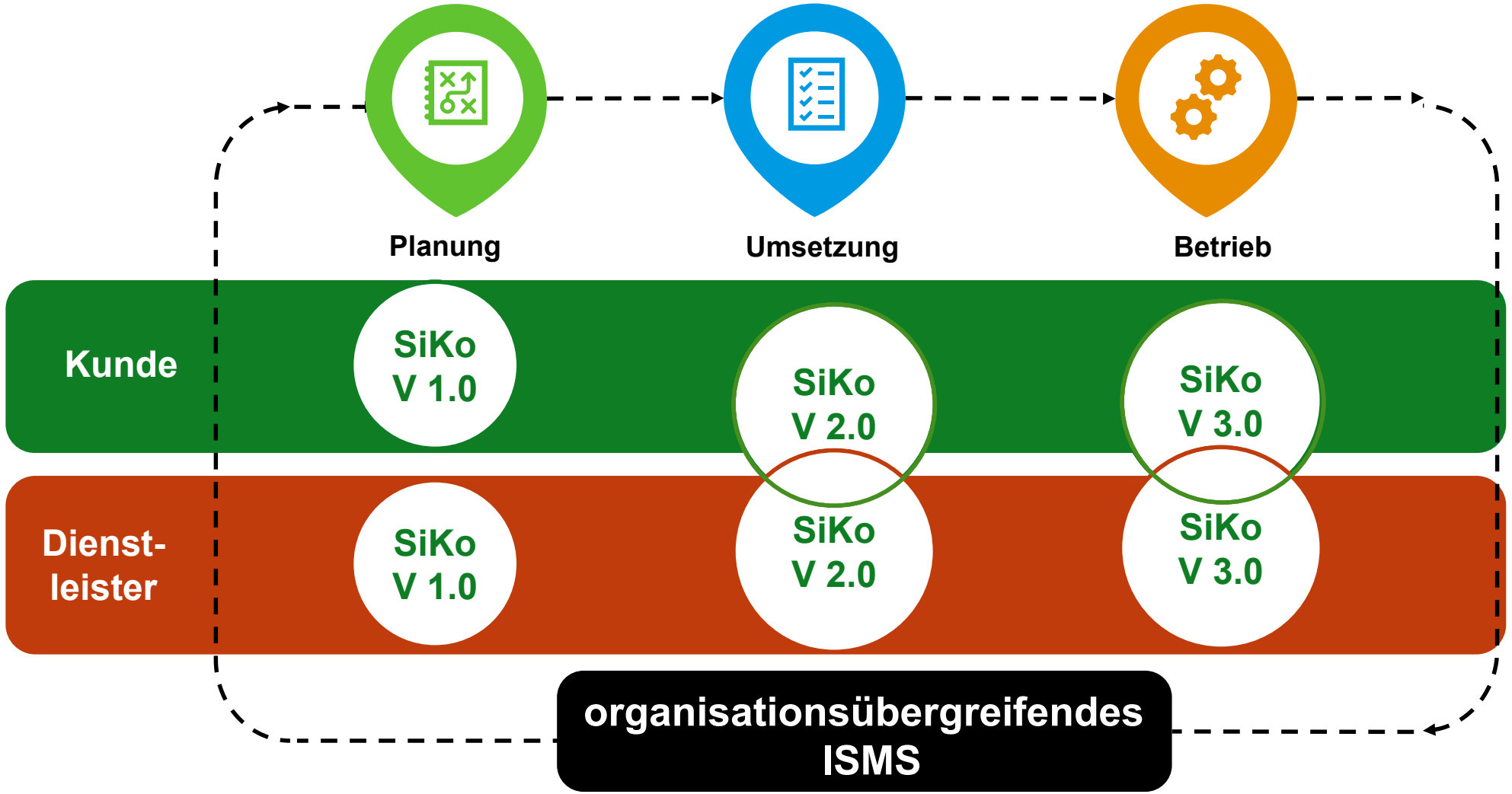
- Informationssicherheitsmanagement muss einem systematischen und kooperativen Ansatz folgen
- Es muss organisationsübergreifendes ISMS zwischen Kunden und Dienstleistern der Outsourcing-Beziehungen geschaffen werden
- ISMS im Rahmen des Outsourcings soll nicht als singuläres Projekt oder Projektphase, sondern als kontinuierlicher Prozess angelegt sein

