TECHNICAL REPORT

ISO/IEC TR 27103

First edition
2018-02

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

Technologies de l'information — Techniques de sécurité — Cybersécurité et normes ISO et IEC

Reference number
ISO/IEC TR 27103:2018(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, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Document structure **1**
5 Background **1**
5.1 General 1
5.2 Advantages of a risk-based approach to cybersecurity 2
5.3 Stakeholders 2
5.4 Activities of a cybersecurity framework and programme 2
6 Concepts **3**
6.1 Overview of cybersecurity frameworks 3
6.2 Cybersecurity framework functions 3
6.2.1 Overview 3
6.3 Identify 4
6.4 Protect 5
6.5 Detect 6
6.6 Respond 7
6.7 Recover 7
Annex A (informative) **sub-categories** **9**
Annex B (informative) **Three principles and ten essentials of the cybersecurity for top management** **20**
Bibliography **23**

© ISO/IEC 2018 – All rights reserved

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*.

© ISO/IEC 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved