DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27102

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2018-12-24

Voting terminates on:
2019-03-18

Information technology — Security techniques — Information security management guidelines for cyber insurance

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27102:2018(E)

© ISO/IEC 2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2018 – All rights reserved

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, Information technology.

Documents 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 documents 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.

ISO/IEC 27102 was prepared by Joint Technical Committee ISO/IEC JTC1, *Information Technology*, SubCommittee SC27, *Security Techniques*.

© ISO/IEC 2018 – All rights reserved

Introduction

The threat of a cyber-attack against an organization is very real and an organization is not easily able to predict when a cyber attack can occur. 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.

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

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 technology — Security techniques — Information security management guidelines for cyber insurance

1 Scope

This document gives guidelines for:

a) information security professionals 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 as the insured and an insurer of cyber insurance.

This document covers organizations that choose to insure with a 3rd party also known as an insurer.

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 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*

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

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:

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

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

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

© ISO/IEC 2018 – All rights reserved

3.2
cyber insurance
insurance that covers or reduces financial loss to the insured 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 – 8.

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

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

Annex A provides example documentation the 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, including information incidents, business interruption, and network damage.

Adoption of cyber insurance should assist the insured to:

a) minimise 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.

© ISO/IEC 2018 – All rights reserved

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 through loss of confidentiality, integrity, or availability of information 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 and is not standardised.

Cyber insurance coverage varies depending on:

a) limitations posed by laws and regulations;

b) generally accepted market practices;

c) business decisions of an insurer; and

d) needs of the insured.

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

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

6 Cyber risk and insurance coverage

6.1 Overview

A broad range of cyber insurance coverage is available from the insurance industry. The coverage offered by cyber insurance products typically span a broad range of threats, including cyber threats that can cause incidents and consequential business impacts.

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

6.2 Risk process and cyber insurance

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

The 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 avoidance, removing the threat, changing the likelihood or consequences of the risk, retaining the risk or sharing the risk with other parties.

The treatment of cyber risks should consider the incorporation of cyber insurance, similar to that used to insure other risks of doing business to improve resilience against such risks. Knowledge of the risks and business consequences allows a cyber insurance policy to be in alignment with the security risk management strategy and risk acceptance criteria of the organization.

6.3 Cyber incidents

6.3.1 General

A cyber incident contains a series of events. When a cyber incident is detected, the event initially identified can be:

a) loss of confidentiality, integrity or availability of information;

b) unavailability or malfunction of a device, information system, network or service;

c) unavailability or malfunction of operational technology; or

d) impact to business operations.

A cyber incident occurs where a cyber risk becomes a reality. To become a reality a threat needs to successfully exploit a vulnerability that results in an impact to an asset.

A cyber risk is a risk caused by a threat that exploits a cyberspace 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 intending to exploit a vulnerability, unintentional error, or a system malfunction. A cyber incident can impact the insured’s technology and, as a result, require repair or replacement of the impacted asset. Examples of impacted assets include information, intellectual property, reputation, as well as infrastructure, such as a website, application, network, or industrial control system.

6.3.2 Cyber incident types

Cyber incidents can be categorised into primary incident types:

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 digital operations;

b) **data confidentiality breach**: data stored in the insured’s system (managed on premise or hosted/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 or hosted/managed by third party) has been corrupted or deleted;

d) **malicious activity**: misuse of a technology system to inflict harm (such as cyber bullying over social platforms or phishing attempts to delete data) 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.

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

6.4 Business impact and insurable losses

6.4.1 Overview

A cyber incident can result in business impacts to the insured. These impacts can include loss of e-commerce revenue, disruption of supply chains and business interruption due to loss of availability of data, networks and technology systems. During and after a cyber incident, the insured 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, the 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 or leakage of trade secrets and other infringement of intellectual property rights.

6.4.2 Type of coverage

The following primary categories of business impacts can be covered by cyber insurance:

a) business interruption (6.4.3);

b) liability (6.4.4);

c) incident response costs (6.4.5); and

d) legal and regulatory fines and penalties (6.4.6).

NOTE Item (d) applies only in jurisdictions where it is allowed.

It is important for the insured to select the cyber insurance coverage that best suits its identified risks.

6.4.3 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.

6.4.4 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) lawsuit by another organization following a cyber incident for damages;

b) errors, omissions or failure by the insured to follow “best practices” in applying controls to protect information or assets under the control of the insured;

c) data breach of personal or customer information.

