Hallo!

Von 0 auf Zertifizierung?

Wir haben ein Problem - wirklich?

Agenda

Agenda

1. Kurze Vorstellung
2. Was sind Deine Vorteile einer 27001-Zertifizierung?
3. Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?
4. Wie sollte/kann Dein Handbuch nach ISO 27001 aufgebaut sein?
(Demonstration via Screensharing)
5. Kleine Hilfen

Kurze Vorstellung

Mike Peter

Mike Peter
Sachverständiger für Datenschutz
BDSF MITGLIED

Sachverständiger für Datenschutz | Externer Datenschutzbeauftragter

Externer ISMS Security Officer (Professional) nach ISO/IEC 27001 - ISB

Externer CCISO (Chief Information Security Officer)

Certified Information Systems Security Professional (CISSP)

Auditor

ISO/IEC 27001 Compliance / - Audits

DiGA-Compliance / - Audits

EU Representative for data privacy for companies outside the EU

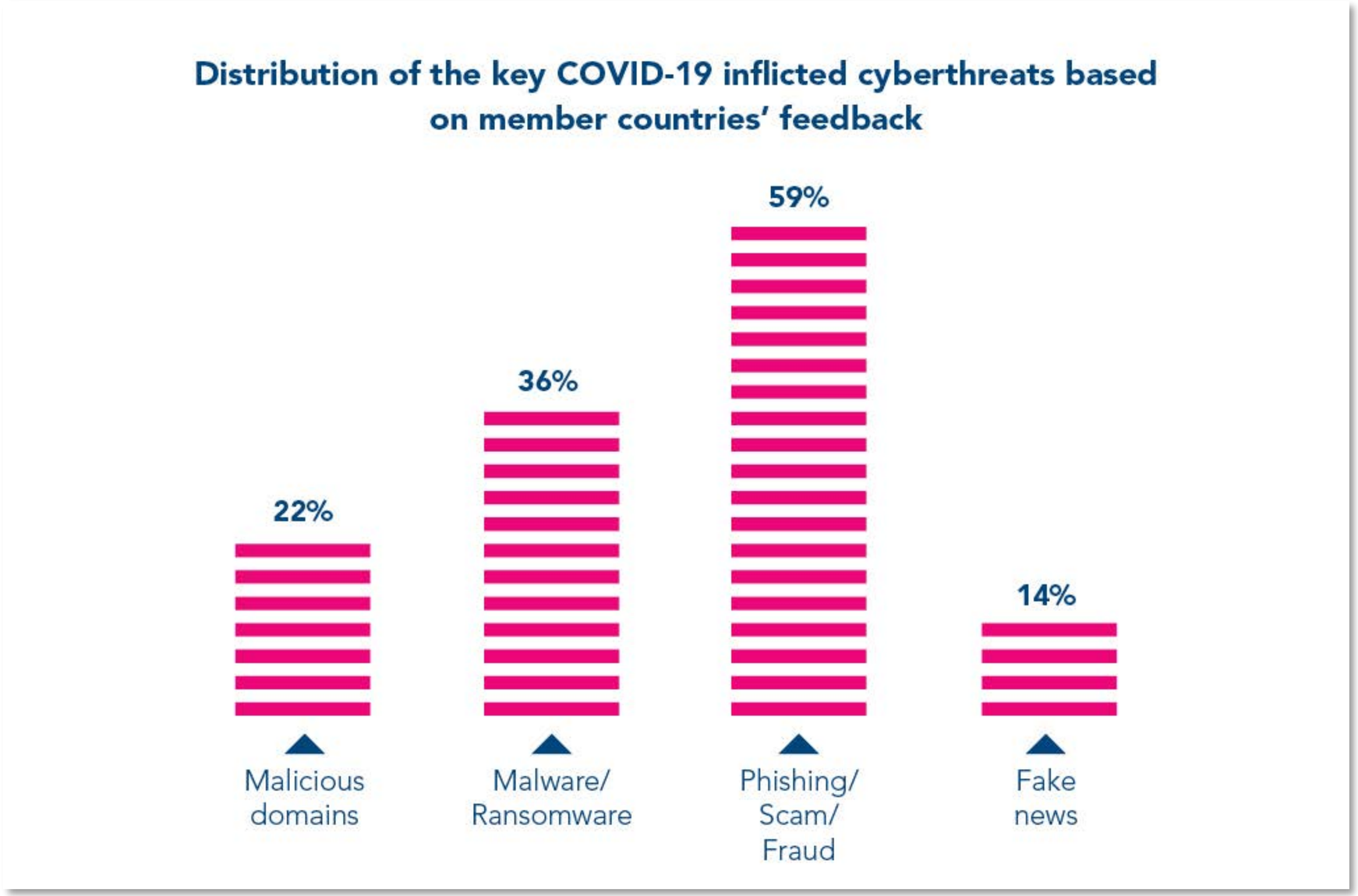
Global Startup Mentor (Digital Health)

