
**Technologies de l'information —
Techniques de sécurité — Code de bonne
pratique pour la gestion de la sécurité de
l'information**

*Information technology — Security techniques — Code of practice for
information security management*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

[https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-
a6f756320ba3/iso-iec-27002-2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

<https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/CEI 2005

Droits de reproduction réservés. Sauf prescription différente, 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 et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI 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 collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI 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 sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

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 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 la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27002 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

La première édition de l'ISO/CEI 27002 comprend l'ISO/CEI 17799:2005 et l'ISO/CEI 17799:2005/Cor.1:2007. Son contenu technique est identique à celui de l'ISO/CEI 17799:2005. L'ISO/CEI 17799:2005/Cor.1:2007 modifie le numéro de référence de la norme de 17799 en 27002. L'ISO/CEI 17799:2005 et l'ISO/CEI 17799:2005/Cor.1:2007 sont provisoirement retenus jusqu'à la publication de la deuxième édition de l'ISO/CEI 27002.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

<https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005>



NORME INTERNATIONALE ISO/CEI 17799:2005
RECTIFICATIF TECHNIQUE 1

Publié 2007-07-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**Technologies de l'information — Techniques de sécurité —
Code de bonne pratique pour la gestion de la sécurité de
l'information**

RECTIFICATIF TECHNIQUE 1

Information technology — Security techniques — Code of practice for information security management

TECHNICAL CORRIGENDUM 1

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Le Rectificatif technique 1 à l'ISO/CEI 17799:2005 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

<https://standards.iteh.ai/catalog/standards/sist/105-1c317-0ccc-4ac0-a86c-a6f756320ba3/iso-iec-27002-2005>

Dans tout le document:

Remplacer «17799» par «27002».

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](#)

<https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005>

**Technologies de l'information —
Techniques de sécurité — Code de bonne
pratique pour la gestion de la sécurité de
l'information**

*Information technology — Security techniques — Code of practice for
information security management*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

[https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-
a6f756320ba3/iso-iec-27002-2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 27002:2005](https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005)

<https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005>

© ISO/CEI 2005

Droits de reproduction réservés. Sauf prescription différente, 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 et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

Sommaire

Page

Avant-propos.....	vii
0 Introduction.....	viii
1 Domaine d'application.....	1
2 Termes et définitions.....	1
3 Structure de la présente Norme internationale.....	3
3.1 Articles.....	3
3.2 Principales rubriques.....	4
4 Appréciation et traitement du risque.....	4
4.1 Appréciation du risque lié à la sécurité.....	4
4.2 Traitement du risque lié à la sécurité.....	5
5 Politique de sécurité.....	6
5.1 Politique de sécurité de l'information.....	6
5.1.1 Document de politique de sécurité de l'information.....	6
5.1.2 Réexamen de la politique de sécurité de l'information.....	7
6 Organisation de la sécurité de l'information.....	8
6.1 Organisation interne.....	8
6.1.1 Engagement de la direction vis-à-vis de la sécurité de l'information.....	8
6.1.2 Coordination de la sécurité de l'information.....	9
6.1.3 Attribution des responsabilités en matière de sécurité de l'information.....	9
6.1.4 Système d'autorisation concernant les moyens de traitement de l'information.....	10
6.1.5 Engagements de confidentialité.....	10
6.1.6 Relations avec les autorités.....	11
6.1.7 Relations avec des groupes de spécialistes.....	12
6.1.8 Revue indépendante de la sécurité de l'information.....	12
6.2 Tiers.....	13
6.2.1 Identification des risques provenant des tiers.....	13
6.2.2 La sécurité et les clients.....	15
6.2.3 La sécurité dans les accords conclus avec des tiers.....	16
7 Gestion des biens.....	18
7.1 Responsabilités relatives aux biens.....	18
7.1.1 Inventaire des biens.....	19
7.1.2 Propriété des biens.....	20
7.1.3 Utilisation correcte des biens.....	20
7.2 Classification des informations.....	21
7.2.1 Lignes directrices pour la classification.....	21
7.2.2 Marquage et manipulation de l'information.....	22
8 Sécurité liée aux ressources humaines.....	22
8.1 Avant le recrutement.....	22
8.1.1 Rôles et responsabilités.....	22
8.1.2 Sélection.....	23
8.1.3 Conditions d'embauche.....	24
8.2 Pendant la durée du contrat.....	25
8.2.1 Responsabilités de la direction.....	25
8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information.....	26
8.2.3 Processus disciplinaire.....	26
8.3 Fin ou modification de contrat.....	27
8.3.1 Responsabilités en fin de contrat.....	27
8.3.2 Restitution des biens.....	27

