TOPCERTIFIER

Governance, Risk & Compliance Consultants

ISO 27001 GAP ANALYSIS TEMPLATE

INTRODUCTION:

TopCertifier presents a Simplified ISO 27001 Gap Analysis Checklist to help you identify areas in which your organization may need improvements to comply with ISO 27001 standards. This checklist offers a fundamental framework for evaluating your alignment with ISO 27001:2013 and serves as an initial step in assessing your information security.

SECTION 1: LEADERSHIP AND COMMITMENT

- ☐ Is there clear leadership commitment to quality and ISO 27001 compliance?
- ☐ Are roles, responsibilities, and authorities regarding 27001 communicated?
- ☐ Is there active worker participation in the development, implementation, and improvement of the ISO 27001 principles?

SECTION 2: PLANNING

- ☐ Have information security risks been identified and assessed?
- ☐ Are information security objectives measurable and consistent?
- ☐ Is there a documented process for IS management system (ISMS) planning?

SECTION 3: SUPPORT

- ☐ Are resources (human, infrastructure, and environment) available?
- ☐ Is there an awareness program for employees regarding ISO 27001?
- ☐ Are documented procedures in place for competence, awareness, and communication?

SECTION 4: OPERATION

- ☐ Are processes determined, documented, and consistently followed?
- ☐ Are criteria for ISMS performance, including legal requirements, defined and monitored?
- ☐ Is there a process for identifying actions related to ISMS?

SECTION 5: PERFORMANCE EVALUATION

- ☐ Are internal audits conducted to assess ISMS Compliance?
- ☐ Are data and information collected and analyzed to evaluate ISMS performance?
- ☐ Is there a process for conducting management reviews?

SECTION 6: IMPROVEMENT

- ☐ Are corrective actions taken when non-conformities are identified?
- ☐ Is there a process for continuous improvement based on ISMS performance data?
- ☐ Are preventive actions implemented to address potential ISMS issues and risks?

SECTION 7: DOCUMENTATION AND RECORDS

☐ Are procedures and processes documented as required by ISO 27001?
☐ Are records maintained to demonstrate ISMS conformity and effectiveness?
☐ Is document control in place to ensure the latest versions of documents are used?

Please note that this checklist provides a high-level overview, and it's essential to conduct a more in-depth analysis specific to your organization's information security processes and context. Additionally, engaging with ISO 27001 experts or consultants is recommended for a comprehensive gap analysis tailored to your organization's needs.