



Information Security Implementation Module

Supporting certification towards ISO 27001:2005

What is Information Security and why is it important to you and the business?

Governments, corporates, financial institutions, hospitals, and private businesses produce a great deal of confidential information about their employees, customers, patients, products, research, and financial status. Most of this information is collected, processed and stored on electronic computers and transmitted across networks to other computers, not to mention the information kept on paper.

Should confidential information about a business, its customers, finances or new products fall into the wrong hands, such a breach of security could lead to lost business, law suits or even bankruptcy. Protecting confidential information is a corporate requirement, and in many cases also an ethical and legal requirement. Recently a large number of high profile security breaches have been reported, such as the following headlines:

“HMRC fiasco over security policy and procedures is an accident waiting to happen for numerous organisations”

“Antiquated systems fail to communicate key procedures or track employee comprehension and agreement”

These events demonstrated clearly that corporate management had failed to meet their obligations and responsibilities in ensuring staff were fully aware of their roles in protecting sensitive personal information.

How can jComply ISIM help you with your Information Security needs?

This module has been especially designed to help managers implement pre-written security policies

based on ISO 27001:2005. Module also includes a library of questions and answers through which the managers can train and test their team thus improving the overall compliance to information security standards and regulations.

By adopting the jComply concepts and that of the Information Security Compliance application in particular demonstrates a commitment by you that all staff and associated contractors have the appropriate training and preparation, based on ISO 27001:2005, for them to handle securely sensitive information internally and externally.

What are the benefits associated with developing an information security management system to ISO27001:2005 standard?

Confidentiality: A high level of confidentiality through the reduction of associated risks, by the implementation of appropriate controls.

Availability: The guarantee of the availability of company information through the implementation of a data centre which would be available in a crisis.

Integrity: The identification and standardisation of information processing services together with the control of software development and evaluation.

Legal Compliance: The compliance with the standard demonstrates, to clients and major stakeholders that the organisation follows industrial regulations, legal standards and “best practice”.

Enhanced Profitability: Enhanced business profitability due to the efficiency and performance of your information systems being secured, monitored and managed using cost effective solutions.

Information Security Implementation Module

Supporting certification towards ISO 27001:2005



What is included in the jComply ISIM?

By adopting the jComply ISIM approach the following security policies based on ISO 27001:2005 will be addressed:

- Security Policy
- Organisation of Information Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communication and Operation Management
- Access Control
- System Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Furthermore the module also includes a library of questions and answers designed to help managers train the company employees on relevant information security policies.

Finally, by implementing and adopting an Information Security programme, as outlined in jComply, will provide your business with 6 basic business aims:

- Strategic alignment of security with business strategy and organisational objectives
- Risk reduction and mitigation of threats to the business
- Objectives are met through KPI measurement and monitoring
- Increased security awareness
- Improved response mechanisms to security incidents and breaches
- Assured business continuity and disaster recovery mechanisms.

What is the importance of Information Security in Healthcare?

ISO 27799 is an information security standard developed by the International Organisation for Standardisation (ISO). The purpose of ISO 27799 is to provide guidelines to healthcare organisations and other institutes that hold personal health related information on how to protect such information through the implementation of ISO/IEC 27002.



The security information can be applicable to any information related to health. This information can be in any form. Anyone operating in the healthcare industry is required to protect this information. ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides best practice guidelines.

To find out how your organisation can benefit from jComply ISIM visit our website at www.tabaqsoftware.com or give us a call at the telephone number mentioned below.