



**Norme
internationale**

ISO/IEC 29151

**Sécurité de l'information,
cybersécurité et protection de la
vie privée – Mesures de contrôle,
prescriptions et conseils pour
la protection des informations
d'identification personnelle**

*Information security, cybersecurity and privacy protection —
Controls, requirements, and guidance for personally identifiable
information protection*

**Deuxième édition
2026-07**

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2026

Tous droits réservés.

La présente publication de l'ISO est protégée par le droit d'auteur et demeure la propriété de l'ISO et/ou de ses concédants de licence.

Le contenu de la présente publication de l'ISO est fourni sous licence, et n'est pas vendu. Son utilisation est soumise aux conditions de licence applicables définies par l'ISO, un organisme membre de l'ISO, ou un distributeur tiers agréé.

Sous réserve des besoins liés à sa mise en œuvre ou d'une autorisation expresse prévue aux termes d'une licence distincte, aucune partie de la présente publication de l'ISO ne peut être reproduite, distribuée, modifiée, utilisée ou mise à disposition sous quelque forme ou par quelque moyen que ce soit – électronique ou mécanique, y compris la photocopie, la numérisation, l'enregistrement ou la publication sur des plateformes numériques internes ou externes.

Toute utilisation hors du champ d'application des droits accordés est interdite et peut donner lieu à des poursuites judiciaires.

ISO copyright office

Case postale 401 • CH-1214 Vernier, Genève

Tél.: +41 22 749 01 11

E-mail: copyright@iso.org

Web: www.iso.org

Publié en Suisse

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 organisations internationales, gouvernementales et non gouvernementales, 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 documents.

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et [https://patents.iec.ch](http://patents.iec.ch). L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par L'UIT en tant que X.1058 (2025) rédigé conformément à ses règles de rédaction, en collaboration avec 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*, et en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données*, du Comité européen de normalisation (CEN) conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO/IEC 29151:2017), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

- le contenu des recommandations relatives aux mesures de sécurité figurant dans le corps du texte et aux mesures de protection de la vie privée figurant à l'Annexe A a été harmonisé avec la norme ISO/IEC 27002:2022.

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 et www.iec.ch/national-committees.

TABLE DES MATIÈRES

	Page
1	Domaine d'application..... 1
2	Références normatives 1
3	Termes, définitions et abréviations 1
3.1	Termes et définitions 1
3.2	Abréviations 2
4	Aperçu général 2
4.1	Protection des IIP 2
4.2	Besoins en matière de protection des IIP..... 2
4.3	Mesures de contrôle découlant de l'évaluation des risques pour la vie privée..... 3
4.4	Choix des mesures de contrôle 3
4.5	Élaboration de lignes directrices propres à l'organisation 4
4.6	Éléments concernant le cycle de vie..... 4
4.7	Structure de la présente Recommandation Norme internationale..... 4
5	Mesures de sécurité organisationnelles 9
5.1	Politiques de sécurité de l'information 9
5.2	Fonctions et responsabilités liées à la sécurité de l'information 9
5.3	Séparation des tâches..... 10
5.4	Responsabilités en matière de gestion 10
5.5	Contacts avec les autorités 10
5.6	Contacts avec des groupes d'intérêt spécifiques 10
5.7	Renseignements sur les menaces..... 10
5.8	Sécurité de l'information dans la gestion de projet..... 10
5.9	Inventaire des informations et autres actifs associés 11
5.10	Utilisation correcte des informations et autres actifs associés..... 11
5.11	Restitution des actifs 12
5.12	Classification des informations 12
5.13	Marquage des informations 12
5.14	Transfert des informations..... 12
5.15	Contrôle d'accès 12
5.16	Gestion des identités..... 12
5.17	Informations d'authentification..... 13
5.18	Droits d'accès 13
5.19	Sécurité de l'information dans les relations avec les fournisseurs..... 13
5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs..... 13
5.21	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC 14
5.22	Surveillance, révision et gestion des changements des services fournisseurs 14
5.23	Sécurité de l'information dans l'utilisation de services en nuage..... 14
5.24	Planification et préparation de la gestion des incidents de sécurité de l'information 14
5.25	Évaluation des événements de sécurité de l'information et prise de décision..... 15
5.26	Réponse aux incidents de sécurité de l'information..... 15
5.27	Tirer des enseignements des incidents de sécurité de l'information 15
5.28	Collecte des preuves..... 15
5.29	Sécurité de l'information pendant une perturbation..... 16

