

---

---

**Information technology — Security  
techniques — Code of practice for  
information security management**

*Technologies de l'information — Techniques de sécurité — Code de  
pratique pour la gestion de sécurité d'information*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 17799:2005](https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005)

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 17799:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

<b>Contents</b>	<b>Page</b>
<b>FOREWORD</b> .....	<b>VII</b>
<b>0 INTRODUCTION</b> .....	<b>VIII</b>
0.1 WHAT IS INFORMATION SECURITY?.....	VIII
0.2 WHY INFORMATION SECURITY IS NEEDED? .....	VIII
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS .....	IX
0.4 ASSESSING SECURITY RISKS .....	IX
0.5 SELECTING CONTROLS.....	IX
0.6 INFORMATION SECURITY STARTING POINT.....	IX
0.7 CRITICAL SUCCESS FACTORS .....	X
0.8 DEVELOPING YOUR OWN GUIDELINES .....	XI
<b>1 SCOPE</b> .....	<b>1</b>
<b>2 TERMS AND DEFINITIONS</b> .....	<b>1</b>
<b>3 STRUCTURE OF THIS STANDARD</b> .....	<b>4</b>
3.1 CLAUSES .....	4
3.2 MAIN SECURITY CATEGORIES .....	4
<b>4 RISK ASSESSMENT AND TREATMENT</b> .....	<b>5</b>
4.1 ASSESSING SECURITY RISKS .....	5
4.2 TREATING SECURITY RISKS.....	5
<b>5 SECURITY POLICY</b> .....	<b>7</b>
5.1 INFORMATION SECURITY POLICY.....	7
5.1.1 <i>Information security policy document</i> .....	7
5.1.2 <i>Review of the information security policy</i> .....	8
<b>6 ORGANIZATION OF INFORMATION SECURITY</b> .....	<b>9</b>
6.1 INTERNAL ORGANIZATION .....	9
6.1.1 <i>Management commitment to information security</i> .....	9
6.1.2 <i>Information security co-ordination</i> .....	10
6.1.3 <i>Allocation of information security responsibilities</i> .....	10
6.1.4 <i>Authorization process for information processing facilities</i> .....	11
6.1.5 <i>Confidentiality agreements</i> .....	11
6.1.6 <i>Contact with authorities</i> .....	12
6.1.7 <i>Contact with special interest groups</i> .....	12
6.1.8 <i>Independent review of information security</i> .....	13
6.2 EXTERNAL PARTIES .....	14
6.2.1 <i>Identification of risks related to external parties</i> .....	14
6.2.2 <i>Addressing security when dealing with customers</i> .....	15
6.2.3 <i>Addressing security in third party agreements</i> .....	16
<b>7 ASSET MANAGEMENT</b> .....	<b>19</b>
7.1 RESPONSIBILITY FOR ASSETS.....	19
7.1.1 <i>Inventory of assets</i> .....	19
7.1.2 <i>Ownership of assets</i> .....	20
7.1.3 <i>Acceptable use of assets</i> .....	20
7.2 INFORMATION CLASSIFICATION .....	21
7.2.1 <i>Classification guidelines</i> .....	21
7.2.2 <i>Information labeling and handling</i> .....	21
<b>8 HUMAN RESOURCES SECURITY</b> .....	<b>23</b>
8.1 PRIOR TO EMPLOYMENT .....	23
8.1.1 <i>Roles and responsibilities</i> .....	23

