PRISM 4 ISO ISO 27001 Fact Sheet

Costs of ISO 27001 Certification & PRISM 4 ISO

- Direct Costs
  - Licenses:
    - PRISM 4 ISO License: 3,995 EUR
    - AI Component (u-know): 1,500 EUR
    - Technical Support: 1,600 EUR
  - Implementation:
    - Premium support for implementation (24 PT/3 months): 39,750 EUR
  - Certification:
    - ISO 27001 certification by auditors: 17,550 EUR
  - Total Certification Costs:64,395 EUR + VAT (19%)
    - plus statutory VAT of 19%
- Indirect Costs
  - Internal resource effort for implementation
  - Time investment for audits & documentation
  - Adjustment of existing IT security measures
- Savings through PRISM 4 ISO
  - Faster implementation & reduced internal resources
  - Minimization of compliance risks
  - Competitive advantage through certification

Customer Experiences

- Fast and precise implementation
- Structured approach
- Clear plan with SECaaS
- Organized processes

Implementation of PRISM 4 ISO & ISO 27001 Certification

- Steps for Implementation & Certification
  - Phase 1: Analysis & Planning
    - Gap analysis & status assessment
    - Scope definition & project planning
  - Phase 2: Implementation of Requirements
    - Documentation of policies & procedures
    - Employee training & awareness measures
    - Introduction of security measures (SIEM, IAM, Emergency Management)
  - Phase 3: Internal Audit & Certification
    - Conducting internal audits
    - Selection of certification body (e.g., BFMT Audit GmbH)
      - The BFMT is set in the package
    - External audit & certification
- Advantages of PRISM 4 ISO
  - Automated documentation & control
  - Efficient implementation & audit preparation
  - Integrated interfaces to compliance tools
- Timeline
  - 1st to 2nd Month
    - Phase 1 and 2
  - 3rd Month
    - Phas 3

Overview of PRISM 4 ISO & ISO 27001

- What is PRISM 4 ISO?
  - Software to support ISO 27001 implementation and certification
  - Automation of ISMS processes
  - Documentation, reporting & audit preparation
  - Wiki system and ISMS database for daily operations
- What is ISO 27001?
  - International standard for Information Security Management Systems (ISMS)
  - Focus on risk management and continuous improvement
  - Certification required by independent auditors
- Target Groups for PRISM 4 ISO & ISO 27001
  - SMEs with increased security requirements
  - Critical Infrastructures (KRITIS)
  - Cloud service providers, IT companies & SaaS providers
  - Regulated industries (banks, insurance, healthcare)

Legal & Regulatory Requirements for ISO 27001

- Why is ISO 27001 certification important?
  - Compliance with legal requirements (e.g., GDPR, NIS2)
  - Risk minimization & protection of sensitive data
  - Commitment required by customers & partners
  - Increasing demand from international cooperation to prove IT security activities
- ISO 27001 in Combination with Other Standards
  - ISO 27017 / ISO 27018:Cloud security & data protection
  - TISAX:Automotive industry
  - C5 Certification (BSI):Cloud service providers
  - SOC 2 & ISAE 3402:International compliance / Internal Control System
- Industries & Regulations with Mandatory ISO 27001 or Relevance
  - Banks & Insurance:BaFin, DORA
  - Healthcare Sector:GDPR, NIS2, KRITIS, B3S
  - IT Service Providers:NIS2, KRITIS, C5 Certification
  - Public Procurement:IT security requirements

Presented with xmind