

---

---

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

*Information technology — Security techniques — Vulnerability  
handling processes*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 30111:2019](https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019)

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>



## iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/IEC 30111:2019

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>



### DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2019

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office  
Case postale 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Genève  
Tél.: +41 22 749 01 11  
Fax: +41 22 749 09 47  
E-mail: [copyright@iso.org](mailto:copyright@iso.org)  
Web: [www.iso.org](http://www.iso.org)

Publié en Suisse

## Sommaire

Page

<b>Avant-propos</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Domaine d'application</b> .....	<b>1</b>
<b>2 Références normatives</b> .....	<b>1</b>
<b>3 Termes et définitions</b> .....	<b>1</b>
<b>4 Abréviations</b> .....	<b>1</b>
<b>5 Relations aux autres Normes internationales</b> .....	<b>1</b>
5.1 ISO/IEC 29147 .....	1
5.2 ISO/IEC 27034 (toutes les parties) .....	3
5.3 ISO/IEC 27036-3 .....	4
5.4 ISO/IEC 15408-3 .....	4
<b>6 Politique et cadre organisationnel</b> .....	<b>4</b>
6.1 Généralités .....	4
6.2 Leadership .....	4
6.2.1 Leadership et engagement .....	4
6.2.2 Politique .....	5
6.2.3 Rôles, responsabilités et autorités au sein de l'organisme .....	5
6.3 Élaboration de la politique de traitement des vulnérabilités .....	5
6.4 Développement du cadre organisationnel .....	5
6.5 CSIRT ou PSIRT du fournisseur .....	6
6.5.1 Généralités .....	6
6.5.2 Mission d'une PSIRT .....	6
6.5.3 Responsabilités d'une PSIRT .....	6
6.5.4 Capacités du personnel .....	8
6.6 Responsabilités de la division d'activités produit .....	8
6.7 Responsabilités du support client et des relations publiques .....	8
6.8 Consultation juridique .....	9
<b>7 Processus de traitement des vulnérabilités</b> .....	<b>9</b>
7.1 Phases de traitement des vulnérabilités .....	9
7.1.1 Généralités .....	9
7.1.2 Préparation .....	10
7.1.3 Réception .....	10
7.1.4 Vérification .....	10
7.1.5 Développement d'une remédiation .....	11
7.1.6 Publication .....	12
7.1.7 Post-publication .....	12
7.2 Surveillance du processus .....	12
7.3 Confidentialité des informations de vulnérabilité .....	13
<b>8 Considérations relatives à la chaîne d'approvisionnement</b> .....	<b>13</b>
<b>Bibliographie</b> .....	<b>15</b>

## Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de document. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir [www.iso.org/directives](http://www.iso.org/directives)).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir [www.iso.org/brevets](http://www.iso.org/brevets)) ou dans la liste des déclarations de brevets reçues par l'IEC (voir <https://patents.iec.c>).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: [www.iso.org/iso/fr/avant-propos](http://www.iso.org/iso/fr/avant-propos).

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse [www.iso.org/fr/members.html](http://www.iso.org/fr/members.html).

Cette deuxième édition annule et remplace la première édition (ISO/IEC 30111:2013), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

- certaines dispositions normatives ont été révisées ou ajoutées (synthétisées à l'Annexe A);
- des modifications organisationnelles et rédactionnelles ont été apportées à des fins de clarté et d'harmonisation avec l'ISO/IEC 29147:2018.

Le présent document est destiné à être utilisé avec l'ISO/IEC 29147.

## Introduction

Le présent document décrit des processus à l'attention des fournisseurs pour traiter les signalements de vulnérabilités potentielles dans leurs produits et services.

Le présent document s'adresse aux développeurs, fournisseurs, évaluateurs et utilisateurs de produits et services de technologies de l'information. Il peut être utilisé par:

- les développeurs et les fournisseurs, lorsqu'ils répondent à des signalements de vulnérabilités réelles ou potentielles;
- les évaluateurs, lorsqu'ils évaluent l'assurance de sécurité permise par les processus de traitement de vulnérabilités de fournisseurs et de développeurs;
- les utilisateurs, pour exprimer des besoins d'achat à des développeurs, des fournisseurs et des intégrateurs.

