DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?

Vermögenswerte zu identifizieren ist wie das Suchen nach Trüffeln: es braucht Fantasie und Hartnäckigkeit!

Netzwerk Risikomanagement

Cornel Furrer, Managing Consultant

23. Juni 2022
Kulturhof Schloss Köniz, Bern-Köniz

Cornel Furrer

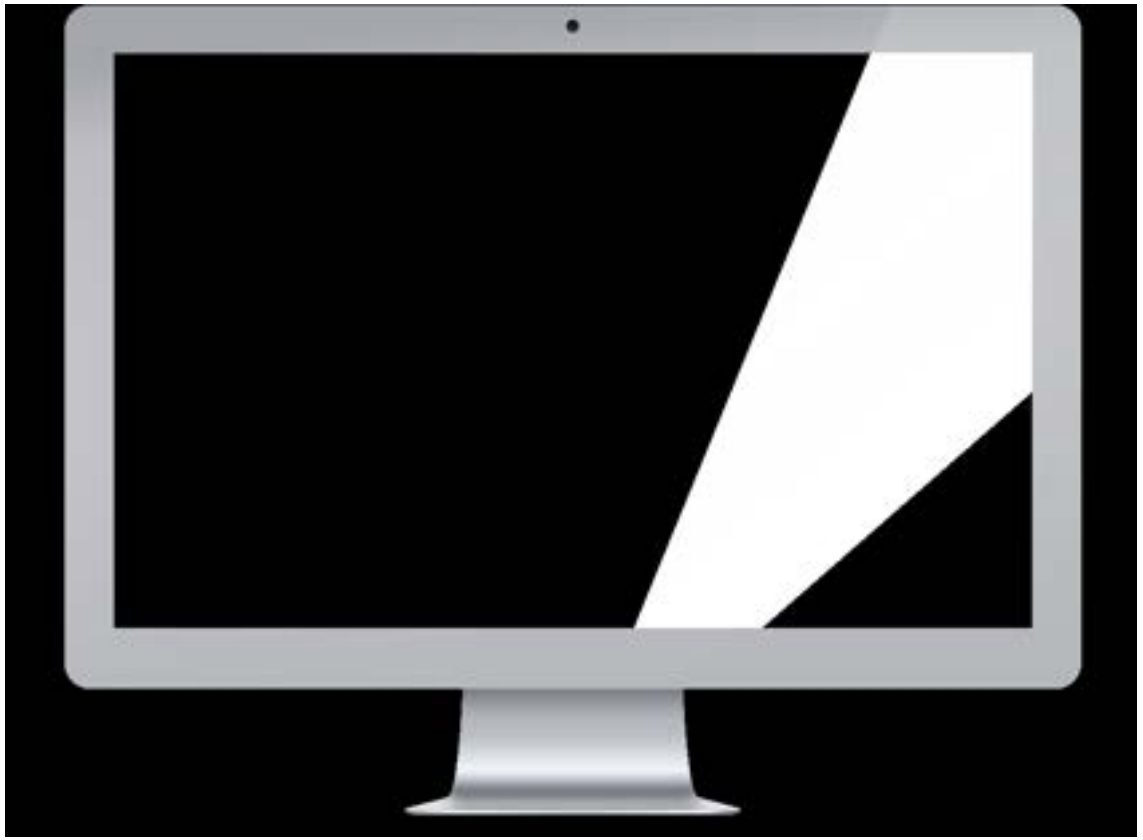
Cornel Furrer

Managing Consultant, Member of the Executive Board
BSI zertifizierter ISO 27001 / ISO 22301 Lead Auditor
Certified Senior Project Manager (IPMA Level B)
SWISSs zertifizierter Sicherheitsbeauftragter Brandschutz

SPEZIALGEBIETE

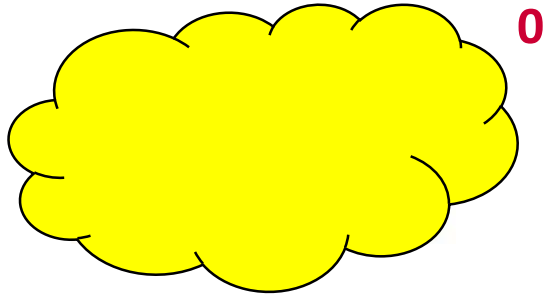
- Informationssicherheit-Managementsystem
- Risikomanagementsystem
- Business Continuity Managementsystem
- Notfall- und Krisenmanagementsystem
- Physische Sicherheits Managementsystem
- Psychologische Aspekte / Awareness
- Menschenführung / Coaching / Mediation

