

INFORMATION

Is The Most Valuable Asset Of Every Organization

Is Your Corporate Information Secure?



Learn How To Protect Them

Get Yourself Trained and Certified in

Information Security Foundation Course based on ISO/IEC 27002

ITSM EXPERTS Sdn Bhd (771169H)

6th Floor, Suite 17, IOI Business Park, Persiaran Puchong Jaya Selatan, Bandar Puchong Jaya, 47100 Puchong, Selangor

☎ +603-80644220

☎ +603-80642037

✉ training@itsm-experts.com

🌐 www.itsm-experts.com

 facebook.com/itsmexperts

 twitter.com/itsmexperts



GET CERTIFIED IN INFORMATION SECURITY



An essential security certificate

EXIN now offers you another essential add-on to ITIL® certification: Information Security according to ISO/IEC 27002.

Organizations want ISO/IEC 27000

Security is currently the fastest growing industry. Most organizations today are seeking certification for the ISO/IEC 27000 standard in information security. The question is: are you ready for security?

ITIL® is not security

Although being slightly mentioned as a process in the ITIL® V3 framework, none of the ITIL books refer to the ISO/IEC 27000 global standard and no integrated approach is given.

Focus on the non-technical

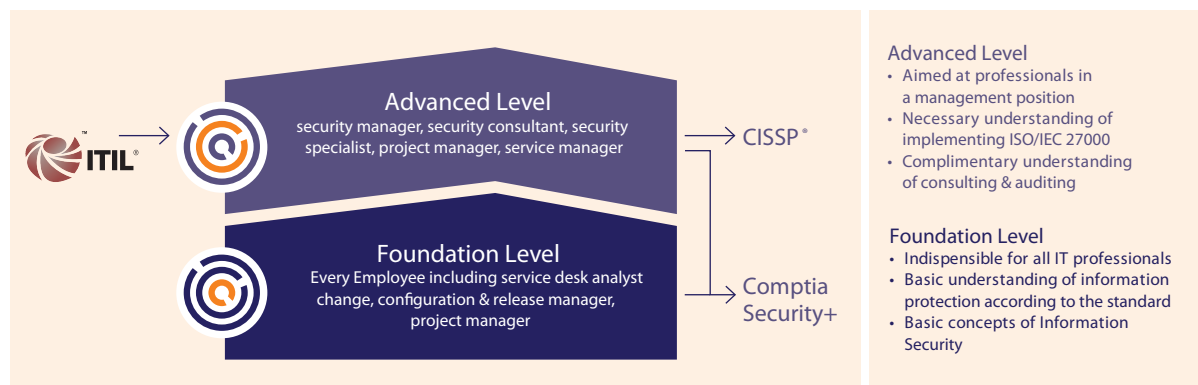
Where other security certifications deal primarily with the technical aspects of security protection, EXIN's program focuses on people, and actually teaching you to manage security.

Follow the course & take the exam

Learn the essentials of information security management during a value-added course offered by ITSM EXPERTS and get certified.

Benefits:

- Extend your ITIL expertise
- Learn about the ISO/IEC 27000 standard
- Boost your résumé



www.itsm-experts.com



INFORMATION SECURITY

Information Security Foundation based on ISO/IEC 27002

Information security is becoming increasingly important. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the Internet. Furthermore, activities of many companies now rely on ICT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable.

In the Information Security Foundation module, based on ISO/IEC 27002 (ISFS), the basic concepts of information security and their coherence are tested.

Target Group

The target group of ISFS is everyone in the organization. The basic knowledge that is tested in this module contributes to the understanding that information is vulnerable and that measures are necessary to protect this information. The module is also suitable for small independent businesses for whom some basic knowledge of information security is necessary. This module can be a good start for new information security professionals.

The Certificate Information Security Management Advanced based on ISO/IEC 27002 is a follow up of the Certificate Information Security Foundation based on ISO/IEC 27002.

Prerequisites

None

Examination details

Examination type: Computer-based or paper-based multiple choice.

Time allotted for examination: 60 minutes

Number of multiple-choice questions: 40

Pass mark: 65% (26 out of 40)

Exam requirements

1. Information and security 10%
 - 1.1 The concept of information (2.5%)
 - 1.2 Value of information (2.5%)
 - 1.3 Reliability aspects (5%)
2. Threats and risks 30%
 - 2.1 Threat and risk (15%)
 - 2.2 Relationships between threats, risks and the reliability of information (15%)
3. Approach and organization 10%
 - 3.1 Security policy and security organization (2.5%)
 - 3.2 Components (2.5%)
 - 3.3 Incident Management (5%)
4. Measures 40%
 - 4.1 Importance of measures (10%)
 - 4.2 Physical security measures (10%)
 - 4.3 Technical measures (10%)
 - 4.4 Organizational measures (10%)
5. Legislation and regulations 10%
 - 5.1 Legislation and regulations (10%)

An Introduction To ISO 27001

The ISO 27001 standard was published in October 2005, essentially replacing the old BS7799-2 standard. It is the specification for an ISMS, an Information Security Management System. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted. Today in excess of a thousand certificates are in place, across the world.

ISO 27001 enhanced the content of BS7799-2 and harmonized it with other standards. A scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification.

The objective of the standard itself is to "provide a model for establishing, **implementing, operating, monitoring, reviewing, maintaining,** and improving an **Information Security Management System**".

Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organization".

The standard defines its 'process approach' as "The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management". It employs the PDCA, Plan-Do-Check-Act model to structure the processes, and reflects the principles set out in the OIEC guidelines.

THE CONTENTS OF ISO 27001

The content sections of the standard are:

- Management Responsibility
- Internal Audits
- ISMS Improvement
- Control objectives and controls
- OIEC principles and this international standard
- Correspondence between ISO 9001, ISO 14001 and this standard

Introduction To ISO 27002

The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.

The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

The basis of the standard was originally a document published by the UK government, which became a standard 'proper' in 1995, when it was re-published by BSI as BS7799. In 2000 it was again re-published, this time by ISO, as ISO 17799. A new version of this appeared in 2005, along with a new publication, ISO 27001. These two documents are intended to be used together, with one complimenting the other.

ISO's future plans for this standard are focused largely around the development and publication of industry specific versions (for example: health sector, manufacturing, and so on). Note that this is a lengthy process, so the new standards will take some time to appear.

THE CONTENTS OF ISO 17799 / 27002

The content sections are:

- Structure
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical Security
- Communications and Ops Management
- Access Control
- Information Systems Acquisition, Development, Maintenance
- Information Security Incident management
- Business Continuity
- Compliance