Cassini I Guiding ahead

Der Migrationsweg zum neuen IT-Grundschutz

Erfahrungen und Hinweise aus der Zertifizierung im ITDZ Berlin

Inna Maliucova I Consultant, Cassini Consulting
Karsten Pirschel I Informationssicherheitsbeauftragter, IT-Dienstleistungszentrum Berlin

Die Referenten

Karsten Pirschel
ITDZ Berlin

- Informationssicherheits-beauftragter
- stlv. Leiter Berlin CERT

Das ITDZ Berlin ist der IT-Dienstleister für die Berliner Verwaltung mit rund 700 Mitarbeiterinnen und Mitarbeitern.

Inna Maliucova
Consultant
Cassini Consulting

- Management- und Organisationsberaterin
- Sicherheitsexpertin

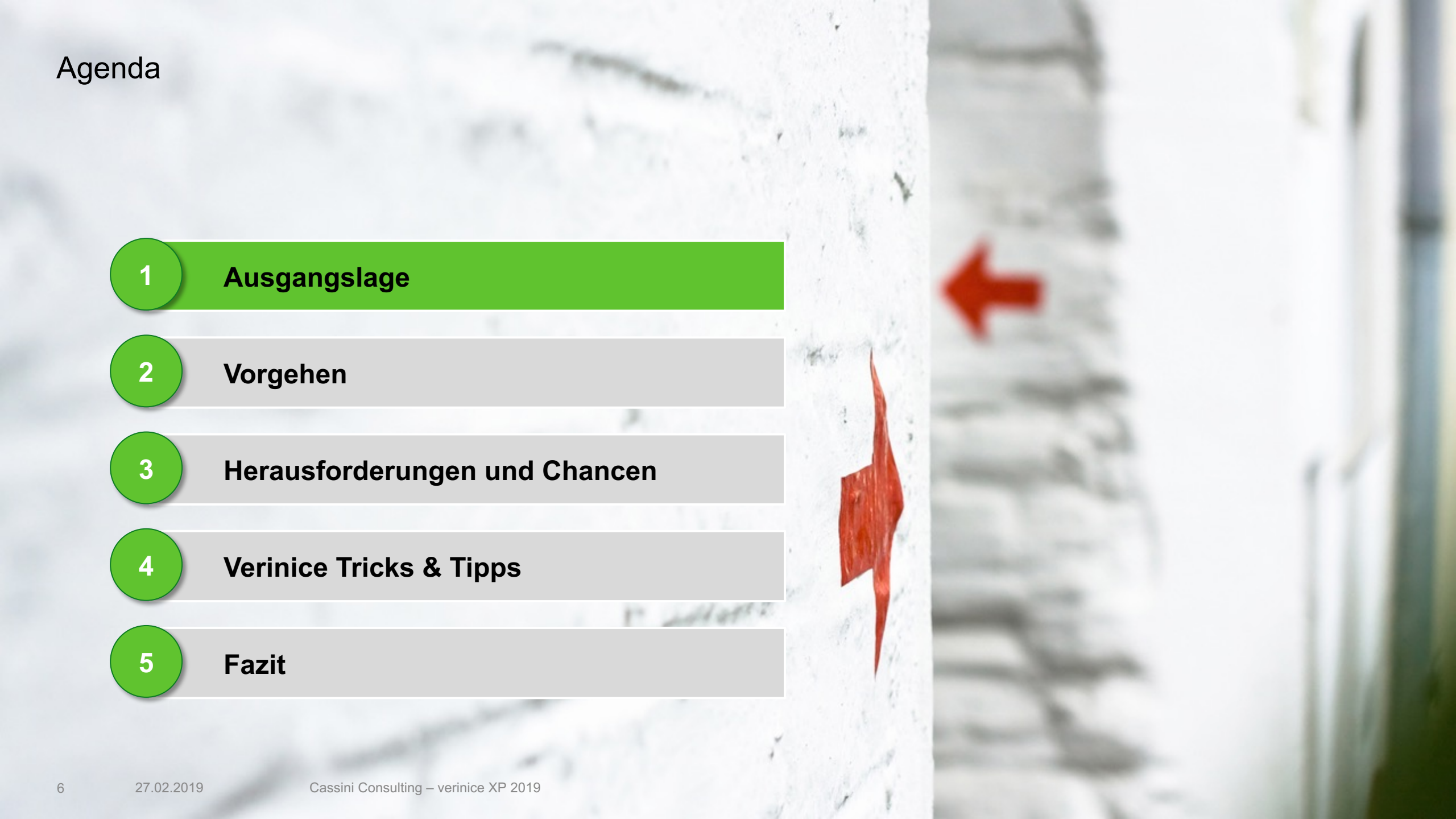
Cassini Consulting ist eine Management- und Technologie-Beratung mit 250 Beraterinnen und Beratern.

Der Weg zum modernisierten Grundschutz

Der Weg zum modernisierten Grundschutz

Agenda

1. **Ausgangslage**
2. **Vorgehen**
3. **Herausforderungen und Chancen**
4. **Verinice Tricks & Tipps**
5. **Fazit**



1. Ausgangslage: Berlin

- Gesetzliche Rahmenbedingungen: EGovG Bln
  - IKT-StS und IKT-Steuerung
  - Grundsätzliche Abnahmepflicht der Berliner Verwaltung beim ITDZ Berlin
  - Bündelung der IT beim ITDZ Berlin,
    primär verfahrensunabhängige IKT (Basis-Infrastruktur)
  - Ausbau des Berlin CERT
  - Verpflichtung zum Aufbau eines ISMS
  - Umsetzung IT-Grundschutz / IT-Sicherheitskonzepte gemäß BSI
- Heterogene IT-Landschaft,
  perspektivische Bündelung beim ITDZ

