INTERNATIONAL STANDARD

**ISO/IEC 27102**

First edition
2019-08

# Information security management — Guidelines for cyber-insurance

*Gestion de la sécurité de l'information — Lignes directrices pour la cyber-assurance*

Reference number
ISO/IEC 27102:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

# Introduction

Cyber-incidents can occur at any time with various potential impacts to an organization. For example, an organization's information and assets are under constant attack as cyber-threats become more pervasive, persistent and sophisticated.

The adoption of cyber-insurance to reduce the impacts of the consequences arising from a cyber-incident should be considered by an organization in addition to information security controls as part of an effective risk treatment approach.

Cyber-insurance is no substitute for robust security and effective incident response plans, along with rigorous training of all employees.

Cyber-insurance should be considered as an important component of an organization's overall security risk treatment plan to increase resilience.

# Information security management — Guidelines for cyber-insurance

## 1 Scope

This document provides guidelines when considering purchasing cyber-insurance as a risk treatment option to manage the impact of a cyber-incident within the organization's information security risk management framework.

This document gives guidelines for:

a) considering the purchase of cyber-insurance as a risk treatment option to share cyber-risks;

b) leveraging cyber-insurance to assist manage the impact of a cyber-incident;

c) sharing of data and information between the insured and an insurer to support underwriting, monitoring and claims activities associated with a cyber-insurance policy;

d) leveraging an information security management system when sharing relevant data and information with an insurer.

This document is applicable to organizations of all types, sizes and nature to assist in the planning and purchase of cyber-insurance by the organization.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

**3.1**
**cyber-incident**
cyber-event that involves a loss of information security or impacts business operations

**3.2**
**cyber-insurance**
insurance that covers or reduces financial loss to the *insured* (3.7) caused by a *cyber-incident* (3.1)

**3.3**
**cyber-insurance policy**
contract for *cyber-insurance* (3.2) coverage

**3.4**
**cyber-risk**
risk caused by a *cyber-threat* (3.5)

**3.5**
**cyber-threat**
threat that exploits a *cyberspace* (3.6)

**3.6**
**cyberspace**
interconnected digital environment of networks, services, systems, and processes

**3.7**
**insured**
entity that shares or considers sharing *cyber-risk* (3.4) with an insurer

## 4 Structure of this document

Guidelines are given in Clauses 5 to 8.

Clause 5 provides information and a general description of cyber-insurance; Clause 6 discusses cyber-risk of an organization that can be covered under a cyber-insurance policy. Both Clause 5 and Clause 6 are of relevance to both the organization and an insurer.

Clause 7 describes the generic risk assessment an insurer typically undertakes as part of its cyber-insurance underwriting and Clause 8 describes the use of an information security management system (ISMS) by an insured to produce data, information and documentation that can be shared with an insurer.

Annex A provides examples of ISMS documents that an insured can provide to an insurer.

## 5 Overview of cyber-insurance and cyber-insurance policy

### 5.1 Cyber-insurance

Cyber-insurance is a risk treatment option that can compensate the insured against potentially significant financial losses associated with a cyber-incident. Cyber-insurance is provided by an insurer who underwrites risks by signing and accepting liability, thus guaranteeing payment to the insured in case loss or damage occurs.

Cyber-insurance is designed to compensate for losses from a variety of cyber-incidents, for example: data breaches, business interruption, and network damage.

Adoption of cyber-insurance can assist the insured to:

a) minimize the impact of a cyber-incident;

b) provide funding mechanisms for recovery from major losses;

c) assist the return to normal operations; and

d) increase resilience of the insured business to cyber-incidents.

The insured can be required to demonstrate their compliance with any conditions imposed by the cyber-insurance policy relating to the on-going management of the cyber-risk covered.

### 5.2 Cyber-insurance policy

Contractual terms for cyber-insurance are given in a cyber-insurance policy. A cyber-insurance policy can be either a stand-alone policy or be included as special endorsements as a part of general liability, property or other insurance policy.

Coverage offered by a cyber-insurance policy typically takes a wide perspective and covers a broad range of threats that can cause financial or other forms of impact. Impact can occur through loss of confidentiality, integrity, or availability of information or systems irrespective of the exact cause of a cyber-incident and whether it was accidental or deliberate. Cyber-insurance coverage varies quite a lot between different cyber-insurance products, is not standardized and varies depending on:

a) needs of the insured;

b) limitations posed by laws and regulations;

c) generally accepted market practices;

d) business decisions of an insurer.

