

Redline version  
compare la Deuxième édition  
à la Troisième édition



---

---

## Sécurité de l'information, cybersécurité et protection de la vie privée — Moyens de maîtrise de l'information

*Information security, cybersecurity and privacy protection —  
Information security controls*

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/IEC 27002:2022](https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022)

<https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>



Numéro de référence  
ISO/IEC27002:redline:2023(F)

### IMPORTANT — PLEASE NOTE

This is a provisional mark-up copy and uses the following colour coding:

- Text example 1 — indicates added text (in green)
- ~~Text example 2~~ — indicates removed text (in red)
- indicates added graphic figure
- indicates removed graphic figure
- 1.x ... — Heading numbers containing modifications are highlighted in yellow in the Table of Contents

All changes in this document have yet to reach consensus by vote and as such should only be used internally for review purposes.

### DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.



### DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2023

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

Avant-propos .....	ix
<del>0</del> Introduction .....	xi
<b>1</b> <del>Domaine d'application</del> d'application .....	1
<b>2</b> Références normatives .....	1
<b>3</b> <del>Termes et définitions</del> , définitions et abréviations .....	1
3.1 Termes et définitions .....	1
3.2 Abréviations .....	7
<b>4</b> <del>Structure de la présente norme</del> du présent document .....	8
4.1 Articles .....	8
4.2 <del>Thèmes et attributs</del> .....	9
<del>4.2</del> <del>Catégories de mesures</del> .....	10
<del>4.2</del> <del>4.3</del> .....	
Structure des moyens de maîtrise .....	10
<b>5</b> <del>Politiques de sécurité de l'information</del> .....	11
5.1 <del>Orientations de la direction en matière de sécurité de l'information</del> .....	11
5.1.1 <del>Politiques de sécurité de l'information</del> .....	11
5.1.2 <del>Revue des politiques de sécurité de l'information</del> .....	12
<b>6</b> <del>Organisation de la sécurité de l'information</del> .....	13
6.1 <del>Organisation interne</del> .....	13
6.1.1 <del>Fonctions et responsabilités liées à la sécurité de l'information</del> .....	13
6.1.2 <del>Séparation des tâches</del> .....	14
6.1.3 <del>Relations avec les autorités</del> .....	14
6.1.4 <del>Relations avec des groupes de travail spécialisés</del> .....	14
6.1.5 <del>La sécurité de l'information dans la gestion de projet</del> .....	15
6.2 <del>Appareils mobiles et télétravail</del> .....	15
6.2.1 <del>Politique en matière d'appareils mobiles</del> .....	16
6.2.2 <del>Télétravail</del> .....	17
<b>7</b> <del>La sécurité des ressources humaines</del> .....	18
7.1 <del>Avant l'embauche</del> .....	18
7.1.1 <del>Sélection des candidats</del> .....	19
7.1.2 <del>Termes et conditions d'embauche</del> .....	19
7.2 <del>Pendant la durée du contrat</del> .....	20
7.2.1 <del>Responsabilités de la direction</del> .....	20
7.2.2 <del>Sensibilisation, apprentissage et formation à la sécurité de l'information</del> .....	21
7.2.3 <del>Processus disciplinaire</del> .....	22
7.3 <del>Rupture, terme ou modification du contrat de travail</del> .....	23
7.3.1 <del>Achèvement ou modification des responsabilités associées au contrat de travail</del> .....	23
<b>8</b> <del>Gestion des actifs</del> .....	24
8.1 <del>Responsabilités relatives aux actifs</del> .....	24
8.1.1 <del>Inventaire des actifs</del> .....	24
8.1.2 <del>Propriété des actifs</del> .....	24
8.1.3 <del>Utilisation correcte des actifs</del> .....	25
8.1.4 <del>Restitution des actifs</del> .....	25
8.2 <del>Classification de l'information</del> .....	25
8.2.1 <del>Classification des informations</del> .....	26
8.2.2 <del>Marquage des informations</del> .....	27
8.2.3 <del>Manipulation des actifs</del> .....	27
8.3 <del>Manipulation des supports</del> .....	28
8.3.1 <del>Gestion des supports amovibles</del> .....	28
8.3.2 <del>Mise au rebut des supports</del> .....	28

