ISO-27001 SEVEN-STEP READINESS PROCESS

Developing an end-to-end Information Security Management System (ISMS) while preparing for an ISO 27001 audit is strenuous and time-consuming. Ensuring all the dots connect between the stack of documents is difficult and the difference between a fully integrated security program and one that is disjointed with contradictory policies or policies with gaps between them. This silo-approach, although common, adds an inordinate amount of stress to your audits. **GoldSky Security begins this process by listening to you.** We are committed to understanding your organization, your environment, and what is driving your need for implementing an ISO 27001-compliant and certifiable ISMS.

The following is our **proven Seven-Step Approach** that will result in your success in implementing world-class Information Security Management System that will pass the necessary audits, without undo stress.

STEP ONE — DETERMINE THE ISMS BOUNDARY

Boundary determination includes:

1. WHAT NEEDS TO BE PROTECTED? What information needs to be included in the ISMS Scope? Once that is determined, we will work with you to understand the included systems, locations, and stakeholders.

2. WHAT NEEDS TO BE EXCLUDED? Implementing an ISMS for your entire organization may be cost prohibitive or operationally unfeasible.

3. WHO IS INVOLVED? Stakeholders typically impose requirements that are not captured in specific documentation.

4. WHAT ARE THE IMPEDIMENTS? Most organizations have to consider such hindrances such as budget constraints, technology limitations, push-back from users, or critical vendors who have their own security policies and procedures that may be at odds with our client's security requirements.

5. GOVERNANCE STRUCTURES. Security implementation may be mandated by contractual obligations, regulations, or legislation.

STEP TWO — LEADERSHIP

GoldSky will work with you to establish the vision for security management. We will help obtain leadership buy-in to include crafting the message from leadership to your employees.

STEP THREE — DEVELOP AN IMPLEMENTATION PLAN

GoldSky will work with you to establish a risk-based plan to implement the ISMS that fulfills Leadership's vision. This plan will include:

STEP THREE — (CONTINUED)

- **DEVELOPING A PROCESS** for conducting consistent risk assessments with an approved threshold for risk tolerance that meets your organization's operational environment.
- **CONDUCT A RISK ASSESSMENT** with you to determine: assets to be protected, vulnerabilities that may be exploited, threats that could exploit those vulnerabilities, and work with you to determine likelihood so that you don't wast money on risks that may not materialize.
- **MAP MITIGATION STRATEGIES** to the controls and develop a Statement of Applicability to identify all controls that need to be implemented as well as those that are excluded.

STEP FOUR — SUPPORT

GoldSky will coordinate with you to determine the resources necessary to effectively implement the implementation plan:

- **AWARENESS** for your employees
- **PERSONNEL** skill sets (competencies)
- **COMMUNICATIONS** plan
- **ISMS** supporting documentation

STEP FIVE — OPERATION

GoldSky will be your partner in executing all aspects of the implementation plan that meets Leadership's vision. What we will do is sculpt how you currently do business to meet requirements, minimizing the impact to your operations. What we will not do is waste your time and resources tearing down your current security practices to build new methodologies, paradigms, and unnecessary processes that just meet the standard. Operating the plan includes:

- **SECURITY** awareness and training
- **IMPLEMENTING** the technical, administrative, and operational controls
- **DEVELOPING** the necessary policies and procedures to support the ISMS

STEP SIX — PERFORMANCE EVALUATION

GoldSky will conduct your internal audit to ensure the ISMS was correctly implemented and identify any lingering weaknesses that need to be addressed prior to your certification audit activities. We will also sit with you during your certification audit activities to support and help clarify the auditor's requests.

STEP SEVEN — IMPROVEMENT

GoldSky will stand with you as your trusted agent to correct any weaknesses and help you meet the ISO Standard's mandate for continual improvement. As your Leadership evolves your organization, we will work to ensure security and the ISMS keeps pace.

Scan to learn more about GoldSky's **ISO-27001 Readiness Process**

GOLDSKY
CYBER SECURITY SOLUTIONS