Cyber-insurance policies cover certain costs associated with cyber-incidents and can provide access to services that support the insured after a cyber-incident. These services include, for example, evaluating the impact of the attack; implementation of response and recovery plans; legal expertise; forensics expertise; public relations and communications support; customer notification; and restoration of business operations after a cyber-incident.

Cyber-insurance coverage offers the ability to recover some or all internal and external costs of the cyber-incident and varies depending on the specific policies and endorsements selected by the insured.

## 6 Cyber-risk and insurance coverage

### 6.1 Risk management process and cyber-insurance

A cyber-insurance policy generally allows the insured to reduce losses from cyber-risks through the sharing of these risks with an insurer.

An organization should be protected from cyber-risks by using a process that actively predicts, identifies, assesses, treats and responds to cyber-incidents as part of an effective risk management approach.

The risk assessment process should include appropriate translation of cyber-risks into business terms to highlight the business consequences of cyber-incidents. Such translation can allow risk treatment decisions to determine how risks are to be treated through:

a) avoidance;

b) removing the threat;

c) changing the likelihood or consequences of the risk;

d) retaining the risk; or

e) sharing the risk with other parties, such as insurers.

Risk treatment decisions should consider the incorporation of cyber-insurance, to improve resilience against such risks. The risk management process provides information on risks and business consequences to align a cyber-insurance policy with the security risk management strategy and risk acceptance criteria of the organization.

## 6.2 Cyber-incidents

### 6.2.1 General

A cyber-incident occurs where a cyber-risk becomes a reality and leads to a loss of confidentiality, integrity or availability of data or other assets.

A cyber-incident is caused by a threat that exploits a cyberspace vulnerability typically relating to the use of information systems and networks. The use of the cyberspace brings threats such as denial of service attack, intrusion to an organization's network, malware dissemination, improper use of information or information systems, and extortion. In addition, there are also other threats such as errors and omissions and system malfunctions. The organization should identify relevant threats in light of its business and technological contexts.

A cyber-incident can be caused by an actor exploiting a vulnerability, by unintentional error, or by a system malfunction. A cyber-incident can impact the organization’s technology and, as a result, require repair or replacement of the impacted asset.

### 6.2.2 Cyber-incident types

Cyber-incidents, originating from internal or external threat sources, belong to one or more of the following categories:

a) **system malfunction**: the insured’s system or network is malfunctioning or creating damage to a third-party system or a supplier's system is not functioning, impacting operations;

b) **data confidentiality breach**: data stored in the insured’s system (managed on premise, hosted or managed by a third party) has been stolen or exposed;

c) **data integrity or availability loss**: data stored in the insured’s system (managed on premise, hosted or managed by third party) has been corrupted or deleted;

d) **other malicious activity**: misuse of a technology system to inflict harm (such as cyber-bullying over social platforms or phishing attempts) or to illicitly gain profit (such as cyber-fraud); and

e) **human error**: where something unintentional has been done by a human resulting in harm to a system, network or information.

Root causes for incidents can usually be attributed to failure of people, systems or processes.

Each of these incident types can be covered by cyber-insurance.

## 6.3 Business impact and insurable losses

### 6.3.1 Overview

A cyber-incident can result in business impacts to the organization. These impacts can include the loss or compromise of personal data, loss of e-commerce revenue, disruption of supply chains and business interruption. During and after a cyber-incident, the organization can be faced with significant costs to restore operations, conduct investigations and settle regulatory fines and legal cases.

Certain business impacts resulting from a cyber-incident can be quantified, for example: loss of sales, lost profit, cost of crisis management, forensic investigations, lawsuits and indemnification, notifications to business partners and customers, regulatory investigations, fines, attorneys and consultants, public relation professionals, and remedial measures. Some business impacts can be difficult to quantify, for example reputational damage, impact or damages to business executives, management, staff and related personnel or leakage of trade secrets and other infringement of intellectual property rights.

A cyber-incident affecting the organization can also occur at a supplier or another third-party organization supplying goods or performing services for the organization.

### 6.3.2 Type of coverage

Cyber-insurance can cover primary categories of business impacts including the following:

a) liability (6.3.3);

b) incident response costs (6.3.4);

c) cyber-extortion costs (6.3.5)

d) business interruption (6.3.6);

e) legal and regulatory fines and penalties (6.3.7);

f) contractual penalties (6.3.8); and

g) systems damage (6.3.9).