5.30	Préparation des TIC pour la continuité d'activité	16
5.31	Exigences légales, statutaires, réglementaires et contractuelles	16
5.32	Droits de propriété intellectuelle	16
5.33	Protection des enregistrements	16
5.34	Protection de la vie privée et des DCP	16
5.35	Révision indépendante de la sécurité de l'information	16
5.36	Conformité aux politiques, règles et normes de sécurité de l'information.....	17
5.37	Procédures d'exploitation documentées.....	17
6	Mesures de sécurité applicables aux personnes.....	17
6.1	Sélection des candidats.....	17
6.2	Termes et conditions du contrat de travail.....	17
6.3	Sensibilisation, enseignement et formation en sécurité de l'information.....	17
6.4	Processus disciplinaire	18
6.5	Responsabilité après la fin ou le changement d'un emploi	18
6.6	Accords de confidentialité ou de non-divulagation.....	18
6.7	Travail à distance	18
6.8	Déclaration des événements de sécurité de l'information.....	18
7	Mesures de sécurité physique.....	18
7.1	Périmètres de sécurité physique	18
7.2	Les entrées physiques.....	18
7.3	Sécurisation des bureaux, des salles et des installations.....	19
7.4	Surveillance de la sécurité physique.....	19
7.5	Protection contre les menaces physiques et environnementales.....	19
7.6	Travail dans les zones sécurisées	19
7.7	Bureau vide et écran vide	19
7.8	Emplacement et protection du matériel.....	19
7.9	Sécurité des actifs hors des locaux	19
7.10	Supports de stockage	19
7.11	Services supports.....	19
7.12	Sécurité du câblage.....	20
7.13	Maintenance du matériel	20
7.14	Élimination ou recyclage sécurisé(e) du matériel.....	20
8	Mesures de sécurité technologiques	20
8.1	Terminaux finaux des utilisateurs	20
8.2	Droits d'accès privilégiés.....	20
8.3	Restrictions d'accès aux informations	20
8.4	Accès aux codes source.....	21
8.5	Authentification sécurisée	21
8.6	Dimensionnement.....	21
8.7	Protection contre les programmes malveillants (malware).....	21
8.8	Gestion des vulnérabilités techniques	21
8.9	Gestion des configurations	21
8.10	Suppression des informations.....	21
8.11	Masquage des données	21
8.12	Prévention de la fuite de données.....	21

8.13	Sauvegarde des informations.....	21
8.14	Redondance des moyens de traitement de l'information	22
8.15	Journalisation	22
8.16	Activités de surveillance	22
8.17	Synchronisation des horloges	22
8.18	Utilisation de programmes utilitaires à privilèges	22
8.19	Installation de logiciels sur des systèmes opérationnels.....	22
8.20	Sécurité des réseaux	23
8.21	Sécurité des services réseau	23
8.22	Cloisonnement des réseaux	23
8.23	Filtrage web.....	23
8.24	Utilisation de la cryptographie	23
8.25	Cycle de vie de développement sécurisé	23
8.26	Exigences de sécurité des applications.....	23
8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés	23
8.28	Codage sécurisé.....	23
8.29	Tests de sécurité dans le développement et l'acceptation	23
8.30	Développement externalisé	23
8.31	Séparation des environnements de développement, de test et opérationnels.....	23
8.32	Gestion des changements	24
8.33	Informations de test.....	24
8.34	Protection des systèmes d'information pendant les tests d'audit.....	24
Annexe A	– Extension des mesures de contrôle à la protection des IIP	25
A.1	Considérations générales.....	25
A.2	Politiques générales concernant l'utilisation et la protection des IIP	25
A.3	Consentement et choix	26
A.4	Légitimité et définition du but.....	28
A.5	Limites du recueil d'informations.....	29
A.6	Réduction des informations au minimum.....	30
A.7	Limites d'utilisation, de conservation et de divulgation	31
A.8	Exactitude et qualité	34
A.9	Ouverture, transparence et note d'information	35
A.10	Participation et accès de l'entité principale des IIP.....	36
A.11	Responsabilité	39
A.12	Sécurité des informations	42
A.13	Respect de la vie privée.....	42
Annexe B	– Correspondance entre la présente spécification et la Recommandation UIT-T X.1058:2017 norme ISO/CEI 29151:2017.....	44
Bibliographie		47