1. Ausgangslage: ITDZ Berlin

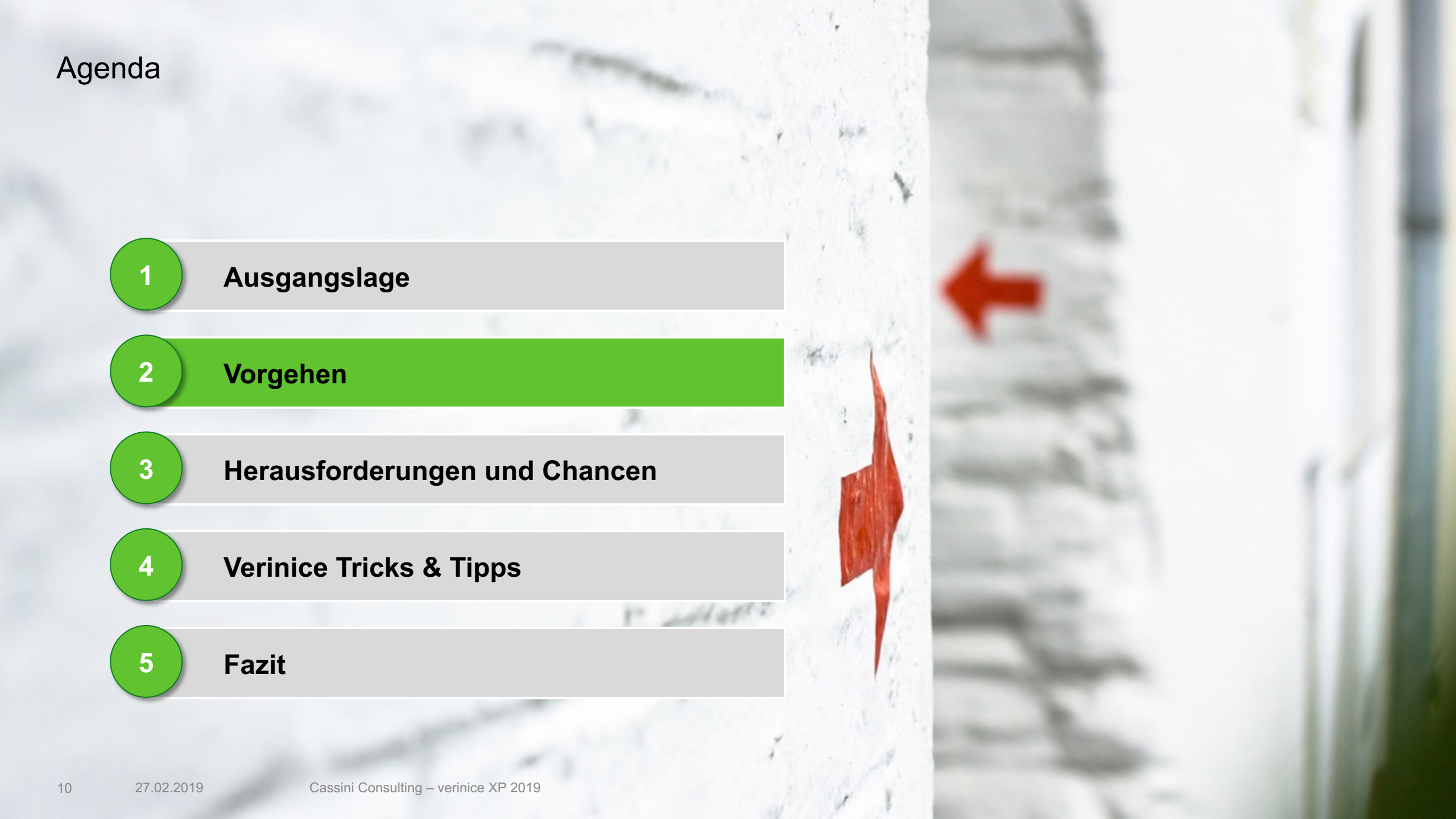
- IT-Dienstleister für die Berliner Verwaltung
- Rund 700 Mitarbeiterinnen und Mitarbeiter
- Betrieb von 2 RZs, 6 ITDZ Liegenschaften, Call-Center, Druckzentrum, Berliner Landesnetz, 600 erschlossene Standorte
- derzeit zahlreiche Großprojekte im ITDZ Berlin
  - BerlinPC
  - Migration der Behörden-IT auf IT-Standardarchitektur
  - Redesign Netzarchitektur
  - Anpassung Organisationsstrukturen
- Laufender Aus- und Aufbau der IT-Infrastruktur
- Aufnahme neuer Kunden

1. Ausgangslage: ITDZ Berlin

- Erste BSI-Zertifizierung des ITDZ im Herbst 2015 nach 100-x
- Scope der BSI-Zertifizierung 2018
  - Vorgehen nach 200-x
  - ISMS
  - Liegenschaften (Dienstgebäude/ RZs)/ Räume
  - zentrale IKT-Basisdienste, darunter u.a. LANs, die Netzwerktechnik zur verschlüsselten Kommunikation, Anbindung an Fremdnetze, private Cloud-Infrastruktur
  - Clients/ Standardarbeitsplatz, MuFus und Server
  - Anwendungen/ Dienste, sowie SAP-Fachverfahren als Beispiel für eine Anwendung mit hohem Schutzbedarf
  - 48 angewendete Bausteine (einfache Zählung)
  - Kernteam: 4 Personen (2 intern / 2 extern)
  - Anlassbezogene Unterstützung weiterer Personen notwendig, insbesondere aus Fachbereichen

Agenda

1. Ausgangslage
2. **Vorgehen**
3. Herausforderungen und Chancen
4. Verinice Tricks & Tipps
5. Fazit



2. Vorgehen: Überblick

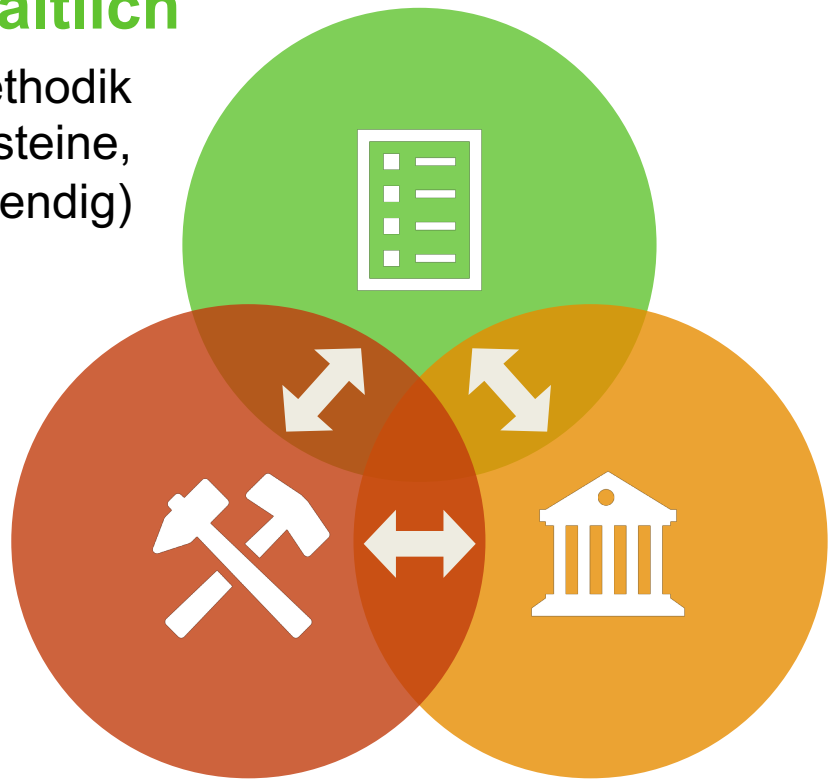
- Umsetzung „Auflagen“ aus Ü-Audit 2017 und neuer Grundschutz
- Arbeit fokussiert auf drei Dimensionen:
  - Inhaltlich
  - Technisch
  - Organisatorisch
- Kommunikation mit Beteiligten (BSI, SerNet, Auditor)
- Kein klassisches Wasserfall-Projektmanagement

Mut haben und anfangen!