8.1.2	Screening .....	23
8.1.3	Terms and conditions of employment .....	24
8.2	DURING EMPLOYMENT .....	25
8.2.1	Management responsibilities .....	25
8.2.2	Information security awareness, education, and training .....	26
8.2.3	Disciplinary process .....	26
8.3	TERMINATION OR CHANGE OF EMPLOYMENT .....	27
8.3.1	Termination responsibilities .....	27
8.3.2	Return of assets .....	27
8.3.3	Removal of access rights .....	28
<b>9</b>	<b>PHYSICAL AND ENVIRONMENTAL SECURITY .....</b>	<b>29</b>
9.1	SECURE AREAS .....	29
9.1.1	Physical security perimeter .....	29
9.1.2	Physical entry controls .....	30
9.1.3	Securing offices, rooms, and facilities .....	30
9.1.4	Protecting against external and environmental threats .....	31
9.1.5	Working in secure areas .....	31
9.1.6	Public access, delivery, and loading areas .....	32
9.2	EQUIPMENT SECURITY .....	32
9.2.1	Equipment siting and protection .....	32
9.2.2	Supporting utilities .....	33
9.2.3	Cabling security .....	34
9.2.4	Equipment maintenance .....	34
9.2.5	Security of equipment off-premises .....	35
9.2.6	Secure disposal or re-use of equipment .....	35
9.2.7	Removal of property .....	36
<b>10</b>	<b>COMMUNICATIONS AND OPERATIONS MANAGEMENT .....</b>	<b>37</b>
10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES .....	37
10.1.1	Documented operating procedures .....	37
10.1.2	Change management .....	37
10.1.3	Segregation of duties .....	38
10.1.4	Separation of development, test, and operational facilities .....	38
10.2	THIRD PARTY SERVICE DELIVERY MANAGEMENT .....	39
10.2.1	Service delivery .....	39
10.2.2	Monitoring and review of third party services .....	40
10.2.3	Managing changes to third party services .....	40
10.3	SYSTEM PLANNING AND ACCEPTANCE .....	41
10.3.1	Capacity management .....	41
10.3.2	System acceptance .....	41
10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE .....	42
10.4.1	Controls against malicious code .....	42
10.4.2	Controls against mobile code .....	43
10.5	BACK-UP .....	44
10.5.1	Information back-up .....	44
10.6	NETWORK SECURITY MANAGEMENT .....	45
10.6.1	Network controls .....	45
10.6.2	Security of network services .....	46
10.7	MEDIA HANDLING .....	46
10.7.1	Management of removable media .....	46
10.7.2	Disposal of media .....	47
10.7.3	Information handling procedures .....	47
10.7.4	Security of system documentation .....	48
10.8	EXCHANGE OF INFORMATION .....	48
10.8.1	Information exchange policies and procedures .....	49
10.8.2	Exchange agreements .....	50
10.8.3	Physical media in transit .....	51
10.8.4	Electronic messaging .....	52
10.8.5	Business information systems .....	52