8.3.3	Retrait des droits d'accès	28
9	Sécurité physique et environnementale	29
9.1	Zones sécurisées	29
9.1.1	Périmètre de sécurité physique	29
9.1.2	Contrôles physiques des accès	30
9.1.3	Sécurisation des bureaux, des salles et des équipements	30
9.1.4	Protection contre les menaces extérieures et environnementales	31
9.1.5	Travail dans les zones sécurisées	31
9.1.6	Zones d'accès public, de livraison et de chargement	32
9.2	Sécurité du matériel	32
9.2.1	Choix de l'emplacement et protection du matériel	33
9.2.2	Services généraux	33
9.2.3	Sécurité du câblage	34
9.2.4	Maintenance du matériel	35
9.2.5	Sécurité du matériel hors des locaux	35
9.2.6	Mise au rebut ou recyclage sécurisé(e) du matériel	36
9.2.7	Sortie d'un bien	36
10	Gestion de l'exploitation et des télécommunications	37
10.1	Procédures et responsabilités liées à l'exploitation	37
10.1.1	Procédures d'exploitation documentées	37
10.1.2	Gestion des modifications	38
10.1.3	Séparation des tâches	38
10.1.4	Séparation des équipements de développement, de test et d'exploitation	39
10.2	Gestion de la prestation de service par un tiers	40
10.2.1	Prestation de service	40
10.2.2	Surveillance et réexamen des services tiers	40
10.2.3	Gestion des modifications dans les services tiers	41
10.3	Planification et acceptation du système	42
10.3.1	Dimensionnement	42
10.3.2	Acceptation du système	42
10.4	Protection contre les codes malveillants et mobile	43
10.4.1	Mesures contre les codes malveillants	43
10.4.2	Mesures contre le code mobile	44
10.5	Sauvegarde	45
10.5.1	Sauvegarde des informations	45
10.6	Gestion de la sécurité des réseaux	46
10.6.1	Mesures sur les réseaux	46
10.6.2	Sécurité des services réseau	47
10.7	Manipulation des supports	48
10.7.1	Gestion des supports amovibles	48
10.7.2	Mise au rebut des supports	48
10.7.3	Procédures de manipulation des informations	49
10.7.4	Sécurité de la documentation système	50
10.8	Échange des informations	50
10.8.1	Politiques et procédures d'échange des informations	50
10.8.2	Accords d'échange	52
10.8.3	Supports physiques en transit	53
10.8.4	Messagerie électronique	54
10.8.5	Systèmes d'information d'entreprise	54
10.9	Services de commerce électronique	55
10.9.1	Commerce électronique	55
10.9.2	Transactions en ligne	56
10.9.3	Informations à disposition du public	57
10.10	Surveillance	58
10.10.1	Rapport d'audit	58
10.10.2	Surveillance de l'exploitation du système	59
10.10.3	Protection des informations journalisées	60
10.10.4	Journal administrateur et journal des opérations	61
10.10.5	Rapports de défaut	61