2. Vorgehen: Arbeitsfokus

Inhaltlich

neue Systematik, neue Methodik (Risikoanalyse), neue Bausteine, neue Anforderungen (Migration notwendig)



Technisch

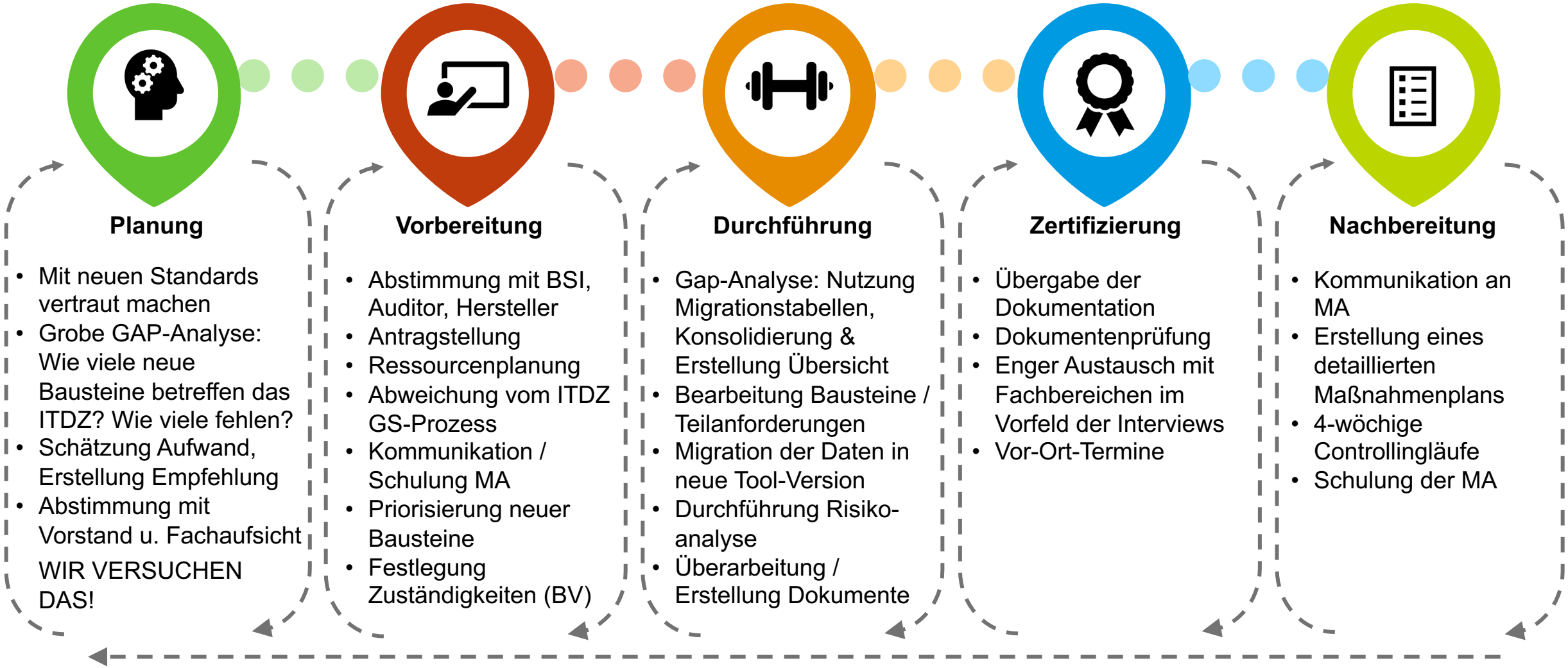
Umsetzung neue Systematik im Tool, Gap- und Risikoanalyse, Tool-Migration

Organisatorisch

Überarbeitung Policies, Sensibilisierung Mitarbeiter, Definition Verantwortlichkeiten

Bei der Umstellung auf den modernisierten Grundschutz mussten wir in drei Dimensionen tätig werden

2. Vorgehen: Vorbereitung der Zertifizierung



Planung

- Mit neuen Standards vertraut machen
- Grobe GAP-Analyse: Wie viele neue Bausteine betreffen das ITDZ? Wie viele fehlen?
- Schätzung Aufwand, Erstellung Empfehlung
- Abstimmung mit Vorstand u. Fachaufsicht

WIR VERSUCHEN DAS!

Vorbereitung

- Abstimmung mit BSI, Auditor, Hersteller
- Antragstellung
- Ressourcenplanung
- Abweichung vom ITDZ GS-Prozess
- Kommunikation / Schulung MA
- Priorisierung neuer Bausteine
- Festlegung Zuständigkeiten (BV)

Durchführung

- Gap-Analyse: Nutzung Migrationstabellen, Konsolidierung & Erstellung Übersicht
- Bearbeitung Bausteine / Teilanforderungen
- Migration der Daten in neue Tool-Version
- Durchführung Risiko-analyse
- Überarbeitung / Erstellung Dokumente