Le présent document est intégré à l'ISO/IEC 29147 au point de réception de signalements de vulnérabilités potentielles et au point de diffusion d'informations sur la remédiation de vulnérabilités (voir [5.1](#)).

Les relations avec d'autres normes sont précisées dans l'[Article 5](#).

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 30111:2019](#)

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 30111:2019

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>

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

## 1 Domaine d'application

Le présent document fournit des exigences et des recommandations sur la manière de traiter et résoudre les vulnérabilités potentielles signalées dans un produit ou un service.

Le présent document s'applique aux fournisseurs impliqués dans le traitement des vulnérabilités.

## 2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 29147:2018, *Technologies de l'information — Techniques de sécurité — Divulcation de vulnérabilité*

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000 et l'ISO/IEC 29147 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>
- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>

## 4 Abréviations

Les abréviations suivantes sont utilisées dans le présent document:

CSIRT	Équipe d'intervention en cas d'incidents de sécurité informatique (Computer Security Incident Response Team)
PSIRT	Équipe d'intervention en cas d'incidents de sécurité produit (Product Security Incident Response Team)

## 5 Relations aux autres Normes internationales

### 5.1 ISO/IEC 29147

L'ISO/IEC 29147 doit être utilisée conjointement avec le présent document. La [Figure 1](#) présente la relation entre les deux normes.

## ISO/IEC 30111:2019(F)

Le présent document fournit des lignes directrices à l'attention des fournisseurs afin de traiter et résoudre les informations relatives à des vulnérabilités potentielles signalées par des individus ou organismes internes et externes.

L'ISO/IEC 29147 fournit des lignes directrices à l'attention des fournisseurs à inclure dans leurs processus métier habituels lorsqu'ils reçoivent des signalements concernant des vulnérabilités potentielles de la part d'individus ou organismes externes, et lorsqu'ils transmettent aux utilisateurs concernés des informations relatives à la remédiation de vulnérabilités.

Alors que le présent document traite de la recherche, du tri et de la remédiation des vulnérabilités signalées par une source interne ou externe, l'ISO/IEC 29147 couvre l'interface entre les fournisseurs et les individus ou organismes qui détectent et signalent des vulnérabilités potentielles.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 30111:2019](https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019)