Member of European Association of Data Protection Professionals

Was sind Deine Vorteile einer 27001-Zertifizierung?

Aktuelle Lage

Was sind Deine Vorteile einer 27001-Zertifizierung? Aktuelle Lage



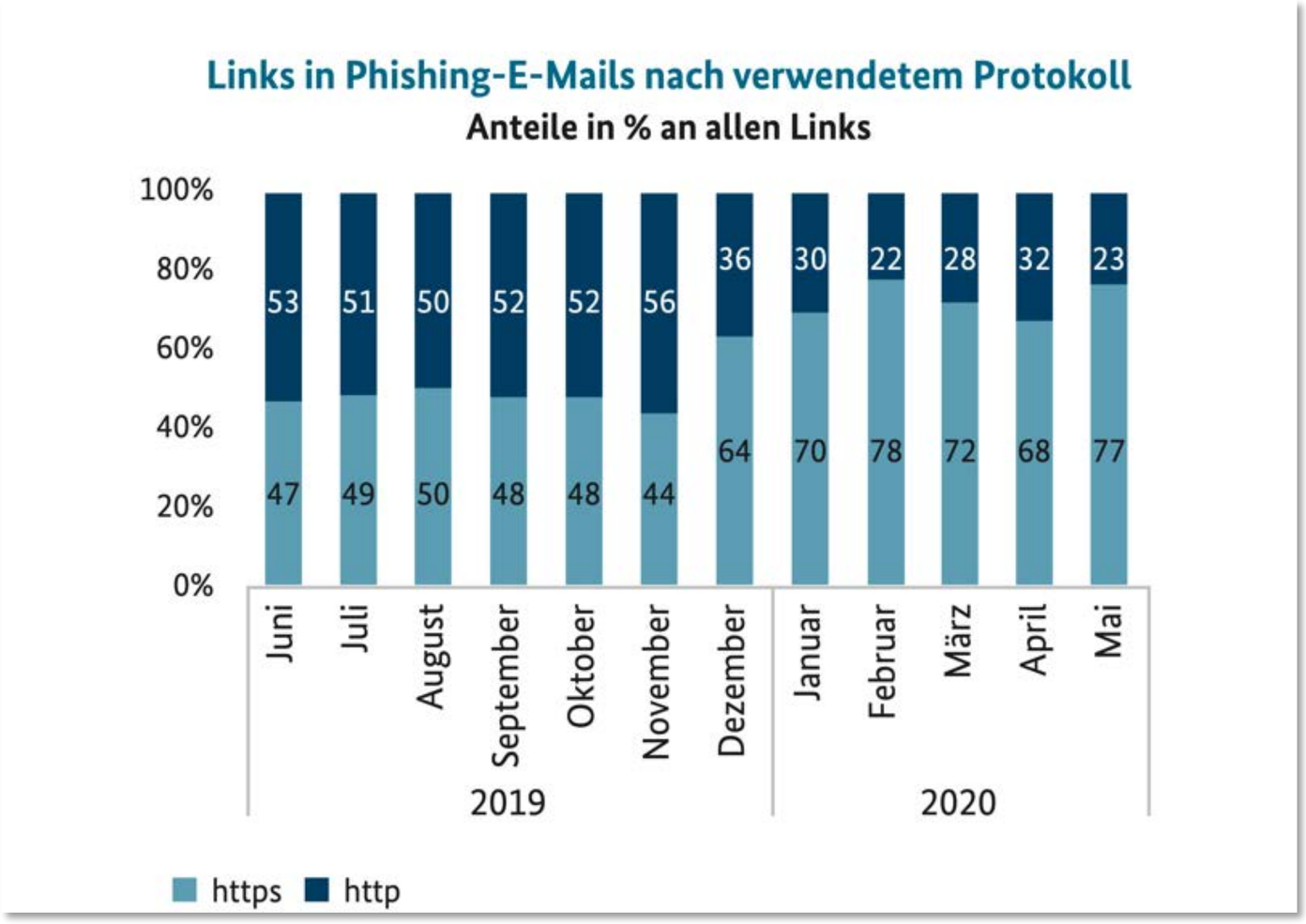
Quelle: Interpol