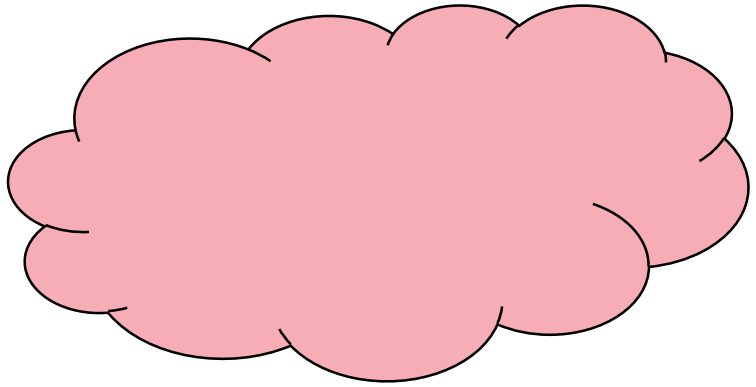
DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?
THEMENÜBERSICHT

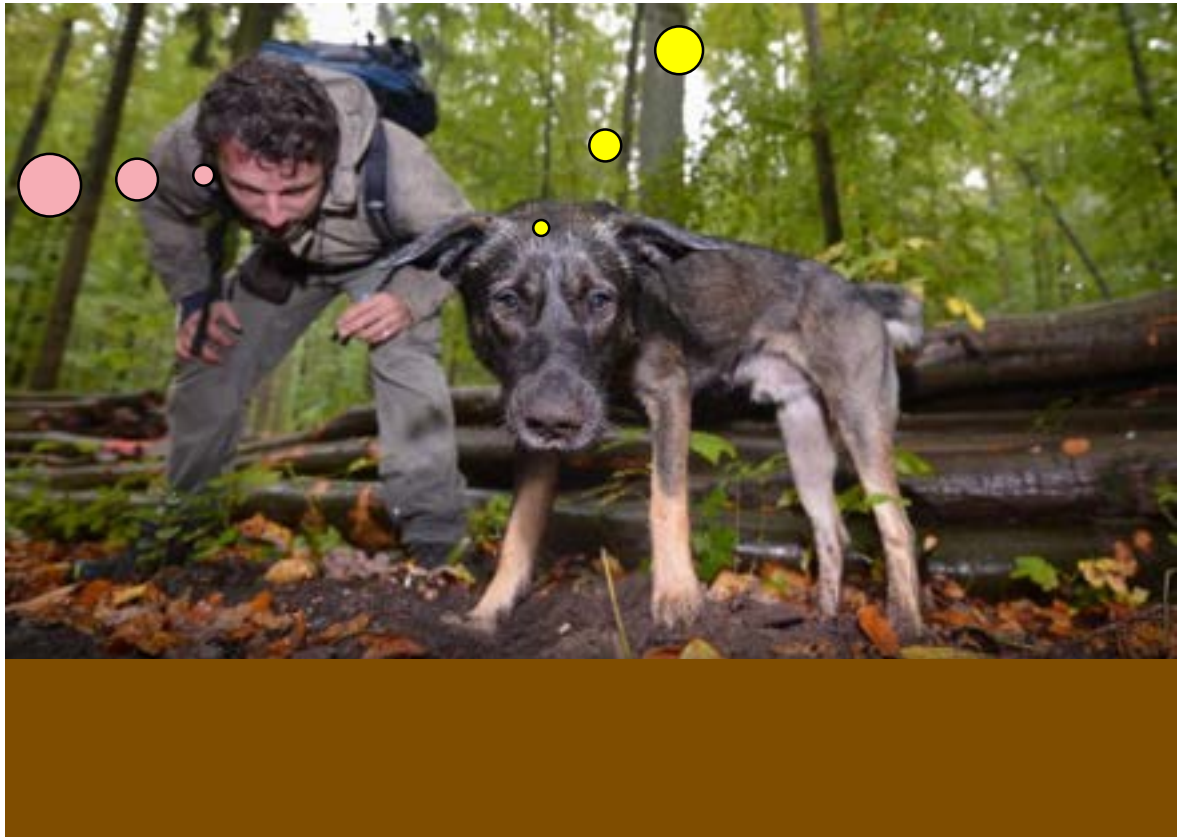


Swiss Infosec AG
Hauptsitz in Sursee

IDENTIFIZIEREN VON WERTEN







Vermögenswerte zu identifizieren ist wie das Suchen nach Trüffeln: es braucht Fantasie und Hartnäckigkeit!

IDENTIFIZIEREN VON WERTEN

SWISS INFOSEC

DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?