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>



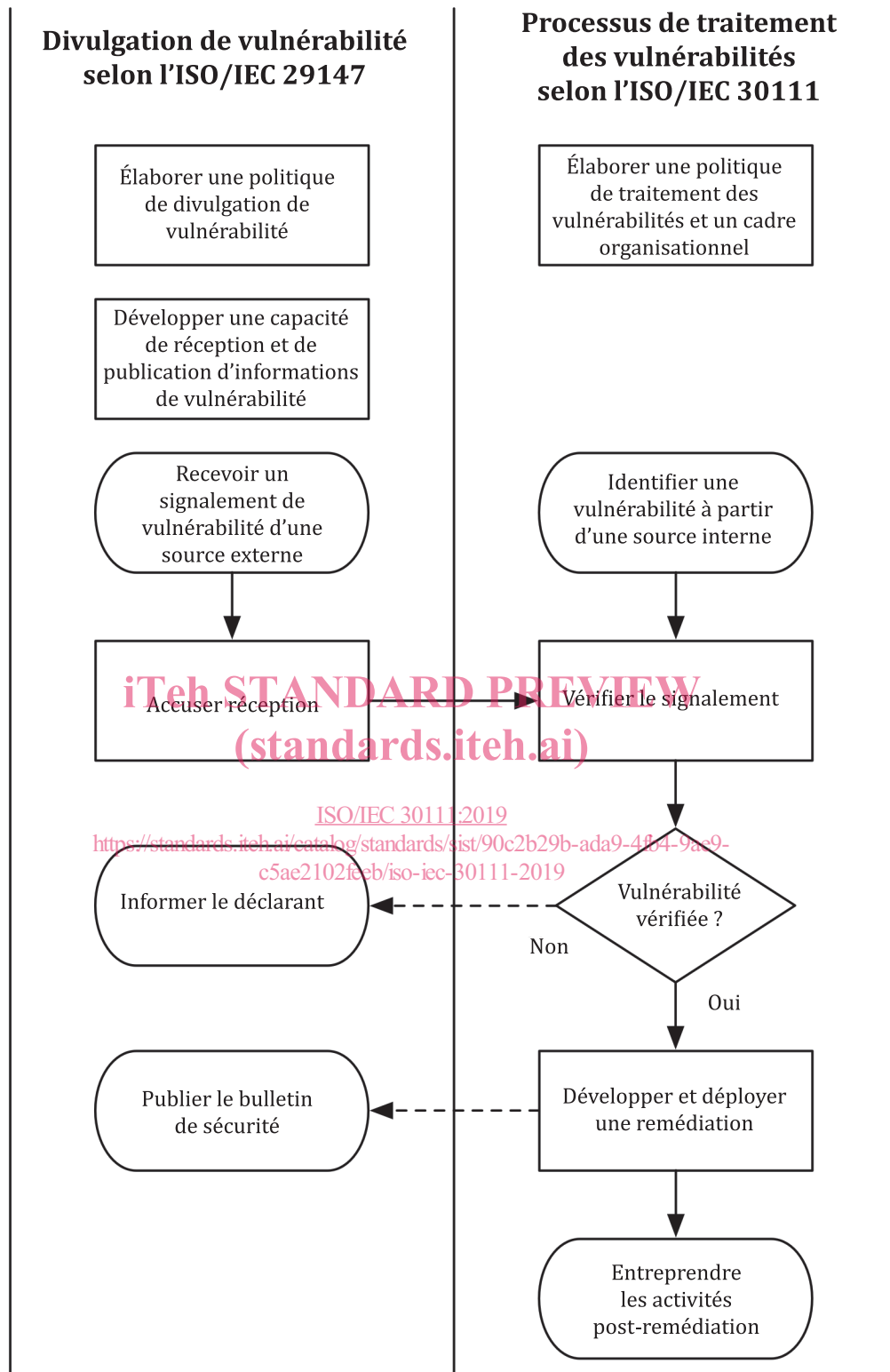


Figure 1 — Relation entre l'ISO/IEC 29147et l'ISO/IEC 30111

## 5.2 ISO/IEC 27034 (toutes les parties)

La sécurité des applications cherche à réduire la création de vulnérabilités d'application (voir l'ISO/IEC 27034-1:2011, 6.5.2<sup>[1]</sup>). Les techniques de sécurité des applications peuvent également être utiles pour la remédiation de vulnérabilités signalées.

### 5.3 ISO/IEC 27036-3

Des processus de traitement des vulnérabilités efficaces nécessitent une compréhension approfondie de la sécurité de la chaîne d'approvisionnement TIC, comme décrit dans l'ISO/IEC 27036-3:2013, 5.4 a), 5.8 i), 6.1.1 a) 2) et 6.3.4<sup>[2]</sup>.

### 5.4 ISO/IEC 15408-3

Le présent document tient compte des éléments pertinents de l'ISO/IEC 15408-3:2008, 13.5<sup>[3]</sup>.

## 6 Politique et cadre organisationnel

### 6.1 Généralités

L'Article 6 décrit les éléments organisationnels qu'il convient que les fournisseurs prennent en compte dans leurs processus de traitement des vulnérabilités. Il convient que les fournisseurs créent un processus de traitement des vulnérabilités conforme au présent document afin de se préparer au travail de recherche et de remédiation des vulnérabilités potentielles. La création d'un processus de traitement des vulnérabilités est une tâche effectuée par un fournisseur, et il convient de l'évaluer régulièrement afin de s'assurer que le processus présente les performances attendues et de garantir l'amélioration des processus. Il convient que les fournisseurs documentent leurs processus de traitement des vulnérabilités pour en assurer la répétabilité. Il convient que la documentation décrive les procédures et les méthodes utilisées pour suivre l'ensemble des vulnérabilités signalées.

Voir l'ISO/IEC 27034 (toutes les parties)<sup>[4]</sup> pour des informations sur la manière dont l'identification de la cause fondamentale d'une vulnérabilité, qui constitue l'une des étapes du processus de traitement des vulnérabilités, peut aider à améliorer les cycles de vie de développement de logiciels sécurisés et conduire, par voie de conséquence, au développement de produits plus sécurisés.