yourprivacyfirst.de

Was sind Deine Vorteile einer 27001-Zertifizierung? Aktuelle Lage

Quelle: Agentur der Europäischen Union für Cybersicherheit

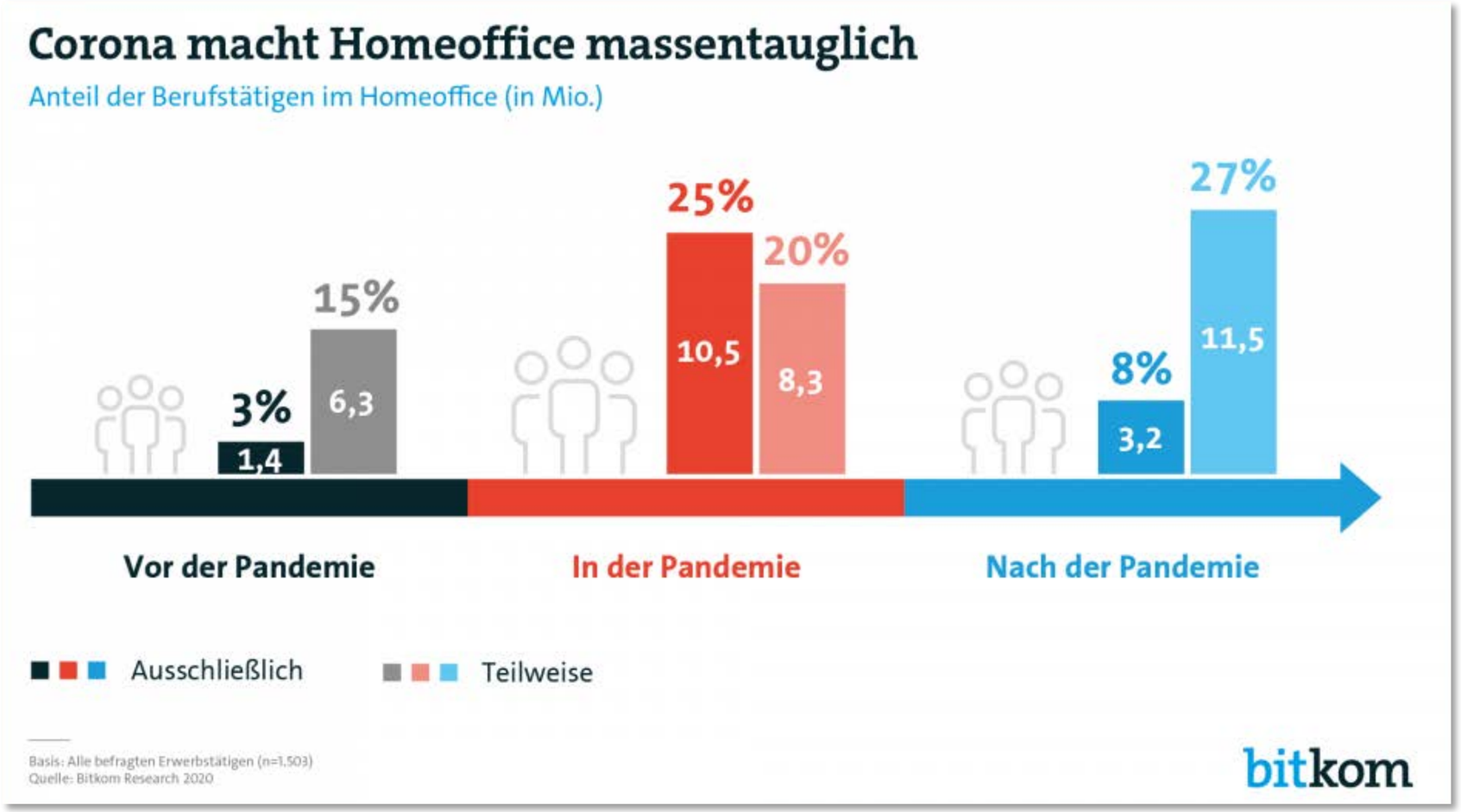
Was sind Deine Vorteile einer 27001-Zertifizierung? Aktuelle Lage