10.10.6	Synchronisation des horloges	62
11	Contrôle d'accès	62
11.1	Exigences métier relatives au contrôle d'accès	62
11.1.1	Politique de contrôle d'accès	62
11.2	Gestion de l'accès utilisateur	63
11.2.1	Enregistrement des utilisateurs	64
11.2.2	Gestion des privilèges.....	65
11.2.3	Gestion du mot de passe utilisateur	65
11.2.4	Réexamen des droits d'accès utilisateurs	66
11.3	Responsabilités utilisateurs	67
11.3.1	Utilisation du mot de passe	67
11.3.2	Matériel utilisateur laissé sans surveillance.....	68
11.3.3	Politique du bureau propre et de l'écran vide	68
11.4	Contrôle d'accès au réseau	69
11.4.1	Politique relative à l'utilisation des services en réseau	69
11.4.2	Authentification de l'utilisateur pour les connexions externes	70
11.4.3	Identification des matériels en réseau.....	71
11.4.4	Protection des ports de diagnostic et de configuration à distance	71
11.4.5	Cloisonnement des réseaux	71
11.4.6	Mesure relative à la connexion réseau	72
11.4.7	Contrôle du routage réseau.....	73
11.5	Contrôle d'accès au système d'exploitation.....	73
11.5.1	Ouverture de sessions sécurisées	73
11.5.2	Identification et authentification de l'utilisateur	74
11.5.3	Système de gestion des mots de passe.....	75
11.5.4	Emploi des utilitaires système	76
11.5.5	Déconnexion automatique des sessions inactives.....	77
11.5.6	Limitation du temps de connexion	77
11.6	Contrôle d'accès aux applications et à l'information	77
11.6.1	Restriction d'accès à l'information.....	78
11.6.2	Isolement des systèmes sensibles	78
11.7	Informatique mobile et télétravail	79
11.7.1	Informatique mobile et télécommunications	79
11.7.2	Télétravail	80
12	Acquisition, développement et maintenance des systèmes d'information.....	81
12.1	Exigences de sécurité applicables aux systèmes d'information	81
12.1.1	Analyse et spécification des exigences de sécurité	82
12.2	Bon fonctionnement des applications.....	82
12.2.1	Validation des données d'entrée.....	83
12.2.2	Mesure relative au traitement interne	83
12.2.3	Intégrité des messages	84
12.2.4	Validation des données de sortie.....	85
12.3	Mesures cryptographiques.....	85
12.3.1	Politique d'utilisation des mesures cryptographiques.....	85
12.3.2	Gestion des clés	87
12.4	Sécurité des fichiers système	88
12.4.1	Mesure relative aux logiciels en exploitation	88
12.4.2	Protection des données système d'essai	89
12.4.3	Contrôle d'accès au code source du programme	90
12.5	Sécurité en matière de développement et d'assistance technique.....	91
12.5.1	Procédures de contrôle des modifications.....	91
12.5.2	Réexamen technique des applications après modification du système d'exploitation.....	92
12.5.3	Restrictions relatives à la modification des progiciels.....	92
12.5.4	Fuite d'informations	93
12.5.5	Externalisation du développement logiciel.....	93
12.6	Gestion des vulnérabilités techniques	94
12.6.1	Mesure relative aux vulnérabilités techniques	94
13	Gestion des incidents liés à la sécurité de l'information	95