### 6.2 Leadership

<https://standards.iteh.ai/catalog/standards/sist/90c2b29b-ada9-4fb4-9ae9-c5ae2102feeb/iso-iec-30111-2019>

#### 6.2.1 Leadership et engagement

Il convient que la direction démontre son leadership et son engagement en faveur du traitement des vulnérabilités:

- a) en s'assurant que la politique et les objectifs de traitement des vulnérabilités sont établis et qu'ils sont compatibles avec l'orientation stratégique de l'organisme;
- b) en s'assurant que le traitement des vulnérabilités est intégré dans les processus de l'organisme;
- c) en s'assurant que les ressources nécessaires pour le traitement des vulnérabilités sont disponibles;
- d) en communiquant l'importance d'un traitement efficace des vulnérabilités;
- e) en s'assurant que le processus de traitement des vulnérabilités atteint le ou les résultats escomptés;
- f) en orientant et en soutenant les personnes pour qu'elles contribuent à l'efficacité du processus de traitement des vulnérabilités;
- g) en promouvant l'amélioration continue; et
- h) en aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

## 6.2.2 Politique

Il convient que la direction établisse une politique de traitement des vulnérabilités qui:

- a) est appropriée à la mission de l'organisme;
- b) inclut un engagement au mieux des possibilités pour satisfaire aux exigences de l'utilisateur en ce qui concerne la sécurité de son produit ou de son service en ligne; et
- c) inclut un engagement pour l'amélioration continue du processus de traitement des vulnérabilités.

Des informations supplémentaires concernant la politique de traitement des vulnérabilités sont fournies en [6.3](#).

## 6.2.3 Rôles, responsabilités et autorités au sein de l'organisme

Il convient que la direction s'assure que les responsabilités et autorités des rôles concernés par le traitement des vulnérabilités sont attribuées et communiquées.

Il convient que la direction désigne qui a la responsabilité et l'autorité de:

- a) s'assurer que le processus de traitement des vulnérabilités est conforme aux exigences du présent document; et
- b) rendre compte à la direction de la performance du traitement des vulnérabilités.

## 6.3 Élaboration de la politique de traitement des vulnérabilités

Un fournisseur doit élaborer et tenir à jour une politique interne de traitement des vulnérabilités pour définir et clarifier ses intentions en matière de recherche et de remédiation des vulnérabilités dans le cadre d'un processus de traitement des vulnérabilités. Il convient que cette politique soit compatible avec la politique de divulgation de vulnérabilité externe exigée par l'ISO/IEC 29147.

La politique interne de traitement des vulnérabilités est destinée au personnel du fournisseur et définit qui est responsable à chaque étape du processus de traitement des vulnérabilités et la manière dont il convient que le personnel traite les signalements de vulnérabilités potentielles. Il convient qu'elle comprenne les éléments suivants:

- a) les recommandations de base, principes et responsabilités pour le traitement des vulnérabilités potentielles dans des produits ou services;
- b) une liste des départements et rôles responsables du traitement des vulnérabilités potentielles;
- c) les moyens de protection pour empêcher une divulgation prématurée d'informations concernant des vulnérabilités potentielles avant leur résolution;
- d) un objectif de calendrier pour le développement de remédiations.

La politique de divulgation de vulnérabilité externe s'adresse à des parties prenantes internes et externes, y compris des déclarants qui souhaitent signaler des vulnérabilités potentielles et des utilisateurs de produits ou de services du fournisseur. Cette politique informe son public sur la manière dont le fournisseur entend interagir avec lui lorsqu'une vulnérabilité potentielle est détectée dans le produit ou les services du fournisseur. Des recommandations, des détails et des exemples de politiques de divulgation de vulnérabilité publique sont fournis dans l'ISO/IEC 29147:2018, Article 9 et Annexe A.

## 6.4 Développement du cadre organisationnel

Le traitement des vulnérabilités présente des aspects qui dépassent le simple cadre de l'ingénierie et de la technologie (par exemple, le service client et les relations publiques). Il convient que les divisions parties prenantes du fournisseur qui sont responsables de chaque aspect conçoivent, reconnaissent et soutiennent un cadre organisationnel.