8.3.3	<del>Transfert physique des supports</del>	29
<b>9</b>	<b><del>Contrôle d'accès</del></b>	<b>30</b>
9.1	<del>Exigences métier en matière de contrôle d'accès</del>	30
9.1.1	<del>Politique de contrôle d'accès</del>	30
9.1.2	<del>Accès aux réseaux et aux services en réseau</del>	31
9.2	<del>Gestion de l'accès utilisateur</del>	32
9.2.1	<del>Enregistrement et désinscription des utilisateurs</del>	32
9.2.2	<del>Maîtrise de la gestion des accès utilisateur</del>	32
9.2.3	<del>Gestion des privilèges d'accès</del>	33
9.2.4	<del>Gestion des informations secrètes d'authentification des utilisateurs</del>	34
9.2.5	<del>Revue des droits d'accès utilisateur</del>	34
9.2.6	<del>Suppression ou adaptation des droits d'accès</del>	35
9.3	<del>Responsabilités des utilisateurs</del>	36
9.3.1	<del>Utilisation d'informations secrètes d'authentification</del>	36
9.4	<del>Contrôle de l'accès au système et aux applications</del>	37
9.4.1	<del>Restriction d'accès à l'information</del>	37
9.4.2	<del>Sécuriser les procédures de connexion</del>	37
9.4.3	<del>Système de gestion des mots de passe</del>	38
9.4.4	<del>Utilisation de programmes utilitaires à privilèges</del>	39
9.4.5	<del>Contrôle d'accès au code source des programmes</del>	39
<b>10</b>	<b><del>Cryptographie</del></b>	<b>40</b>
10.1	<del>Mesures cryptographiques</del>	40
10.1.1	<del>Politique d'utilisation des mesures cryptographiques</del>	40
10.1.2	<del>Gestion des clés</del>	41
<b>11</b>	<b><del>Sécurité physique et environnementale</del></b>	<b>43</b>
11.1	<del>Zones sécurisées</del>	43
11.1.1	<del>Périmètre de sécurité physique</del>	43
11.1.2	<del>Contrôles physiques des accès</del>	44
11.1.3	<del>Sécurisation des bureaux, des salles et des équipements</del>	44
11.1.4	<del>Protection contre les menaces extérieures et environnementales</del>	45
11.1.5	<del>Travail dans les zones sécurisées</del>	45
11.1.6	<del>Zones de livraison et de chargement</del>	45
11.2	<del>Matériels</del>	46
11.2.1	<del>Emplacement et protection du matériel</del>	46
11.2.2	<del>Services généraux</del>	47
11.2.3	<del>Sécurité du câblage</del>	47
11.2.4	<del>Maintenance du matériel</del>	48
11.2.5	<del>Sortie des actifs</del>	48
11.2.6	<del>Sécurité du matériel et des actifs hors des locaux</del>	49
11.2.7	<del>Mise au rebut ou recyclage sécurisé(e) du matériel</del>	50
11.2.8	<del>Matériel utilisateur laissé sans surveillance</del>	50
11.2.9	<del>Politique du bureau propre et de l'écran vide</del>	51
<b>12</b>	<b><del>Sécurité liée à l'exploitation</del></b>	<b>51</b>
12.1	<del>Procédures et responsabilités liées à l'exploitation</del>	51
12.1.1	<del>Procédures d'exploitation documentées</del>	52
12.1.2	<del>Gestion des changements</del>	52
12.1.3	<del>Dimensionnement</del>	53
12.1.4	<del>Séparation des environnements de développement, de test et d'exploitation</del>	54
12.2	<del>Protection contre les logiciels malveillants</del>	55
12.2.1	<del>Mesures contre les logiciels malveillants</del>	55
12.3	<del>Sauvegarde</del>	56
12.3.1	<del>Sauvegarde des informations</del>	56
12.4	<del>Journalisation et surveillance</del>	57
12.4.1	<del>Journalisation des événements</del>	57
12.4.2	<del>Protection de l'information journalisée</del>	58
12.4.3	<del>Journaux administrateur et opérateur</del>	59