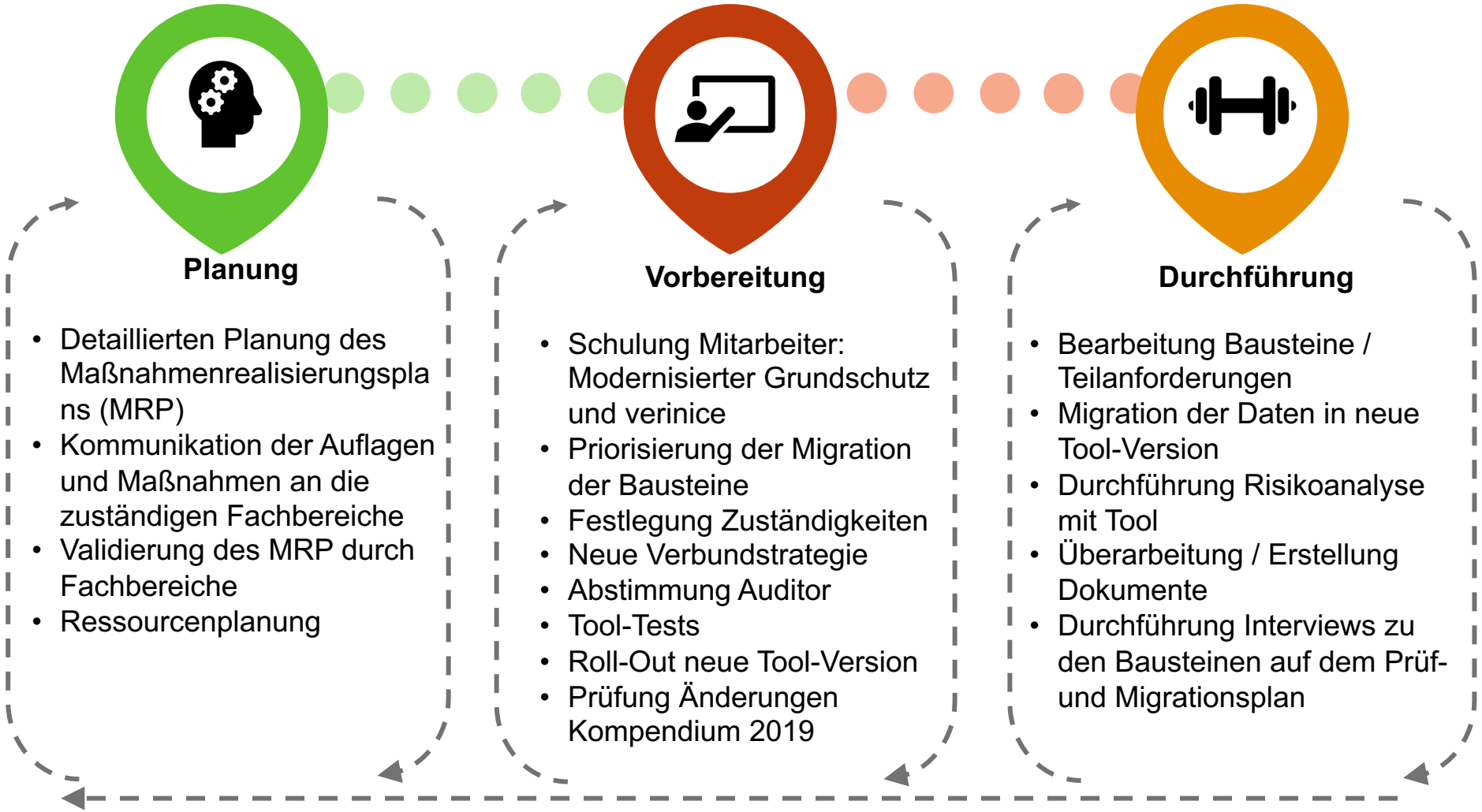
Zertifizierung

- Übergabe der Dokumentation
- Dokumentenprüfung
- Enger Austausch mit Fachbereichen im Vorfeld der Interviews
- Vor-Ort-Termine

Nachbereitung

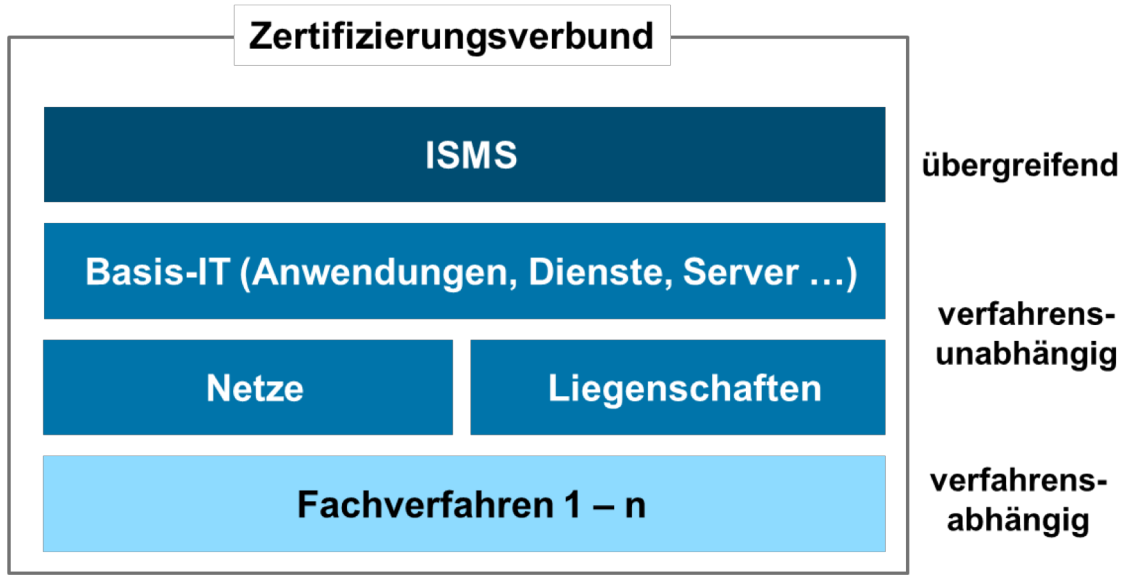
- Kommunikation an MA
- Erstellung eines detaillierten Maßnahmenplans
- 4-wöchige Controllingläufe
- Schulung der MA

2. Vorgehen: Nach dem Audit ist vor dem Audit



2. Vorgehen: Verbundstrategie

- Aufteilung in 4 + n Verbünde
- Klare Definition von Rollen und Rechten
- Festlegung der Arbeitsebene: Maßnahmen vs. Anforderungen
- Entscheidung Umgang mit BSI Drafts
- Festlegung der Detailtiefe der Dokumentation
- Formulierung der internen Modellierungsvorgaben (z.B. IDs, Tags)



→ Bessere Übersichtlichkeit und Nachvollziehbarkeit

→ Vermeidung von Pflege an mehreren Stellen

→ Vereinfachung der Erstellung von fachverfahrensspezifischen SiKos

Die Verbundstrategie sollte gut durchdacht sein – weniger ist nicht immer mehr!

2. Vorgehen: Risikoanalyse – viele Clicks führen zum Ziel

- Neue 200-3 Methodik
  - **Zeitaufwändig**: Alle Zielobjekte mit hohem Schutzbedarf (in mindestens einem Wert) + Zielobjekte, die mit den existierenden Bausteinen des IT-Grundschutzes nicht modelliert werden können (fehlende Bausteine) > 90%
  - **Methodische Unklarheiten**:

