Teknisk rapport
SIS-ISO/IEC TR 27103:2018

Publicerad/Published: 2018-03-15
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 35.030

Informationsteknik - Säkerhetstekniker - Cybersäkerhet i ISO- och IEC-standarder (ISO/IEC TR 27103:2018, IDT)

Information technology - Security techniques - Cybersecurity and ISO and IEC Standards (ISO/IEC TR 27103:2018, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Denna tekniska rapport är inte en svensk standard. Detta dokument innehåller den engelska språkversionen ISO/IEC TR 27103:2018.

This Technical Report is not a Swedish Standard. This document contains the English version of ISO/IEC TR 27103:2018.

Upplysningar om sakinnehållet i detta dokument lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of this document is available from the SIS, Swedish Standards Institute, telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about national and international standards.

Detta dokument är framtaget av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i det här dokumentet, vill du delta i ett kommande revideringsarbete eller vara med och ta fram standarder inom området? Gå in på www.sis.se - där hittar du mer information.

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

Security on the Internet and other networks is a subject of growing concern. Organizations around the world, in both government and industry sectors, are seeking ways to address and manage cybersecurity risks, including via baseline cybersecurity measures that can be implemented as requirements or guidance. The demonstrated security and economic value of utilising existing best practices to develop approaches to cyber risk management has led organizations to assess how to use and improve upon existing approaches.

Perspectives, and consequent approaches, to risk management are affected by the terminology used, e.g. “cybersecurity” versus “information security”. Where similar risks are addressed, this different perspective can result in “cybersecurity” approaches focusing on external threats and the need to use information for organizational purposes, while, in contrast, ”information security” approaches consider all risks whether from internal or external sources. There can also be a perception that cybersecurity risks are primarily related to antagonistic threats, and that a lack of “cybersecurity” can create worse consequences to the organization than a lack of “information security”. Thus, cybersecurity can be perceived as more relevant to the organization than information security. This perception can cause confusion and also reduces the effectiveness of risk assessment and treatment.

Regardless of perception, the concepts behind information security can be used to assess and manage cybersecurity risks. The key question is how to manage cybersecurity risk in a comprehensive and structured manner, and ensure that processes, governance and controls exist and are fit for purpose. This can be done through a management systems approach. An Information Security Management System (ISMS) as described in ISO/IEC 27001 is a well proven way for any organization to implement a risk-based approach to cybersecurity.

This document demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.

Information technology — Security techniques — Cybersecurity and ISO and IEC Standards

1 Scope

This document provides guidance on how to leverage existing standards in a cybersecurity framework.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
information security
preservation of confidentiality, integrity and availability of information

[SOURCE: ISO/IEC 27000:2016 2.33]

4 Document structure

This document provides background on the reasons why having a risk-based, prioritized, flexible, outcome-focused, and communications-enabling framework for cybersecurity is important. It then describes the objectives of a strong cybersecurity framework and includes mapping to existing standards that can be used to achieve these objectives.

5 Background

5.1 General

Cybersecurity is a relatively new discipline. ISO, IEC, and ISO/IEC standards developed over the last 25 years can be applied to help solve the challenges of cybersecurity. Existing and emerging cybersecurity frameworks throughout the world reference ISO, IEC, and ISO/IEC standards as useful sources of information.

Implementing cybersecurity framework, or a cybersecurity programme, requires a consistent and iterative approach to identifying, assessing, and managing risk and evaluating implementation of the framework. ISO/IEC 27001 already provides a risk management framework that can be applied to prioritize and implement cybersecurity activities within an organization.

5.2 Advantages of a risk-based approach to cybersecurity

A risk-based approach to cybersecurity:

- enables organizations to measure the impact of cybersecurity investments and improve their cybersecurity risk management over time;
- is prioritized, flexible, and outcome-focused;
- enables organizations to make security investment decisions that address risk, implement risk mitigations in a way that is most effective for their environments, and advance security improvements and innovations;
- facilitates communication across boundaries, both within and between organizations;
- is responsive to the actual risks faced by an organization, while recognizing that organizational resources are limited;
- reflects a clear understanding of the organization's particular business drivers and security considerations;
- allows an organization to manage risks in ways that are consistent with their own business priorities;
- enables organizations to have flexibility in a rapidly changing technology and threat landscape, and helps to address the varying needs of organizations and sectors.

More detailed and prescriptive guidance (e.g. detailed standards and guidelines) required by specific stakeholders for specific purposes can be provided on demand. Organizations that implement a risk-based cybersecurity framework can therefore take advantage of the benefits without being limited by the need for a full set of detailed implementation guidance.

5.3 Stakeholders

Stakeholders need to play an active role, beyond protecting their own assets, in order for the organization to realize the benefits of a connected global environment. Internet-enabled systems and applications are expanding beyond the business-to-business, business-to-consumer, and consumer-to-consumer models, to include many-to-many interactions and transactions. Individuals and organizations need to be prepared to address emerging security risks and challenges and effectively prevent and respond to misuse and criminal exploitation.

5.4 Activities of a cybersecurity framework and programme

The activities of a cybersecurity framework and programme are:

a) describe the organization's current cybersecurity status;

b) describe the organization's target state for cybersecurity;

c) identify and prioritize opportunities for improvement;

d) assess progress toward the target state;

e) communicate among internal and external stakeholders about cybersecurity risk.

6 Concepts

6.1 Overview of cybersecurity frameworks

A cybersecurity framework captures a set of desired cybersecurity outcomes that are common across all sectors and organizations. A framework facilitates communication about implementation of these desired outcomes and associated cybersecurity activities across the organization, from the executive level to the implementation and operations levels. The framework should consist of five functions, or high-level descriptions of desired outcomes, which are concurrent and continuous:

— Identify;

— Protect;

— Detect;

— Respond;

— Recover.

When considered together, these functions provide a high-level, strategic view of an organization's management of cybersecurity risk. Within each function, there are also categories and sub-categories, a prioritized set of activities that are important for achieving the specified outcomes.

Categories are the subdivisions of a function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Sub-categories further divide a category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each category.

Organizing a cybersecurity framework into multiple levels, such as functions, categories, and sub-categories, helps to enable communication across boundaries. While many executives can seek to understand and make investments to more effectively mitigate organizational risk at the level of functions, operational practitioners can benefit from the more nuanced description of desired outcomes at the category or sub-category level. Importantly, though, if high-level and more nuanced descriptions of outcomes are organized within a single reference point that uses a common language, communication between executives and practitioners is facilitated, supporting strategic planning.

NOTE Annex B provides an example of another cybersecurity framework.

6.2 Cybersecurity framework functions

6.2.1 Overview

Functions organize basic cybersecurity outcomes and activities at their highest level. Important functions to include in a framework, as noted previously, are:

— Identify;

— Protect;

— Detect;

— Respond;

— Recover.

Each of these functions represents an area that an organization can use to express how it manages cybersecurity risk. These functions aid in organizing activities, enabling risk management decisions, addressing threats, and improving by learning from previous experiences.