REGULATORY COMPLIANCE READINESS CONSULTING SERVICE

EXECUTIVE SUMMARY

As concerns over information security continue to increase, a growing number of business partners, customers, regulators, and other stakeholders require the organizations they do business with to demonstrate that the organizations have a sound information security management system (ISMS) in place. The most widely recognized data security standard is ISO/IEC 27001.

Increasingly, having ISO/IEC 27001 certification is essential for doing business with many leading enterprises globally

Our proven methodology over many years of projects will save your team months of effort in implementing ISO 27001 and making a workable plan to achieve it. And our experts guides you through all things needed to come into full compliance with ISO/IEC 27001.

Once this project is completed, You will achieve the following goals:
- Identification and risk assessment of all information assets
- Security Vulnerability Test and Penetration Test for Information Systems
- ISMS Assessment and Implementation in accordance with the ISO/IEC 27001 requirements
- ISO/IEC 27001 Certification Audit of Global Certification Body (optional)

1

wiki

SERVICE STRATEGY

Our strategies to achieve successful ISO / IEC 27001 certification based on many years of experience and know-how is as follows.
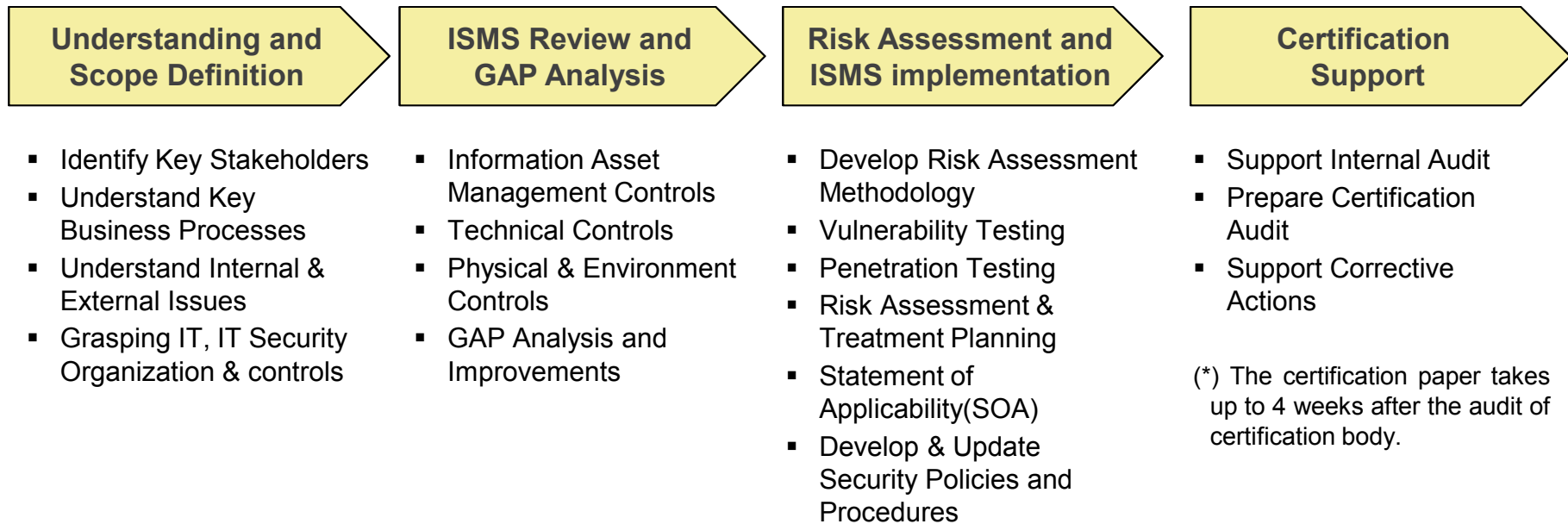
- **Professional Consultant T / F Team Composition**
  - Consists of ISO / IEC 27001 Lead Auditor, Auditor qualification consultant
  - Many years of experienced staff in ISO / IEC 27001 ISMS Assessment and Implementation
  - Experts of security vulnerabilities and Penetration Testing technicians in various industries

- **Integration with Global Certification Body**
  - Proposal including Certification Body Auditing to overcome Initial Audit failover
  - Certification acquired in a short period of time (minimum 3 months)

- **Know-how and technology transfer in project process**
  - Establishing consensus with stakeholders through training on ISO / IEC 27001 certification
  - Technical transfer of technical security including security vulnerability testing

METHODOLOGY

The consulting methodology consists of 4 phases from Understanding to Certification Support. Depending on the scope of project, there are a little bit deference tasks and steps of each phase.

Understanding and Scope Definition	ISMS Review and GAP Analysis	Risk Assessment and ISMS implementation	Certification Support
- Identify Key Stakeholders - Understand Key Business Processes - Understand Internal & External Issues - Grasping IT, IT Security Organization & controls	- Information Asset Management Controls - Technical Controls - Physical & Environment Controls - GAP Analysis and Improvements	- Develop Risk Assessment Methodology - Vulnerability Testing - Penetration Testing - Risk Assessment & Treatment Planning - Statement of Applicability(SOA) - Develop & Update Security Policies and Procedures	- Support Internal Audit - Prepare Certification Audit - Support Corrective Actions (*) The certification paper takes up to 4 weeks after the audit of certification body.

Deliverables

Scope Statement, GAP Analysis, Information Asset Inventory, Penetration Testing Report, Vulnerability Testing Report, Risk Assessment Methodology, Risk Treatment Plan

Internal Audit Plan & Results, Statement of Applicability(SOA), Information Security Policies & Procedures, ISO/IEC 27001 Training Materials, Corrective Plan, etc.

woki

PROJECT CASES

- **Client**: KT Rwanda Networks Ltd. (in Rwanda)

- **Project Scope** : (completed)
  All the necessary tasks for obtaining ISO/IEC 27001 certification (including certification audit of certification body)

- **Main Activities**
  [SD] ISMS scope Definition
  [RM] Risk Assessment and Treatment (including Vulnerability Test and Penetration test)
  [IM] ISMS Implementation and Training
  [OE] Operation and Performance Evaluation
  [CS] Certification Support

- **Deliverables**
  - About 18 Mandatory Documents and Records
  - About 20 non-mandatory Documents and Records

- **Peculiar Activities**
  - Educating and cooperating on ISMS review and improvements
  - Training and sharing the testing role on Security Vulnerability Testing
  - Know-how and technology transfer in all project process

ISO/IEC 27001 Certification Readiness Consulting WBS(Sumarry)

PROJECT CASES

- **Client**: Daewoo Engineering & Construction (in Korea)

- **Project Scope** : (complete)
  All the necessary tasks and documents for obtaining ISO/IEC 27001 certification (including certification audit of certification body)

- **Certification Background**:
  ISO/IEC 27001 certificate is required to strengthen competitiveness of overseas construction business

- **Certification Scope:** Operation of IT Infrastructure

- **Main History(with our consulting service)**
  - in 2013, Initial Certification
  - in 2015, Surveillance Certification
  - in 2016, Upgrade Certification(version 2013)

- **Peculiar Activities**
  - Minimize the scope of certification with
    "Operate of IT Infrastructure"
  - Provided readiness consulting service for certification
    preparation every year after obtaining initial certification
  - Provide technical assistance for security hardening
    against vulnerabilities found in the technical vulnerability test

DAEWOO E&C

WIKI