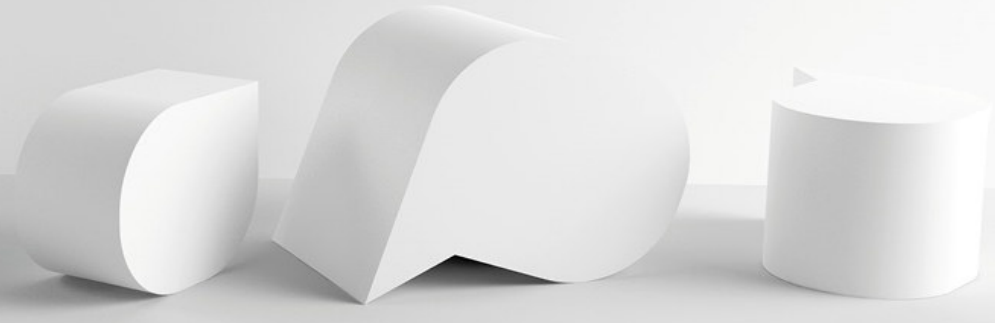
Information Security in Healthcare

APP Unternehmensberatung AG

Das Management im Spannungsfeld zwischen IT und DSDS



Information Security in Healthcare Conference 2019 | Jana Papritz & Marcel Schmid | 06. Juni 2019

Wer wir sind

T +41 58 320 30 38
M jana.papritz@app.ch

Jana Papritz

Dipl.Inf.UniBE

Consultant, bei APP seit 2007; Schwerpunkte:

- Informationssicherheit und Datenschutz
- Projektmanagement
- IT Service Management

T +41 58 320 30 62
M marcel.schmid@app.ch

Marcel Schmid

BSc in Wirtschaftsinformatik

Cand. BSc in Psychologie

Consultant, bei APP seit 2017, Schwerpunkte:

- Informationssicherheit im Gesundheitswesen
- Human Ressource Management
- Projektmanagement

Veranstaltungsziele

Sie wissen …

- warum es ein zielgruppenorientiertes Sensibilisierungsprogramm braucht.
- wie ein Sensibilisierungsprogramm aufgebaut sein könnte.

Sie kennen …

- die wichtigsten Inhalte eines Sensibilisierungsprogrammes.
- die wichtigsten Erfolgsfaktoren zur Verbesserung der Sicherheit in ihrer Organisation.

Wozu IT-Sicherheit

Faktor Mitarbeiter

vom wandelnden Risiko zum sicherheitsbewussten Mitarbeiter

Risiko ist…

- Mitarbeiter und das Management, welche den Fokus auf alles andere als auf die Sicherheit haben.
- die Verantwortung auf die Schultern eines einzelnen «Polizisten» zu legen (DSDS-Verantwortlicher).

Besser wäre…

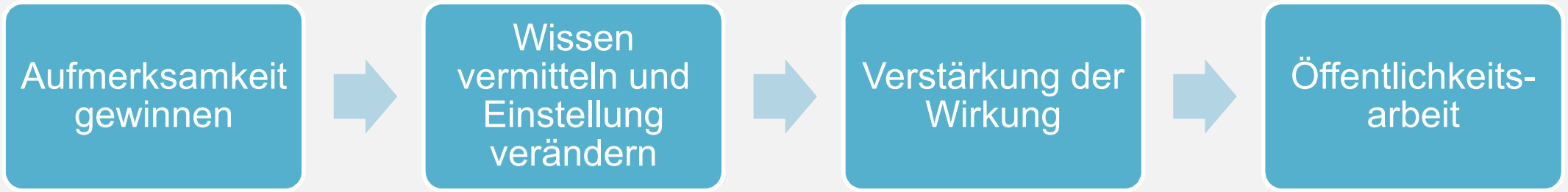
- eine gesunde/angemessene Sicherheitskultur in den Arbeitsalltag zu integrieren.
- jeder Einzelne hat das Wissen im eigenen Umfeld «sicher» zu arbeiten.

Mitarbeiter befähigen

Mitarbeiter werden befähigt und ändern ihr Verhalten, wenn….

