PRISM 4 ISO ISO 27001 Fact Sheet

Kosten der ISO 27001-Zertifizierung & PRISM 4 ISO

- Direkte Kosten
  - Lizenzen
    - Lizenz PRISM 4 ISO: 3.995 EUR
    - AI Komponente - u-know: 1.500 EUR
    - Technischer Support: 1.600 EUR
  - Implementierung
    - Premium Support für Implementierung (24 PT/3 Monate): 39.750 EUR
  - Zertifizierung
    - ISO 27001 Testierung durch Wirtschaftsprüfer: 17.550 EUR
  - Gesamtkosten der Zertifizierung: 64.395,00 EUR
    - zzgl. gsetzlicher MwSt. von 19%
- Indirekte Kosten
  - Interner Ressourcenaufwand für Umsetzung
  - Zeitaufwand für Audits & Dokumentation
  - Anpassung bestehender IT-Sicherheitsmaßnahmen
- Einsparungen durch PRISM 4 ISO
  - Schnellere Umsetzung & weniger interne Ressourcen
  - Reduzierung von Compliance-Risiken
  - Wettbewerbsvorteil durch Zertifizierung

Kundenerfahrungen

- schnelle und präzise Umsetzung
- strukturiertes Vorgehen
- SECaaS kommt mit einem klaren Plan
- strukturierte Prozesse

Implementierung von PRISM 4 ISO & ISO 27001-Zertifizierung

- Schritte zur Einführung & Zertifizierung
  - Phase 1: Analyse & Planung
    - Gap-Analyse & Statusbewertung
    - Definition des Scopes & Projektplanung
  - Phase 2: Umsetzung der Anforderungen
    - Dokumentation von Richtlinien & Verfahren
    - Schulung der Mitarbeiter & Awareness-Maßnahmen
    - Einführung von Sicherheitsmaßnahmen (SIEM, IAM, Notfallmanagement)
  - Phase 3: Internes Audit & Testierung
    - Durchführung interner Audits
    - Auswahl des Zertifizierers (z. B. BFMT Audit GmbH)
      - Im Paket ist die BFMT gesetzt
    - Externes Audit & Zertifizierung
- Vorteile von PRISM 4 ISO
  - Automatisierte Dokumentation & Kontrolle
  - Effiziente Umsetzung & Audit-Vorbereitung
  - Integrierte Schnittstellen zu Compliance-Tools
- Laufzeit
  - 1. Monat bis 2. Monat
    - Phase 1 und 2
  - 3. Monat
    - Phase 3

PRISM 4 ISO & ISO 27001 Überblick

- Was ist PRISM 4 ISO?
  - Software zur Unterstützung der ISO 27001-Zertifizierung
  - Automatisierung von ISMS-Prozessen
  - Dokumentation, Reporting & Audit-Vorbereitung
  - Wiki System und ISMS Datenbank für den täglichen Betrieb
- Was ist ISO 27001?
  - Internationaler Standard für Informationssicherheitsmanagementsysteme (ISMS)
  - Fokus auf Risikomanagement und kontinuierliche Verbesserung
  - Zertifizierung durch unabhängige Prüfer erforderlich
- Zielgruppen für PRISM 4 ISO & ISO 27001
  - KMU mit erhöhten Sicherheitsanforderungen
  - Kritische Infrastrukturen (KRITIS)
  - Cloud-Dienstleister, IT-Unternehmen & SaaS-Anbieter
  - Regulierte Branchen (Banken, Versicherungen, Gesundheitswesen)

Gesetzliche & regulatorische Anforderungen für ISO 27001

- Warum ist eine ISO 27001-Zertifizierung wichtig?
  - Erfüllung gesetzlicher Anforderungen (z. B. DSGVO, NIS2)
  - Risikominimierung & Schutz sensibler Daten
  - Verpflichtung durch Kunden & Partner
  - Gerade in der internationalen Zusammenarbeit wird dieser Standard von Kunden verlangt, um die Aktivitäten in der IT-Sicherheit nachzuweisen
- ISO 27001 in Kombination mit anderen Standards
  - ISO 27017 / ISO 27018 → Cloud-Sicherheit & Datenschutz
  - TISAX (Automobilindustrie)
  - C5 Testat (BSI) → Cloud-Dienstleister
  - SOC 2 & ISAE 3402 für internationale Compliance / Internal Control System
- Branchen & Regularien mit ISO 27001-Pflicht oder Relevanz
  - Banken & Versicherungen: BaFin, DORA
  - Gesundheitssektor: DSGVO, NIS2, KRITIS, B3S
  - IT-Dienstleister: NIS2, KRITIS, C5 Testat
  - Öffentliche Vergaben: IT-Sicherheitsanforderungen

Presented with xmind