6.4.5 Incident response costs

6.4.5.1 Overview

Different types of costs can result from a cyber incident. Cyber insurance typically provides coverage of some but not necessarily all costs. Clauses 6.4.5.2 to 6.4.5.10 provide typical examples of cost incurring scenarios.

NOTE An insurer, because of their business practices, can exclude certain items from their coverage of cyber insurance.

6.4.5.2 External entity payment costs

A cyber incident can result in the leakage of the insured’s confidential information. The 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 / 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 business processes of the insured including its internal operations, service delivery, manufacturing and operational technology.

Other type of cyber incident is theft of money in electronic form where money can be illicitly transferred from an account.

6.4.5.3 Loss, theft or damage to information

A cyber incident can result in the insured's information being damaged or stolen resulting in costs being incurred to replace or repair the impacted information. Information if lost, stolen or damaged, needs to be protected through restoring, updating, recreating or replacing to the same condition the information prior to the loss, theft or damage.

In some cases, a cyber incident can damage the systems storing or processing the information, leading to higher replacement or repair costs. Stolen information has a value to the insured and this value should be considered a cost where the stolen information is not recoverable. Additionally, where information is copied in an unauthorized manner, the current value of the information can be diminished as a result. Costs can be incurred by the insured in attempting to recover their information.

A special case is the loss or theft of intellectual property. 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 lost or 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 lost intellectual property.

6.4.5.4 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.

6.4.5.5 Customer notification costs

A cyber incident can involve customer data and potentially impose an impact to the insured's customers. Where customer information is involved, it is possible that customers, 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 is expected to 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 center to handle calls from the notified individuals.

6.4.5.6 Customer protection costs

When a cyber incident that includes loss of customer data occurs, customers 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 program 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 program and public relations media assistance costs.

6.4.5.7 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 legislative requirements which require specialist knowledge to determine how best to comply. Another example can be to assist the insured in drafting incident communication documents and notification letters to impacted customers. 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.

6.4.5.8 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 across to being part of a rapid response team to consult with the insured.

6.4.5.9 Supplier risk costs

A cyber incident can occur at a supplier or another third-party organization contracted to provide goods or perform services for the insured. The cyber incident can result in the loss of data or can disrupt one or more services provided to the insured by the supplier or another contracting third-party. The insured can be responsible for recompensing its customers.

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

A cyber incident at the insured can impact external entities, whereby the losses incurred by these external entities can result in claims or financial obligations against the insured.

6.4.5.10 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. A common example of extortion is where the insured's information is encrypted by malware and thus made inaccessible. Other examples of extortion risks include:

a) 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.

6.4.6 Legal and regulatory fines and penalties

A cyber incident can result in the insured being subjected to costs related to forensic investigations to support legal proceedings. Other costs can be incurred as a result of subsequent legal actions where defense costs are incurred and the associated expenses arising from regulatory proceedings not related to compensatory awards. Other forms of costs can include:

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.

6.5 Silent coverage insurance and counsel

6.5.1 Silent coverage in other insurance polices

Some potential impacts of a cyber incident can already be covered in the insured's existing insurance policies. An example can be cyber incidents creating a fire or explosion, which would be covered in the regular property policies and not in explicit cyber covers.

The insured should consider potential coverage as well as exclusions of cyber risks in existing policies. Further the insured should consider the sufficiency of the liability insurance coverage.

6.5.2 Vendors and counsel for incident response

The insured should maintain pre-existing relationships with professional vendors and counsel, who would be available to increase preparedness for cyber incident response and deal with a cyber incident. Such relationships can be either managed by the insured, or it can be a service offered by an insurer.

6.6 Cyber insurance policy exclusions

A cyber insurance policy cannot cover all types of losses. The purpose of cyber insurance is to provide the insured with a risk treatment option to compensate the insured from the impact of a cyber incident. Therefore, it is important that the insured understands what risks are excluded from a cyber insurance policy. Policy exclusions can include the following:

a) bodily injury and property damage: 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 threat affecting the insured by hacking groups, which can be classified as terrorist organizations in some countries. Cyber insurance coverage can exclude incidents caused by acts of terrorism or acts of war. Some cyber insurance policies can be silent on terrorism, while other cyber insurance policies can contain specific terrorism exclusions;

c) intellectual property: the insured can maintain intellectual property, including trade secrets that should be protected. If stolen it is important to consider if such high value intellectual property information would be covered by the cyber insurance policy. Cyber insurance cannot cover all actual or alleged infringement, use, misappropriation or disclosure of a patent or a trade secret. Some cyber insurance policies, however, can offer coverage for infringement of intellectual property such as copyrights and trademarks;

d) confidential information: the insured should be aware that some cyber insurance can cover theft or an unintentional cyber incident of confidential information where the information is not directly owned by the insured; and

e) reputation: loss of reputation is another possible impact of a cyber incident that is usually excluded from a cyber insurance policy.