	<del>12.4.4</del> Synchronisation des horloges.....	59
<del>12.5</del>	<del>Maîtrise des logiciels en exploitation.....</del>	<del>59</del>
	<del>12.5.1</del> Installation de logiciels sur des systèmes en exploitation.....	<del>60</del>
<del>12.6</del>	<del>Gestion des vulnérabilités techniques.....</del>	<del>61</del>
	<del>12.6.1</del> Gestion des vulnérabilités techniques.....	<del>61</del>
	<del>12.6.2</del> Restrictions liées à l'installation de logiciels.....	<del>62</del>
<del>12.7</del>	<del>Considérations sur l'audit du système d'information.....</del>	<del>63</del>
	<del>12.7.1</del> Mesures relatives à l'audit des systèmes d'information.....	<del>63</del>
<del>13</del>	<del>Sécurité des communications.....</del>	<del>63</del>
	<del>13.1</del> Management de la sécurité des réseaux.....	<del>63</del>
	<del>13.1.1</del> Contrôle des réseaux.....	<del>63</del>
	<del>13.1.2</del> Sécurité des services de réseau.....	<del>64</del>
	<del>13.1.3</del> Cloisonnement des réseaux.....	<del>64</del>
<del>13.2</del>	<del>Transfert de l'information.....</del>	<del>65</del>
	<del>13.2.1</del> Politiques et procédures de transfert de l'information.....	<del>65</del>
	<del>13.2.2</del> Accords en matière de transfert d'information.....	<del>66</del>
	<del>13.2.3</del> Messagerie électronique.....	<del>67</del>
	<del>13.2.4</del> Engagements de confidentialité ou de non-divuligation.....	<del>68</del>
<del>14</del>	<del>Acquisition, développement et maintenance des systèmes d'information.....</del>	<del>69</del>
	<del>14.1</del> Exigences de sécurité applicables aux systèmes d'information.....	<del>69</del>
	<del>14.1.1</del> Analyse et spécification des exigences de sécurité de l'information.....	<del>69</del>
	<del>14.1.2</del> Sécurisation des services d'application sur les réseaux publics.....	<del>70</del>
	<del>14.1.3</del> Protection des transactions liées aux services d'application.....	<del>71</del>
<del>14.2</del>	<del>Sécurité des processus de développement et d'assistance technique.....</del>	<del>72</del>
	<del>14.2.1</del> Politique de développement sécurisé.....	<del>72</del>
	<del>14.2.2</del> Procédures de contrôle des changements apportés au système.....	<del>73</del>
	<del>14.2.3</del> Revue technique des applications après changement apporté à la plateforme d'exploitation.....	<del>74</del>
	<del>14.2.4</del> Restrictions relatives aux changements apportés aux logiciels.....	<del>74</del>
	<del>14.2.5</del> Principes d'ingénierie de la sécurité des systèmes.....	<del>75</del>
	<del>14.2.6</del> Environnement de développement sécurisé.....	<del>75</del>
	<del>14.2.7</del> Développement externalisé.....	<del>76</del>
	<del>14.2.8</del> Phase de test de la sécurité du système.....	<del>77</del>
	<del>14.2.9</del> Test de conformité du système.....	<del>77</del>
<del>14.3</del>	<del>Données de test.....</del>	<del>77</del>
	<del>14.3.1</del> Protection des données de test.....	<del>77</del>
<del>15</del>	<del>Relations avec les fournisseurs.....</del>	<del>78</del>
<del>15</del>	<del>5.....</del>	<del>78</del>
	<b>Moyens de maîtrise organisationnels.....</b>	<b>78</b>
	5.1 Politiques de sécurité de l'information.....	78
	5.2 Fonctions et responsabilités liées à la sécurité de l'information.....	80
	5.3 Séparation des tâches.....	81
	5.4 Responsabilités de la direction.....	82
	5.5 Contacts avec les autorités.....	83
	5.6 Contacts avec des groupes d'intérêt spécifiques.....	84
	5.7 Renseignements sur les menaces.....	85
	5.8 Sécurité de l'information dans la gestion de projet.....	86
	5.9 Inventaire des informations et autres actifs associés.....	88
	5.10 Utilisation correcte des informations et autres actifs associés.....	90
	5.11 Restitution des actifs.....	91
	5.12 Classification des informations.....	92
	5.13 Marquage des informations.....	93
	5.14 Transfert des informations.....	95
	5.15 Contrôle d'accès.....	97
	5.16 Gestion des identités.....	99
	5.17 Informations d'authentification.....	100

5.18	Droits d'accès	102
5.19	Sécurité de l'information dans les relations avec les fournisseurs	104
5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs	106
<del>15.1</del>	<del>Sécurité de l'information dans les relations avec les fournisseurs</del>	<del>108</del>
<del>15.1.1</del>	<del>Politique de sécurité de l'information dans les relations avec les fournisseurs</del>	<del>108</del>
<del>15.1.2</del>	<del>La sécurité dans les accords conclus avec les fournisseurs</del>	<del>109</del>
<del>15.1.3</del>	<del>Chaîne d'approvisionnement informatique</del>	<del>111</del>
<del>15.1</del>	<del>5.21</del>	<del>112</del>
	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC	112
<del>15.2</del>	<del>Gestion de la prestation du service</del>	<del>114</del>
<del>15.2</del>	<del>5.22</del>	<del>114</del>
	Surveillance, révision et gestion des changements des services fournisseurs	114
<del>15.2.1</del>	<del>Surveillance et revue des services des fournisseurs</del>	<del>114</del>
<del>15.2.2</del>	<del>Gestion des changements apportés dans les services des fournisseurs</del>	<del>115</del>
5.23	Sécurité de l'information dans l'utilisation de services en nuage	117
5.24	Planification et préparation de la gestion des incidents liés à la sécurité de l'information	120
5.25	Évaluation des événements liés à la sécurité de l'information et prise de décision	122
5.26	Réponse aux incidents liés à la sécurité de l'information	122
5.27	Tirer des enseignements des incidents liés à la sécurité de l'information	123
5.28	Collecte des preuves	124
5.29	Sécurité de l'information pendant une perturbation	125
5.30	Préparation des TIC pour la continuité d'activité	126
5.31	Exigences légales, statutaires, réglementaires et contractuelles	127
5.32	Droits de propriété intellectuelle	129
5.33	Protection des documents d'activité	130
5.34	Protection de la vie privée et des DCP	132
5.35	Révision indépendante de la sécurité de l'information	133
5.36	Conformité aux politiques, règles et normes de sécurité de l'information	134
5.37	Procédures d'exploitation documentées	135
<del>16</del>	<del>Gestion des incidents liés à la sécurité de l'information</del>	<del>136</del>
<del>16</del>	<del>6</del>	<del>136</del>
	Moyens de maîtrise applicables aux personnes	136
6.1	Sélection des candidats	136
6.2	Termes et conditions du contrat de travail	137
<del>16.1</del>	<del>6.3</del>	<del>138</del>
	Gestion des incidents liés à la sécurité de l'information et améliorations	138
<del>16.1</del>	<del>6.3</del>	<del>138</del>
	Sensibilisation, enseignement et formation en sécurité de l'information	138
<del>16.1.1</del>	<del>Responsabilités et procédures</del>	<del>139</del>
<del>16.1.2</del>	<del>Signalement des événements liés à la sécurité de l'information</del>	<del>140</del>
<del>16.1.3</del>	<del>Signalement des failles liées à la sécurité de l'information</del>	<del>141</del>
<del>16.1.4</del>	<del>Appréciation des événements liés à la sécurité de l'information et prise de décision</del>	<del>141</del>
<del>16.1.5</del>	<del>Réponse aux incidents liés à la sécurité de l'information</del>	<del>141</del>
<del>16.1.6</del>	<del>Tirer des enseignements des incidents liés à la sécurité de l'information</del>	<del>142</del>
<del>16.1.7</del>	<del>Recueil de preuves</del>	<del>142</del>
6.4	Processus disciplinaire	145
6.5	Responsabilités après la fin ou le changement d'un emploi	146
6.6	Accords de confidentialité ou de non-divulgateion	147
6.7	Travail à distance	148
6.8	Déclaration des événements liés à la sécurité de l'information	150
<del>17</del>	<del>Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité</del>	<del>151</del>
<del>17</del>	<del>7</del>	<del>151</del>
	Moyens de maîtrise physique	151