NOTE 1 Item e) applies only where it is allowed.

NOTE 2 With ongoing cyber-insurance product development, additional categories of coverage can emerge over time.

The insured should select the cyber-insurance coverage that best suits its identified risks.

### 6.3.3 Liability

A cyber-incident can lead to liability costs for the insured through indemnification for losses to other parties. Examples of such liability can include:

a) damages caused by a cyber-incident at the insured affecting individuals or other organizations;

c) data breach of personal, customer or supplier information.

### 6.3.4 Incident response costs

#### 6.3.4.1 Overview

Different types of response costs can result from a cyber-incident. Cyber-insurance typically provides coverage of some but not necessarily all costs. Subclauses 6.3.4.2 to 6.4.8 provide typical examples of cost-incurring scenarios.

NOTE Insurers, because of their business practices, can exclude certain items from their coverage of cyber-insurance, or they can decide not to underwrite and cover certain aspects.

#### 6.3.4.2 Loss, theft or damage to information

A cyber-incident can result in the leakage of the insured's confidential information. The financial and non-financial value of the information for the insured is lost if it is leaked. A typical example of information leakage resulting in significant damage to the insured occurs when competitors obtain trade secret or invention information before public disclosure as a patent. Leakage of personal information can accompany payment and other costs in relation to the individual.

A cyber-incident can result in loss of integrity or availability of the insured's information, information systems and other assets. The loss can adversely affect the business processes of the insured including its internal operations, service delivery, manufacturing and operational technology.

An insured's information can be damaged or stolen in a cyber-incident. This can incur costs to replace or repair the impacted information through restoring, updating, recreating or replacing to the same condition the information prior to the loss, theft or damage.

Stolen information has a value to the insured and this value should be considered a cost where the stolen information is not recoverable. Costs can be incurred by the insured in attempting to recover their information. Additionally, where information is copied in an unauthorized manner, the current value of the information can be diminished as a result.

A special case is the loss or theft of intellectual property, e.g. trade secret, invention before disclosure as a patent and copyrighted material, through a cyber-incident. Lost intellectual property has a current and future value to the insured and this value should be considered a cost where the lost information is not recoverable. Additionally, when intellectual property is copied, the value of the intellectual property can be diminished or reduced to zero as a result. The insured may not be able to recover for the lost value of the intellectual property.

#### 6.3.4.3 Reputational damage

Reputation is a significant business asset for most organizations and incurring reputational damage can be disastrous. It is important for the insured to restore its reputation when it has been damaged as a result of a cyber-incident. The insured should have a suitable communications plan to acknowledge its concern and commitment to resolve the incident, while showing that the insured is in control of the situation. Insurers may be supportive to pay for public relations consultants to assist mitigate reputational damage.

#### 6.3.4.4 Customer or employee notification costs

A cyber-incident can involve customer or employee data and potentially impact the insured's customers or employees. Where individual's information is involved, it is possible that these individuals, as well as regulators, can seek responses to questions about the extent of the cyber-incident and the steps taken to minimize the damage that has already been incurred. Where such a cyber-incident occurs, the insured can incur costs associated with notifying the affected individuals when their information has been impacted. These costs can include the need to establish a special cyber-incident customer call centre to handle calls from the notified individuals.

NOTE Certain jurisdictions, laws, regulations or regulators require that notification to affected individuals occurs. Unless the costs of notification are specifically covered in a cyber-insurance policy, then the insured pays such costs.

#### 6.3.4.5 Customer or employee protection costs

When a cyber-incident that includes loss of customer or employee data occurs, these individuals are more susceptible to risks such as identity or medical fraud. Expenses can be incurred in that the insured needs to provide credit or identity theft monitoring services to decrease the level of risk exposure for a defined period of time. Costs incurred can also include legal, postage, and advertising expenses where there is a legal or regulatory requirement to notify individuals of a cyber-incident, including credit monitoring and public relations media assistance costs.

#### 6.3.4.6 Specialist expertise costs

A cyber-incident can raise complex issues that can incur costs associated with the engagement of a specialist individual or team to assist the insured respond adequately. For example, a cyber-incident can be associated with national and international legal and regulatory requirements which require specialist knowledge to determine how best to comply. Another example can be to assist the insured with a crisis communication specialist to advise on media communications and media relations and drafting crisis communication plans and appropriate incident communication documents and notification letters to affected and interested parties. Special resources to assist the insured through a cyber-incident can include the establishment of a special cyber-incident 24/7 hotline and associated call centre to handle calls from the notified individuals, IT forensics specialists to stop an ongoing breach from continuing and to investigate the breach.