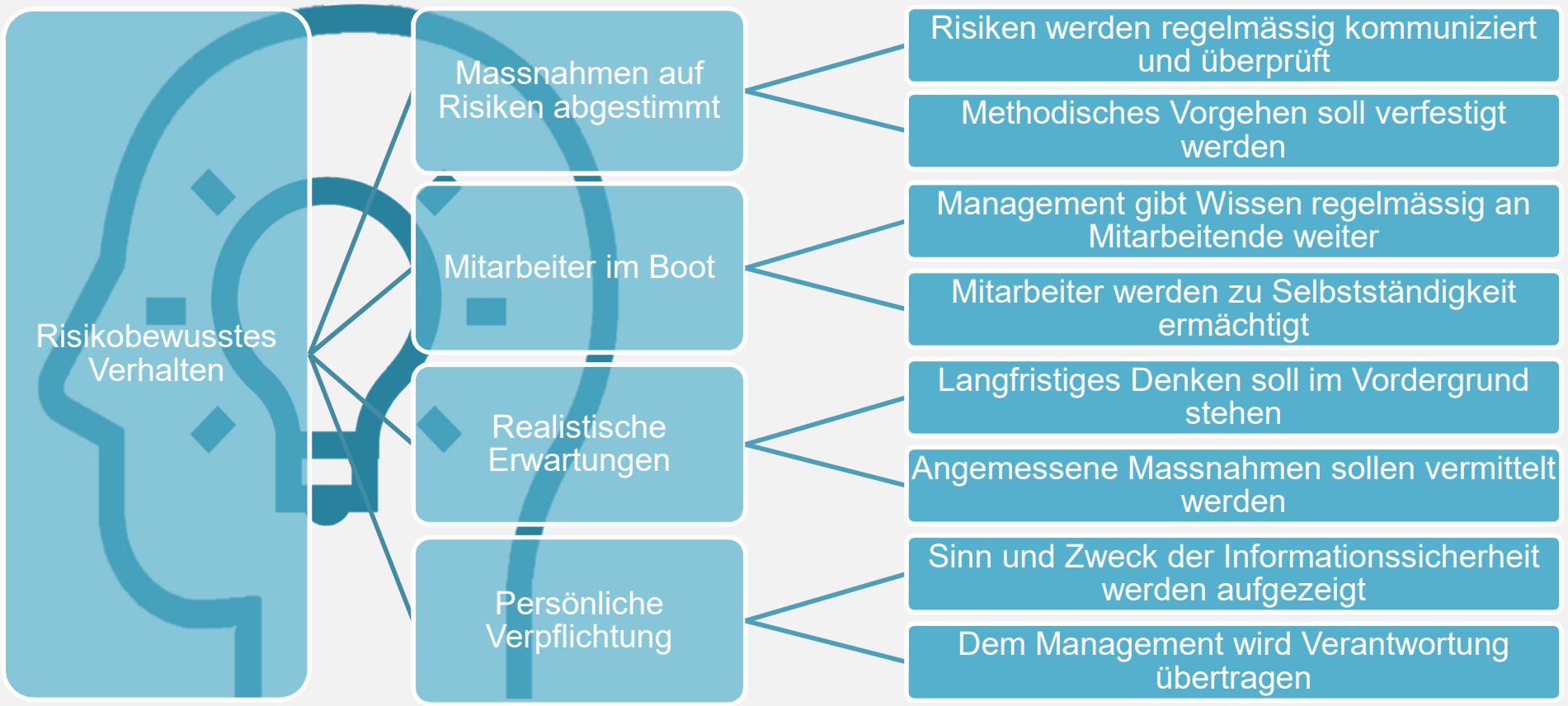
- die Visionen und Strategien im Unternehmen von allen mitgetragen werden.
- eine gesunde Sicherheitskultur etabliert wird; also ein angemessenes Risikobewusstsein vorhanden ist.
- Sensibilisierung und Wissensaufbau zielgruppenorientiert erfolgt.