7.1	Périmètres de sécurité physique	151
7.2	Les entrées physiques	152
7.3	Sécurisation des bureaux, des salles et des installations	154
7.4	Surveillance de la sécurité physique	154
7.5	Protection contre les menaces physiques et environnementales	155
7.6	Travail dans les zones sécurisées	157
7.7	Bureau vide et écran vide	157
7.8	Emplacement et protection du matériel	158
7.9	Sécurité des actifs hors des locaux	159
<del>17.1</del>	<del>Continuité de la sécurité de l'information</del>	<del>160</del>
<del>17.1</del>	<del>7.10</del>	<del>160</del>
	Supports de stockage	160
<del>17.1.1</del>	<del>Organisation de la continuité de la sécurité de l'information</del>	<del>161</del>
<del>17.1.2</del>	<del>Mise en œuvre de la continuité de la sécurité de l'information</del>	<del>161</del>
<del>17.1.3</del>	<del>Vérifier, revoir et évaluer la continuité de la sécurité de l'information</del>	<del>162</del>
7.11	Services supports	164
7.12	Sécurité du câblage	165
7.13	Maintenance du matériel	166
<del>17.2</del>	<del>Redondances</del>	<del>167</del>
<del>17.2</del>	<del>7.14</del>	<del>167</del>
	Élimination ou recyclage sécurisé(e) du matériel	167
<del>17.2.1</del>	<del>Disponibilité des moyens de traitement de l'information</del>	<del>167</del>
<del>18</del>	<del>Conformité</del>	<del>169</del>
<del>18</del>	<del>8</del>	<del>169</del>
	<b>Moyens de maîtrise technologiques</b>	<b>169</b>
8.1	Terminaux utilisateurs	169
8.2	Droits d'accès privilégiés	171
8.3	Restrictions d'accès aux informations	173
8.4	Accès aux codes source	175
<del>18.1</del>	<del>Conformité aux obligations légales et réglementaires</del>	<del>176</del>
<del>18.1</del>	<del>8.5</del>	<del>176</del>
	Authentification sécurisée	176
<del>18.1.1</del>	<del>Identification de la législation et des exigences contractuelles applicables</del>	<del>176</del>
<del>18.1.2</del>	<del>Droits de propriété intellectuelle</del>	<del>176</del>
<del>18.1.3</del>	<del>Protection des enregistrements</del>	<del>177</del>
<del>18.1.4</del>	<del>Protection de la vie privée et protection des données à caractère personnel</del>	<del>178</del>
<del>18.1.5</del>	<del>Réglementation relative aux mesures cryptographiques</del>	<del>179</del>
8.6	Dimensionnement	181
8.7	Protection contre les programmes malveillants ( <i>malware</i> )	182
8.8	Gestion des vulnérabilités techniques	184
8.9	Gestion des configurations	188
8.10	Suppression des informations	190
8.11	Masquage des données	191
8.12	Prévention la fuite de données	193
8.13	Sauvegarde des informations	194
8.14	Redondance des moyens de traitement de l'information	196
8.15	Journalisation	197
8.16	Activités de surveillance	200
8.17	Synchronisation des horloges	202
8.18	Utilisation de programmes utilitaires à privilèges	203
8.19	Installation de logiciels sur des systèmes opérationnels	204
8.20	Sécurité des réseaux	205
8.21	Sécurité des services réseau	207
8.22	Cloisonnement des réseaux	208
8.23	Filtrage web	209
8.24	Utilisation de la cryptographie	210
<del>18.2</del>	<del>Revue de la sécurité de l'information</del>	<del>212</del>