#### 6.3.4.7 Operational cost to manage incidents

Costs can be incurred to manage a response to the cyber-incident and to contain any business impact resulting from the incident. For example, the redirection of existing experts away from their normal duties to being part of a rapid response team, overtime costs, operational costs to restore systems, networks or data.

#### 6.3.4.8 Staff and personnel costs

A cyber-incident can result in costs that affect staff and personnel, for example, time off work, loss of productivity, staff replacement and loss of personal reputation.

### 6.3.5 Cyber-extortion costs

Cyber-extortion involves attempts to extort money by threatening to damage or restricting the insured's use of technology, or releasing information copied or stolen from the insured. Examples of cyber-extortion risks include:

a) making the insured's information inaccessible through encryption by malware;

b) undertaking, or threatening to undertake, a hacking attack, denial of service, or introduce malware into the insured's information systems;

b) deleting, disseminating, divulging or utilizing information stored in the insured's information systems;

c) damaging, destroying or altering the insured's information systems; and

d) requesting a ransom to decrypt information.

NOTE There are jurisdictions where insurance coverage for selected cyber-extortion risks is not permitted.

### 6.3.6 Business interruption

Business interruption involves a loss of income or loss of profit and increased operating expenses resulting from a cyber-incident. Further business interruption impacts can include reduced operational effectiveness and efficiency, failure to meet deadlines and delayed deliveries to customers.

### 6.3.7 Legal and regulatory fines and penalties

A cyber-incident can result in the insured being subjected to:

a) civil penalties;

b) regulatory penalties and fines resulting from an investigation or enforcement action by a regulator; or

c) other compensatory awards decided by a legal system.

NOTE There are jurisdictions where insurance coverage for certain legal and regulatory fines or penalties is not permitted.

### 6.3.8 Contractual penalties

A cyber-incident can result in the insured not fulfilling contractual obligations. This can result in penalties from these parties.

### 6.3.9 Systems damage

A cyber-incident can result in costs to repair or restore systems, data and software applications not otherwise covered by the insured's existing insurance policies; for example, where these are specifically excluded.

## 6.4 Supplier risk

A cyber-incident affecting the insured can also occur at a supplier or another third-party organization providing goods or performing services for the insured. Such cyber-incident can result in the loss of data or can disrupt one or more services provided to the insured. The insured should seek confirmation that costs due to a cyber-incident at a supplier or another third-party organization contracted to provide goods or perform services will be recoverable either through the third party's own insurance arrangements or that of the insured.

The insured can also be subject to investigation costs, defence costs, and civil damages as a result of a cyber-incident at its supplier or other contracting third-party organization.

On the other hand, a cyber-incident at the insured can impact customers or other external entities, whereby the losses incurred by these external entities can result in claims or financial obligations against the insured.

## 6.5 Silent or non-affirmative coverage in other insurance policies

Some potential impacts of a cyber-incident can already be covered in the insured's existing insurance policies, if cyber-incidents are not excluded as a clause. An example is a cyber-incident creating a fire or explosion, which can be covered in a property policy.

The insured should consider potential coverage as well as exclusions of cyber-risks in existing policies.

## 6.6 Vendors and counsel for incident response

The insured should develop and maintain relationships with suppliers, vendors and counsel in order to prepare for a cyber-incident and to enhance their ability to respond in an effective and timely manner. These preparations should be regularly tested and reviewed as part of the insured's business continuity planning. These services can be available as a service from the insurer or sourced independently by the insured.

## 6.7 Cyber-insurance policy exclusions

A cyber-insurance policy cannot cover all types of losses. Therefore, it is important that the insured understands what risks are excluded from a cyber-insurance policy. Policy exclusions can include the following:

a) first-party and third-party bodily injury and property damage arising from a cyber-incident are usually excluded under a cyber-insurance policy;

b) terrorism: a cyber-loss caused by hacking groups that are classified as terrorist organizations in some countries, or by internationally recognized organizations;

c) acts of war and other hostile acts: there is no generally recognized definition of cyber-war. The definition is expected to be linked to actors, for example nation state, and to the level of disruptive or destructive impact, whether war is declared or not;

d) impacts due to loss of intellectual property, for example, patents, copyrights or trade secrets;

e) theft or loss of confidential information where the information is not directly owned by the insured; and

e) loss of reputation.