Quelle: BSI – „Die Lage der IT-Sicherheit in Deutschland 2020“

yourprivacyfirst.de

Was sind Deine Vorteile einer 27001-Zertifizierung? Aktuelle Lage



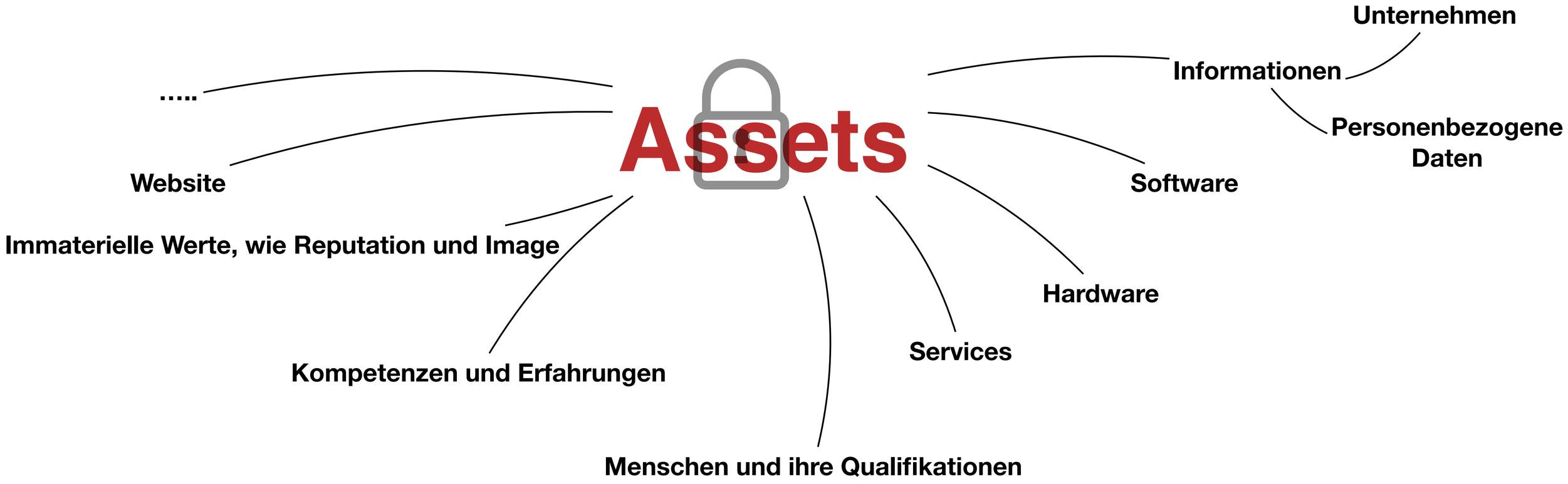
Quelle: bitkom

Was sind Deine Vorteile einer 27001-Zertifizierung? Aktuelle Lage

Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten					
1.	Informations-sicherheits- und Service-Management	Hat der Hersteller der digitalen Gesundheitsanwendung ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO 27000-Reihe oder BSI-Standard 200-2 oder ein vergleichbares System umgesetzt und kann auf Verlangen des Bundesinstituts für Arzneimittel und Medizinprodukte ein entsprechendes anerkanntes Zertifikat oder einen vergleichbaren Nachweis vorlegen?			Das Antragsdatum liegt vor dem 1. Januar 2022.