01 EIN BEISPIEL

WERT DER INFORMATIONEN

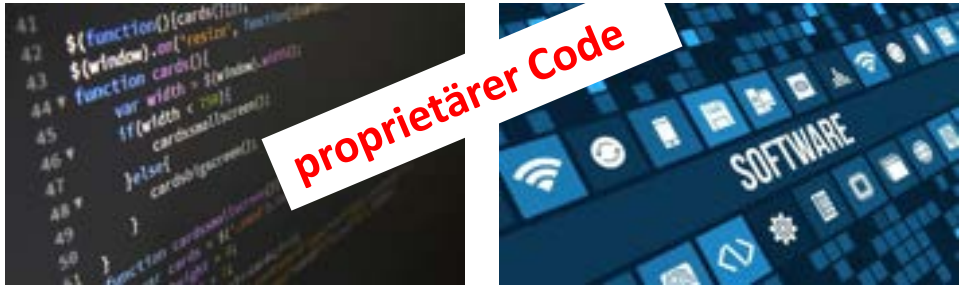
?

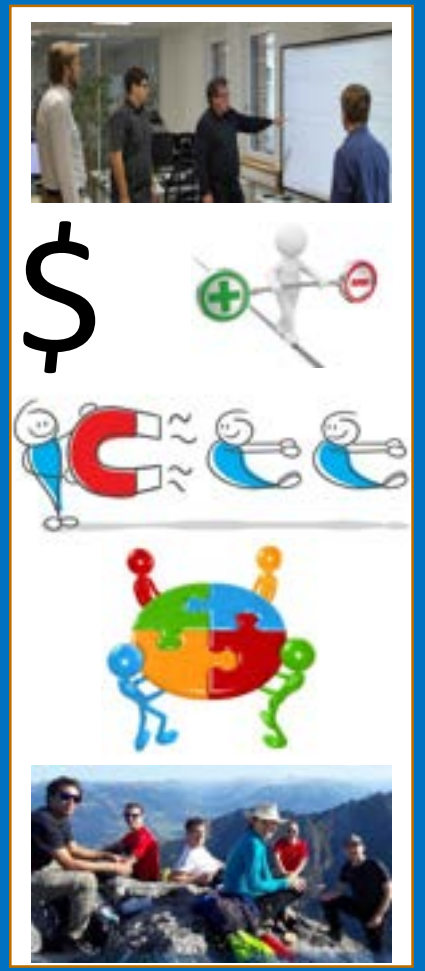
?

SWISS INFOSEC

DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?
01 EIN BEISPIEL

WERTE SCHÜTZEN





WAS VERSTEHT MAN UNTER DIGITALE ASSETS?

- Sämtliche Informationen, welche für ein Unternehmen einen Wert darstellt und in elektronischer Form vorliegt. Beispiele:
  - Geschäftsstrategien
  - Kundeninformationen (Personendaten, Sachinformationen)
  - Konstruktionspläne
  - Versicherungspolicen
  - Wertschriften
  - Rezepturen
  - Digitale Währung
  - Digitale Signaturen
  - Protokolle
  - Verträge (Arbeitsverträge, Kundenverträge)
  - Projekte / Entwicklungsprojekte
  - Sicherheitskonzepte
  - …