The insured should check all exclusions in their cyber-insurance coverage.

### 6.8 Coverage amount limits

The potential business impact and losses that can be incurred by the insured should be reviewed and clarified to carefully determine and consider how much cyber-insurance coverage to buy. The amount of cyber-insurance the insured can purchase can vary depending on the insured's financials, industry, operations, and cyber-risk exposure. For example, the number of personal records held by the insured.

Cyber-insurance policies can have an excess or deductible applied, which is the amount of money the insured should pay before a claim can be made against the cyber-insurance policy. There can be an aggregate limit either as a policy whole or an aggregate for a single event per annum. The size, and nature of the excess or deductible should be agreed during the preparation of the cyber-insurance policy. Cyber-insurance policies can also include a waiting period of several days before business interruption cover begins to apply. Further, the length of business interruption coverage in a cyber-insurance policy can be limited. Most policies cover lost income resulting from a cyber-incident only for a certain period of time.

To assist in evaluating potential cyber-losses that would allow determination of the appropriate amount of coverage to purchase, advice can be sought from research organizations that regularly publish industry benchmark information on the cost of past cyber-incidents around the world.

## 7 Risk assessment supporting cyber-insurance underwriting

### 7.1 Overview

The process for creating a cyber-insurance policy, also referred to as the underwriting process, typically involves a number of preparatory activities to assist in determining whether to accept the insured's cyber-risk and to determine an adequate price for the cyber-risk coverage. These activities include:

a) acquiring information about the insured's cyber-security practices;

b) assessing the insured's cyber-risks;

c) assessing the insured's business risks;

d) determining the insured's insurability; and

e) creating a cyber-insurance policy with the necessary price.

### 7.2 Information collection

An insurer identifies required data and information about the insured to assist in the cyber-underwriting process. Required insured data and information can include:

a) understanding of the mission and business;

b) identification of key stakeholders including customers and business partners;

c) information retained and processed;

d) details of information systems and any outsourcing arrangements;

e) details of the ISMS;

f) list and description of applied information security controls;

g) records of previous incidents; and

h) additional assurance of the status of information security controls, such as audit reports and follow-up results.

Information being collected needs to be properly protected and delivered in an up-to-date and complete manner. An insurer can request regular updates of the information in a defined frequency.

An insurer can also collect additional information on the insured's cyber-risk from third-party providers, such as a specialized risk assessment service provider. The depth of such information collection depends on the amount and extent of the desired insurance coverage, which typically relates to the size of the insured. An insurer can decide whether to share such additional information with the insured.

## 7.3 Cyber-risk assessment of the insured

### 7.3.1 General

An insurer assesses cyber-risks of the insured to assist in determining whether to accept the insured and to determine an adequate price for the desired coverage. The risk assessment can look at both the risk exposure of the insured and the status of in place information security controls.

### 7.3.2 Inherent cyber-risk assessment

An insurer generally determines a typical level of risk for the insured based on knowledge of industry sectors, sometimes known as the inherent risk exposure of the insured, taking into account the following example factors:

a) industry sector;

b) size of organization;

c) business activities;

d) extent and type of information stored and used;

e) dependency on externally managed or outsourced systems;

f) countries where business activities are performed; and

g) whether the insured is subject to regulation.

Industries which process highly sensitive information are generally considered to be subject to higher risk exposure.

### 7.3.3 Information security controls assessment

An insurer assesses the extent to which the insured has implemented information security controls to protect its information and assets, and the extent to which the inherent cyber-exposure is mitigated. An insurer assessment can consider technology, process and people, and can reference an established control set. For example, ISO/IEC 27002:2013 which includes:

a) Information security policies — define a set of policies to clarify the insured's direction of, and support for, information security;

b) Organization of information security — define and allocate segregated roles and responsibilities for information security to avoid conflicts of interest and prevent inappropriate activities;

c) Human resource security — responsibilities taken into account when managing the lifecycle of employees, contractors and temporary staff;

d) Asset management — assets contained in an inventory, owners identified and accountable for asset security assigned;

e) Access control — limit access to information and information processing facilities;

f) Cryptography — use of encryption, cryptographic authentication and integrity controls such as digital signatures and message authentication codes, and cryptographic key management;