10.9	ELECTRONIC COMMERCE SERVICES .....	53
10.9.1	<i>Electronic commerce</i> .....	53
10.9.2	<i>On-Line Transactions</i> .....	54
10.9.3	<i>Publicly available information</i> .....	55
10.10	MONITORING .....	55
10.10.1	<i>Audit logging</i> .....	55
10.10.2	<i>Monitoring system use</i> .....	56
10.10.3	<i>Protection of log information</i> .....	57
10.10.4	<i>Administrator and operator logs</i> .....	58
10.10.5	<i>Fault logging</i> .....	58
10.10.6	<i>Clock synchronization</i> .....	58
<b>11</b>	<b>ACCESS CONTROL .....</b>	<b>60</b>
11.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL .....	60
11.1.1	<i>Access control policy</i> .....	60
11.2	USER ACCESS MANAGEMENT .....	61
11.2.1	<i>User registration</i> .....	61
11.2.2	<i>Privilege management</i> .....	62
11.2.3	<i>User password management</i> .....	62
11.2.4	<i>Review of user access rights</i> .....	63
11.3	USER RESPONSIBILITIES .....	63
11.3.1	<i>Password use</i> .....	64
11.3.2	<i>Unattended user equipment</i> .....	64
11.3.3	<i>Clear desk and clear screen policy</i> .....	65
11.4	NETWORK ACCESS CONTROL .....	65
11.4.1	<i>Policy on use of network services</i> .....	66
11.4.2	<i>User authentication for external connections</i> .....	66
11.4.3	<i>Equipment identification in networks</i> .....	67
11.4.4	<i>Remote diagnostic and configuration port protection</i> .....	67
11.4.5	<i>Segregation in networks</i> .....	68
11.4.6	<i>Network connection control</i> .....	68
11.4.7	<i>Network routing control</i> .....	69
11.5	OPERATING SYSTEM ACCESS CONTROL .....	69
11.5.1	<i>Secure log-on procedures</i> .....	69
11.5.2	<i>User identification and authentication</i> .....	70
11.5.3	<i>Password management system</i> .....	71
11.5.4	<i>Use of system utilities</i> .....	72
11.5.5	<i>Session time-out</i> .....	72
11.5.6	<i>Limitation of connection time</i> .....	72
11.6	APPLICATION AND INFORMATION ACCESS CONTROL .....	73
11.6.1	<i>Information access restriction</i> .....	73
11.6.2	<i>Sensitive system isolation</i> .....	74
11.7	MOBILE COMPUTING AND TELEWORKING .....	74
11.7.1	<i>Mobile computing and communications</i> .....	74
11.7.2	<i>Teleworking</i> .....	75
<b>12</b>	<b>INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE .....</b>	<b>77</b>
12.1	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS .....	77
12.1.1	<i>Security requirements analysis and specification</i> .....	77
12.2	CORRECT PROCESSING IN APPLICATIONS .....	78
12.2.1	<i>Input data validation</i> .....	78
12.2.2	<i>Control of internal processing</i> .....	78
12.2.3	<i>Message integrity</i> .....	79
12.2.4	<i>Output data validation</i> .....	79
12.3	CRYPTOGRAPHIC CONTROLS .....	80
12.3.1	<i>Policy on the use of cryptographic controls</i> .....	80
12.3.2	<i>Key management</i> .....	81
12.4	SECURITY OF SYSTEM FILES .....	83
12.4.1	<i>Control of operational software</i> .....	83
12.4.2	<i>Protection of system test data</i> .....	84

12.4.3	Access control to program source code.....	84
12.5	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES .....	85
12.5.1	Change control procedures .....	85
12.5.2	Technical review of applications after operating system changes.....	86
12.5.3	Restrictions on changes to software packages.....	86
12.5.4	Information leakage.....	87
12.5.5	Outsourced software development.....	87
12.6	TECHNICAL VULNERABILITY MANAGEMENT .....	88
12.6.1	Control of technical vulnerabilities .....	88
<b>13</b>	<b>INFORMATION SECURITY INCIDENT MANAGEMENT .....</b>	<b>90</b>
13.1	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES .....	90
13.1.1	Reporting information security events.....	90
13.1.2	Reporting security weaknesses .....	91
13.2	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS .....	91
13.2.1	Responsibilities and procedures .....	92
13.2.2	Learning from information security incidents .....	93
13.2.3	Collection of evidence.....	93
<b>14</b>	<b>BUSINESS CONTINUITY MANAGEMENT .....</b>	<b>95</b>
14.1	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT .....	95
14.1.1	Including information security in the business continuity management process.....	95
14.1.2	Business continuity and risk assessment.....	96
14.1.3	Developing and implementing continuity plans including information security .....	96
14.1.4	Business continuity planning framework.....	97
14.1.5	Testing, maintaining and re-assessing business continuity plans.....	98
<b>15</b>	<b>COMPLIANCE..... (standards.iteh.ai)</b>	<b>100</b>
15.1	COMPLIANCE WITH LEGAL REQUIREMENTS .....	100
15.1.1	Identification of applicable legislation.....	100
15.1.2	Intellectual property rights (IPR).....	100
15.1.3	Protection of organizational records.....	101
15.1.4	Data protection and privacy of personal information .....	102
15.1.5	Prevention of misuse of information processing facilities .....	102
15.1.6	Regulation of cryptographic controls.....	103
15.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE .....	103
15.2.1	Compliance with security policies and standards.....	104
15.2.2	Technical compliance checking.....	104
15.3	INFORMATION SYSTEMS AUDIT CONSIDERATIONS .....	105
15.3.1	Information systems audit controls.....	105
15.3.2	Protection of information systems audit tools .....	105
<b>BIBLIOGRAPHY.....</b>		<b>107</b>
<b>INDEX.....</b>		<b>108</b>

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17799 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

## 0 Introduction

### 0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

### 0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.



### 0.3 How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.
2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.