Introduction

Le nombre d'organisations chargées de traiter des informations d'identification personnelle (IIP) ne cesse de croître, tout comme le volume de données que ces organisations doivent gérer. Parallèlement, la société exige toujours plus de protection de ces informations et de sécurité des données personnelles. Face au nombre croissant d'atteintes sophistiquées à des données personnelles, un certain nombre de pays ont entrepris de renforcer leur législation.

Alors que ces atteintes se multiplient, les organisations qui recueillent ou traitent les IIP vont avoir de plus en plus besoin de conseils sur la manière de protéger ces informations pour réduire les risques d'atteinte et d'atténuer l'incidence de ces atteintes sur l'organisation ou la personne qui en est victime. La présente spécification fournit précisément ce type de conseils.

La présente spécification contient des conseils destinés aux contrôleurs des IIP et couvre un large éventail de mesures sur la sécurité de l'information et la protection des IIP. Ces mesures sont fréquemment employées par des organisations très diverses chargées de protéger des informations. D'autres normes internationales contiennent des conseils ou des prescriptions sur d'autres aspects du processus global de protection des IIP:

- La norme ISO/CEI 27001 définit un système de gestion de la sécurité de l'information, qui constitue un bon point de départ pour la protection de l'information, notamment les IIP.
- La norme ISO/CEI 27002 établit des lignes directrices concernant les mesures relatives à la sécurité de l'information d'ordre organisationnel, personnel, physique et technologique qui peuvent servir à protéger toutes sortes d'informations, par exemple les IIP.
- La norme ISO/CEI 27005 fournit des conseils pour aider les organisations à traiter les risques liés à la sécurité de l'information et à mettre en œuvre des activités permettant de gérer ces risques, couvrant plus précisément l'évaluation des risques et la manière d'y remédier.
- La norme ISO/CEI 27018 contient des conseils pour les prestataires de services chargés de traiter des IIP qui proposent des services en nuage.
- La norme ISO/CEI 27701 définit les exigences relatives à la création, la mise en œuvre, le maintien et l'amélioration continue d'un système de gestion de la protection de la vie privée (PIMS) et fournit des recommandations pour mettre en pratique ces exigences.
- La norme ISO/CEI 29100 fournit un cadre pour la protection de la vie privée qui spécifie une terminologie commune relative à la protection de la vie privée, définit les acteurs et leurs rôles dans le traitement des données à caractère personnel (DCP) (ou informations d'identification personnelle (IIP)), décrit les éléments à prendre en considération pour la protection de la vie privée, et fournit des références à des principes connus de protection de la vie privée pour les technologies de l'information.
- La norme ISO/CEI 29134 établit des lignes directrices permettant d'étudier les éventuelles répercussions sur la vie privée d'un processus, d'un système d'information, d'un programme, d'un module logiciel, d'un appareil ou de toute autre initiative amenée à traiter des informations d'identification personnelle (IIP), tandis que les normes ISO/CEI 27001 et ISO/CEI 27005 fournissent ensemble des conseils pour mener les activités de gestion des risques liées à la sécurité de l'information.

Les mesures de contrôle sont choisies en fonction des risques recensés au terme d'une analyse de risque afin de mettre en place un système de contrôle global et cohérent. Ces mesures sont adaptées au contexte du traitement particulier des IIP.

La présente spécification comporte deux parties:

- le corps principal du texte qui va des articles 1 à 8;
- les Annexes A et B.

La structure de la présente spécification, y compris le titre des articles, reprend celle du corps principal de la norme ISO/CEI 27002:2022 pour l'extension de la norme au domaine particulier des IIP.