g) Physical and environmental security — define physical perimeters and barriers, with physical entry controls and working procedures, to protect the premises, offices, rooms, delivery or loading areas against unauthorized access;

h) Operational security — procedures and responsibilities, protection from malware, backup, logging and monitoring, control of operational software, technical vulnerability management and information systems audit coordination;

i) Communications security — network security management and Information transfer;

j) System acquisition, development and maintenance — Security requirements of information systems, security in development and support processes and test information;

k) Supplier relationships — information security in supplier relationships and supplier service delivery management;

l) Information security incident management — management of information security incidents and improvements;

m) Information security aspects of business continuity management — information security continuity and redundancies; and

n) Compliance — compliance with legal and contractual requirements and information security reviews.

### 7.3.4 Review prior cyber-losses

Where substantial prior losses have occurred, an increased level of understanding is required as to the steps taken by the insured to reduce future losses. This review can include the insured's financial condition (balance sheet, income statement and cash flow statement). The adoption of certain new information security controls or the strengthening of existing controls can be required to minimize future cyber-losses prior to an insurance decision being determined.

# 8 Role of ISMS in support of cyber-insurance

## 8.1 Overview

ISO/IEC 27001 provides organizations with a structured management framework for an ISMS designed to establish, implement, maintain and continually information security. An effective ISMS allows an organization to:

a) identify, analyze, and address its information security risks;

b) continually secure itself adequately against information security risks; and

c) review and improve information security controls to keep pace with changes to security threats, vulnerabilities and business impacts.

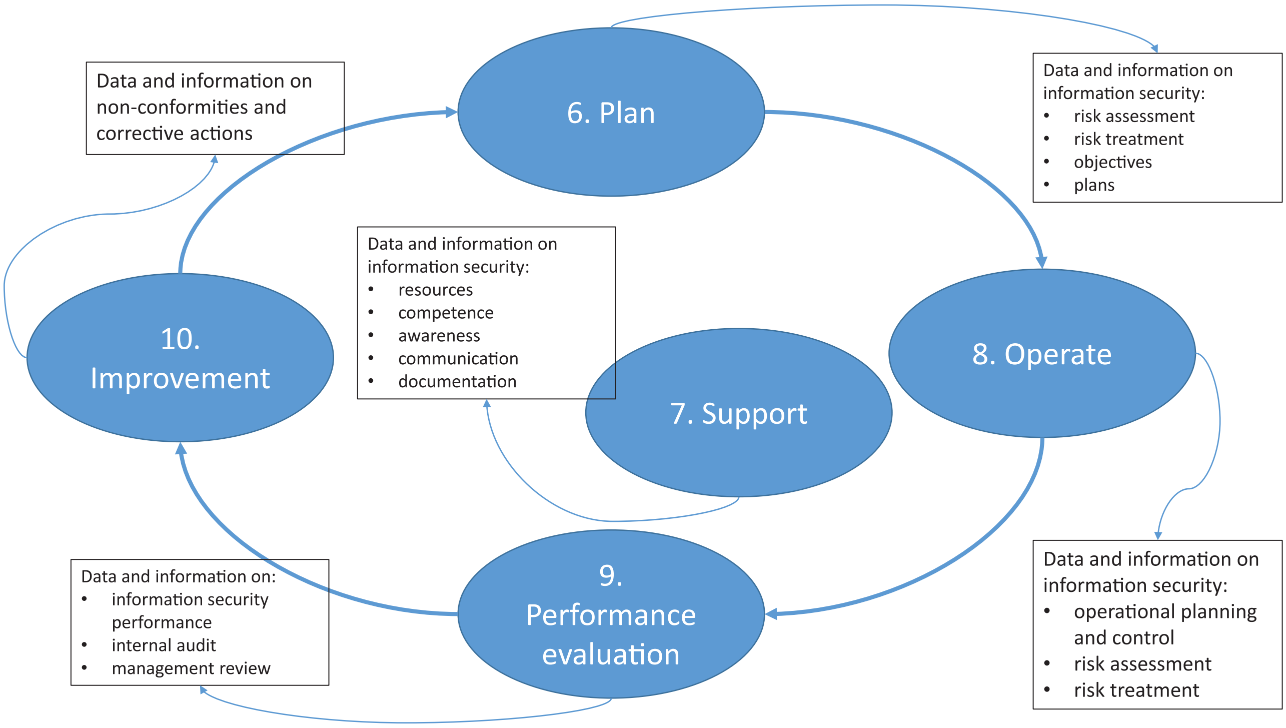
An ISMS can provide the insured and insurer with data, information and documentation that can be used in cyber-insurance policy inception, cyber-insurance policy renewal and throughout the lifetime of that cyber-insurance policy. Since cyber-insurance is a risk sharing option, providing cyber-risk management information to an insurer can assist the insurer to broker a more suitable cyber-insurance policy.