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

6.7 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. 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

© ISO/IEC 2018 – All rights reserved

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 should 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 making available 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 an insurer's business risks;

d) determining the insured insurability and price; and

e) creating a cyber insurance policy.

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 processing systems and any outsourcing arrangements;

e) details of an Information security management system;

f) list of applied 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 information on the insured's cyber risk from third party providers, such as a specialised risk assessment service provider. The depth of such information 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 this additional information with the insured.

7.3 Assess the insured's cyber risks

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 should look at both the risk exposure of the insured and the status of in place security controls.

7.3.2 Cyber risk assessment

An insurer generally takes into account a number of factors to determine the inherent risk exposure of the insured, including:

a) the 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 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 inherent cyber risks are mitigated. An insurer assessment can consider technology, process and people, and can reference an established control set. For example ISO/IEC 27002, 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 – control access to information with network access and connections being restricted;

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

© ISO/IEC 2018 – All rights reserved

i) Communication 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.

7.4 Understand cyber losses and accumulation risk

7.4.1 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, cash flow statement). The adoption of certain new information security controls or the strengthening of existing controls can be required to minimise future cyber losses prior to an insurance decision being determined.

7.4.2 Assess accumulation risk

The underwriting decision of an insurer considers risk accumulation scenarios, i.e. events that can result in claims across a large part of the portfolio of insurance policies. Examples of such scenarios for cyber insurance include: outage of a major cloud service provider, Internet meltdown, large-scale infection of information systems by malware (e.g. worm exploiting a zero-day vulnerability), or loss of electricity in a large geographical area. To better understand maximum losses due to such scenarios an insurer collects information from the insured as necessary to assess accumulation risk.

8 Role of ISMS in support of cyber insurance

8.1 Overview

This clause describes the use of an information security management system (ISMS) by the insured to produce data, information and documentation that can be shared with an insurer. Since cyber insurance is a risk sharing option, by providing cyber risk management information to an insurer, the insured is able to broker a more suitable cyber insurance policy.

An information security management system designed to establish, implement, maintain and continually improve information security in accordance with ISO/IEC 27001, can provide the insured and an 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.

ISO/IEC 27001 provides organizations with a structured management framework for an information security management system through which the organization identifies, analyzes and addresses its information security risks. An effective information security management system allows an organization to continually secure itself adequately against information security risks and review and improve information security controls to keep pace with changes to security threats, vulnerabilities and business impacts.

8.2 ISMS as a source of information

8.2.1 ISMS

An information security management system 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, provides examples of the information that can be produced from an information security management system.

The insured should collect and collate the outputs from its information security management system, 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 with an insurer. Annex A provides examples on the documentation that can be produced from the use of an information security management system by the insured.