Agenda

1. Ausgangslage und Erkenntnisse
2. ISMS und Outsourcing-Zyklus
3. Beispiele
4. Fazit



Aktives und abgestimmtes Sicherheitsmanagement in allen Phasen des Outsourcing-Lebenszyklus



In der Planungs- und Vertragsabschlussphase muss eine Balance zwischen Kundenanforderungen und Standardisierung des Dienstleisters erreicht werden

ITO Kunde

- Outsourcing-Strategie und Kriterien für Anbieterauswahl
- Identifikation schützenswerter Informationen
- Bedarfs- und Marktanalyse
- Definition von Sicherheitsanforderungen
- Modularer Aufbau der SiKos, Verbundstrategie
- Sicherheits- und risikoorientierter Beschaffungsprozess

Zusammenarbeit

- Abstimmung SiKos
- Festlegung Informations-bereitstellung
- Definition von Prozessen und Verantwortlichkeiten
- Definition von Schnittstellen
- Einigung auf Standards
- Gemeinsame Risikobewertung
- Dokumentation der Abweichungen
- Beteiligung von Fachexperten an Vertragsverhandlungen

ITO Dienstleister

- Security by Design
- Ausrichtung des ISMS auf Kerngeschäft und Kunden
- Gewährleistung der Transparenz: Dokumentation der Service- und Security-Spezifikation
- Standardisierung der IT-Sicherheit und der Dokumentation
- Einbindung des Service-Delivery-Managements

cassini GUIDING AHEAD

In der Phase der Migration sind verschiedene gemeinsame Maßnahmen notwendig, um die Sicherheit weiterhin zu gewährleisten

ITO Kunde

- Begleitung der Migration durch die IT-Sicherheitsexperte
- Schrittweise Abnahme der Migration
- Anfordern von Sicherheitsdokumentation
- Anpassung der internen Architektur-Dokumentation
- Etablierung von Outsourcing Management
- Integration ITO-Services in ITSM-Prozesse

Zusammenarbeit

- Migrationskonzept
- Etablierung des gemischten Security-Teams als Teil des Migrationsteams
- Sicherer Informationsaustausch
- Abstimmung von SiKos
- Identifikation Anpassungs-bedarf
- Festlegung der Standards für die Dokumentation
- Fortschreibung der Sicherheitsdokumentation

ITO Dienstleister

- Etablierung der Rollen Customer Security und Quality Manager
- Übergabe von Vertrieb-Management an Service-Delivery-Management
- Einbindung der Kunden-schnittstellen in ITSM-Prozesse
- Bereitstellung von Dokumentation

cassini GUIDING AHEAD

Während der Betriebsphase müssen IT-Services nicht nur vertragsgerecht bereitgestellt und genutzt, sondern auch gemeinsam weiterentwickelt werden

ITO Kunde

- Anpassung interner Richtlinien
- Überprüfung der Umsetzung und Wirksamkeit der Sicherheitsanforderungen
- Prüfung der Angemessenheit der Sicherheitsanforderungen, Anpassung und Kommunikation Änderungsbedarf
- Auswertung von Sicherheitsberichten