## 8.2 ISMS as a source of information

### 8.2.1 ISMS

An ISMS that is established, implemented, maintained and continually improved in accordance with ISO/IEC 27001 can be used to collect data and information relevant to a cyber-insurance policy. Figure 1, based on ISO/IEC 27001:2013, provides examples of the information that can be produced from an ISMS.

The insured should collect and collate the outputs from its ISMS, information security measurement programmes (e.g. based on ISO/IEC 27004), and risk management activities (e.g. based on ISO/IEC 27005) and submit required data to an insurer. Annex A provides examples on the documentation that can be produced from the use of an ISMS by the insured.


Data and information on non-conformities and corrective actions
6. Plan
Data and information on information security:
• risk assessment
• risk treatment
• objectives
• plans
Data and information on information security:
• resources
• competence
• awareness
• communication
• documentation
10. Improvement
7. Support
8. Operate
Data and information on:
• information security performance
• internal audit
• management review
9. Performance evaluation
Data and information on information security:
• operational planning and control
• risk assessment
• risk treatment

NOTE The numbers in Figure 1 refer to the respective clauses of ISO/IEC 27001:2013.

**Figure 1 — Data and information provided by use of an ISMS**

### 8.2.2 Planning

In the planning, the insured determines the risks that need to be addressed to:

a) ensure the ISMS can achieve its intended outcome(s);

b) prevent, or reduce, undesired effects; and

c) achieve continual improvement.

The insured defines and applies an information security risk assessment and treatment process and retains relevant documented information.

Risk treatment plans determine the controls that the insured considers necessary to reduce cyber-risk. Such necessary controls are documented in the insured’s Statement of Applicability (SoA).

The documented information on the processes, risks identified and the risk assessment and treatment plans can be shared with an insurer.

### 8.2.3 Support

Individuals doing work under the insured's control and leading or involved in establishing, implementing, maintaining and continually improving an ISMS need to be aware of:

a) the information security policy;

b) their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance; and

c) the implications of not conforming with the ISMS requirements.

Information about awareness training of individuals can be shared with an insurer.

The insured determines the need for internal and external communications relevant to the ISMS including:

a) what to communicate on;

b) when to communicate;

c) whom to communicate with;

d) who communicates; and

e) the processes which cause communications to start.

The insured should apply the above guidance to determine how best to communicate with an insurer.

When implementing, operating or maintaining an ISMS, the insured creates the documentation:

a) as stated in ISO/IEC 27001; and

b) determined by the insured as being necessary for the effectiveness of the ISMS.

NOTE See ISO/IEC 27003 for examples of such additional documentation.

The documentation created above can be shared with an insurer.

### 8.2.4 Operation

When following the requirements of the ISMS during operations, the insured needs to:

a) plan, implement and control the processes needed to meet information security requirements, and implement the initial plans and actions determined in the planning phase;

b) keep documented information to the extent necessary to have confidence that defined processes have been carried out as planned;

c) control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary;

d) ensure that outsourced processes are determined and controlled;

e) perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in the planning phase, and retain documented information of the results of the information security risk assessments; and

f) implement the information security risk treatment plan and retain documented information of the results of the information security risk treatment.

The insured can share the documentation produced in this phase with an insurer.

### 8.2.5 Performance evaluation

Performance evaluations can produce data on the performance of information security controls (whether technical or otherwise), allowing the insured to collate and present information on the effectiveness and performance of those implemented controls. The data can be collected:

a) from the controls themselves;

b) by measurements of the controls;

c) by the use of metrics, such as those presented in ISO/IEC 27004;

d) by regular monitoring, review or assessment of the controls or the processes they support.

Internal audits of the information security function, information security controls or the ISMS can be used to gather further data on the efficiency and effectiveness of information security controls and the ISMS; and provide business context for this data. When required, third-party audits can also be used to gather this data.

Management reviews at planned intervals are required by the insured's ISMS to ensure its continuing suitability, adequacy and effectiveness.