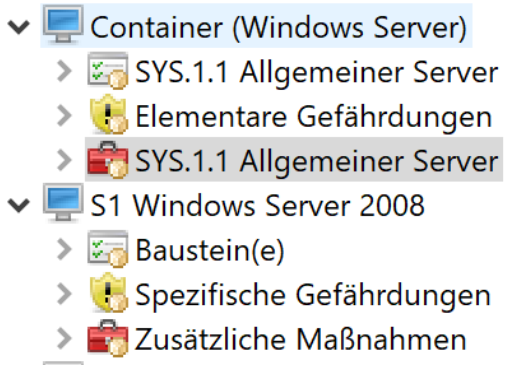
Im vorliegenden BSI-Standard 200-3 ist die Risikoanalyse zweistufig angelegt. In einem ersten Schritt wird die in Kapitel 4 erstellte Gefährdungsübersicht systematisch abgearbeitet. Dabei wird für jedes Zielobjekt und jede Gefährdung eine Bewertung unter der Annahme vorgenommen, dass bereits Sicherheitsmaßnahmen umgesetzt oder geplant worden sind (siehe Beispiele in Kapitel 5). In der Regel wird es sich hierbei um Sicherheitsmaßnahmen handeln, die aus den Basis- und Standard-Anforderungen des IT-Grundschutz-Kompendiums abgeleitet worden sind. An die erste Bewertung schließt sich eine erneute Bewertung an, bei der Sicherheitsmaßnahmen zur Risikobehandlung betrachtet werden (siehe Beispiele in Kapitel 6). Durch einen Vorher-Nachher-Vergleich lässt sich die Wirksamkeit der Sicherheitsmaßnahmen prüfen, die zur Risikobehandlung eingesetzt worden sind.

→*"Risiko ohne zusätzliche Maßnahme"* = Nachdem die BSI Basis- und Standard Anforderungen umgesetzt wurden

→Arbeiten auf der Maßnahmenebene zahlt sich aus

2. Vorgehen: Risikoanalyse – viele Clicks führen zum Ziel

- **Tool Umsetzung:** Bei Arbeiten auf mehreren Ebenen ist einfach den Überblick zu verlieren bzw. Fehler zu machen
- **Komplexität**: Nutzung der Gruppierung (wo möglich): Anlegen von „Container“-Zielobjekten