DIGITALISIERUNG UND VERNETZUNG DER WERTE

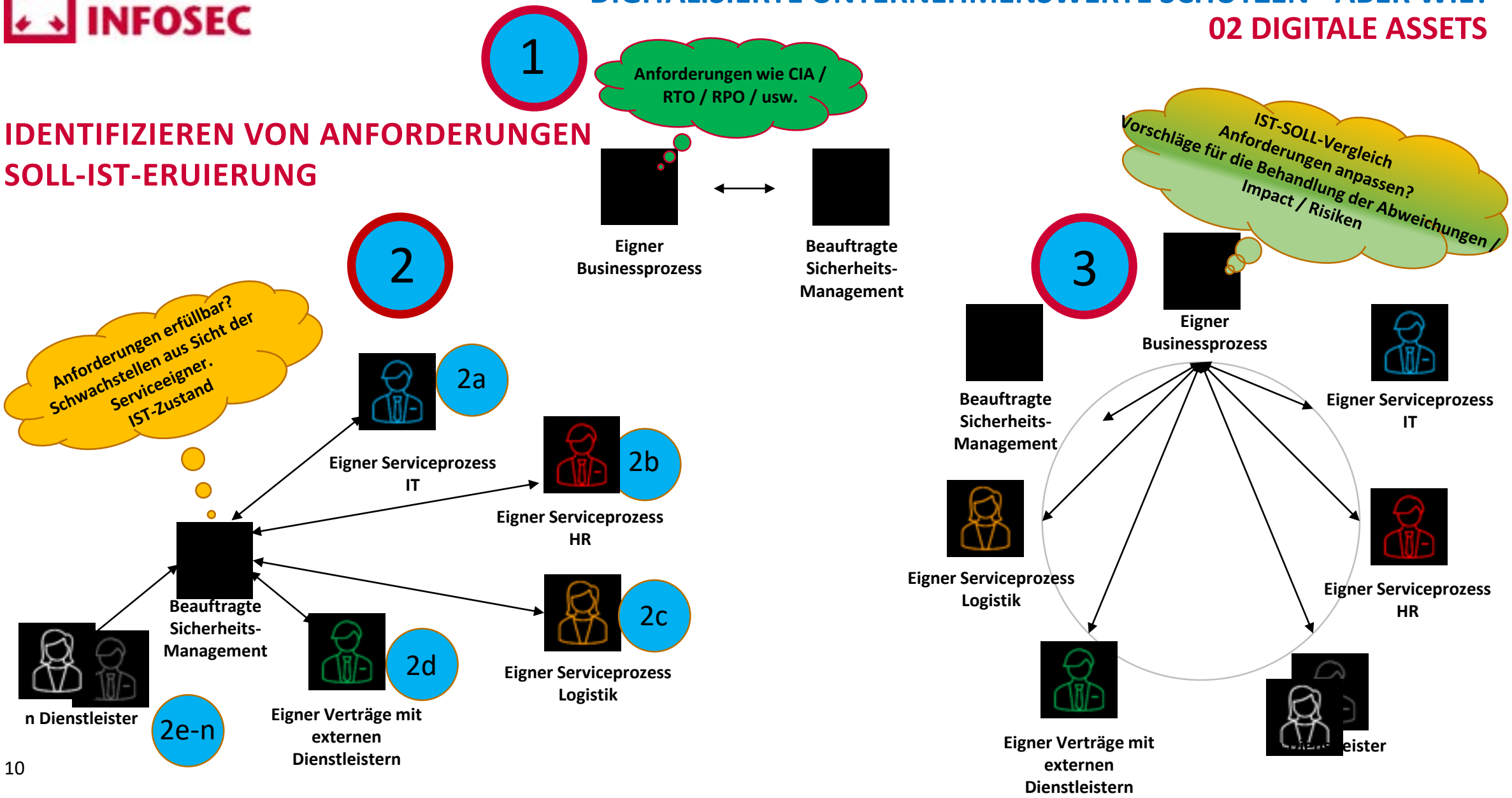
- Vermögenswerte sind zunehmend digitalisiert
- Für Aufbewahrungs- und Speicherorte existieren keine Grenzen (Länder, Rechtsräume, Kulturen)
- Die Verletzlichkeit gegen Verlust von Vertraulichkeit, Verfügbarkeit und Integrität steigt mit der Digitalisierung
- Unternehmen werden handlungsunfähig, wenn Systeme und Netzwerke ausfallen
- Verlust wird nicht erkannt, da nichts fehlt
  → Auswirkungen werden erst spät erkannt
- Verfälschte Informationen können zu Fehlentscheidungen führen – ja sogar zum Tod!

SWISS INFOSEC

DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?

02 DIGITALE ASSETS

IDENTIFIZIEREN VON ANFORDERUNGEN
SOLL-IST-ERUIERUNG



BEDROHUNGEN FÜR WERTE

- Zerstörung, Aushorchung durch Hackerangriffe
- Diebstahl durch internes oder externes Personal
- Verfälschung durch Hardware- oder Software-Fehler
- Zugang infolge Sicherheitslücken in Hard- oder Software
- Unrechtmässige Veröffentlichung infolge Verlust von Geräten
- Absichtliche Verschlüsselung und Erpressung
- Zerstörung durch Elementarereignisse
- Offenlegung durch bösartige Software (Malware)
- Unbefugter Zugang zu Gebäude und Räumlichkeiten
- u.v.m.




- u.v.m.

SWISS INFOSEC

SOCIAL ENGINEERING







Unter Social Engineering verstehen wir das Planen und Durchführen von Angriffen auf Informationen und Systeme unter Ausnutzung der „Schwachstelle Mensch», indem wir zu den Zielpersonen eine ver-trauenerweckende Beziehung aufbauen und diese so zwischen-menschlich beeinflussen.

- **Industriespionage**
- **Datendiebstahl**
- **Identitätsdiebstahl**

KLASSIFIZIERUNG VON WERTEN

Die Werte werden nach je nach ihrer Bedeutung klassifiziert nach

- Vertraulichkeit
- Verfügbarkeit
- Integrität

Die Klassifizierung bestimmt den Schutzbedarfs

KLASSIFIZIERUNGSARTEN – KLASSIFIZIERUNGSSTUFEN (BEISPIEL)

