INTERNATIONAL **ISO/IEC**

First edition
2011-09-01

Information technology — Security techniques — Information security incident management

Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information

Reference number
ISO/IEC 27035:2011(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards 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 International Standards 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.

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.

ISO/IEC 27035 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27035 cancels and replaces ISO/IEC TR 18044:2004, which has been technically revised.

Introduction

In general, information security policies or controls alone will not guarantee total protection of information, information systems, services or networks. After controls have been implemented, residual vulnerabilities are likely to remain that can make information security ineffective and thus information security incidents possible. This can potentially have both direct and indirect adverse impacts on an organization's business operations. Further, it is inevitable that new instances of previously unidentified threats will occur. Insufficient preparation by an organization to deal with such incidents will make any response less effective, and increase the degree of potential adverse business impact. Therefore, it is essential for any organization serious about information security to have a structured and planned approach to:

- detect, report and assess information security incidents;
- respond to information security incidents, including the activation of appropriate controls for the prevention and reduction of, and recovery from, impacts (for example in the support of crisis management areas);
- report information security vulnerabilities that have not yet been exploited to cause information security events and possibly information security incidents, and assess and deal with them appropriately;
- learn from information security incidents and vulnerabilities, institute preventive controls, and make improvements to the overall approach to information security incident management.

This International Standard provides guidance on information security incident management in Clause 4 to Clause 9. These clauses consist of several subclauses, which include a detailed description of each phase.

The term ‘information security incident management’ is used in this International Standard to encompass the management of not just information security incidents but also information security vulnerabilities.