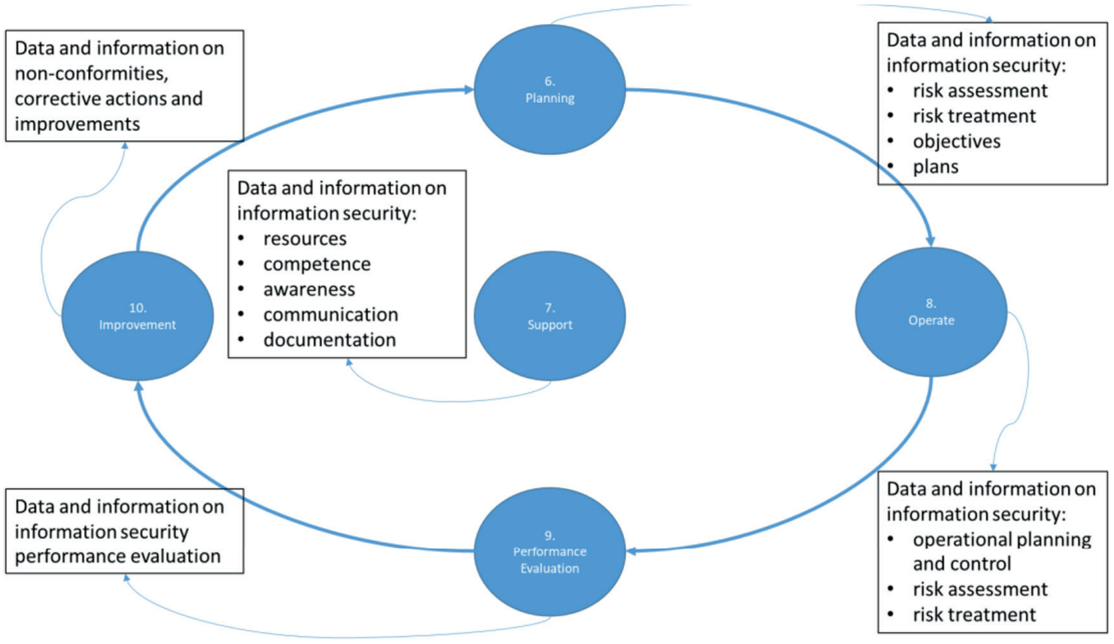
Data and information on non-conformities, corrective actions and improvements
6. Planning
Data and information on information security:
• risk assessment
• risk treatment
• objectives
• plans
Data and information on information security:
• resources
• competence
• awareness
• communication
• documentation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

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

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

8.2.2 Planning

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

a) ensure the information security management system 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.

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

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.

© ISO/IEC 2018 – All rights reserved

8.2.3 Support

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

a) the information security policy;

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

c) the implications of not conforming with the information security management system 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 information security management system including:

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) who communicates; and

e) the processes by which communications are effected.

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

When implementing, operating or maintaining an information security management system, 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 information security management system.

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

During operation, following the requirements of information security management system, 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

The performance evaluation 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 information security management system can be used to gather further data on the efficiency and effectiveness of information security controls and the information security management system; 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 information security management system 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 communicated to an insurer.

8.2.6 Improvement

When reacting to identified non-conformance, the steps taken can assist in the treatment of information security risks. The treatment should be documented and an insurer informed of the steps taken and the risk treatment applied.

The insured can also document the steps taken to improve the suitability, adequacy and effectiveness of the information security management system.

8.3 Sharing of information about risks and controls

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, with any deductibles or exclusions clearly stated.

There are challenges in putting together an appropriately designed cyber insurance policy that can reinforce risk management and treatment, and most importantly, to address losses as intended.

Cyber insurance is a risk sharing option, which is part of the insured's information security management, as such there is value in the insured regularly providing relevant cyber security information to an insurer. Such information should be agreed between the insured and an insurer as stated in the cyber

© ISO/IEC 2018 – All rights reserved

insurance policy. 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, upon request, any documentation held by the insured relating to its information security or cyber risk activities. Such documents can include information security management system documentation, internal or external audit reports and follow-up results, information security or security certifications held by the insured or individuals, policies, procedures, and guidelines.

8.4 Meeting cyber insurance policy obligations

An insurer usually requires 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 has usually shared information about the adopted security controls. These controls need to be maintained during the validity of the contract.

An information security management system 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. Such obligations can include a statement covering:

a) overall risk exposure of the insured, including the insured's loss history, years in business, and financial condition;

b) frequency or likelihood that an incident will occur at the insured;

c) frequency or likelihood that such an event will cause damage to the insured or to others for which the insured is legally liable;

d) scope and effectiveness of an implemented information security management system;

e) expected loss should such a loss event occur;

f) extent of use of outsourced security services and dependency on vendor and supplier networks; and

g) steps for prevention and treatment adopted to avoid or reduce any cyber loss.

Annex A
(informative)

Examples of ISMS documents for sharing

This Annex provides examples of documented information relating to the insured's information security management system 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 information security management system 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

27001:2013 Clause / Sub Clause	**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	Process processes and records of processes being carried out
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 internal an insurer's roles and responsibilities;

c) plans and records of awareness programmes;

d) documents on the management of outsourced processes;

© ISO/IEC 2018 – All rights reserved

e) records of incident response.

Bibliography

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

[2] ISO/IEC 27003:—, *Information technology — Security techniques — Information security management – Guidance*

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

[4] ISO/IEC 27005:—, *Informationtechnology — Security techniques — Information security risk management*

© ISO/IEC 2018 – All rights reserved