

ISO 27001:2013 Services: Audit Readiness and Program Design

In the current global business landscape, the information security programs of potential vendors and business partners are continuously being scrutinized; the ability to demonstrate your organization's security posture to customers and prospects is becoming increasingly important. ISO 27001 Certification is one of the most comprehensive and cost-effective ways to increase information security, provide management with visibility into organizational strengths and weaknesses, and reduce sales friction. The ISO 27001 framework is a globally recognized industry standard, providing a solid foundation on which to build or improve your security and compliance programs.

AppSec Consulting is here to help you through each step of the ISO 27001:2013 certification process, providing you with a strategic plan and hands-on assistance to help you prepare for a certification audit. Our ISO 27001 experts make sure our clients understand not just the Annex Controls, but also the requisite leadership activities that will move your organization from simply implementing security controls to realizing a true Information Security Management System (ISMS) based on your real-world risks.

Our qualified consultants bring years of experience in the information risk management, security and compliance fields, with expertise in various security and reporting standards and best practices such as ISO 27001, NIST, SOC 2 and PCI DSS; this means we tailor our ISO 27001:2013 preparation process in a manner that best suits your needs. We provide clear remediation advice that fits your unique situation, strategic direction to ensure that cyber-risk management processes and required controls are in place and working effectively, and guidance as to how best to document and organize required evidence. **Our approach is designed to save your organization time, money, and give you the confidence that there will be no "surprises" during the audit.**

Our proven ISO 27001:2013 preparation services are design to help your organization:

- ✓ Understand how to properly scope and create your Statement of Applicability (SOA)
- ✓ Leverage your existing security program to meet compliance requirements
- ✓ Attain a detailed audit readiness assessment along with expert remediation advice
- ✓ Demonstrate board and management cyber-risk due diligence
- ✓ Get assistance with remediation and evidence collection prior to and during the audit
- ✓ Leverage our expert assistance during the audit to ensure minimal impact on your resources
- ✓ Fully prepare you to get an independent ISO 27001:2013 certification that you can share with clients and prospects, providing assurances regarding the continual improvement of your ISMS

How We Do It:

Every engagement starts with detailed discussions and a healthy dose of listening to make sure we clearly understand your needs and objectives. A typical ISO 27001:2013 certification readiness engagement includes:

- ✓ **Scoping:** AppSec Consulting works closely with client management and stakeholders to properly identify all services/solutions, people and facilities to be considered in-scope for the certification report. Additionally, AppSec Consulting works with the service organization to create an appropriate Statement of Applicability (SOA). This is important; an improper scope or SOA can make the final report insufficient for satisfying the organization's needs, or too exhaustive for the organization to attain certification within the required timeframe.
- ✓ **Planning:** AppSec Consulting works closely with your team to develop a customized project plan that takes into consideration all available resources (internal and external), competing initiatives, and organizational size, culture, goals and objectives. This plan includes the following:
 - Key project milestones
 - Identification of business process owners
 - Initial risk assessment
 - Development of control objectives
 - Development of related policies and procedures
 - Describing likely audit testing procedures
 - Management Cyber-Risk oversight assessment
 - Mapping of policies and procedures to control objectives
 - Tracking progress for remediation tasks
 - Reviewing remediation results to ensure they are appropriate and complete
 - Assistance with remediation and remediation project management
 - Pre-audit and audit assistance
- ✓ **Implementation:** AppSec Consulting provides assistance and project management services as necessary to support audit preparation activities, and assistance collecting, reviewing, and organizing required audit evidence and artifacts.

About AppSec Consulting:

We've been doing this for over 12 years, and our continuum of services is designed to fit just about everyone's security needs. Every service we provide comes with a level of experience and focused attention you won't find anywhere else. Our Security Testing team will help you identify the technical issues you should be thinking about, and our Strategic Advisory Services team will work with you to develop strategies for addressing them - that means assurance for you, your customers and your partners. And because we're independently owned, you'll find us completely agnostic regarding the solutions and vendors we recommend - this means you get the solution that fits your needs, not ours.

This can't wait, so give us a call at 408.224.1110 today.

You'll speak with an Information Security expert, not a sales person - we'll listen a lot, determine your needs, and provide clear, actionable recommendations. We look forward to seeing how we can help.

Information. Security. Handled.™

appsecconsulting.com | 408.224.1110