Zusammenarbeit

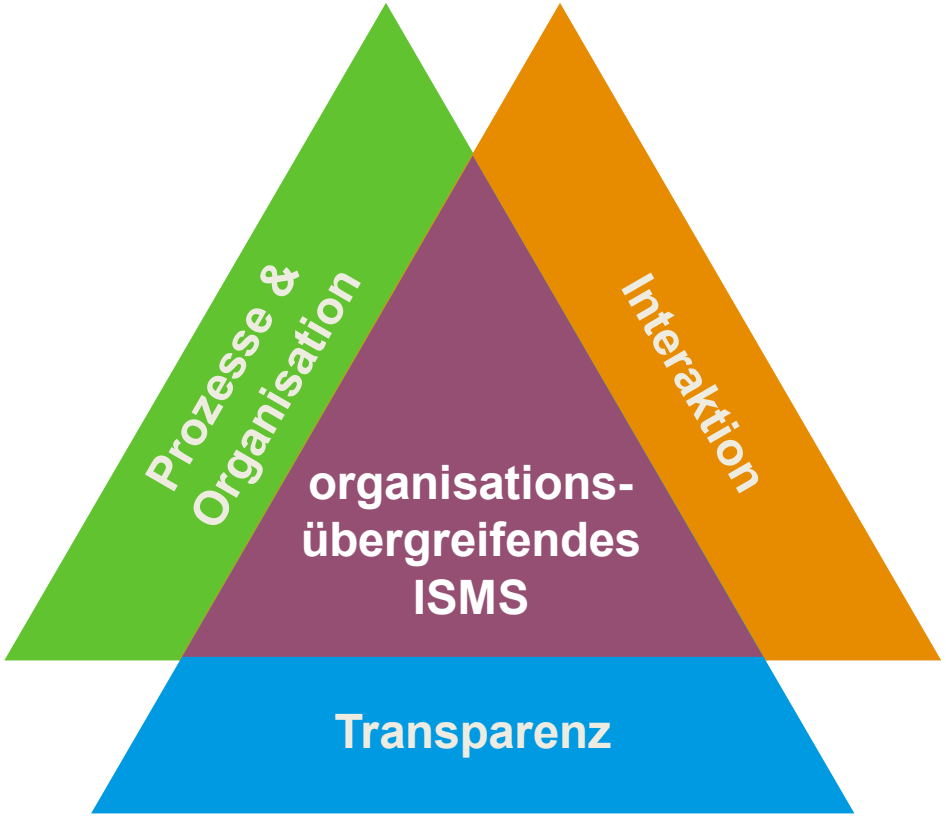
- Durchsetzung der Erfüllung des Vertrages
- Anpassung Sicherheits-maßnahmen
- Umsetzung von Verbesserungen und Innovationen
- Überprüfung und Anpassung von Verträgen
- Anpassung der Dokumentation
- Durchführung Sicherheits- und Notfallübungen

ITO Dienstleister

- Überprüfung der Umsetzung und Wirksamkeit der Sicherheitsanforderungen
- Einhaltung von Berichts- und Meldepflichten
- Unterstützung von Audits
- Prüfung der Umsetzung der Sicherheitsanforderungen bei Zulieferern
- Einbeziehung und Informieren des Kunden bei Weiterentwicklungen

cassini GUIDING AHEAD

Drei Handlungsfelder für organisationsübergreifendes Informationssicherheitsmanagement



Transparenz

- standardisierte, modular aufgebaute, verständliche und für die Nachnutzung geeignete Dokumentation

