BS ISO/IEC 30111:2013

BSI Standards Publication

Information technology — Security techniques — Vulnerability handling processes

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 30111:2013.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013. Published by BSI Standards Limited 2013

ISBN 978 0 580 75882 9

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2013.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30111:2013

INTERNATIONAL STANDARD

ISO/IEC 30111

First edition
2013-11-01

Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Reference number
ISO/IEC 30111:2013(E)

Documents
Document Sharing Hub

© ISO/IEC 2013

Full document details: BS ISO/IEC 30111:2013

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, 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
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

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30111:2013

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**

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30111:2013

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*.

© ISO/IEC 2013 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30111:2013

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).

© ISO/IEC 2013 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30111:2013

Documents
Document Sharing Hub