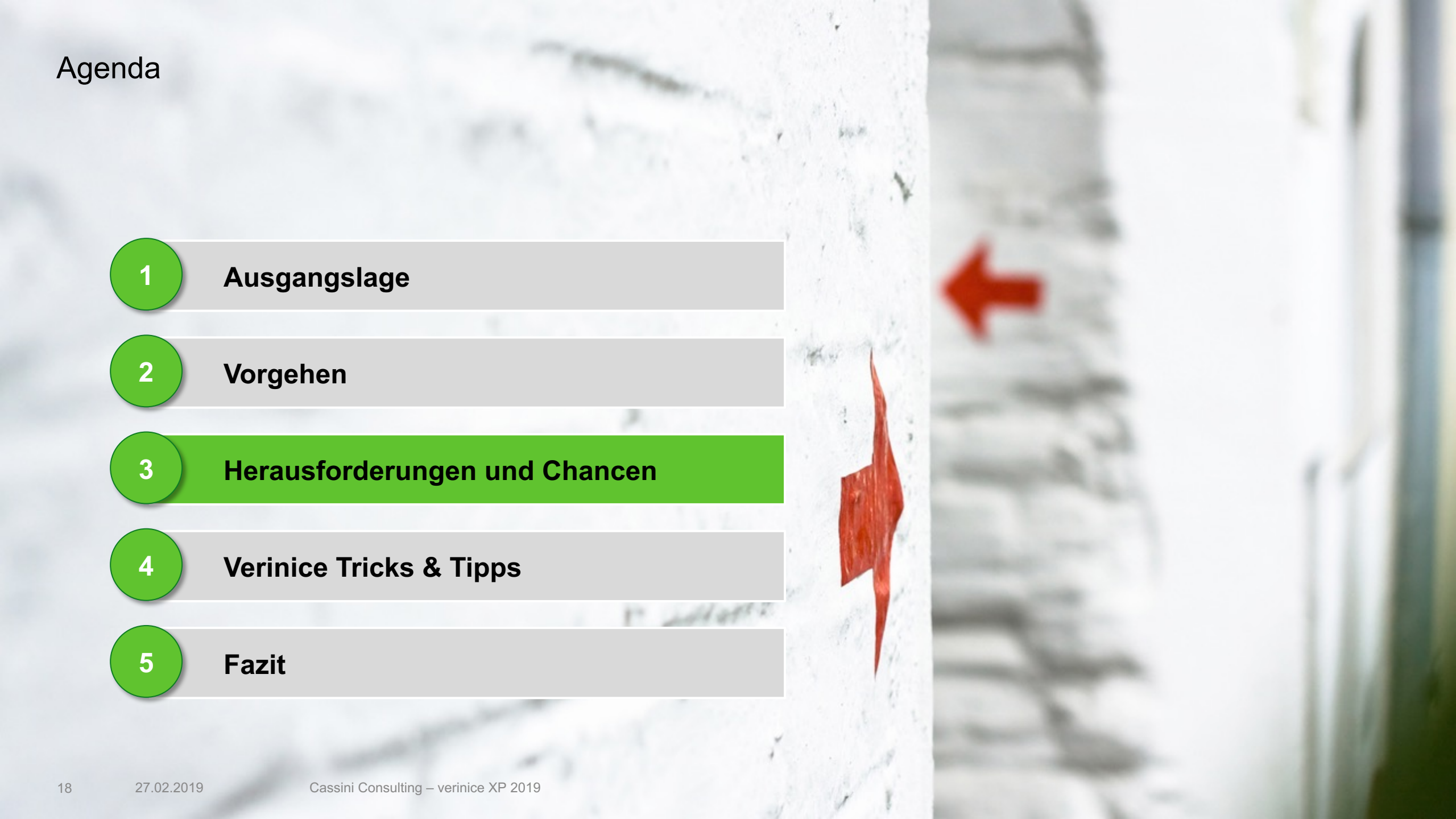


→ Interne Dokumentation der Vorgehensweise empfehlenswert

→ iteratives Vorgehen mit Qualitätssicherungsschleifen

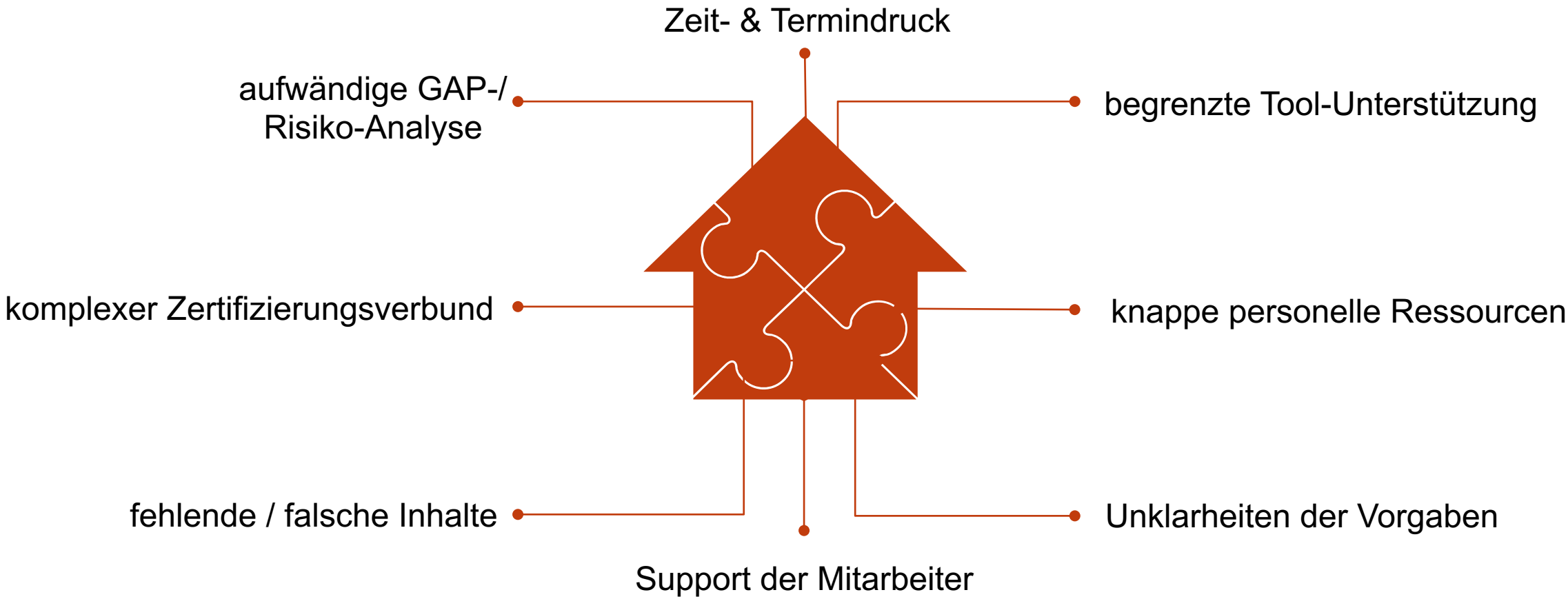
Planen Sie längere Zeit für die Risikoanalyse ein!

Agenda



1. **Ausgangslage**
2. **Vorgehen**
3. **Herausforderungen und Chancen**
4. **Verinice Tricks & Tipps**
5. **Fazit**