Prozesse und Organisation

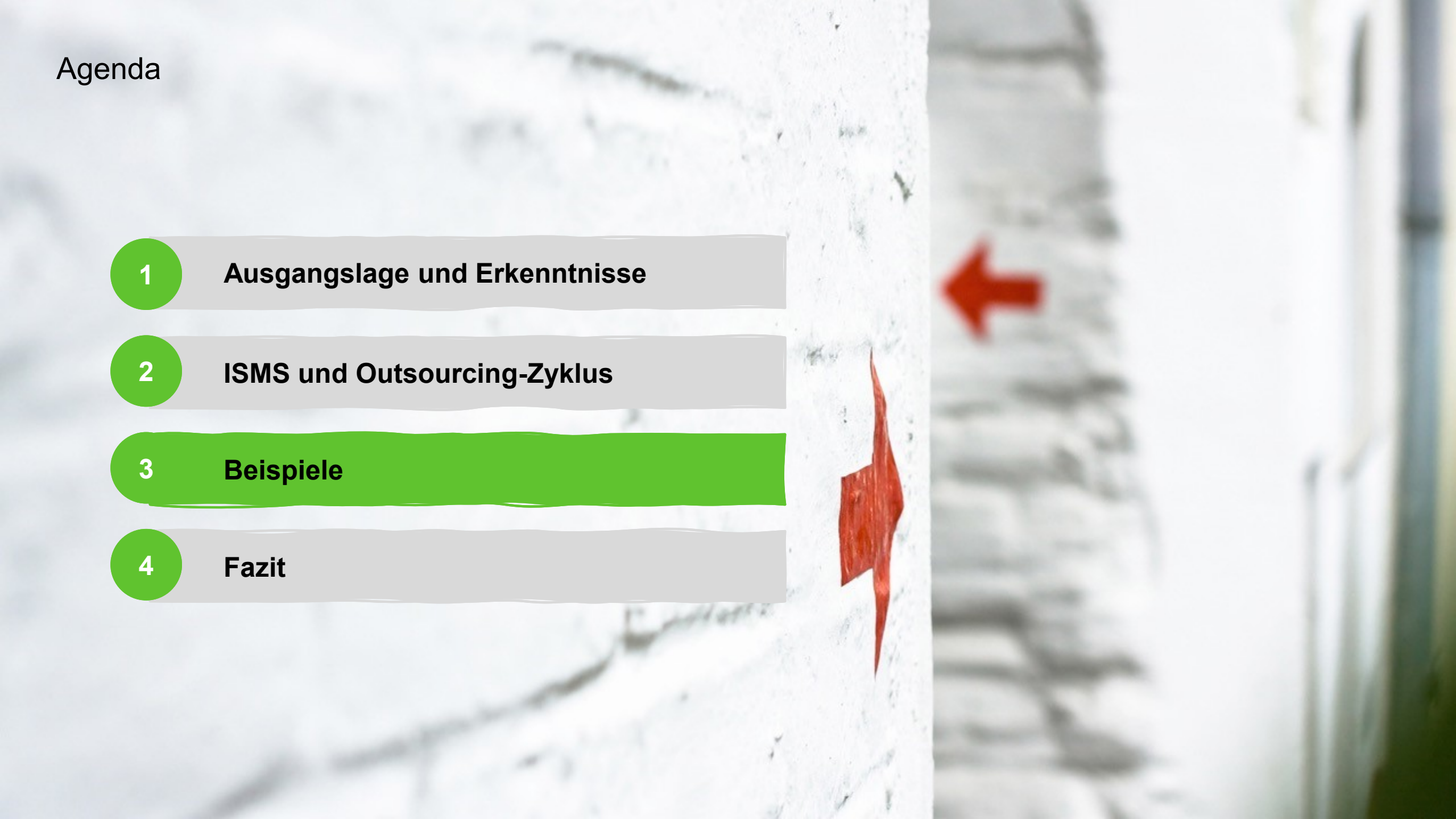
- prozessual verankerte und organisatorisch integrierte Schnittstellen
- neue Prozesse und Organisationsformen

Interaktion

- kooperative Partnerschaft und Informationsaustausch in allen Phasen des Outsourcing-Lebenszyklus