Aufbau Sensibilisierungskampagne



Awareness / Sensibilisierung - Psychologische Aspekte

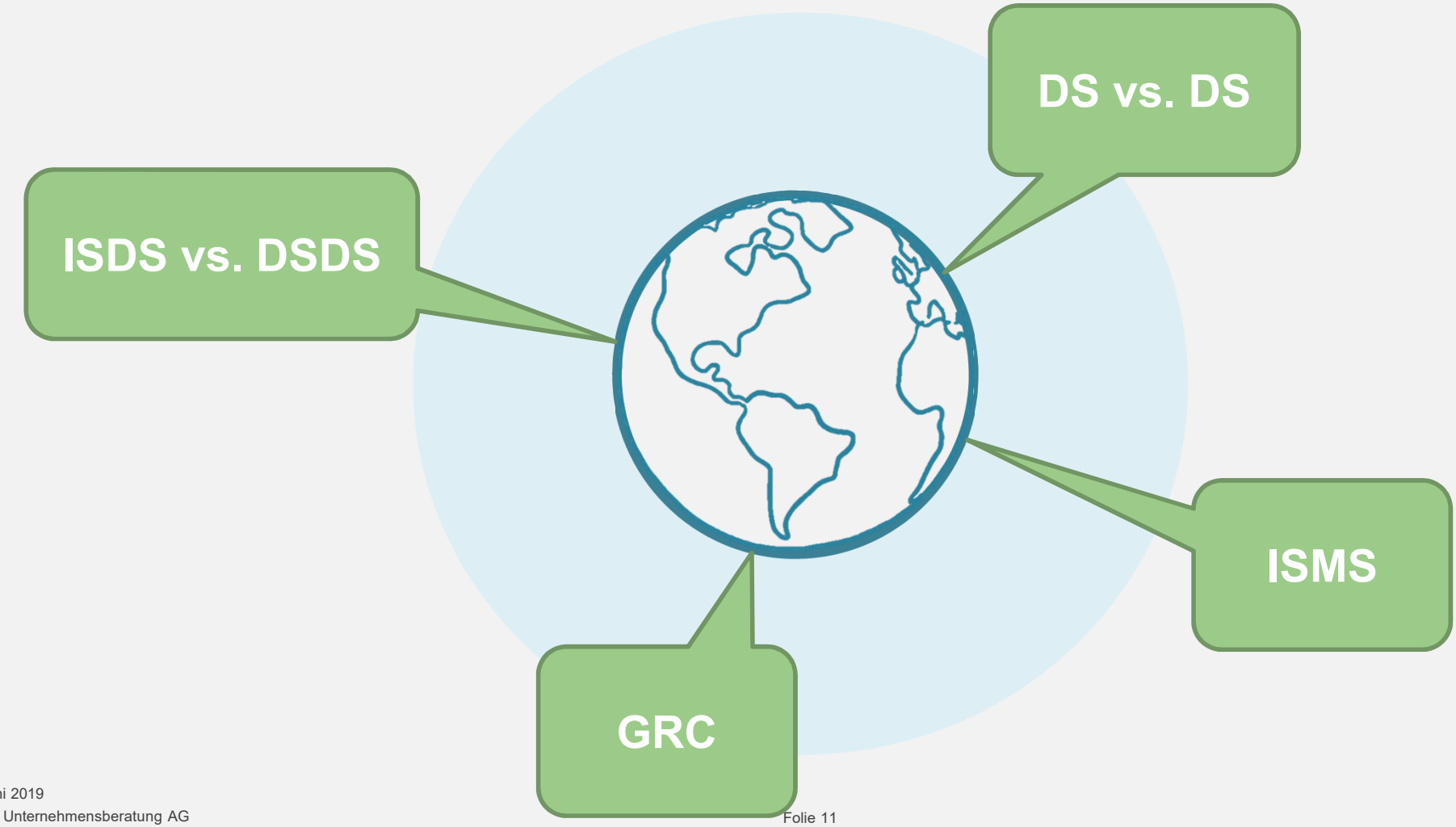
Verhalten verankern - Zukunft sichern



Das Management im Spannungsfeld IT und DSDS

Security Awareness im Management

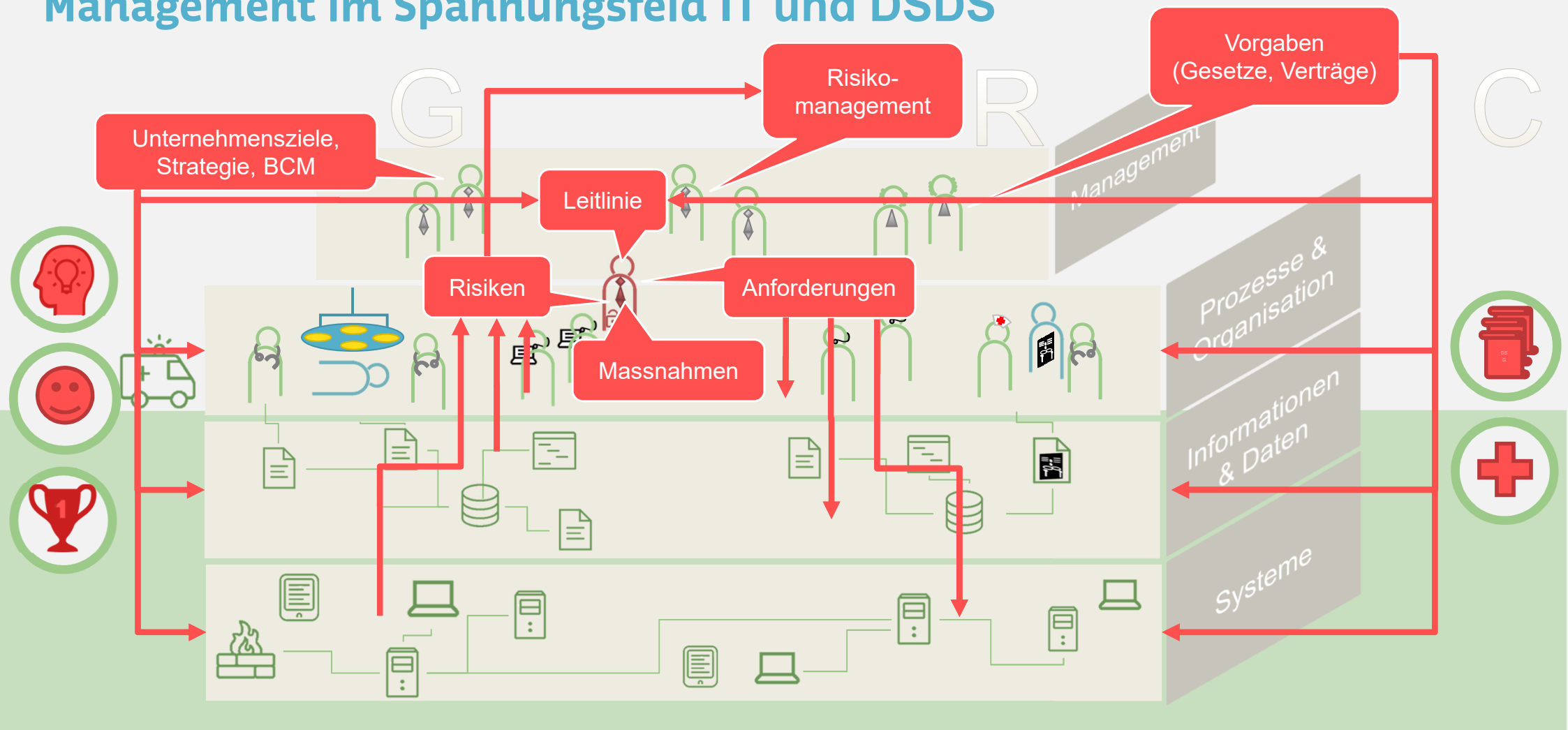
Im Universum der Begriffe



Das Universum der Begriffe

- **DSDS vs. ISDS**
  Ob Cybersicherheit, Informationssicherheit und Datenschutz oder Datensicherheit und Datenschutz – die Schutzziele sind dieselben. DSDS wird als gängige Abkürzung weiterverwendet.
- **DS vs. DS**
  Primärziele von Datensicherheit ist der Schutz der Daten vor Zerstörung, Missbrauch und Verlust während Datenschutz auf den Schutz der informationellen Selbstbestimmung zielt. Dies kann zu Widersprüchen führen (Beispiel Cloud).
- **ISMS**
  Ein Informationssicherheitsmanagementsystem ist keine Anwendung im klassischen Sinn – die Gestaltung des Sicherheitsprozesses steht im Vordergrund.
- **GRC**
  Governance, Risk and Compliance dient einer vorgaben- und gesetzeskonformen Unternehmensführung aufgrund von risikobasierten Entscheiden.

Management im Spannungsfeld IT und DSDS



Die Rolle des Managements

Das Management **übernimmt**

- die Steuerung und die Kontrolle des Sicherheitsprozesses.
- die Gesamtverantwortung über Risiken in der Organisation.
- die Verantwortung bei der Formulierung der Leitlinie zur Datensicherheit und zum Datenschutz.
- die Rolle eines Vorbildes.

Das Management ist **verpflichtet**

- einen klaren Auftrag zum Sicherheitsmanagement (ISMS) zu formulieren.
- genügend Ressourcen zur Verfügung zu stellen.
- Sensibilisierungsmassnahmen für alle Zielgruppen (Mitarbeiter) zu etablieren.

