

American National Standard

INCITS/ISO/IEC 30111:2013[2014]

(ISO/IEC 30111:2013, IDT)

Reaffirmed as INCITS/ISO/IEC 30111:2013
(R2019)

*Information technology - Security techniques -
Vulnerability handling processes*

Developed by



Where IT all begins



INCITS/ISO/IEC 30111:2013[2014]

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 6/25/2014

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2014 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

This is a preview of "INCITS/ISO/IEC 30111...". Click [here](#) to purchase the full version from the ANSI store.

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Interface between ISO/IEC 29147 - Vulnerability disclosure and ISO/IEC 30111 - Vulnerability handling processes	2
6 Policy and Organizational Framework for Vulnerability Handling Processes	3
6.1 General.....	3
6.2 Vulnerability Handling Policy Development.....	4
6.3 Development of an Organizational Framework to Support the Vulnerability Handling Process.....	4
6.4 Vendor CSIRT or PSIRT.....	5
6.5 Responsibilities of the Product Business Division.....	6
6.6 Responsibilities of the Customer Support Division and Public Relation Division.....	6
6.7 Legal Consultation.....	6
7 Vulnerability handling process	7
7.1 Introduction to vulnerability handling phases.....	7
7.2 Vulnerability handling phases.....	8
7.3 Monitoring of Vulnerability handling phases.....	10
7.4 Confidentiality of Vulnerability Information.....	10
8 Supply chain vulnerability handling process	11
Bibliography	12

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 30111 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This is a preview of "INCITS/ISO/IEC 30111...". [Click here to purchase the full version from the ANSI store.](#)

Introduction

This International Standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services.

The audience for this standard includes consumers, developers, vendors, and evaluators of secure IT products. The following audiences may use this standard:

- developers and vendors, when responding to reported actual or potential vulnerabilities;
- evaluators, when assessing the security assurance afforded by vendors' and developers' vulnerability handling processes and the associated products and services;
- consumers, when selecting product and online service vendors to express best practice assurance requirements to developers, vendors and integrators.

This International Standard is related to ISO/IEC 29147.^[5] It interfaces with elements described in ISO/IEC 29147 at the point of receiving potential vulnerability reports, and at the point of distributing vulnerability resolution information.

This International Standard takes into consideration the relevant elements of ISO/IEC 15408-3,^[1] 13.5 Flaw remediation (ALC_FLR).

This is a preview of "INCITS/ISO/IEC 30111...". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "INCITS/ISO/IEC 30111...". Click [here](#) to purchase the full version from the ANSI store.

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This International Standard gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

This International Standard is applicable to vendors involved in handling vulnerabilities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. 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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1

coordinator

optional participant that can assist vendors and finders in handling and disclosing vulnerability information

Note 1 to entry: Acts as trusted liaison between involved parties, enabling communication between involved parties (vendors and finders).

3.2

online service

service which is implemented by hardware, software or a combination of them, and provided over a communication line or network

EXAMPLE Search engines, online backup services, Internet-hosted email, and software as a service are considered to be online services.

3.3

product

system or service implemented or refined for sale or to be offered for free

Note 1 to entry: In information technology, a distinction is often made between hardware and software products, although the boundary is not always clear.

EXAMPLE A router can be seen as a hardware product even though a vital component of it is software and/or firmware.

3.4

remediation

patch, fix, upgrade, configuration or documentation change to address a vulnerability

Note 1 to entry: A change intended to resolve or mitigate a vulnerability. A remediation typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Remediations are usually provided by vendors. Vendors use different terms including update, patch, fix, hotfix, and upgrade.