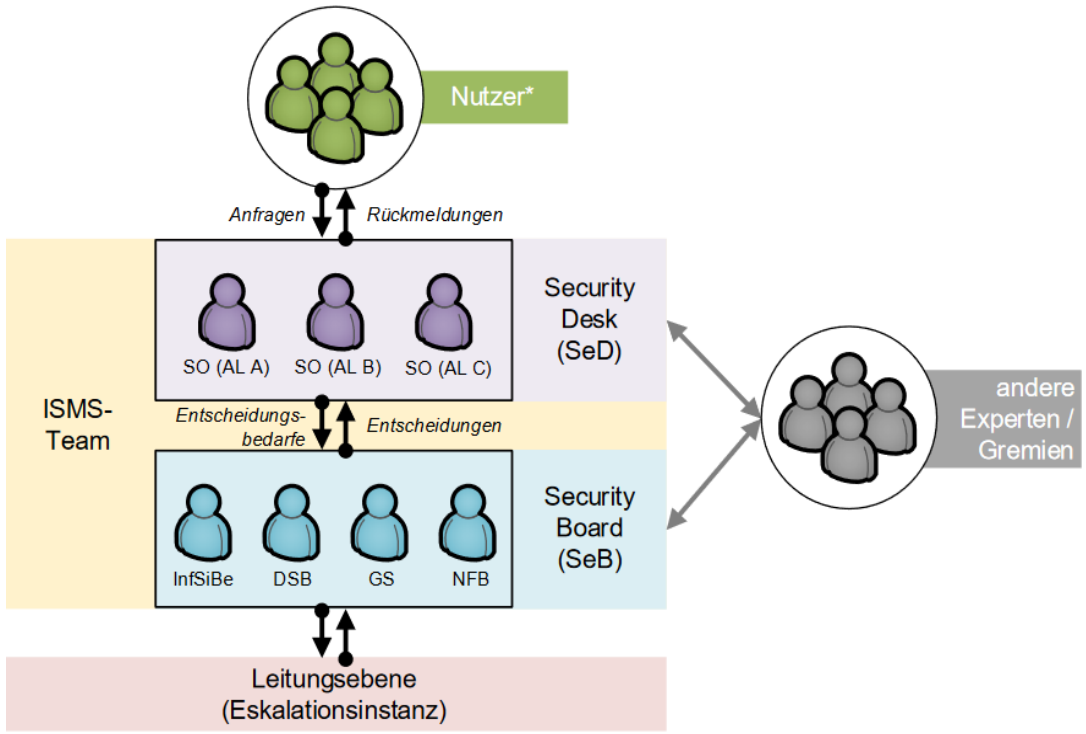
Agenda

1. Ausgangslage und Erkenntnisse
2. ISMS und Outsourcing-Zyklus
3. **Beispiele**
4. Fazit



Bessere Steuerung durch neue Organisation

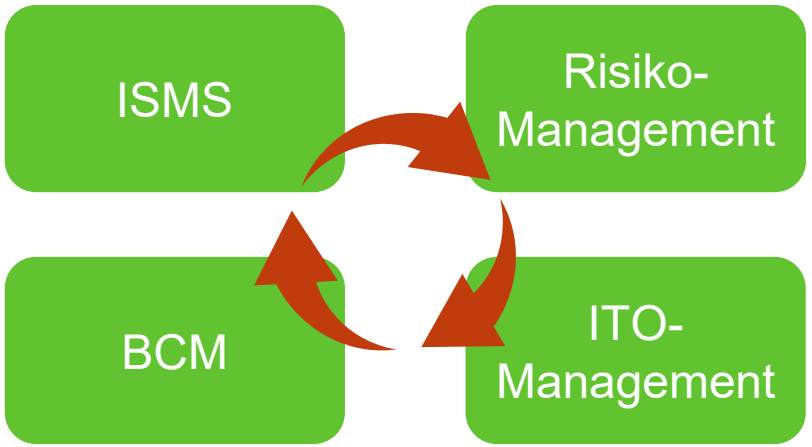
- Etablierung von Security Compliance Board und Security Officers zur Steuerung von allen Vorhaben, die IT-Sicherheit betreffen



*Anwender, Planer, Administratoren, Führungskräfte etc.

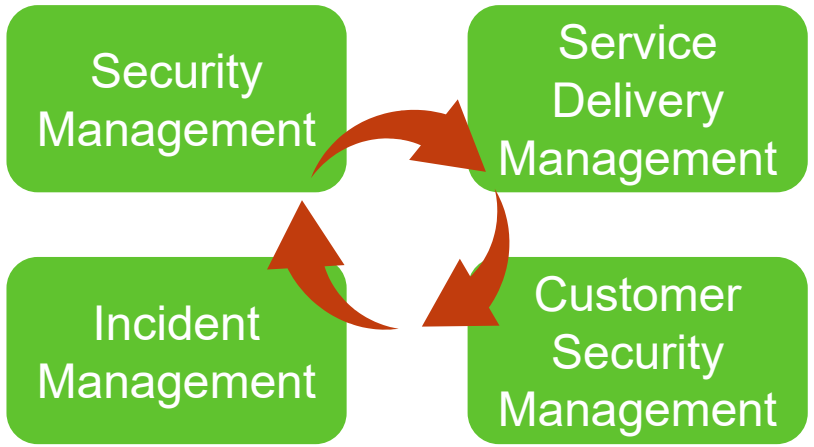
Bessere Steuerung durch neue Organisation

- Etablierung von Outsourcing Management und Definition des Sourcing-Prozesses
- Einbindung des Outsourcing Managements in Management-Systeme der Organisation



Erhöhte Transparenz durch neue Organisation

- Etablierung von der Rolle Customer Security Manager
- Unterstützung des Service Delivery Managements in Bezug auf sicherheitsrelevante Aspekte
- Hauptansprechpartner für die Kundenorganisation zum Thema Sicherheit



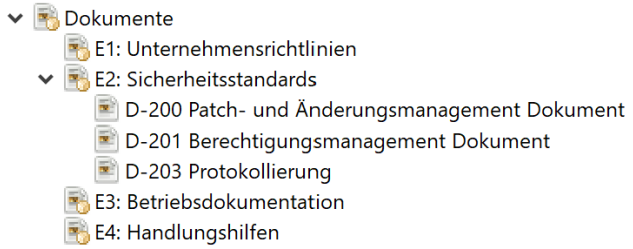
Verantwortlichkeiten gemeinsam festlegen