<del>18.2</del>	<del>8.25</del> .....	212
	Cycle de vie de développement sécurisé .....	212
<del>18.2.1</del>	<del>Revue indépendante de la sécurité de l'information</del> .....	212
<del>18.2.2</del>	<del>Conformité avec les politiques et les normes de sécurité</del> .....	213
<del>18.2.3</del>	<del>Examen de la conformité technique</del> .....	213
8.26	Exigences de sécurité des applications .....	215
8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés .....	217
8.28	Codage sécurisé .....	219
8.29	Tests de sécurité dans le développement et l'acceptation .....	222
8.30	Développement externalisé .....	223
8.31	Séparation des environnements de développement, de test et opérationnels .....	224
8.32	Gestion des changements .....	226
8.33	Informations de test .....	227
8.34	Protection des systèmes d'information pendant les tests d'audit .....	228
<b>Annexe A</b> (informative)	<b>Utilisation des attributs</b> .....	<b>230</b>
<b>Annexe B</b> (informative)	<b>Correspondance de l'ISO/IEC 27002:2022 (le présent document) avec l'ISO/IEC 27002:2013</b> .....	<b>241</b>
<b>Bibliographie</b>	.....	<b>249</b>

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

ISO/IEC 27002:2022

<https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>

## Avant-propos

L'ISO (Organisation internationale de normalisation) et ~~la CEI~~ IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de ~~la CEI~~ 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 ~~la CEI~~ IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et ~~la CEI~~ IEC, participent également aux travaux. ~~Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.~~

Les ~~Normes internationales~~ 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 documents ~~ISO~~. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/~~CEI~~ IEC, Partie 2 (voir [www.iso.org/directives](http://www.iso.org/directives) ou [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

~~La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.~~

L'attention est ~~appelée~~ 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 ~~ne saurait être tenue pour responsable~~ 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.ch>).

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 [www.iso.org/iso/avant-propos](http://www.iso.org/iso/avant-propos). Pour l'IEC, voir [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

~~L'ISO/CEI 27002~~ Le présent document a été ~~élaborée~~ élaboré par le comité technique mixte ISO/~~CEI~~ IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information* ~~Sécurité de l'information, cybersécurité et protection de la vie privée~~.

Cette ~~deuxième~~ troisième édition annule et remplace la ~~première~~ deuxième édition (ISO/~~CEI~~ IEC 27002:2005/2013), qui a fait l'objet d'une ~~révision technique~~ objet d'une révision technique. Elle incorpore également les Rectificatifs techniques ISO/IEC 27002:2013/Cor. 1:2014 et ~~structure~~ ISO/IEC 27002:2013/Cor. 2:2015.

Les principales modifications sont les suivantes:

- le titre a été modifié;
- la structure du document a été modifiée, présentant les moyens de maîtrise avec une taxonomie simple et des attributs associés;
- certains moyens de maîtrise ont été fusionnés, d'autres ont été supprimés, et plusieurs nouveaux moyens de maîtrise ont été ajoutés. La correspondance complète se trouve à l'Annexe B.

La présente version française de l'ISO/IEC 27002:2022 correspond à la version anglaise publiée le 2022-02 et corrigé le 2022-03.

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/members.html](http://www.iso.org/members.html) et [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

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

ISO/IEC 27002:2022

<https://standards.itih.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>

## 0 Introduction

### 0.1 Historique et contexte

La présente Norme internationale a pour objet de servir d'outil de référence permettant aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur l'ISO/IEC 27001<sup>[10]</sup> ou de guide. Il peut également être utilisé comme guide de bonnes pratiques pour les organisations mettant en œuvre des mesures de sécurité de l'information largement reconnues. La présente norme a également pour objet d'établir des lignes directrices qui déterminent et mettent en œuvre les moyens de maîtrise de l'information communément admis. De plus, le présent document a pour objet d'être utilisé lors de l'élaboration des lignes directrices de management de la sécurité de l'information spécifiques aux organisations et aux entreprises industrielles, en tenant compte de leur(s) environnement(s) particulier(s) de risques liés à la sécurité de l'information. Des moyens de maîtrise organisationnels ou spécifiques à l'environnement autres que ceux qui figurent dans le présent document peuvent, si nécessaire, être déterminés par le biais de l'appréciation du risque.