3. **Herausforderungen** und Chancen



3. Herausforderungen und **Chancen**

Intensive Auseinandersetzung mit neuem Grundschutz

Steigerung Top-Management Support

Steigerung Mitarbeiter-Verständnis

Berücksichtigung IT-Grundschutz bei neuen Vorhaben

Gute Zusammenarbeit mit BSI

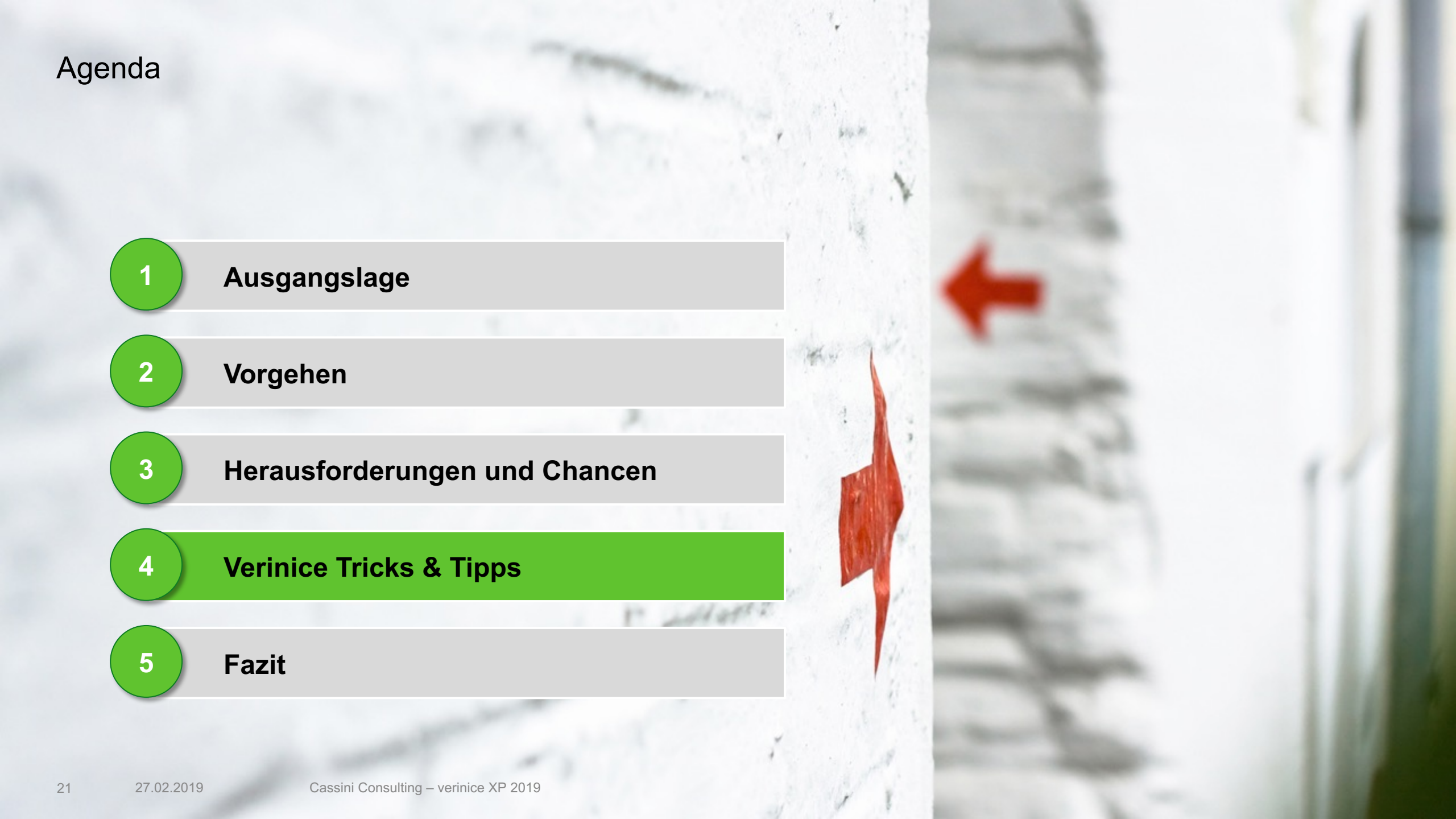
Anpassung Security Policy-Struktur

Gute Zusammenarbeit mit SerNet

Bearbeitung von „Prio3-Themen“

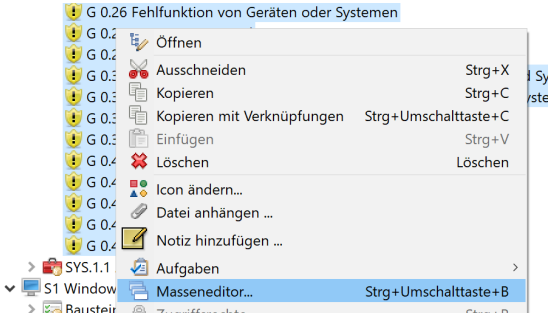
Agenda

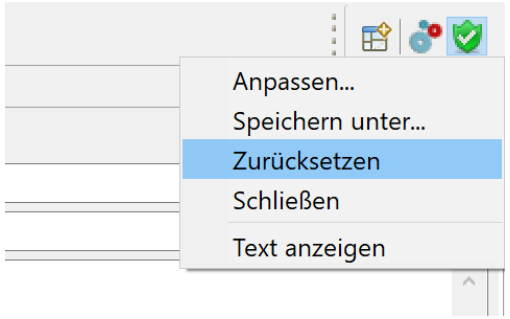
1. **Ausgangslage**
2. **Vorgehen**
3. **Herausforderungen und Chancen**
4. **Verinice Tricks & Tipps**
5. **Fazit**



4. Verinice Tricks & Tipps

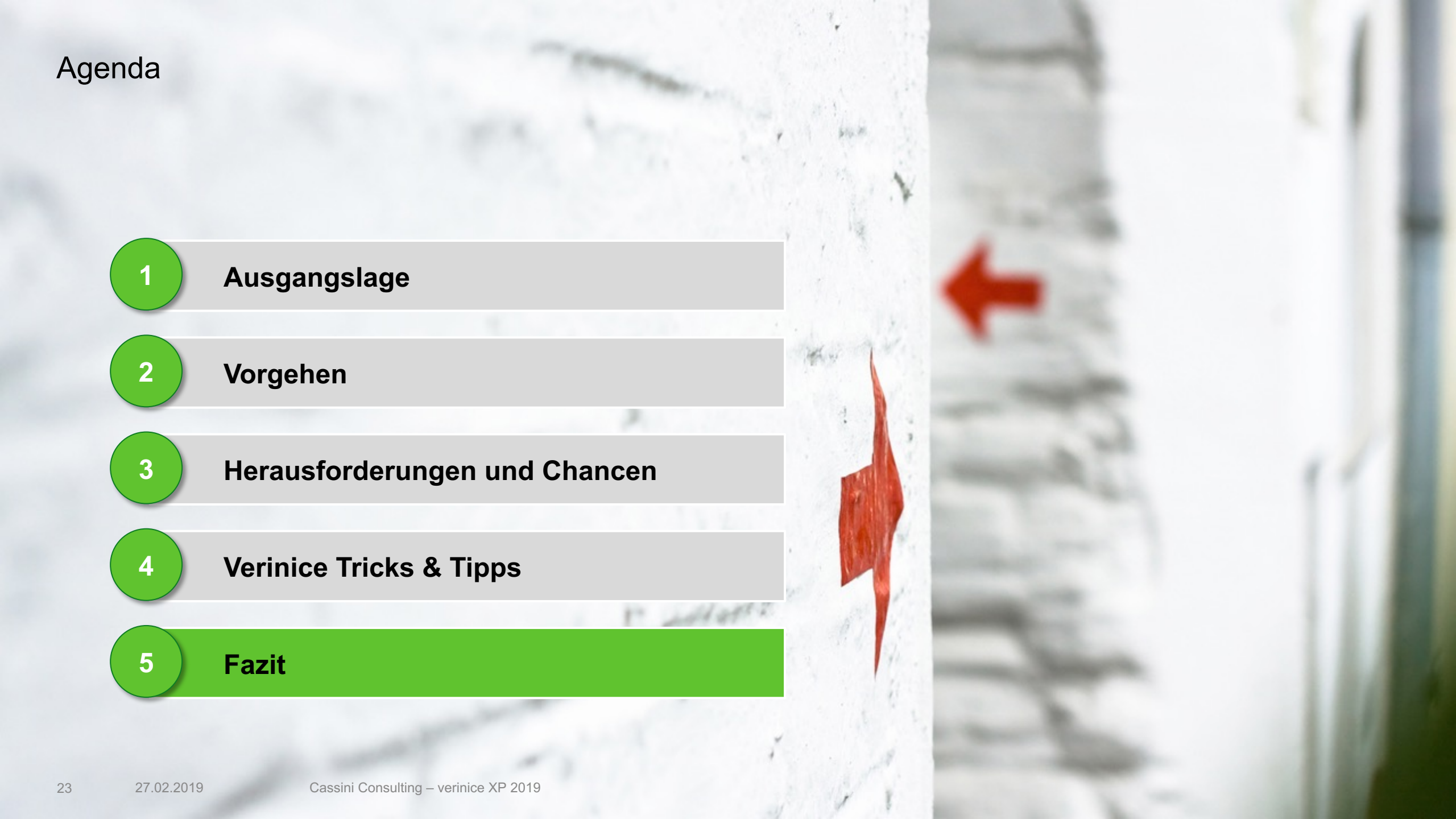
- Es gibt kein Richtig oder Falsch
- Masseneditor (vor allem bei der Risikoanalyse) ist oft hilfreich!
  - Leider fehlt (noch) der Konsolidator
- Setzen Sie die Gruppierungen mit Bedacht!
- Arbeiten auf der Maßnahmenebene zahlt sich aus (z.B. bei der Risikoanalyse), auch wenn dies Mehraufwand bedeutet
- Die Funktion „View zurücksetzen“ braucht man öfter als man denkt
- Aktualisierung durchführen, sofern Informationen vermisst werde
- Dropdown Felder können leicht verstellt werden
- Ansichten einstellen (irrelevante Felder ausblenden)
- Nutzung mehrere Versionen parallel möglich / DB anpassen
- Nutzen sie die neuste Version von verinice und Kompendium