Was sind Deine Vorteile einer 27001-Zertifizierung?

Was sind Deine Vorteile einer 27001-Zertifizierung?



yourprivacyfirst.de

Was sind Deine Vorteile einer 27001-Zertifizierung?

Die 13485 und die 27001

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

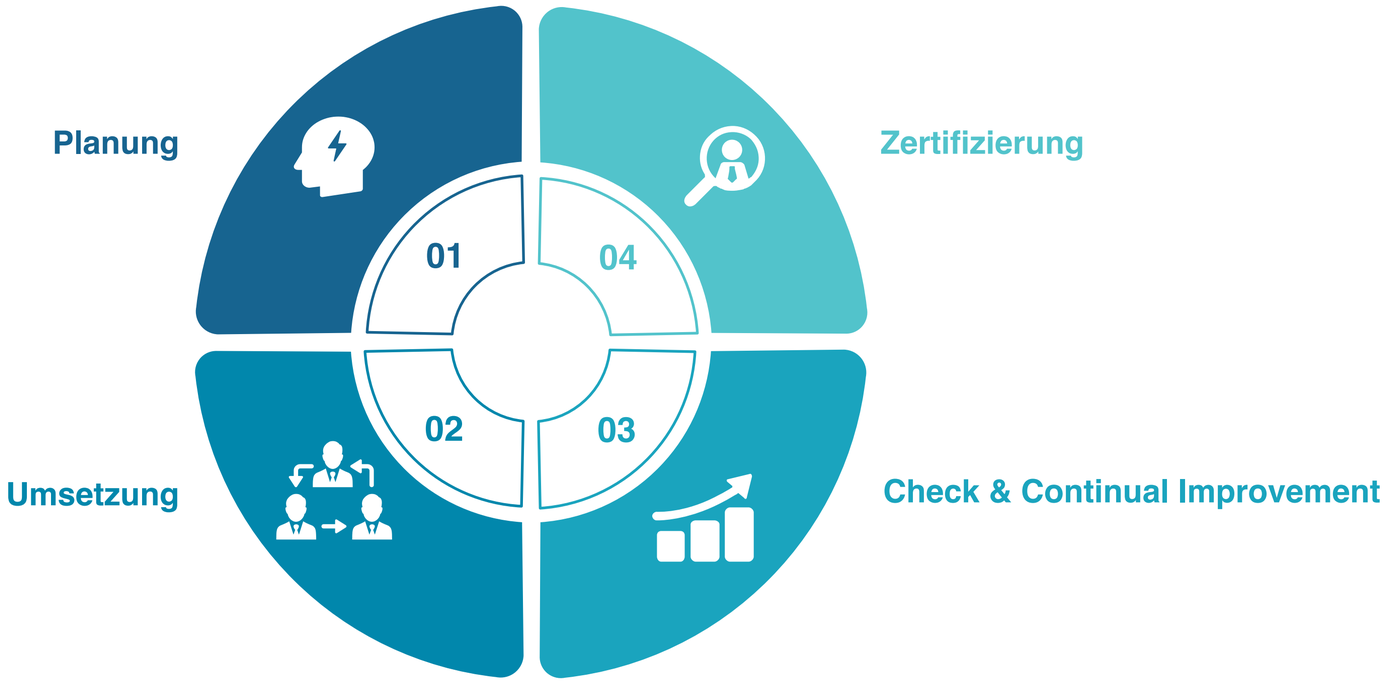
Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

ca. 10 -12 Monate

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen



yourprivacyfirst.de

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

Festlegen der Timeline/Ziele
Festlegen des Scopes
Erstellen der ISP
Erklärung zur Anwendbarkeit (SoA, Annex A)
Festlegen der Verantwortlichkeiten im Projekt
Festlegen der Tools
Unterstützung des Managements
(Ziele, Verantwortlichkeiten im Unternehmen, Politik,
Rollen: DSB, ISB)