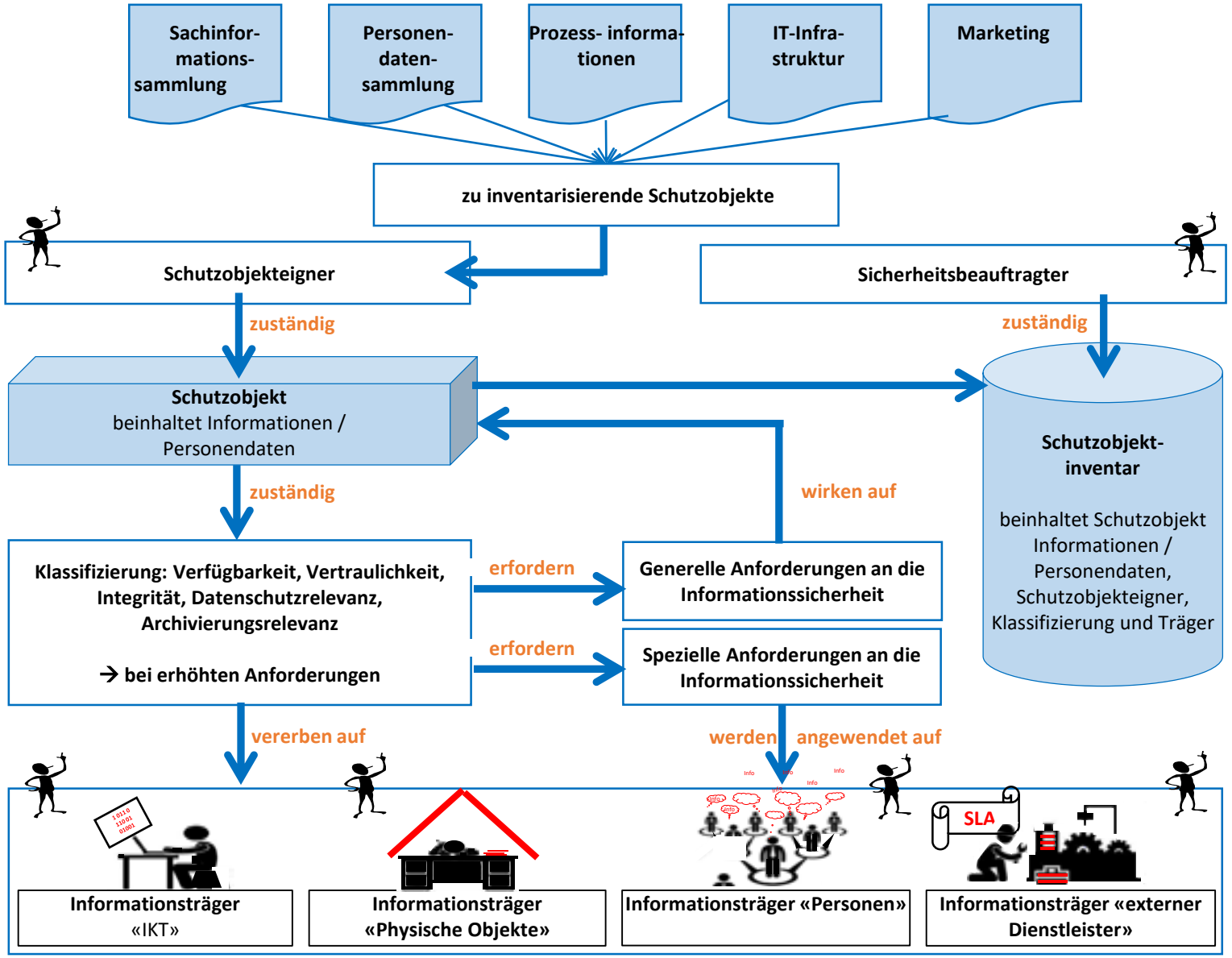
Klassifizierungsarten	Klassifizierungsstufen
❖ **Vertraulichkeit**	• C1 = öffentlich → GL / VR / Marketing / Kommunikation / … • C2 = intern → Mitarbeiter relevant • C3 = vertraulich → Mitarbeiter relevant • C4 = streng vertraulich → GL / VR / …
❖ **Integrität**	• I1 = Ja • I2 = Nein
❖ **Verfügbarkeit**	• V1 = innert ½ Arbeitstag während Betriebszeiten (07.00-12.00 / 13.15-17.00) • V2 = innert 1 Arbeitstag während Betriebszeiten • V3 = innert > 1 bis > 3 Arbeitstage während Betriebszeiten • V4 = Innert > 3 Arbeitstage während Betriebszeiten
❖ **Datenschutzrelevanz**	• D1 = Personendaten • D2 = besonders schützenswerte Personendaten
❖ **Archivierungsrelevanz**	• A1 = Ja • A2 = Nein

AKV EINES SCHUTZOBJEKTEIGNERS (BEISPIEL)