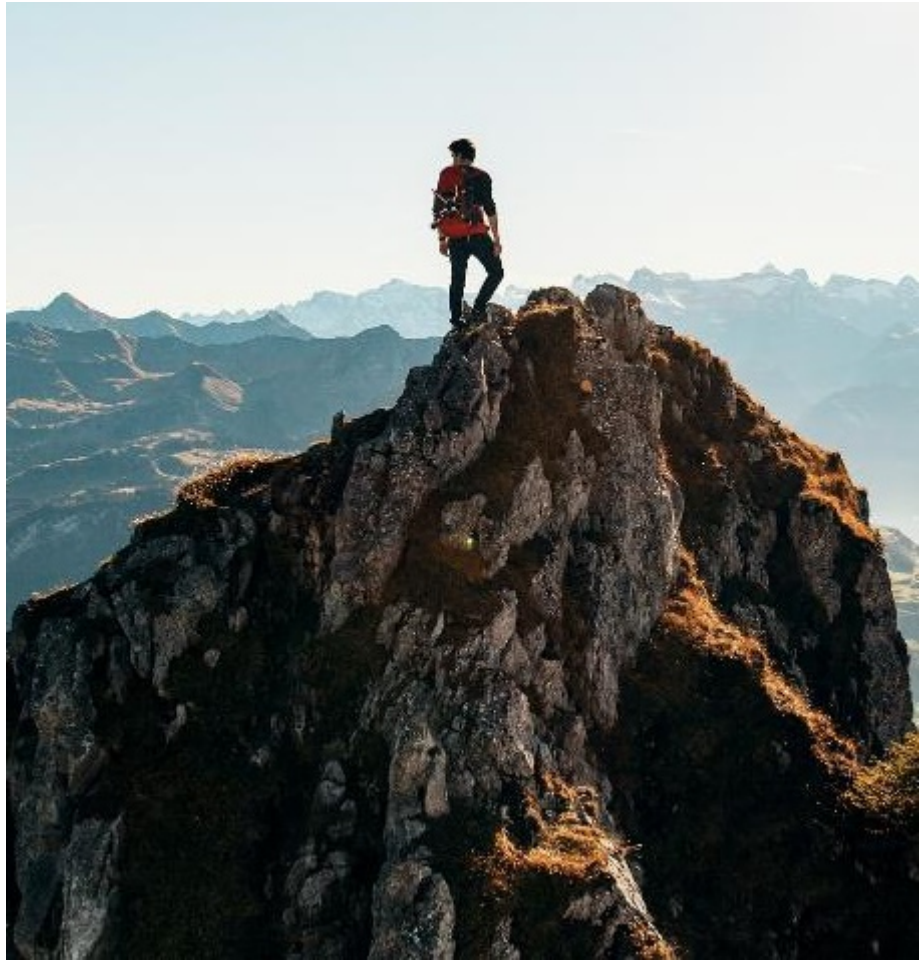
Agenda

1. Ausgangslage
2. Vorgehen
3. Herausforderungen und Chancen
4. Verinice Tricks & Tipps
5. Fazit



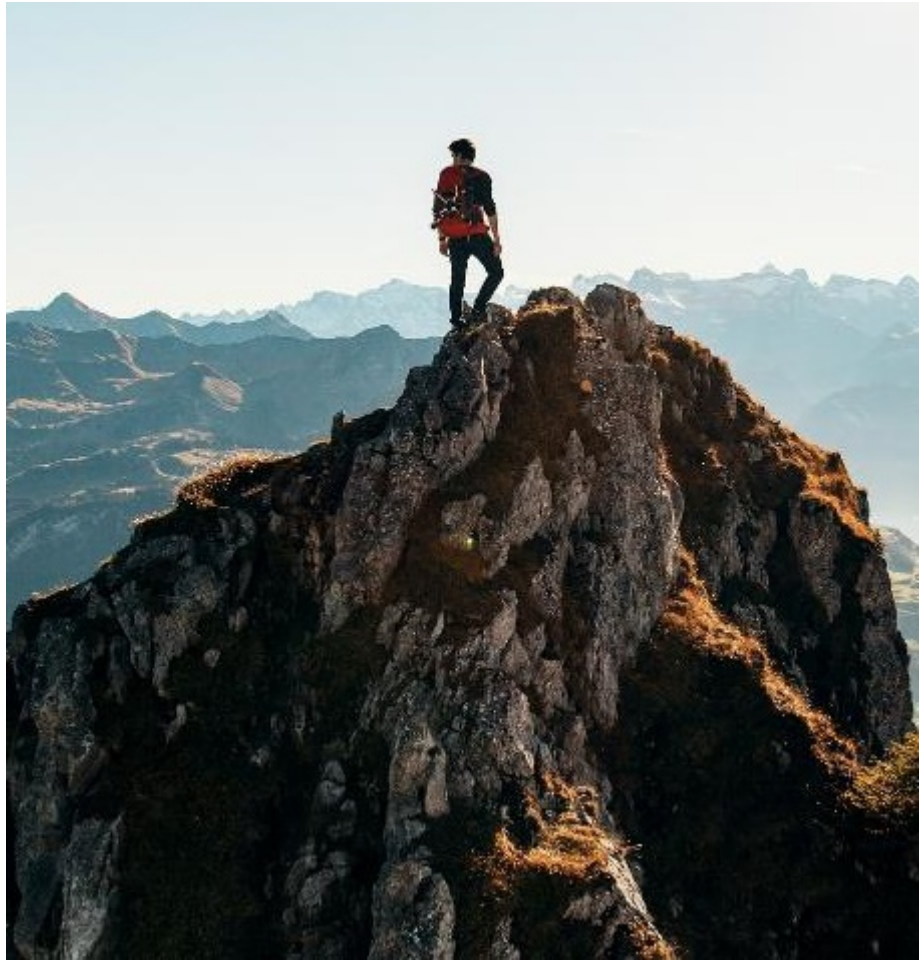
5. Fazit aus Migration

- **Handhabbaren Zertifizierungsverbund wählen**
  - richtige Balance finden
  - für Bedeutung der Zertifizierung / Umfang sensibilisieren
  - Migrationsaufwände großzügig einplanen
- **Zusammenarbeit und Kommunikation ist die Basis für alles!**
  - Auditor, BSI und Tool-Hersteller als Partner verstehen
  - Security als Service: Inhouse Beratung etablieren
  - Sicherheitskoordinatoren in Abteilungen etablieren
- **Vorhaben sind Projekte und müssen eng gesteuert werden**
  - Stabile Projektorganisation notwendig
  - Umsetzung begleiten / Nachweise prüfen
  - Priorisierung und Fokussierung
- **Beteiligte vor Umsetzung inhaltlich abholen**



5. Fazit : Allgemeine Empfehlungen

- **Inhaltliche Herausforderungen bewusst machen**
  - Sicherstellung Schutzniveau / Nachweisbarkeit Sicherheitsmaßnahmen bei Nutzung von Produkten Dritter
  - Patch- und Lifecycle-Management
  - Beschaffungen
  - Sicherheitsmeldungen und Sicherheitslücken
- **Agile und proaktive Strukturen etablieren**
  - Regelmäßige Netzscans
  - Prozesse zur Steuerung und Bearbeitung von Security Incidents etablieren



4. Fazit

Quelle: ITDZ Berlin

Es hat Kraft gekostet, es hat sich aber gelohnt!

Cassini Consulting
Niederlassung Berlin

Inna Maliucova

Oberwallstraße 24
10117 Berlin
Deutschland
T +49 (0)151 11 45 93 74
F +49 (0) 30 50 10 14 14
inna.maliucova@cassini.de
visit www.cassini.de