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

Umsetzung

GAP-Analyse

Kick off

Assets identifizieren und managen:
Geschäftsbereiche
Prozesse
Werte und Anforderungen identifizieren
Schnittstellen (Dienstleister, Provider, interne Bereiche…..)
interne und externe Anforderungen
weitere Stakeholder
Risikomanagement aufbauen
(Kontext: Scope und Assets)
Schutzbedarfe definieren
Richtlinien erstellen
KPIs erstellen

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

Check & Continual Improvement

- Interne ISMS-Audits
- Reviews
- Externe Audits
- CAPA
- Management-Review
- Vor-Audit

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

Zertifizierung

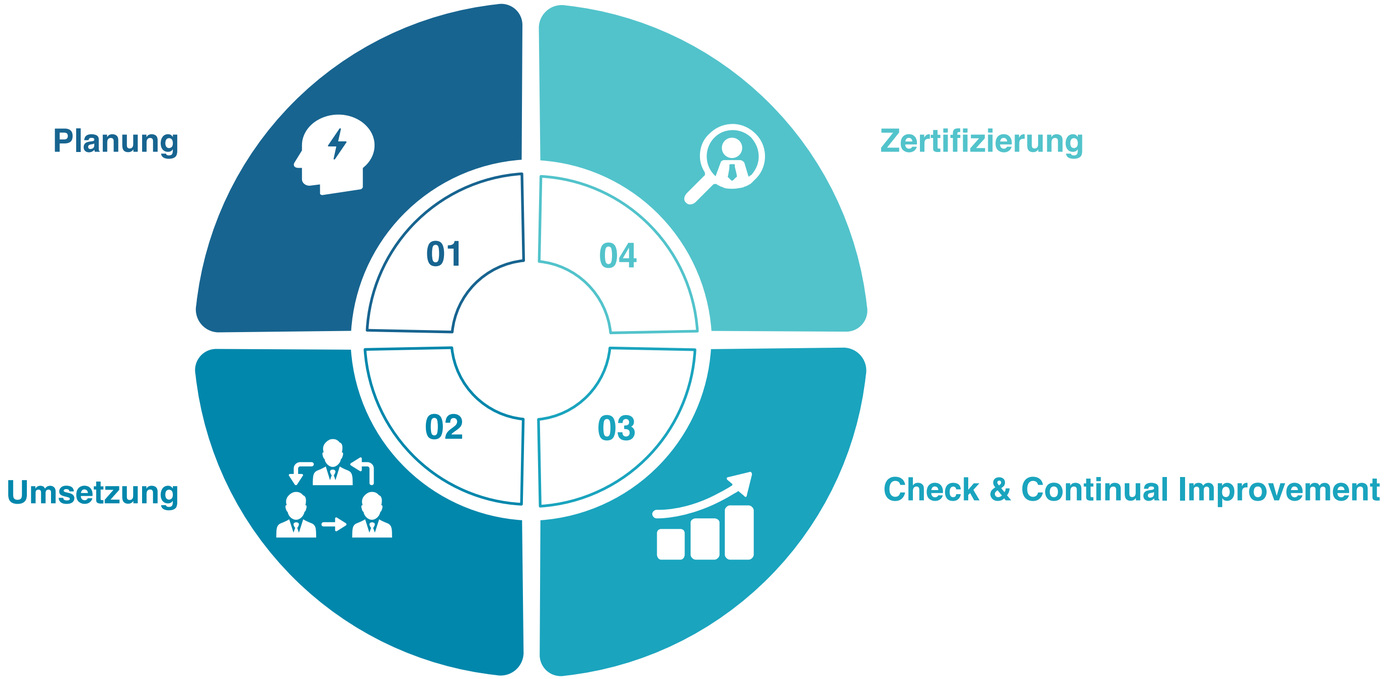
Erstzertifizierung → **Überwachungs-audit** → **Überwachungs-audit** → **Rezertifizierung**

yourprivacyfirst.de

Wie sollte/kann Dein Projektplan für die ISO 27001-Implementierung aussehen?