Les paragraphes des articles 5 à 8 ont le même titre que ceux de la norme ISO/CEI 27002:2022, compte tenu du fait que la présente spécification s'inspire des conseils fournis dans cette norme en y ajoutant des mesures de contrôle propres à la protection des IIP. Il n'est pas exigé d'étendre bon nombre des mesures de la norme ISO/CEI 27002:2022 pour pouvoir les appliquer aux contrôleurs des IIP. Toutefois, dans certains cas, il a été nécessaire d'ajouter des conseils supplémentaires sur la mise en œuvre de ces mesures; ces conseils apparaissent alors sous le titre (et le numéro d'article) correspondants de la norme ISO/CEI 27002:2022.

On trouvera dans l'Annexe A de nombreuses mesures de contrôle qui visent spécifiquement à protéger les IIP. Ces nouvelles mesures de protection des IIP, ainsi que les conseils qui les accompagnent, sont répartis en douze catégories correspondant à la politique de protection de la vie privée et aux onze principes relatifs à la vie privée qui sont énoncés dans la norme ISO/CEI 29100:

- consentement et choix;

- légitimité et définition du but;
- limites du recueil d'informations;
- réduction des informations au minimum;
- limites d'utilisation, de conservation et de divulgation;
- exactitude et qualité;
- ouverture, transparence et note d'information;
- participation et accès de l'entité principale;
- responsabilité;
- sécurité des informations; et
- respect de la vie privée.

On trouvera dans la Figure 1 ci-après une description de la relation entre la présente spécification et d'autres normes internationales.

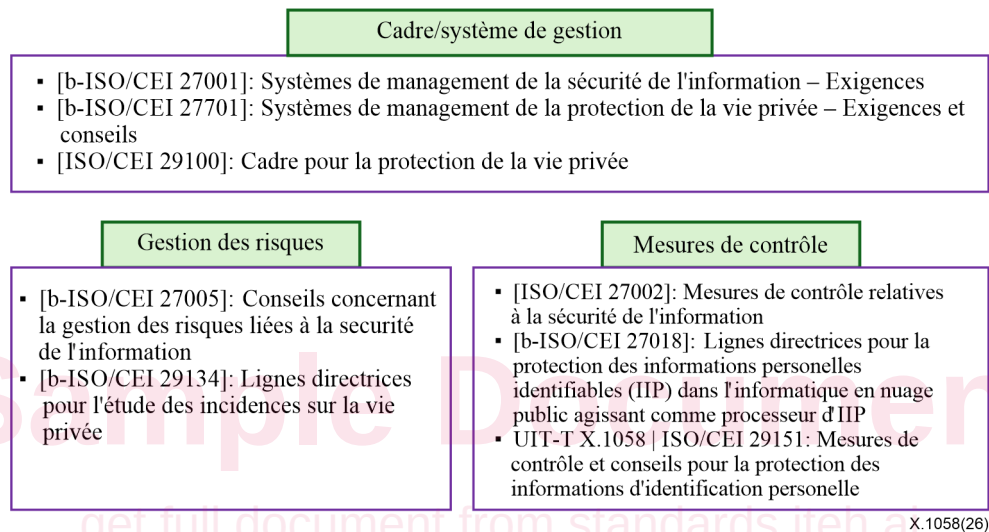


Figure 1 – Relation entre la présente spécification et d'autres normes internationales

La présente spécification contient des conseils fondés sur la norme ISO/CEI 27002. Ces conseils sont adaptés si nécessaire afin de répondre aux besoins de protection de la vie privée découlant du traitement des IIP:

- a) dans différents domaines de traitement, notamment:
 - les services publics en nuage;
 - les applications de réseaux sociaux;
 - les appareils domestiques connectés à l'Internet;
 - la recherche et l'analyse;
 - le ciblage d'IIP à des fins de publicité et d'autres fins analogues;
 - les programmes d'analyse des grands volumes de données;
 - le traitement des données relatives à l'emploi;
 - la gestion des ventes et des services (planification des ressources de l'entreprise, gestion de la relation client);
- b) sur différentes plates-formes de traitement, notamment:
 - sur une plate-forme de traitement personnelle fournie à une personne (comme une carte à puce, un téléphone intelligent équipé d'applications, un compteur électrique intelligent, des dispositifs à porter sur soi);
 - dans des réseaux de transmission et de recueil de données (par exemple, lorsque l'administration d'un réseau permet de localiser un téléphone mobile, cette information pouvant être considérée comme une IIP sous certaines juridictions);
 - dans l'infrastructure de traitement propre à une organisation;