The data gathered from the evaluation phase can be used to identify non-conformance and areas requiring continual improvement and can also be captured as documented information which can be used as evidence of the monitoring and measurement results, which can be passed to an insurer.

The evaluation of information security can highlight new information security risks or changes in previously identified information security risks, which can be documented and shared with an insurer.

### 8.2.6 Improvement

When reacting to identified non-conformance, the steps taken assist in the treatment of information security risks. The treatment should be documented.

The insured can also document the steps taken to improve the suitability, adequacy and effectiveness of the ISMS. The insured can share the documentation on improvements of the ISMS with an insurer.

## 8.3 Sharing of information about risks and controls

As cyber-insurance is a risk sharing option that is part of the insured's information security management, there is value in the insured regularly providing relevant cybersecurity information to an insurer. Such information exchange should be agreed between the insured and an insurer.

To create a cyber-insurance policy, both the insured and an insurer exchange information so that:

a) the insured can demonstrate its efforts to protect itself from cyber-threats;

b) the insured can define which risks it wants to share; and

c) an insurer estimates the risk it is accepting and then creates and prices a cyber-insurance policy, including applicable deductibles or exclusions.

The information should be as complete and as up-to-date as possible. Failure to do so can invalidate or revoke the cyber-insurance policy, so that the insured cannot make a claim. Providing false information can invalidate the cyber-insurance policy and can lead to legal action against the insured or individuals involved in providing that false information.

The insured should have a process to respond to an insurer's requests for data and information at cyber-insurance policy inception, cyber-insurance policy renewal, at defined intervals during the lifetime of the cyber-insurance policy and if a cyber-incident occurs. The insured should also produce the data and information required by an insurer in an agreed format.

The insured should be able to present to an insurer, on request, any documentation held by the insured relating to its information security or cyber-risk activities. Such documents can include ISMS documentation, internal or external audit reports and follow-up results, information security or security certifications held by the insured or individuals, as well as policies, procedures, and guidelines.

## 8.4 Meeting cyber-insurance policy obligations

An insurer can require a level of security as a precondition of coverage. Such conditions are usually stated in the cyber-insurance policy, and the insured needs to meet these conditions during the validity of the contract.

Further, when applying for cyber-insurance coverage, the insured can be asked to share information about the adopted information security controls. These controls should be maintained during the validity of the contract.

An ISMS can assist the insured in completing cyber-insurance policy questionnaires and making sure the insured meets the obligations as set out in a cyber-insurance policy.

# Annex A
(informative)

# Examples of ISMS documents for sharing

This annex provides examples of documented information relating to the insured's ISMS that can be used as evidence in the assessment by an insurer of the insured's risks. The documents can be valid for this purpose if the scope of the ISMS covers the scope of the cyber-insurance.

Examples of the documents fall into two categories:

a) Category 1: the documented information required in ISO/IEC 27001:2013 (see Table A.1); and

b) Category 2: the documents determined by the insured as being necessary.

See ISO/IEC 27001:2013, 7.5.1 a) and b) for supporting requirements.

An insurer and the insured can agree which documented information is to be provided (see Clause 8).

**Table A.1 — Required documented information from ISO/IEC 27001:2013**

| Subclause in ISO/IEC 27001:2013 | Documented information |
|---|---|
| 4.3 | Scope of the ISMS |
| 5.2 | Information security policy |
| 6.1.2 | Information security risk assessment process |
| 6.1.3 | Statement of applicability |
| 6.1.3 | Information security risk treatment process |
| 6.2 | Information security objectives |
| 7.2 | Evidence of person's competence |
| 7.5 | Effectiveness of the ISMS |
| 8.1 | Effectiveness of information security processes |
| 8.2 | Results of information security risk assessment |
| 8.3 | Results of information security risk treatment |
| 9.1 | Evidence of monitoring and measurement results |
| 9.2 | Evidence of audit programme(s) and audit results |
| 9.3 | Evidence of results of management reviews |
| 10.1 | Evidence of nonconformities and any subsequent actions taken |
| 10.1 | Evidence of results of corrective actions |

The documents determined by the insured as being necessary (category 2) can include, for example:

a) information security policies, guidelines and procedures other than the information security policy required in Table A.1;

b) documents about an insured's internal roles and responsibilities;

c) plans and records of awareness programmes;

d) documents on the management of outsourced processes; and

e) records of incident response.

# Bibliography

[1] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[2] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[3] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[4] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

**ICS 35.030**

Price based on 17 pages