- Die Verantwortlichkeiten für Sicherheitsmaßnahmen sollten möglichst konkret jedoch hinreichend abstrakt festgelegt und abgestimmt werden
- Mögliche Lösung: Eine Blaupause für die Zuordnung der Anforderungen abhängig vom Liefermodell

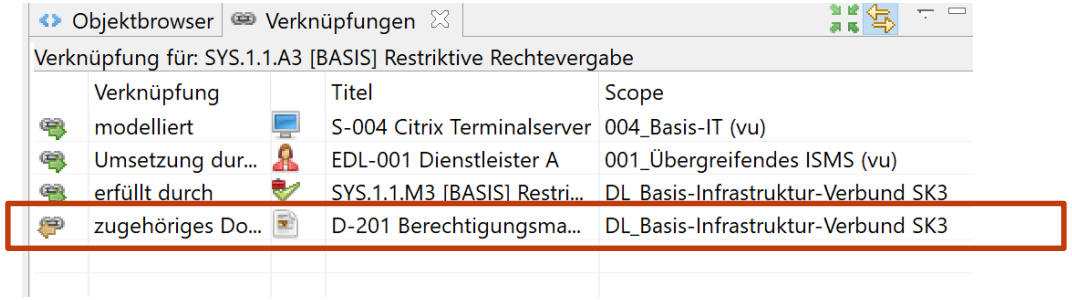
Baustein	PaaS	SaaS	Liefermodell C
ISMS.1 Informations-sicherheitsmanagement	Kunde und Dienstleister: Alle	Kunde und Dienstleister: Alle	…
CON.3 Daten-sicherungskonzept	Kunde: Alle, außer Dienstleister: CON.3.A5 und CON.3.A11	Dienstleister: Alle	…
Baustein 3 …	…	…	…

Gemeinsame Sprache sprechen

- Dokumentation muss so aufgebaut sein, dass die relevanten Informationen leicht als solche identifiziert werden können und in der benötigten Form zur Verfügung stehen.
- Notwendig: Abstimmung der Dokumentenhierarchie, Detailierungsgrad und Bereitstellung



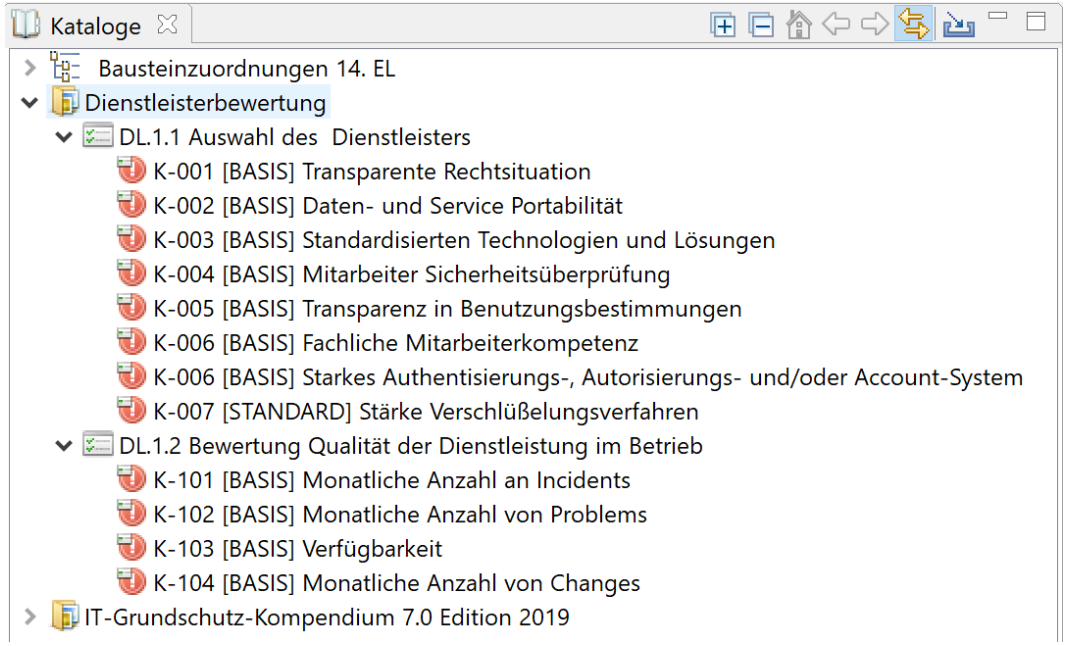
verinice.