- sur la plate-forme de traitement d'un tiers;
- c) pour certains types de recueil de données, notamment:
 - un recueil de données n'intervenant qu'une seule fois (par exemple, lors de la création d'un compte d'accès à un service);
 - le recueil permanent de données (par exemple, dans le cadre de la surveillance de la santé, où des capteurs situés sur ou dans le corps recueillent fréquemment des informations, ou encore les nombreuses opérations de recueil de données intervenant lorsqu'on emploie une carte de paiement sans contact, ou des systèmes de recueil de données par des compteurs électriques intelligents).

Les opérations permanentes de recueil de données peuvent contenir ou produire des IIP concernant le comportement ou l'emplacement des personnes, ainsi que d'autres types de données à caractère personnel. Dans ces cas, il est recommandé d'appliquer des mesures de protection des IIP qui permettent:

- de gérer l'accès et le recueil de ces informations sur la base du consentement; et
- à l'entité principale des IIP de surveiller comme il convient cet accès et ce recueil.

Sample Document

get full document from standards.iteh.ai

NORME INTERNATIONALE
RECOMMANDATION UIT-T**Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de contrôle, prescriptions et conseils pour la protection des informations d'identification personnelle****1 Domaine d'application**

La présente Recommandation | Norme internationale définit un certain nombre de buts et de mesures de contrôle, et contient des recommandations permettant de mettre ces mesures en œuvre. Elle vise à répondre aux besoins recensés dans le cadre des évaluations de risque et d'impact effectuées dans le domaine de la protection des informations d'identification personnelle (IIP).

En particulier, la présente Recommandation | Norme internationale définit des prescriptions et des recommandations qui sont fondées sur la norme ISO/CEI 27002, compte tenu des mesures de contrôle prises dans le cadre du traitement des IIP qui peuvent être pertinentes au regard des risques de sécurité pesant sur les informations d'une organisation particulière.

La présente Recommandation | Norme internationale s'applique aux organisations de tout type et de toute taille ayant pour mission de contrôler les IIP (au sens de la norme ISO/CEI 29100), qu'il s'agisse d'entreprises publiques ou privées, d'organismes publics ou d'ONG, dès lors qu'elles effectuent un traitement des IIP. Elle s'applique en particulier aux organisations dépourvues de système de gestion des informations personnelles.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes Recommandations et Normes sont sujettes à révision et les parties prenantes aux accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur. Le Bureau de la normalisation des télécommunications de l'UIT tient à jour une liste des Recommandations UIT-T en vigueur.

- ISO/CEI 27002:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité de l'information*.
- ISO/CEI 29100:2024, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

3 Termes, définitions et abréviations**3.1 Termes et définitions**

Pour les besoins de la présente Recommandation | Norme internationale, les termes et définitions donnés dans l'ISO/CEI 27000, l'ISO/CEI 27002 et l'ISO/CEI 29100 ainsi que les suivants s'appliquent.

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

- Base de données des termes et définitions de l'UIT: disponible à l'adresse <https://www.itu.int/myworkspace/terminology>.
- Plate-forme de navigation en ligne de l'ISO: disponible à l'adresse <https://www.iso.org/obp>.
- CEI Electropedia: disponible à l'adresse <https://www.electropedia.org/>.

3.1.1 directeur des données personnelles (DDP): cadre supérieur responsable de la protection des *données d'identification personnelle* (IIP) (voir le point 3.1.4) dans une *organisation* (voir le point 3.1.3).

3.1.2 désidentification: opération consistant à supprimer l'association entre un ensemble de données permettant l'identification et l'entité à qui appartiennent ces données en utilisant des techniques de désidentification.

3.1.3 organisation: personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses objectifs.

NOTE – Le concept d'organisation englobe, sans s'y limiter, les travailleurs indépendants, les compagnies, les sociétés, les firmes, les entreprises, les administrations, les partenariats, les organisations caritatives ou les institutions, ou bien une partie ou une combinaison des entités précédentes, à responsabilité limitée ou ayant un autre statut, de droit public ou privé.