4 Phasen

ca. 10 -12 Monate



yourprivacyfirst.de

Wie sollte/kann Dein Handbuch nach ISO 27001 aufgebaut sein?

Wie sollte/kann Dein Handbuch nach ISO 27001 aufgebaut sein?

Vorgaben an die Dokumentation

„Die geforderte dokumentierte Information muss gelenkt werden, um sicherzustellen, dass sie…

- verfügbar und für die Verwendung geeignet, wo und wann sie benötigt wird; und
- angemessen geschützt wird (z.B.vor Verlust der Vertraulichkeit, unsachgemäßem Gebrauch oder Verlust der Integrität)“

Vorgaben an die Dokumentation

„Zur Lenkung dokumentierter Information muss die Organisation, falls zutreffend, folgende Tätigkeiten berücksichtigen:

- Verteilung, Zugriff, Auffindung und Verwendung;
- Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit;
- Überwachung von Änderungen (z.B. Versionskontrolle); und
- Aufbewahrung und Verfügung über den weiteren Verbleib“

…und so kann das aussehen:

Kleine Hilfe(n)

Kleine Hilfe(n

Checkliste ISO 27001

- ⇨ Die genaue Organisation Deines Unternehmens ist aufgeschlüsselt (z.B. als Organigramm).
- ⇨ Der Geltungsbereich Deines ISMS (insbesondere für die Stakeholder) ist festgelegt.
- ⇨ Eine Erklärung zur Anwendbarkeit (engl.: Statement of Applicability, SoA) ist angelegt, worin die begründeten Entscheidungen zur Umsetzung der Maßnahmen dokumentiert sind.
- ⇨ Eine Umfeldanalyse für die Einordnung des ISMS im Unternehmen wurde durchgeführt.
- ⇨ Eine Anforderungsanalyse hinsichtlich der jeweiligen Interessengruppen (Stakeholder) wurde durchgeführt.
- ⇨ Eine Übersicht aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen, die einen Einfluss auf die Informationssicherheitsstrategie und das ISMS haben, wurde zusammengestellt.

- ⇨ Die Geschäftsziele und Anforderungen im Zusammenhang mit der Informationssicherheitspolitik im Unternehmen ist klar definiert und dokumentiert.
- ⇨ Eine konkrete Informationssicherheitsstrategie ist festgelegt.
- ⇨ Das „Top-Management“ wurde definiert, welches für die Steuerung des ISMS der zu schützenden Organisation verantwortlich ist und über den Ressourceneinsatz entscheidet.
- ⇨ Eine Informationssicherheitsleitlinie (engl. Infor- mation Security Policy) ist implementiert.

- ⇨ Du besitzt ein dokumentiertes Risikobewertungsverfahren.
- ⇨ Auch eine umfassende Dokumentation zum Risikobeurteilungsprozess und

Kleine Hilfe(n)

#	Threats	Vulnerabilities	Explanation of the risk	Safeguard	ISO 27001 Annex A Control	Explanation of the safeguard
1	Theft of asset / Data	Inadequate storage	A device left on the desk, or in another unsecure place, when unattended can easily be picked up by an unauthorized person.	Use lockable filing cabinets to increase the difficultly of unauthorized access to the device.	A.11.2.6 - Security of equipment and assets off-premises	When working from home, it is not only important to establish that information is protected – equipment must be physically safe at all times.
2	Theft of asset / data	Free access to working area	A workspace where everyone can freely walk in increases the chance of the device being stolen.	Work in a separate room with a lockable door.	A.11.1.1 - Physical security perimeter A.11.1.2 - Physical entry controls	A dedicated space for work at home not only helps one focus on his/her job, but also on protecting information and equipment.

Kleine Hilfe(n)

Fördergelder

Kleine Hilfe(n)

hello@yourprivacyfirst.de

?

Danke!