PDCA + A - Methodik

- Verbesserungsmassnahmen überprüfen und umsetzen
- Dokumentation sicherstellen

- IT-Sicherheitsprozess planen
- Strukturanalyse durchführen (Unternehmensarchitektur, Inventar, Business Impact Analyse)

- Reviews und Audits durch-führen
- Massahmen prüfen
- Lieferanten und Dienstleister auditieren

- Leitlinien formulieren
- Schutzbedarf feststellen
- Anforderungen, Risiken und Massnahmen ableiten

Plan

Das Management **etabliert** den **Sicherheitsprozess** mit den notwendigen Rollen:

- Der Sicherheitsbeauftragte der Organisation erhält eine leitende Funktion.
- Der Sicherheitsbeauftragte kennt die Organisation und Prozesse und ist im Bereich der IT-Sicherheit auf dem neusten Stand.

Das Management leitet eine **Strukturanalyse** der **Organisation** ein:

- Prozesse & Organisation, Anwendungen & Daten sowie Systeme sind Bestandteil der Analyse.
- Empfehlenswert ist der Aufbau einer Unternehmensarchitektur.
- Die Strukturanalyse gibt Auskunft über die potentiellen Schutzobjekte (Schadensbild)

Do

Anforderungen:

- Der Sicherheitsbeauftragte kann - von der Strategie, den Unternehmenszielen und den Vorgaben an die Organisation sowie Standards abgeleitet – einen Anforderungskatalog (Leitlinie) erstellen.

Risiken:

- Pro Schutzobjekte muss eine Risikoanalyse auf Basis der Anforderungen durchgeführt werden. Es wird entschieden ob Risiken getragen, bewältigt oder verlagert werden.
- Der Sicherheitsbeauftragte unterstützt die Verantwortlichen bei dieser Arbeit.

Massnahmen:

- Massnahmen dienen dazu den Risikograd abhängig von der Risikobereitschaft der Organisation für Schutzobjekte zu minimieren.

Check

Die **Kontrolle** im Sicherheitsprozess ist bedeutsam – um feststellen zu können, ob ein realer **Sicherheitsgewinn** erreicht werden kann:

- Eine periodische Überprüfung der Massnahmenumsetzung dient zur Einschätzung dieser Zielerreichung.
- Reviews und Audits sind – vorzugsweise durch externe Stellen – durchzuführen.
- Vertragsaudits mit Fokus Sicherheit von Lieferanten und Dienstleister dürfen nicht vergessen werden.

Act

Verbesserungen können zum Beispiel durch erlangen von **Zertifikaten** oder **Ausbildungsmassnahmen** erreicht werden:

- Anerkannte Zertifikate im Bereich der Sicherheit sind zum Beispiel
  - ISO 27001 Informationssicherheits-Managementsystem (ISMS)
  - ISO 9001 Qualitäts- und Risikomanagementsystem
  - ISO 20000 IT Service Management (ITSM)
- Anerkannte Qualifikationen können erworben werden – wie zum Beispiel
  - Lehrgänge CAS/MAS Information Security an Fachhochschulen in der Schweiz
  - Certified Information Systems Security Professional (CISSP)
  - ISACA Certified Information System Auditor (CISA), Certified Information Security Manager (CISM)
- Planen von Sensibilisierungskampagnen.


www.app.ch/healthsec

Besten Dank

Für Fragen stehen wir Ihnen auch beim Mittagessen gerne Red und Antwort.

Jana Papritz
Consultant
jana.papritz@app.ch

Marcel Schmid
Consultant
marcel.schmid@app.ch

Bern
APP Unternehmensberatung AG
Monbijoustrasse 10
Postfach
CH-3001 Bern

Zürich
APP Unternehmensberatung AG
Löwenstrasse 40
CH-8001 Zürich

Basel
APP Unternehmensberatung AG
Gartenstrasse 95
CH-4052 Basel

Luzern
APP Unternehmensberatung AG
Werftestrasse 4
CH-6005 Luzern

APP in Kürze

Vielfältige Beratungsschwerpunkte mit über 40ig-jähriger Erfahrung aus verschiedensten Branchen