3.1.4 information d'identification personnelle (IIP): information a) qui peut être utilisée pour établir un lien entre l'information et la personne physique à laquelle l'information appartient, ou b) qui est ou pourrait être directement ou indirectement liée à une personne physique.

NOTE – Dans cette définition, la "personne physique" correspond à l'entité principale des IIP (voir le point 3.1.6). Pour déterminer si l'entité principale des IIP peut être identifiée, il convient de tenir compte de tous les moyens qui peuvent être raisonnablement utilisés par la partie intervenant dans la protection de la vie privée et détenant les données, ou par toute autre partie, pour identifier le lien entre l'ensemble d'IIP et la personne physique.

[SOURCE: ISO/CEI 29100, 3.7]

3.1.5 contrôleur des informations d'identification personnelle (contrôleur des IIP): partie(s) intervenant dans la protection de la vie privée qui détermine(nt) les finalités et les moyens du traitement des *informations d'identification personnelle (IIP)* (voir le point 3.1.4), autre(s) que les personnes physiques qui utilisent les données à des fins personnelles.

NOTE – Un contrôleur des IIP charge parfois d'autres personnes [par exemple, *des prestataires de services chargés de traiter des IIP* (voir le point 3.1.7)] de traiter les PII en son nom, tout en conservant la responsabilité du contrôle.

[SOURCE: ISO/CEI 29100, 3.8]

3.1.6 entité principale des informations d'identification personnelle – sujet des données (entité principale des IIP): personne physique à laquelle les *informations d'identification personnelle (IIP)* (voir le point 3.1.4) se rapportent.

[SOURCE: ISO/CEI 29100, 3.9]

3.1.7 prestataire de services chargé de traiter des informations d'identification personnelle (prestataire de services chargé de traiter des IIP): partie intervenant dans la protection de la vie privée qui traite les *informations d'identification personnelle (IIP)* (voir le point 3.1.4) au nom et conformément aux instructions d'un *contrôleur des IIP* (voir le point 3.1.5).

[SOURCE: ISO/CEI 29100, 3.10]

3.1.8 évaluation des risques pour la vie privée – évaluation des incidences sur la vie privée: processus global d'identification, d'analyse, d'évaluation, de consultation, de communication et de planification du traitement d'éventuelles incidences sur la vie privée en ce qui concerne le traitement des *informations d'identification personnelle* (voir le point 3.1.4), s'inscrivant dans un cadre de gestion des risques plus vaste de l'organisation.

[SOURCE: ISO/CEI 29100, 3.18]

3.2 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent:

DDP	directeur des données personnelles
EIVP	évaluation des incidences sur la vie privée
IIP	informations d'identification personnelle

4 Aperçu général

4.1 Protection des IIP

La présente Recommandation | Norme internationale contient un ensemble de mesures de contrôle destinées à protéger les informations d'identification personnelle (IIP). Ces mesures ont pour but d'aider les organisations à mettre en place un ensemble de mesures de contrôle dans le cadre de leur programme général de protection des IIP. Ces mesures peuvent être appliquées pour apporter la preuve de la conformité de l'organisation à la législation et aux réglementations en matière de données personnelles, ainsi que pour gérer les risques concernant les données personnelles et pour répondre aux attentes des entités principales des IIP, des législateurs ou des clients, conformément aux principes en matière de données personnelles énoncés dans les articles de la norme ISO/CEI 29100.

4.2 Besoins en matière de protection des IIP

Il convient que les organisations recensent leurs besoins en matière de protection des IIP. Pour ce faire, il est possible d'utiliser la norme ISO/CEI 29100. Les besoins dans ce domaine sont dictés par quatre types de facteurs:

- les facteurs juridiques et réglementaires pour la protection des données personnelles de l'entité principale des IIP et la protection de ses IIP;
- les facteurs contractuels, tels que les accords conclus entre plusieurs acteurs différents, les politiques d'entreprise et les règles d'entreprise contraignantes;
- les facteurs liés à l'évaluation des risques, notamment l'évaluation des risques pour la vie privée, qui couvre le contexte externe et interne qu'il est possible de déterminer par le biais de la stratégie et des objectifs de l'organisation; et

- les politiques d'entreprise: une organisation peut volontairement choisir d'aller au-delà des critères découlant des besoins déjà recensés.

