Building an ISO 27001-Compliant Cyber Security Program: Getting Started

with Marc Menninger

LEARNING

ISO 27001 Compliance Plan Outline

Stage 1: Assemble team and develop implementation plan

- Pull the right people together who will be primarily responsible for planning and implementing ISO 27001 compliance
  - Could include:

    Project manager

    Executive sponsor

    Members from security, legal, HR, IT, finance, etc.
- Outline the ISO 27001 compliance implementation plan
  - Define information security objectives
  - Define ISMS goals
- Communicate and raise awareness to your organization about the project

Stage 2: Scope and baseline ISMS

- Define the scope of your ISMS
- Conduct a gap analysis to baseline where your organization is today against the ISO requirements
  - Prioritize gaps based on level of effort, impact, and cost
  - This will give you a roadmap of next steps and identify spin-off projects

Stage 3: Implement the ISMS

- Follow the implementation plan built in Stage 1
- Implement any missing requirements identified during the gap analysis in Stage 2 in order of priority
- Create steering committee
- Write information security policies and get them approved by the steering committee

Stage 4: Define and implement risk management process

- Define how your organization identifies, prioritizes, and remediates risks
- Build the risk treatment plan
- Build the risk register
- Begin listing risks found during the previous stages

Stage 5: Measure, monitor, and review ISMS

- Implement systems and tools necessary to measure and monitor the ISMS
  - Could include security metrics dashboards, regular security reviews processes, log monitoring systems, third-party reviews of your ISMS, etc.
- Use the results of these reviews to continuously improve the state of your ISMS