Gemeinsame Sprache sprechen

- Klare Kommunikation von Bewertungskriterien, Anforderungen, KPIs
- Nachvollziehbare Dokumentation von relevanten Vorgaben und Wissensmanagement
- Vermeidung von Darüber-reden-wir-später-nochmal-Problematik

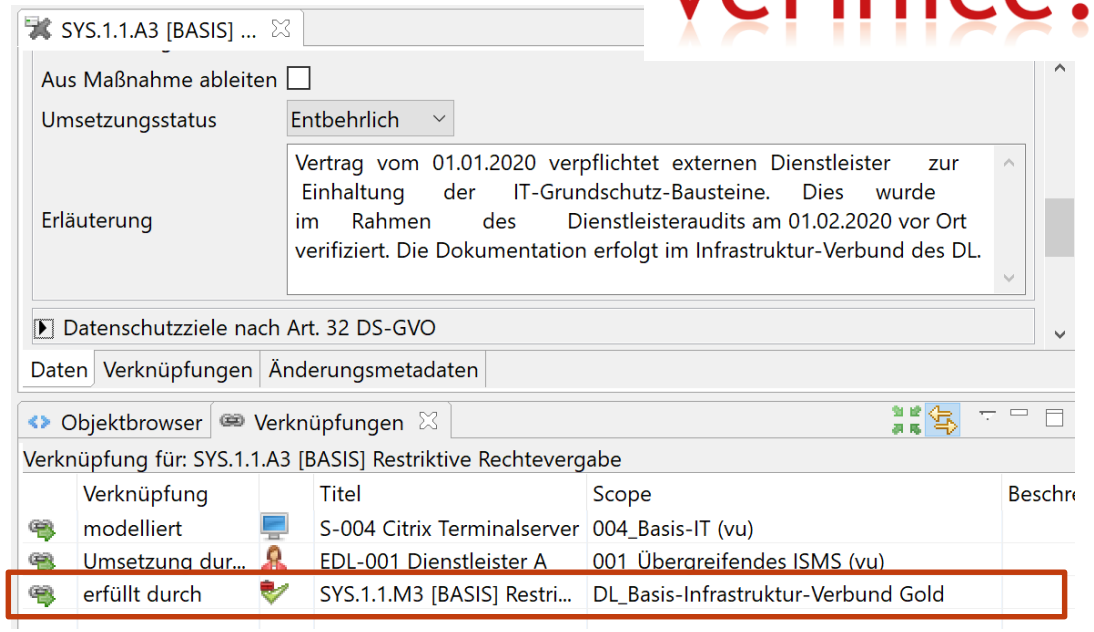
verinice.



Gemeinsame Nutzung von Tools

- Gemeinsame Nutzung von ISMS-Tools schafft Synergien, reduziert Fehler und verschafft besseren Überblick
- Voraussetzung: abgestimmte Verbundstrategie, Konventionen und Detailtiefe

verinice.



Agenda

1. **Ausgangslage und Erkenntnisse**
2. **ISMS und Outsourcing-Zyklus**
3. **Beispiele**
4. **Fazit**

Sicheres IT-Outsourcing ist nötig und möglich

- Nachhaltige und sichere Sourcing-Partnerschaft muss an den richtigen Stellen im Outsourcing-Zyklus und in der richtigen Weise gemeinsam ausgestaltet werden.
- Es gibt viele Ansätze und Möglichkeiten Informationssicherheitsmanagement organisationsübergreifend zu gestalten.
- Prozesse, Organisation und Interaktion müssen derart gestaltet werden, dass möglichst hohe Transparenz besteht, sich möglichst viele Synergieeffekte ergeben und Redundanzen vermieden werden.
- „Kreative“ Nutzung von Tools kann Kunden und Dienstleister dabei unterstützen.


THANKS

Cassini Consulting
Niederlassung Berlin

Inna Thies

Invalidenstraße 74
10557 Berlin
Deutschland
T +49 (0)151 11 45 93 74
F +49 (0) 30 50 10 14 14
inna.thies@cassini.de
visit www.cassini.de