

# ISO 27001:10 WAYS TO CONTINUAL IMPROVEMENT

ISO 27001 requires organisations to demonstrate an ongoing commitment to continual improvement as a pre-requisite to certification.

## 1. Internal Audits

Organisations often worry about internal audits. In fact, these should be seen as a valuable tool.

## 2. External Audits

External audits conducted by a UKAS accredited Certification Body can help to identify areas for improvement.

## 3. Risk Management

A well-documented and maintained risk log will provide evidence of how your risk management methodology is being used to promote improvement.

## 4. Management of Non-Conformities

Non-conformities are a helpful way to identify which parts of your ISMS may require improvement.

## 5. Management Reviews

Top level management can evidence their commitment in enforcing a consistent application of the management system.

## 6. Infosec Objectives

Agreeing to SMART objectives may also enable trending and the monitoring of objectives over a lengthy period of time.

## 7. Training

Training should be delivered to all new starters, and all employees annually to embed an information security culture.

## 8. Security Weaknesses

Having controls in place to identify, report on, and investigate security weaknesses, events and incidents helps support continual improvement.

## 9. Compliance Reviews

The identification and monitoring of legal, regulatory and contractual obligations can help towards continual improvement.

## 10. Improvement Plans

Creating and maintaining an improvement plan is a very helpful way of logging and tracking improvement actions within your organisation.