Il convient de choisir les mesures de protection des IIP (et en particulier les mesures de sécurité de l'information) au regard des résultats de l'évaluation des risques. Les résultats d'une évaluation des incidences sur la vie privée (EIVP) comme celle qui est décrite dans la norme ISO/CEI 29134 peuvent aider à établir, prioriser et mettre en œuvre les mesures de contrôle appropriées pour la gestion des risques liés à la protection des IIP, et la mise en place des mesures de contrôle choisies pour se prémunir contre ces risques.

Le document d'une EIVP tel que défini dans la norme ISO/CEI 29134 facilite ces travaux; il contient notamment des conseils en matière d'évaluation des risques pour la vie privée, un plan de traitement de ces risques et des indications sur l'acceptation et la révision de ces risques.

4.3 Mesures de contrôle découlant de l'évaluation des risques pour la vie privée

L'évaluation des risques pour la vie privée aide les organisations à protéger la confidentialité, l'intégrité et la disponibilité des IIP. Une atteinte à des données peut causer un préjudice important tant pour les organisations que pour les individus. Il convient que les organisations identifient et mettent en œuvre des mesures de contrôle pour remédier aux risques recensés lors du processus d'évaluation de l'incidence des risques. Il convient que le rapport de l'évaluation des risques pour la vie privée décrive au moins les besoins du système, la conception du système ainsi que les plans opérationnels et les procédures. La norme ISO/CEI 29134 fournit des informations sur ce qu'il convient de documenter dans une évaluation des risques pour la vie privée.

NOTE – Certaines juridictions exigent des évaluations des risques pour la vie privée en fonction du niveau du risque associé au traitement des IIP, de la nature de l'organisation (agences gouvernementales par exemple), etc.

4.4 Choix des mesures de contrôle

Les mesures de contrôle peuvent être choisies parmi celles qui sont proposées dans la présente spécification et, par référence, parmi les mesures de la norme ISO/CEI 27002, pour créer un ensemble de mesures de référence mixtes. Au besoin, on peut également choisir des mesures parmi d'autres ensembles, ou en concevoir de nouvelles pour répondre à des besoins particuliers.

Le choix des mesures dépend des décisions que l'organisation va prendre en fonction des options dont elle dispose pour lutter contre les risques, et de sa stratégie générale de gestion des risques. Ces mesures seront appliquées à l'organisation et, par le biais d'accords contractuels, à ses clients et ses fournisseurs.

NOTE – Le choix des mesures de contrôle peut aussi être dicté par des prescriptions légales.

Les organisations doivent tenir compte de l'extension des mesures de contrôle à la protection des IIP figurant dans l'Annexe A pour choisir les mesures de contrôle qui permettront de mettre en œuvre les options choisies pour lutter contre les risques touchant à la vie privée.

Le choix et la mise en œuvre des mesures de contrôle dépendent aussi du rôle que l'organisation joue dans la mise à disposition d'infrastructures ou la prestation de services. De nombreuses organisations peuvent intervenir dans ces deux types d'activités. Dans certains cas, les mesures peuvent être propres à une organisation particulière, tandis que dans d'autres, plusieurs organisations peuvent partager les mêmes rôles dans la mise en œuvre des mesures. Il convient que les accords contractuels définissent clairement les responsabilités de protection des IIP de toutes les organisations concernées dans la prestation ou l'utilisation de ces services.

Les mesures de contrôle figurant dans la présente spécification peuvent servir de point de référence aux organisations qui sont amenées à traiter des IIP, et elles sont applicables par toute organisation ayant pour mission de contrôler des IIP. Il convient que les prestataires de services chargés de traiter des IIP appliquent les mesures de la présente spécification conformément aux instructions du contrôleur des IIP. Il convient que ce dernier s'assure que les prestataires sont en mesure de mettre en œuvre toutes les mesures de contrôle prévues dans leur accord de traitement des IIP, conformément à l'objectif de traitement de ces informations. Si les contrôleurs des IIP utilisent des services en nuage pour le traitement des IIP, ils peuvent aussi examiner la norme ISO/CEI 27018 pour déterminer les mesures de contrôle à appliquer.