13.1	Signalement des événements et des failles liés à la sécurité de l'information.....	95
13.1.1	Signalement des événements liés à la sécurité de l'information.....	96
13.1.2	Signalement des failles de sécurité	97
13.2	Gestion des améliorations et incidents liés à la sécurité de l'information.....	97
13.2.1	Responsabilités et procédures.....	98
13.2.2	Exploitation des incidents liés à la sécurité de l'information déjà survenus	99
13.2.3	Collecte de preuves	99
14	Gestion du plan de continuité de l'activité.....	100
14.1	Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité ...	100
14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	101
14.1.2	Continuité de l'activité et appréciation du risque.....	101
14.1.3	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information.....	102
14.1.4	Cadre de la planification de la continuité de l'activité	103
14.1.5	Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité	104
15	Conformité	105
15.1	Conformité avec les exigences légales	105
15.1.1	Identification de la législation en vigueur	105
15.1.2	Droits de propriété intellectuelle	105
15.1.3	Protection des enregistrements de l'organisme.....	106
15.1.4	Protection des données et confidentialité des informations relatives à la vie privée	107
15.1.5	Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information ..	108
15.1.6	Réglementation relative aux mesures cryptographiques.....	109
15.2	Conformité avec les politiques et normes de sécurité et conformité technique	109
15.2.1	Conformité avec les politiques et les normes de sécurité	109
15.2.2	Vérification de la conformité technique.....	110
15.3	Prises en compte de l'audit du système d'information	110
15.3.1	Contrôles de l'audit du système d'information.....	111
15.3.2	Protection des outils d'audit du système d'information.....	111
Bibliographie	112

ISO/IEC 37003:2005
<https://standards.iteh.ai/catalog/standards/sist/6034c5f7-6eee-4ac0-a8bc-a0f756320ba3/iso-iec-27002-2005>

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée 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 de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 17799 a été élaborée par le comité technique ISO/TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 17799:2000), qui a fait l'objet d'une révision technique. À l'inverse de la version anglaise, la version française ne comporte pas d'Index.

Une famille de Normes internationales concernant le système de gestion de la sécurité de l'information (ISMS, de Information Security Management System) est en préparation au sein de l'ISO/CEI JTC 1/SC 27. La famille inclut des Normes internationales relatives aux exigences du système de gestion de la sécurité de l'information, à la gestion du risque, à la métrologie et au mesurage, ainsi qu'à un guide de mise en application. La famille adoptera un schéma de numérotation utilisant la série des nombres 27000 et suivants.

À partir de 2007, il est proposé d'incorporer la nouvelle édition de l'ISO/CEI 17799 dans ce schéma de numérotation en tant qu'ISO/CEI 27002.

0 Introduction

0.1 Qu'est-ce que la sécurité de l'information ?

L'information constitue un bien important pour l'organisme; elle est à ce titre un élément important de l'activité de l'organisme et elle nécessite une protection adéquate. Ce point s'avère particulièrement important dans l'environnement actuel qui comporte des interconnexions de plus en plus nombreuses. Du fait du nombre croissant de ces interconnexions, l'information est de plus en plus exposée et vulnérable (voir également les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information).

L'information se présente sur des supports variés. Elle peut être disponible sur papier, stockée électroniquement, transmise par voie postale ou électronique, diffusée sur des supports audiovisuels ou verbalement. Quel que soit le support ou le moyen utilisé pour la partager ou la stocker, il convient de toujours protéger l'information de manière adaptée.

La sécurité de l'information vise à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des transactions, à réduire le plus possible le risque et à optimiser le retour sur investissement ainsi que les opportunités en termes d'activité pour l'organisme.

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Ces mesures doivent être spécifiées, mises en œuvre, suivies, réexaminées et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'un organisme. Pour ce faire, il convient d'agir de manière concertée avec les autres processus de gestion de l'organisme.

<https://standards.iteh.ai/catalog/standards/sist/6034c57-6eee-4ac0-a8bc-a6f756320ba3/iso-iec-27002-2005>

0.2 En quoi la sécurité de l'information est-elle nécessaire ?

L'information et les processus, systèmes et réseaux qui en permettent le traitement constituent des biens importants pour un organisme. Il peut s'avérer crucial de définir, réaliser, entretenir et améliorer la sécurité de l'information pour faire face à la concurrence, maintenir les liquidités, la rentabilité, la mise en conformité avec la loi et l'image commerciale.