Des organisations de tous types et de toutes dimensions (incluant le secteur public et le secteur privé, à but lucratif ou non lucratif) créent, collectent, traitent, stockent et transmettent, transmettent et éliminent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, au cours des conversations et des présentations).

La valeur de l'information dépasse les mots, les chiffres et les images : la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles intangibles d'information. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement, ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et, par conséquent, ils méritent ou nécessitent d'être protégés contre les divers risques encourus. Les informations et autres actifs associés méritent ou exigent une protection contre différentes sources de risques, aussi bien naturelles, qu'accidentelles ou délibérées.

Les actifs sont exposés à des menaces tant accidentelles que délibérées, alors que les processus, les systèmes, les réseaux et les personnes qui s'y rattachent présentent des vulnérabilités qui leur sont propres. Des changements apportés aux processus et aux systèmes de l'organisation ou d'autres changements externes (comme l'application de nouvelles lois et réglementations) peuvent engendrer de nouveaux risques pour la sécurité de l'information. Par conséquent, étant donné que les menaces disposent d'une multitude de possibilités d'exploitation des vulnérabilités pour nuire à l'organisation, les risques de sécurité de l'information sont omniprésents. Une sécurité efficace de l'information réduit ces risques en protégeant l'organisation contre les menaces et les vulnérabilités, ce qui réduit les conséquences sur ses actifs.

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des politiques, des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Ces mesures doivent être spécifiques, mises à jour et améliorées. Pour atteindre ses objectifs métier et de sécurité, il convient que l'organisation définisse, mette en œuvre, suive, réexamine et améliore ces mesures aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'une organisation. Un système de management de la sécurité de l'information (SMSI) tel que celui spécifié dans l'ISO/IEC 27001<sup>[10]</sup> appréhende les risques liés à la sécurité de l'information de l'organisation dans une vision globale et coordonnée, de manière à déterminer et mettre en œuvre un ensemble complet de mesures liées à la sécurité de l'information dans le cadre général d'un système de management cohérent.

~~Nombreux sont les systèmes d'information qui n'ont pas été conçus dans un souci de sécurité au sens de l'ISO/CEI 27001<sup>[10]</sup> et de la présente norme. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la soutenir à l'aide de moyens de management et de procédures adaptés. L'identification des mesures qu'il convient de mettre en place nécessite de procéder à une planification minutieuse et de prêter attention aux détails. Un système de management de la sécurité de l'information efficace requiert l'adhésion de tous les salariés de l'organisation. Il peut également nécessiter la participation des actionnaires, des fournisseurs ou d'autres tiers. De même, l'avis de spécialistes tiers peut se révéler nécessaire.~~

~~De manière plus générale, une sécurité de l'information efficace garantit également à la direction et aux parties tiers que les actifs de l'organisation sont, dans des limites raisonnables, sécurisés et à l'abri des préjudices, et contribuent de ce fait au succès de l'organisation.~~

De nombreux systèmes d'information, y compris leur management et leurs opérations, n'ont pas été conçus sécurisés au sens d'un système de management de la sécurité de l'information tel que spécifié dans l'ISO/IEC 27001 et le présent document. Le niveau de sécurité qui peut être atteint seulement par des mesures techniques est limité, et il convient de le renforcer par des processus organisationnels et activités de management appropriés. L'identification des moyens de maîtrise qu'il convient de mettre en place nécessite une planification minutieuse et une attention aux détails lors de la réalisation du traitement du risque.

Un système de management de la sécurité de l'information réussi requiert l'adhésion de tout le personnel de l'organisation. Il peut également nécessiter la participation d'autres parties intéressées, telles que des actionnaires ou des fournisseurs. Des conseils d'experts en la matière peuvent aussi s'avérer nécessaires.

Un système de management de la sécurité de l'information approprié, adéquat et efficace procure la garantie aux dirigeants de l'organisation et autres parties intéressées que leurs informations et autres actifs associés sont suffisamment sécurisés et protégés contre les menaces et dommages, ce qui permet à l'organisation d'atteindre les objectifs métier visés.

## 0.2 Exigences liées à la sécurité de l'information de sécurité de l'information

~~Une organisation doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales.~~

Il est essentiel qu'une organisation détermine ses exigences de sécurité de l'information. Il existe trois principales sources des exigences de sécurité de l'information:

- a) ~~l'appréciation du risque propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux. L'appréciation du risque permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel,~~

l'appréciation du risque de l'organisation, prenant en compte l'ensemble de sa stratégie et objectifs métier. Cela peut être facilité ou appuyé par une appréciation du risque lié à la sécurité de l'information. Il convient que cela aboutisse à la détermination des moyens de maîtrise nécessaires assurant que les risques résiduels pour l'organisation correspondent à ses critères d'acceptation des risques;

- b) les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses parties intéressées (partenaires commerciaux, contractants et prestataires de service, fournisseurs de services, etc.) doivent répondre ainsi que leur environnement socioculturel;

- c) l'ensemble de principes, d'objectifs et d'exigences métier en matière de manipulation, de traitement, de stockage, de communication et d'archivage de l'information que l'organisation s'est constitué pour mener à bien ses activités élaboré pour appuyer son fonctionnement.