Ausschreibung und Evaluation

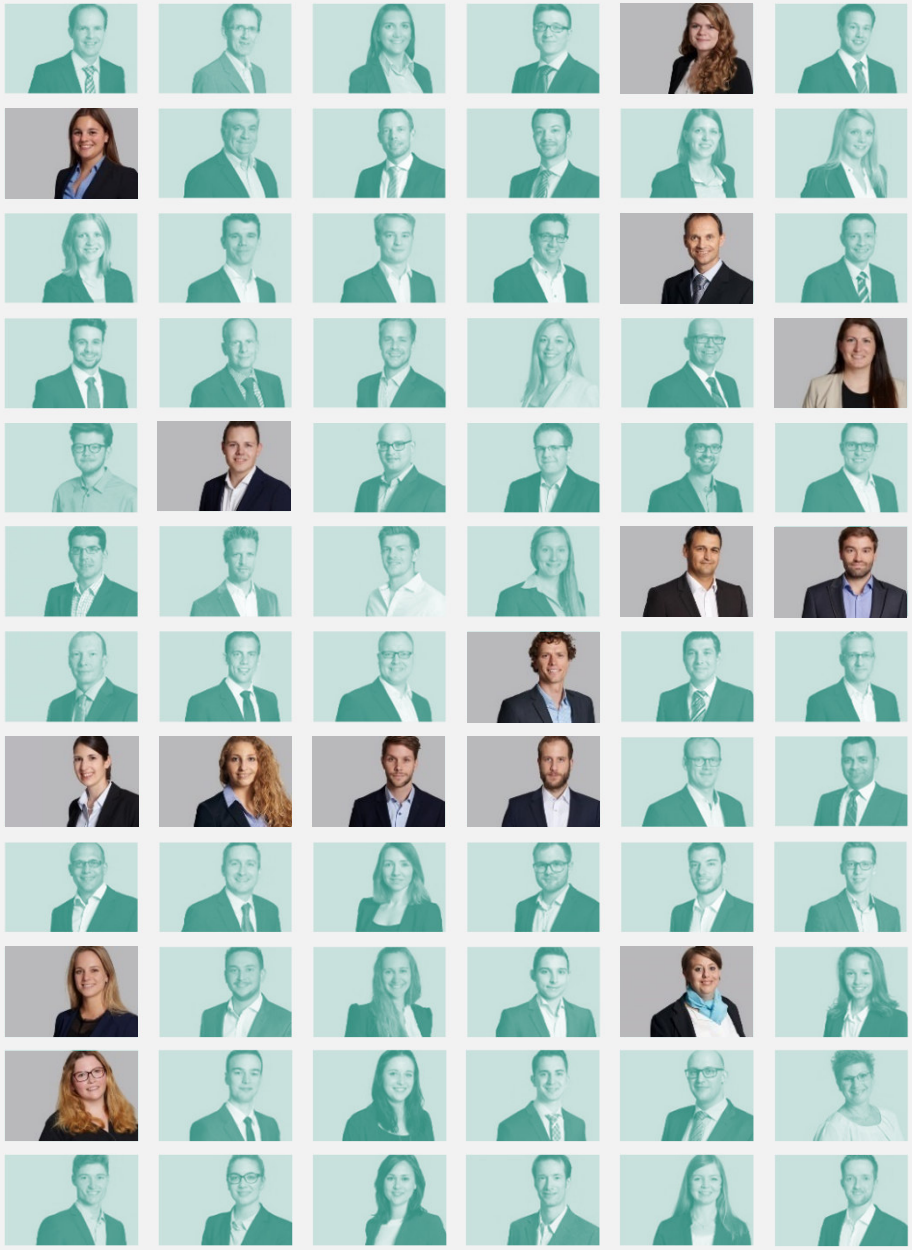
Projektmanagement

Strategieberatung

Prozess- und Organisationsoptimierung

Business Analyse und Requirements Engineering (RE)

Schulung und Training



APP in Kürze

Breit abgestützt, mit schlagkräftigem eHealth Team

- Seit der Gründung im Jahr 1977 stets **unabhängig** und **neutral**
- Standorte in **Bern, Zürich, Basel** und **Luzern**
- Über 70 hochqualifizierte Berater/innen, **methodisch** versiert und **praxisnah**
- Ehrliche «hemdsärmelige» Beratung, in der **Schnittstelle** zwischen IT und Fach
- Wissen, verteilt auf vielen Schultern mit spezifischer Expertise für spezifische Projekte

www.app.ch/health