Les menaces qui pèsent sur les organismes et leurs systèmes et réseaux d'information sont d'origines très diverses: fraude informatique, espionnage, sabotage, vandalisme, incendies ou inondations par exemple. Des techniques d'attaque comme les codes malveillants, le piratage informatique et les attaques par déni de service deviennent de plus en plus répandues et sophistiquées.

La sécurité de l'information revêt de l'importance pour les organismes des secteurs public et privé, et permet de protéger les infrastructures critiques. Dans ces deux secteurs, la sécurité de l'information fait office d'activateur. En d'autres termes, elle rend possible l'administration ou le commerce en ligne, et permet d'éviter le risque qui en découle ou d'en réduire l'impact. L'interconnexion des réseaux public et privé, ainsi que le partage des sources d'information, rendent le contrôle d'accès plus difficile. Le développement de l'informatique distribuée a également affaibli l'efficacité du contrôle spécialisé et centralisé.

De nombreux systèmes d'information ont été spécifiés sans que soient pris en compte les besoins de sécurité. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la prendre en charge à l'aide de moyens de gestion et de procédures adaptés. Pour identifier les mesures à mettre en place, il convient de procéder à une planification minutieuse et de prêter attention aux détails. La participation de tous les salariés d'un organisme est indispensable à une bonne gestion de la sécurité de l'information. La participation des actionnaires, des fournisseurs, des tiers, des clients et autres peut également s'avérer nécessaire. De même, l'avis de spécialistes tiers peut être également nécessaire.

0.3 Définition des exigences en matière de sécurité

Un organisme doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales.

1. La première est l'appréciation du risque propre à l'organisme, en prenant en compte la stratégie et les objectifs généraux de l'organisme. L'appréciation du risque permet d'identifier les menaces pesant sur les biens, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel.
2. La deuxième concerne, d'une part, les exigences légales, statutaires, réglementaires, et contractuelles auxquelles l'organisme et ses partenaires commerciaux, contractants et prestataires de service, doivent répondre et, d'autre part, l'environnement socioculturel.
3. La troisième correspond à l'ensemble de principes, d'objectifs et d'exigences métier en matière de traitement de l'information que l'organisme s'est constitués pour mener à bien ses activités.

0.4 Appréciation du risque lié à la sécurité

Les exigences en matière de sécurité sont identifiées par une évaluation méthodique des risques. Les dépenses consacrées aux mesures et les dommages susceptibles de résulter de défaillances de la sécurité doivent être mis en perspective.

Les résultats de l'appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de management du risque, et d'identifier les mesures adaptées destinées à contrer ces risques.

Il convient de procéder régulièrement à l'appréciation du risque, afin de tenir compte de toute modification pouvant influencer les résultats de l'analyse.

Pour plus ample information sur l'appréciation du risque lié à la sécurité, voir 4.1 «Appréciation du risque lié à la sécurité».

0.5 Sélection des mesures

Lorsque les exigences et les risques liés à la sécurité ont été identifiés, et que les décisions de traitement des risques ont été prises, il convient de sélectionner et de mettre en œuvre des mesures appropriées, afin de ramener les risques à un niveau acceptable. 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 de sécurité dépend des décisions prises par l'organisme en fonction de ses critères d'acceptation du risque, de ses options de traitement du risque, et de son approche du management général du risque. Il convient également de prendre en considération les lois et règlements nationaux et internationaux concernés.

Certaines mesures décrites dans la présente norme peuvent être considérées comme des principes directeurs pour la gestion de la sécurité de l'information et être appliquées à la plupart des organismes. Elles sont détaillées ci-après, sous le titre «Bases de la sécurité de l'information».

Pour plus ample information sur la sélection des mesures et les options de traitement du risque, voir 4.2 «Traitement du risque lié à la sécurité».

0.6 Bases de la sécurité de l'information

Une base solide pour aborder la sécurité de l'information est constituée des mesures suivantes, provenant d'exigences légales essentielles, ou considérées comme faisant partie de la pratique courante dans le domaine de la sécurité de l'information.