Aufgaben	Kompetenzen	Verantwortung
• **Seitens des Sicherheitsverantwortlichen zugewiesene Schutzobjekte inventarisieren und klassifizieren; Vernetzung seines Schutzobjektes zu andern Schutzobjekten erkennen; die Anforderungen sinnvoll an die Subsysteme / Träger vererben** • **IST-SOLL-Vergleich durchführen (Gap-Analyse)** • **Bei erhöhten Schutzanforderungen eine vertiefte Analyse durchführen (lassen): Schutzbedarfsanalyse SCHUBAN / Business Impact Analyse BIA / Datenschutz-Folgenabschätzung DSFA** • **Konzepte für die Behandlung des Deltas erarbeiten** • **Entscheidungsgrundlagen für die Verantwortlichen bezüglich Behandlung der identifizierten Abweichungen erarbeiten** • **Allfällig erforderliche Sicherheitsmassnahmen planen, umsetzen und kontrollieren lassen**	• Festlegen des Schutzbedarfs für sein Schutzobjekt • Beauftragen von vertieften Analysen bei hohem Schutzbedarf • Sicherheitsmass-nahmen bei den Subsystemen / Trägern seines Schutzobjektes anordnen / über-wachen / durchsetzen	Verantwortlich für den Schutz seines Schutzobjektes • Verantwortlich für die Inventarisierung und Klassifizierung seines Schutzobjektes • IST-SOLL-Analyse • Vertiefte Analyse bei hohem Schutzbedarf • Sicherheitskonzepte erstellen • Verantwortlich für die Einhaltung / Umsetzung der Sicherheitsmassnahmen bei seinem Schutzobjekt

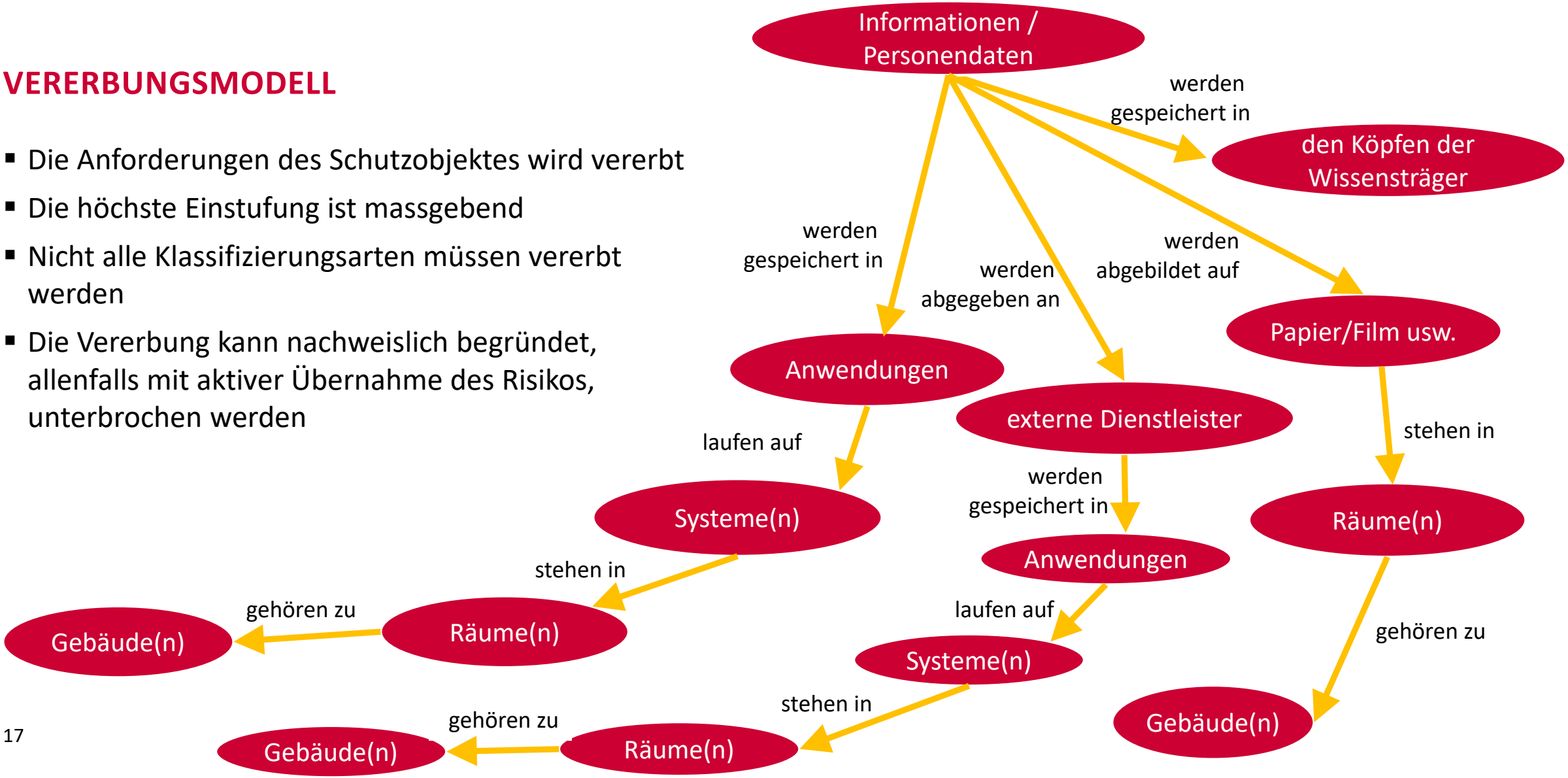
DIGITALISIERTE UNTERNEHMENSWERTE SCHÜTZEN - ABER WIE?
04 KLASSIFIZIERUNG VON WERTEN