~~Il est nécessaire de confronter les ressources mobilisées par la mise en œuvre des mesures avec les dommages susceptibles de résulter de défaillances de la sécurité en l'absence de ces mesures. Les~~

~~résultats d'une appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de gestion des risques liés à la sécurité de l'information, ainsi que de mettre en œuvre les mesures identifiées destinées à contrer ces risques.~~

~~La norme ISO/CEI 27005<sup>[11]</sup> fournit des lignes directrices de gestion du risque lié à la sécurité de l'information, y compris des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque.~~

### 0.3 Moyens de maîtrise

Un moyen de maîtrise est défini comme une mesure qui modifie ou maintient un risque. Certains des moyens de maîtrise dans le présent document sont des moyens qui modifient les risques, tandis que d'autres maintiennent les risques. Une politique de sécurité de l'information, par exemple, permet seulement de maintenir les risques, tandis que la conformité à la politique de sécurité de l'information peut modifier les risques. De plus, certains moyens de maîtrise décrivent la même mesure générique dans différents contextes de risques. Le présent document propose une combinaison générique de moyens de maîtrise de l'information organisationnels, liés aux personnes, physiques et technologiques, issus des bonnes pratiques reconnues au niveau international.

### ~~0.3 Sélection des mesures~~ 0.4 Détermination des moyens de maîtrise

~~Selon les cas, il est possible de sélectionner les mesures dans la présente norme ou dans d'autres guides, ou encore de spécifier de nouvelles mesures en vue de satisfaire des besoins spécifiques.~~

La ~~sélection des mesures~~ détermination des moyens de maîtrise dépend des décisions prises par l'organisation en fonction de ses critères d'acceptation de l'organisation suite à une appréciation du risque, de ses avec un périmètre clairement défini. Il convient de baser les décisions relatives aux risques identifiés sur les critères d'acceptation des risques, les options de traitement du risque et de son approche de la gestion générale du risque des risques et l'approche de gestion des risques appliqués par l'organisation. Il convient également de prendre en considération les lois et règlements nationaux et internationaux concernés. La sélection des mesures de sécurité dépend également que la détermination des moyens de maîtrise tienne compte de toutes les législations et réglementations nationales et internationales pertinentes. La détermination des moyens de maîtrise dépend aussi de la manière dont les ~~mesures interagissent~~ moyens de maîtrise interagissent les uns avec les autres pour assurer une défense en profondeur.

L'organisation peut concevoir des moyens de maîtrise au besoin, ou bien les identifier à partir de n'importe quelle source. Lors de la spécification de ces moyens de maîtrise, il convient que l'organisation tienne compte des ressources et investissements nécessaires pour mettre en œuvre et opérer un moyen de maîtrise par rapport à la valeur métier réalisée. Voir l'ISO/IEC TR 27016 pour les recommandations sur les décisions concernant les investissements dans un SMSI et les conséquences économiques de ces décisions dans le contexte d'exigences concurrentes en matière de ressources.

Il convient qu'il y ait un équilibre entre les ressources déployées pour mettre en œuvre les moyens de maîtrise et l'impact métier possible résultant des incidents de sécurité en l'absence de ces moyens de maîtrise. Il convient que les résultats de l'appréciation du risque aide à guider et à déterminer les actions de gestion appropriées, les priorités pour gérer les risques de sécurité de l'information, et pour mettre en œuvre les moyens de maîtrise identifiés comme nécessaires pour protéger contre ces risques.

~~Certaines mesures décrites dans la présente norme peuvent être considérées~~ Certains moyens de maîtrise dans le présent document peuvent être considérés comme des principes directeurs pour le management de base pour la gestion de la sécurité de l'information et être appliquées l'information et ils sont applicables à la plupart des organisations. Les mesures et des lignes directrices de mise en œuvre sont détaillées ci-dessous. De plus amples informations sur la sélection des mesures et d'autres Plus d'informations sur la détermination des moyens de maîtrise et autres options de traitement du risque figurent peuvent être trouvées dans l'ISO/CEI IEC 27005.<sup>[11]</sup>

### 0.4 Mise au point 0.5 Élaboration de lignes directrices propres à l'organisation spécifiques à une organisation

~~La présente Norme internationale peut servir de base pour la mise au point~~ Le présent document peut être considéré comme point de départ pour l'élaboration de lignes directrices spécifiques à une organisation. ~~Une partie des mesures~~ Tous les moyens de maîtrise et lignes directrices de ce code de bonnes pratiques ~~peuvent~~ du présent document peuvent ne pas être applicables. Par ailleurs, des mesures et des ~~applicables~~ à toutes les organisations. D'autres moyens de maîtrise et lignes directrices ne figurant pas dans ~~la présente norme~~ le présent document peuvent être nécessaires pour traiter les besoins spécifiques de l'organisation et les risques identifiés. Lors de la rédaction de documents contenant des lignes directrices ou des ~~mesures~~ moyens de maîtrise supplémentaires, il peut être utile ~~d'intégrer~~ d'ajouter des références croisées aux articles de la présente norme, le cas échéant, afin de faciliter la vérification de la conformité par les auditeurs et les partenaires commerciaux du présent document en vue d'une consultation ultérieure.

