
Information security management — Guidelines for cyber-insurance

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



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this document	2
5 Overview of cyber-insurance and cyber-insurance policy	2
5.1 Cyber-insurance	2
5.2 Cyber-insurance policy	3
6 Cyber-risk and insurance coverage	3
6.1 Risk management process and cyber-insurance	3
6.2 Cyber-incidents	4
6.2.1 General	4
6.2.2 Cyber-incident types	4
6.3 Business impact and insurable losses	4
6.3.1 Overview	4
6.3.2 Type of coverage	5
6.3.3 Liability	5
6.3.4 Incident response costs	5
6.3.5 Cyber-extortion costs	7
6.3.6 Business interruption	7
6.3.7 Legal and regulatory fines and penalties	7
6.3.8 Contractual penalties	7
6.3.9 Systems damage	8
6.4 Supplier risk	8
6.5 Silent or non-affirmative coverage in other insurance policies	8
6.6 Vendors and counsel for incident response	8
6.7 Cyber-insurance policy exclusions	8
6.8 Coverage amount limits	9
7 Risk assessment supporting cyber-insurance underwriting	9
7.1 Overview	9
7.2 Information collection	9
7.3 Cyber-risk assessment of the insured	10
7.3.1 General	10
7.3.2 Inherent cyber-risk assessment	10
7.3.3 Information security controls assessment	10
7.3.4 Review prior cyber-losses	11
8 Role of ISMS in support of cyber-insurance	11
8.1 Overview	11
8.2 ISMS as a source of information	12
8.2.1 ISMS	12
8.2.2 Planning	12
8.2.3 Support	13
8.2.4 Operation	13
8.2.5 Performance evaluation	14
8.2.6 Improvement	14
8.3 Sharing of information about risks and controls	14
8.4 Meeting cyber-insurance policy obligations	15
Annex A (informative) Examples of ISMS documents for sharing	16
Bibliography	17

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.