VERERBEN VON ANFORDERUNGEN



VERERBUNGSMODELL

- Die Anforderungen des Schutzobjektes wird vererbt
- Die höchste Einstufung ist massgebend
- Nicht alle Klassifizierungsarten müssen vererbt werden
- Die Vererbung kann nachweislich begründet, allenfalls mit aktiver Übernahme des Risikos, unterbrochen werden



BEHANDLUNGSREGELN VERTRAULICHKEIT (BEISPIEL)

KLASSIFIZIE-RUNG/ Mittel	INTERN	VERTRAULICH	STRENG VER-TRAULICH
Klassifizie-rungsvermerk	kein Vermerk	Ja, auf jeder Seite in Kopfzeile. Im Kundenkontakt keine Vermerk angeben.	Gemäss Definition des Eigners
Verschlüsse-lung bei elektronischer Speicherung	Keine Auflage; für alle einsehbar; Speicherung auf unverschlüsseltem Medienspeicher möglich	Zugriff ist durch Rechte-vergabe auf definierte User beschränkt; Ablage nur in definierte Ordner; Speicherung nur auf verschlüsselte Medien-speicher – (auch auf Memorystick).	Filever-schlüsselung erforderlich
physische Ablage	In physisch gesicherten Bereichen der Organisation und des Home-Office.	Clear Desk einhalten; einbruchsnachweisbare Behältnisse mit Sicher-eits-schloss für intern zugängliche Büros.	Gemäss Definition des Eigners (z.B. Tresor)
mündliche Gespräche, Telefon / Mobilephone	keine technischen Auflagen; nur gegenüber internen Mitarbeitenden oder externen Personen mit unterzeichneter Vertraulichkeitserklärung; unberechtigtes Zuhören ausschliessen	keine technischen Auflagen; nur gegenüber definierten internen Mitarbeitenden oder externen Personen mit unterzeichneter Vertraulichkeitserklärung; unberechtigtes Zuhören ausschliessen	Gemäss Definition des Eigners

KLASSIFIZIE-RUNG/ Mittel	INTERN	VERTRAULICH	STRENG VER-TRAULICH
Verschlüsse-lung bei E-Mail-Versand (E-Mail und / oder Anhang)	keine Auflagen; nur gegenüber internen Mitarbeitenden oder externen Personen mit unterzeichneter Vertraulichkeitserklärung	Verschlüsselung des Mails und / oder des Anhangs (heute per ZIP möglich – starkes PW; Mailverschlüsselung nicht vorhanden)	Gemäss Definition des Eigners
Übergabe per Post, Kurier	Normalpost	Eingeschrieben; spezielle Sicherheits-Couverts	Gemäss Definition des Eigners
Bearbeitung mit ICT-Mitteln	Bildschirmsperre bei jedem Verlassen des Arbeitsplatzes einschalten	Bildschirmsperre bei jedem Verlassen des Arbeitsplatzes ein-schalten; Sichtschutz gegenüber Dritten sicherstellen	Gemäss Definition des Eigners
drucken und kopieren	Nur auf Drucker im physisch gesicherten Bereich; persönlich betriebener und überwachter Drucker im Homeoffice	Nur auf Drucker im physisch gesicherten Bereich; Druck nur mit Badge auslösen; persönlich betriebener und überwachter Drucker im Homeoffice	Gemäss Definition des Eigners
vernichten / löschen	Zentrale Sammelstellen für den Schredder oder persönlich shreddern	Persönlich schreddern	Gemäss Definition des Eigners

SCHUTZOBJEKTINVENTAR (BEISPIEL)

