

---

# ISO Standards (ISO 9001 & ISO 27001)

## **Q: What is ISO 9001?**

A: A standard for Quality Management Systems (QMS) focused on consistent product/service quality and customer satisfaction.

---

## **Q: What is ISO 27001?**

A: A standard for Information Security Management Systems (ISMS) focused on protecting data confidentiality, integrity, and availability.

---

## **Q: What does QMS mean in ISO 9001?**

A: Quality Management System — a structured framework of processes to ensure consistent quality delivery.

---

## **Q: What does ISMS mean in ISO 27001?**

A: Information Security Management System — a systematic approach to managing sensitive information securely.

---

## **Q: What is Risk Assessment in ISO 27001?**

A: The process of identifying, analyzing, and evaluating security risks to information assets.

---

## **Q: What does “Documented Information” mean?**

A: Required policies, procedures, and records that must be maintained and controlled as evidence of compliance.

---

## **Q: What is Continuous Improvement?**

A: An ongoing effort to improve processes, products, or systems (core principle in ISO 9001).

---

## **Q: What does Internal Audit mean in ISO context?**

A: A periodic review conducted internally to ensure compliance with ISO standards and identify gaps.

---

**Q: What is Corrective Action?**

A: Steps taken to eliminate the root cause of a detected non-conformity to prevent recurrence.

---

**Q: What is Certification Audit?**

A: An external audit conducted by a certification body to verify compliance with ISO standards.