## ~~0.5 Examen du~~ 0.6 Considérations relatives au cycle de vie

L'information ~~est soumise à~~ un cycle de vie ~~naturel~~, depuis sa création et son origine en passant par son stockage, son traitement, son utilisation, sa transmission, jusqu'à sa destruction finale ou son obsolescence jusqu'à son élimination. La valeur des actifs de l'information et les risques qui y sont liés ~~associés~~ peuvent varier au cours de la durée ce cycle de vie de ces actifs (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise revêt une importance bien moins grande après leur publication officielle), mais dans une certaine mesure l'importance n'a pas d'impact significatif après la publication de ces informations, mais l'intégrité demeure critique). Par conséquent, l'importance de la sécurité de l'information l'information subsiste à tous les stades.

Les systèmes d'information ~~sont soumis à~~ et autres actifs pertinents pour la sécurité de l'information ont des cycles de vie durant lesquels ils sont pensés, caractérisés, spécifiés, conçus, mis au point, développés, testés, mis en œuvre, utilisés, entretenus, maintenus et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit prise en compte à tous les stades. La mise au point ~~considérée~~ à chaque étape. Les projets de développement de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion aux organisations de mettre à jour les mesures de sécurité et de les améliorer en tenant compte des incidents réels survenus et des risques de sécurité de l'information actuels et anticipés d'améliorer les moyens de maîtrise tout en prenant en compte les risques de l'organisation et les leçons tirées des incidents.

## ~~0.6 Normes~~ 0.7 Normes internationales associées

Alors que ~~la présente Norme internationale propose des lignes directrices~~ le présent document propose des recommandations portant sur un vaste éventail de ~~mesures de sécurité liées à l'information d'utilisation courante dans nombre d'organisations différentes, les autres normes~~ moyens de maîtrise qui sont communément utilisés dans plusieurs organisations différentes, d'autres documents de la famille ISO/IEC 27000 ~~présentent~~ proposent des conseils complémentaires ou des exigences relatifs à d'autres aspects de l'ensemble du processus global de ~~management~~ gestion de la sécurité de l'information.

Se reporter à l'ISO/IEC 27000 pour une introduction générale ~~aux systèmes de management de la sécurité de l'information~~ à la fois aux SMSI et à la famille de ~~normes~~ documents. L'ISO/IEC 27000 ~~présente~~ fournit un glossaire, définissant de manière formelle la plupart des termes utilisés dans la famille de ~~normes~~ des documents ISO/IEC 27000, et décrit le ~~domaine d'application~~ périmètre et les objectifs de chaque ~~élément de cette~~ membre de la famille.

Il existe des normes sectorielles qui comportent des moyens de maîtrise supplémentaires destinés à traiter des domaines spécifiques (par exemple, l'ISO/IEC 27017 pour les services en nuage, l'ISO/IEC 27701 pour la protection de la vie privée, l'ISO/IEC 27019 pour l'énergie, l'ISO/IEC 27011 pour les organismes de télécommunications et l'ISO 27799 pour la santé). Ces normes figurent dans la Bibliographie et certaines d'entre elles sont référencées dans les recommandations et autres informations des [Articles 5 à 8](#).

# Sécurité de l'information, cybersécurité et protection de la vie privée — Moyens de maîtrise de l'information

## 1 ~~Domaine d'application~~ d'application

~~La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.~~

~~La présente Norme internationale est élaborée à l'intention des organisations désireuses~~

Le présent document fournit un ensemble de référence de moyens de maîtrise de l'information génériques, y compris des recommandations de mise en œuvre. Le présent document est conçu pour être utilisé par les organisations:

- a) ~~de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre~~ dans le contexte d'un système de ~~management~~ gestion de la sécurité de l'information (SMSI) selon l'ISO/IEC 27001;<sup>[10]</sup>
- b) ~~de mettre en œuvre des mesures de sécurité de l'information largement reconnues,~~ pour la mise en œuvre de moyens de maîtrise de l'information basés sur les bonnes pratiques reconnues au niveau international;
- c) ~~d'élaborer leurs propres lignes directrices de management~~ pour l'élaboration des recommandations de gestion de la sécurité de l'information spécifiques à une organisation.

<https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>

## 2 Références normatives

~~Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. 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~~

Le présent document ne contient aucune référence normative.

## 3 Termes et définitions, définitions et abréviations

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

### 3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants 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 <https://www.electropedia.org/>