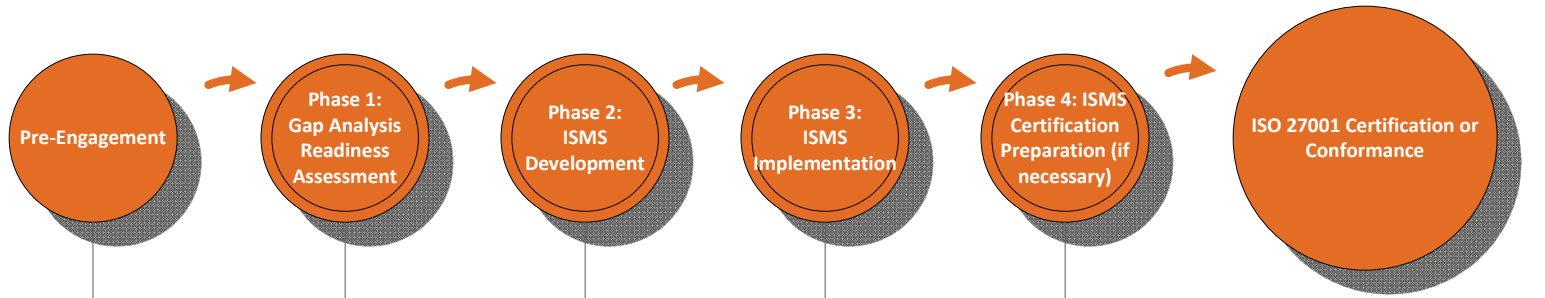


Orange Parachute's Proven Process™



- Initial Meeting
- Discussing Your Vision and Goals
 - Q&A
- Discuss Project Scope
- Submit Statement of Work

- Existing Information Security Management Program is assessed against ISO 27001 strategic, tactical, and operational requirements
- Existing Program is assessed for "re-usability" to prevent "re-inventing the wheel"
- ISMS Structure is Defined

Phase 1 Deliverables:

- ISO 27001 Assessment Tool (reusable internally)
- Written Gap Analysis Report
- ISMS Structure Diagram (Framework)

- ISMS Development Kick-Off Workshop
- ISMS Taxonomy Developed
- Program Scope Developed
- Risk Scope Developed
- Program Direction (What to Do, How to Do It, When to Do It, Who Does It, Why Do It)

Phase 2 Deliverables:

- Developed, documented, and socialized ISMS Taxonomy
- Developed, documented, and socialized Program Scope
- Developed, documented, and socialized Risk Scope
- Developed, documented, and socialized Program Directives (i.e. What to Do)
- Developed, documented, and socialized Program Methodologies (i.e. How to Do It)
- Developed, documented, and socialized Program Activities (i.e. When to Do It)
- Developed, documented, and socialized Role Definitions (i.e. Who Does It)
- Developed, documented, and socialized Program Level Risk Assessment Methodology (i.e. Why Do It)
- Measureable Metrics on the What, How, When, Who, and Why

- Operational Level Domain Definition (Where to Do It)
 - Supporting Collateral Developed
- Further Metrics Developed (Monitor & Measure)

Phase 3 Deliverables:

- Developed, documented, and socialized Operational Level Domain Definition
- Developed, documented, and socialized Operational Level Supporting Collateral
- Defined, documented, and socialized Reporting Channels & Forums
- Developed, documented, and socialized Operational Level Control Assessment

- Audit Preparation
- Audit Participation

Phase 4 Deliverables:

- Pre-Certification Audit Report
- Audit Package for the External ISO 27001 Auditor

Some of the Benefits of ISMS and ISO 27001

- Enhances Infosec interoperability and trust both internally and externally
- The mechanism to manage a flexible & extensible Infosec Program
 - Proactive vs. Reactive Security Management
 - Time Based Assurance
 - Process Definition & Metrics
 - Legal & Regulatory Compliance Umbrella
- Provides a vehicle to document due diligence
- Provides the forum for informed-choice decision making
 - Consistent Third-Party GRC
 - Provides Defensibility
- Creates Market Differentiation

Please Note: Much of what you see here in deliverables may already exist in your organization. It is important to understand that this often becomes an exercise in packaging effectively. We're not here to "re-invent the wheel", rather, we're here to help you package your program for usability, efficiency, and effectiveness.

Helping clients develop more efficient, effective, and usable information security programs, resulting in increased program visibility, informed choice decision making, speed to compliance, and conformance or certification to an international standard (ISO 27001).