### 0.4 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

### 0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading "Information security starting point".

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

### 0.6 Information security starting point

A number of controls can be considered as a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common practice for information security.

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

- a) data protection and privacy of personal information (see 15.1.4);
- b) protection of organizational records (see 15.1.3);
- c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

- a) information security policy document (see 5.1.1);
- b) allocation of information security responsibilities (see 6.1.3);
- c) information security awareness, education, and training (see 8.2.2);
- d) correct processing in applications (see 12.2);
- e) technical vulnerability management (see 12.6);
- f) business continuity management (see 14);
- g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

## 0.7 Critical success factors

ISO/IEC 17799:2005

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a->

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- a) information security policy, objectives, and activities that reflect business objectives;
- b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
- c) visible support and commitment from all levels of management;
- d) a good understanding of the information security requirements, risk assessment, and risk management;
- e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;
- f) distribution of guidance on information security policy and standards to all managers, employees and other parties;
- g) provision to fund information security management activities;
- h) providing appropriate awareness, training, and education;
- i) establishing an effective information security incident management process;
- j) implementation of a measurement<sup>1</sup> system that is used to evaluate performance in information security management and feedback suggestions for improvement.

---

<sup>1</sup> Note that information security measurements are outside of the scope of this standard.

## 0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

# iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 17799:2005](https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005)

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 17799:2005](https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005)

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

# Information technology — Security techniques — Code of practice for information security management

## 1 Scope

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

## 2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

### 2.1

#### **asset**

anything that has value to the organization  
[ISO/IEC 13335-1:2004]

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

### 2.2

#### **control**

means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature  
NOTE Control is also used as a synonym for safeguard or countermeasure.

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

### 2.3

#### **guideline**

a description that clarifies what should be done and how, to achieve the objectives set out in policies  
[ISO/IEC 13335-1:2004]

### 2.4

#### **information processing facilities**

any information processing system, service or infrastructure, or the physical locations housing them

### 2.5

#### **information security**

preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

### 2.6

#### **information security event**

an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant  
[ISO/IEC TR 18044:2004]

2.7

**information security incident**

an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security  
[ISO/IEC TR 18044:2004]

2.8

**policy**

overall intention and direction as formally expressed by management

2.9

**risk**

combination of the probability of an event and its consequence  
[ISO/IEC Guide 73:2002]

2.10

**risk analysis**

systematic use of information to identify sources and to estimate the risk  
[ISO/IEC Guide 73:2002]

2.11

**risk assessment**

overall process of risk analysis and risk evaluation  
[ISO/IEC Guide 73:2002]

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

2.12

**risk evaluation**

process of comparing the estimated risk against given risk criteria to determine the significance of the risk  
[ISO/IEC Guide 73:2002]

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>

2.13

**risk management**

coordinated activities to direct and control an organization with regard to risk  
NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.  
[ISO/IEC Guide 73:2002]

2.14

**risk treatment**

process of selection and implementation of measures to modify risk  
[ISO/IEC Guide 73:2002]

2.15

**third party**

that person or body that is recognized as being independent of the parties involved, as concerns the issue in question  
[ISO/IEC Guide 2:1996]

**2.16**

**threat**

a potential cause of an unwanted incident, which may result in harm to a system or organization  
[ISO/IEC 13335-1:2004]

**2.17**

**vulnerability**

a weakness of an asset or group of assets that can be exploited by one or more threats  
[ISO/IEC 13335-1:2004]

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 17799:2005](https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005)

<https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005>