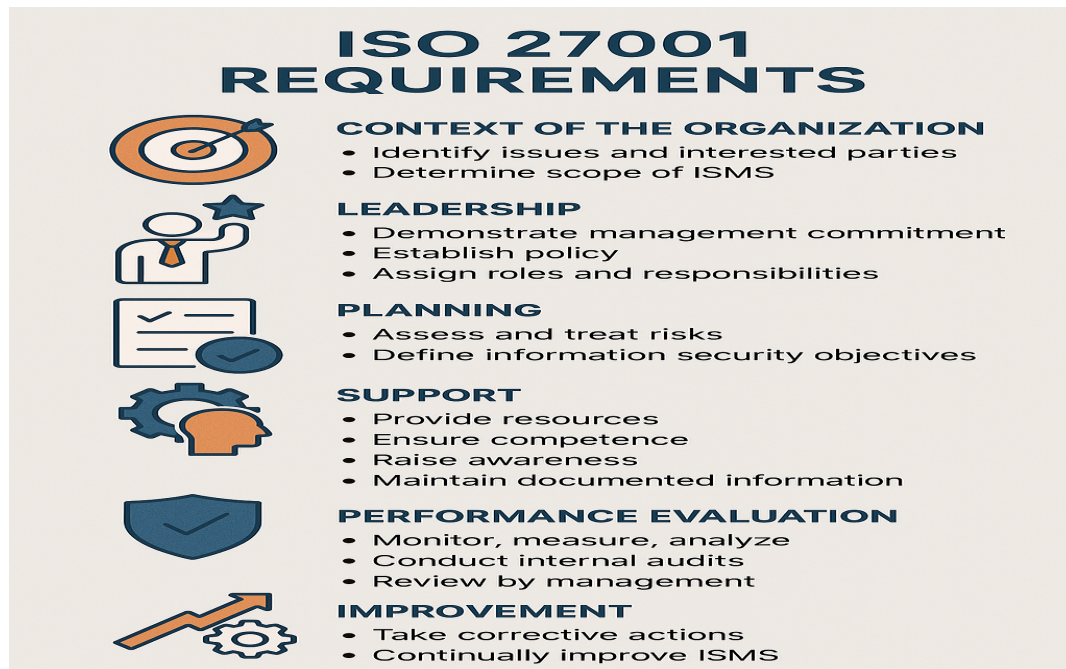


# ISO 27001 REQUIREMENTS

QSL (Logo) – Quality Solutions Limited



## Text Summary of ISO 27001 Requirements

### **1. Context of the Organization**

- Identify internal and external issues affecting information security.
- Define interested parties and their requirements.
- Establish the scope of the ISMS.

### **2. Leadership**

- Top management commitment to ISMS.
- Establish and communicate information security policy.
- Assign roles, responsibilities, and authorities.

### **3. Planning**

- Conduct risk assessment and risk treatment.
- Set measurable information security objectives.
- Develop risk treatment plan aligned with business goals.

### **4. Support**

- Provide necessary resources (people, tech, budget).
- Ensure competence and awareness.
- Establish communication processes.
- Maintain documented information.

## **5. Operation**

- Carry out risk assessments regularly.
- Implement and manage risk treatment plan.
- Control outsourced processes and supplier relationships.

## **6. Performance Evaluation**

- Monitor and measure ISMS effectiveness.
- Conduct internal audits.
- Perform management reviews.

## **7. Improvement**

- Take corrective actions for nonconformities.
- Apply continual improvement to strengthen ISMS.

## **Annex A – Controls**

- 93 controls grouped into 4 themes:
- Organizational (policies, compliance, incident management).
- People (training, awareness, screening).
- Physical (facility access, environmental security).
- Technological (encryption, backup, monitoring).

*Prepared by Quality Solutions Limited*