Schutzobjektinventar für Informationen			Gesetzliche Auflagen: Personen-Datenschutz / Archivierung				Vertraulichkeit				Inte-grität		Verfügbarkeit (Betriebszeit an Arbeitstagen AT 0700-1200/ 1315-1700)				Applikationen / Systeme								Infrastruk-turen (physisch)				Personen / Rollen											Dienstleister	Abhängigkeit zu	Bemerkungen
Nr.	Asset	Eigner	D1 = Personendaten	D2 = besonders schützenswerte Personendaten	A1 = Archivierung JA	A2 = Archivierung NEIN	C1 = ÖFFENTLICH	C2 = INTERN	C3 = VERTRAULICH	C4 = STRENG VERTRAULICH	I1 = Ja	I2 = Nein	V1=1/2 AT	V2=1 AT	V3= 1-3 AT	V4 > 3 AT	E-Mail	GRC Toolbox	OneDrive	Webseite	Telefonie	MS-Teams	CRM	ERP	Hauptgebäude	Rechenzentrum1	Büro Forschung & Entwicklung	Büro der GL-Mitglieder	Mgmt	HR	Finanzen	IT-Team	CISO	Marketing	Sachbearbeiter	Netzbewirtschaftung	Datenschutzbeauftragter	Applikationsverantwortliche	Sicherheitsbeauftragter Brandschutz			
1	Kunden-Informationen/Personendaten																																								
2	Gebäudeinformation																																								
3	ISMS-Informationen																																								
4	Vertrags-Informationen																																								
5	ICT-Security-Informationen																																								
6	Video-Informationen																																								
7	Personaldaten																																								
8	Entwicklungsinformationen																																								
9	…																																								
10																																									
11																																									

REGELKATALOG → IST-SOLL-VERGLEICH → RISIKOBEHANDLUNG

Sind die Informationsschutzobjekte einmal identifiziert, dann

- *sind die Schutzobjekteigner zu definieren – dort wo es Überschneidungen gibt, sind glasklare Verantwortlichkeiten zu definieren (eines der wichtigsten Anliegen des ISO 27001).*

Sind die Informationsschutzobjekte einmal klassifiziert resp. der Schutzbedarf definiert, dann

- *sind die Regeln zu definieren, welche auf dieses Schutzobjekt anzuwenden sind.*

Sind die Regeln definiert, welche auf das jeweilige Schutzobjekt anzuwenden ist, dann

- *ist eine Beurteilung vorzunehmen, inwieweit diese Regel bei diesem Schutzobjekt effektiv angewendet wird → IST-SOLL-Vergleich*

Liegt der IST-SOLL-Vergleich vor, dann

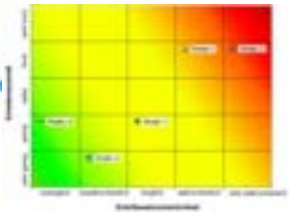
- *haben die Verantwortlichen das Risiko zu analysieren, zu bewerten und festzulegen, wie das Risiko behandelt werden soll: akzeptieren, vermindern und Nettorisiko akzeptieren, vermeiden, transferieren*

Haben die Verantwortlichen die Behandlung des Risiko festgelegt, dann

- *beauftragen sie die Planung – Umsetzung – Kontrolle*

WIE SCHÜTZE ICH MEINE WERTE?

- Aufbau eines Integralen Sicherheitsmanagementsystems (PDCA-Qualitätsmodell, (organisatorische, rechtliche, technische, physische, personelle Sicherheitsaspekte
- Grundsätze, Strategien, Weisungen, Prozesse
- Unterstützung durch das oberste Management (Managementattention)
- Notwendige Ressourcen (Mittel und Personal)
- Welches sind meine schützenswerten Informationen
  → Inventarisierung und Klassifizierung (Schutzbedarfsanalysen)
- Angemessene grundlegende Sicherheitsmassnahmen (Grundschutz)
- SOLL-IST-Vergleich
- Delta analysieren, Schwachstellen bewerten, Behandlung definieren
- Ausbildung und Sensibilisierung aller Mitarbeitenden
- Kontrollen und Audits
- Kontinuierliche Verbesserung KVP



ÜBERPRÜFUNGSFORMEN - MATURITÄT

Level 1: Dokumentenreview
→ Papier nimmt fast alles an

Level 2: Interview
→ Horchaufwörter: erste Ungereimtheiten zwischen Geschriebenem und Gesagten

Level 3: View
→ Konsolentest / Begehungen:
wird Geschriebenes und Gesagtes effektiv eingehalten

Level 4: Penetration
→ Ethical Hacking / Social Engineering

FRAGEN

Haben Sie Fragen?

DISKUSSION – WIDERSPRUCH

Wo habe Sie ergänzende Informationen / gleiche oder andere Erfahrungen?

Wo sehen Sie Vorgetragenes anders?

Wo legen Sie Widerspruch ein?

INTERESSE AN UNSERN KOSTENLOSEN FACHVERANSTALTUNGEN DER SWISS INFOSEC AG UND DER SWISS GRC AG?

MEET SWISS INFOSEC!	Zürich Flughafen, 13 bis 17 Uhr, anschliessend Apéro	Mehr Infos Newsletter & Event-Einladungen
GRC DAY	www.infosec.ch/msi www.swissgrcday.ch	www.infosec.ch/news