Les mesures figurant dans la présente spécification sont exposées plus en détail dans les articles 5 à 8, avec un certain nombre de conseils sur leur mise en œuvre. Celle-ci peut être simplifiée si les besoins de protection des IIP ont été pris en compte dès la conception des systèmes d'information, des services et du fonctionnement de l'organisation. Cette démarche fait partie d'une notion souvent appelée "protection de la vie privée dès la conception" (PVPC). On trouvera de plus amples informations sur le choix des mesures de contrôle et d'autres méthodes de gestion des risques dans la norme ISO/CEI 29134. La bibliographie comporte en outre d'autres documents de référence pertinents.

4.5 Élaboration de lignes directrices propres à l'organisation

La présente Recommandation | Norme internationale peut servir de point de départ pour élaborer des lignes directrices propres à une organisation donnée. Néanmoins, toutes les mesures et les conseils qu'elle présente ne sont pas applicables à toutes les organisations.

Au demeurant, certaines mesures de contrôle ou lignes directrices supplémentaires qui ne figurent pas dans la présente Recommandation | Norme internationale peuvent aussi être exigées. Lorsque d'autres spécifications contenant des lignes directrices ou des mesures de contrôle supplémentaires sont élaborées, il peut être utile d'y inclure des références aux articles de la présente spécification, le cas échéant, afin que les auditeurs et les partenaires commerciaux puissent plus facilement effectuer leurs vérifications de conformité.

4.6 Éléments concernant le cycle de vie

Les IIP ont un cycle de vie naturel, qui commence à leur création ou leur origine, passe par le recueil, le stockage, l'utilisation et la transmission et s'achève par leur suppression éventuelle (par exemple au moyen d'un système de destruction sécurisé). La valeur des IIP et les risques qui lui correspondent varient au cours de ce cycle de vie, mais la protection de ces informations reste importante à toutes les étapes et dans tous les contextes du cycle de vie.

Les systèmes d'information ont également un cycle de vie au cours duquel ils sont conçus, spécifiés, élaborés, développés, testés, mis en œuvre, exploités, maintenus et finalement mis hors service et éliminés. Il convient que la protection des IIP soit également prise en compte à chacune de ces étapes. À l'occasion de la création d'un nouveau système d'information ou de la modification d'un système existant, les organisations peuvent mettre à jour et améliorer leurs mesures de sécurité de l'information ainsi que leurs mesures de protection des IIP en tenant compte des incidents réellement survenus et des risques actuels et futurs pesant sur la sécurité de l'information.

4.7 Structure de la présente Recommandation | Norme internationale

Dans la norme ISO/CEI 27002 et la présente Recommandation | Norme internationale, la description des mesures est structurée comme suit. Chaque mesure comprend les éléments suivants:

- a) intitulé de la mesure: nom de la mesure en quelques mots;
- b) tableau des attributs: tableau donnant la (les) valeur(s) de chaque attribut d'une mesure donnée;
- c) mesure de contrôle: description de la mesure;
- d) finalité: raison pour laquelle il convient de mettre en œuvre la mesure;
- e) conseils: manière dont il convient de mettre en œuvre la mesure;
- f) autres renseignements: texte explicatif ou références à d'autres spécifications connexes.

Certaines mesures de contrôle de la présente spécification comportent un sous-titre pour faciliter la lecture lorsque les conseils sont particulièrement longs et couvrent plusieurs thèmes. Ces sous-titres sont soulignés. Tous les paragraphes contenant des conseils ne possèdent pas nécessairement de sous-titres.

Les articles 5 à 8 contiennent des conseils supplémentaires ainsi que d'autres informations relatives à certaines mesures de contrôle pertinentes figurant dans la norme ISO/CEI 27002. Le format des articles 5 à 8 reprend les titres et la numérotation des articles de la norme ISO/CEI 27002 pour que le lecteur puisse se reporter à l'ISO/CEI 27002.

Plus précisément, les règles suivantes ont été suivies pour reproduire dans la présente spécification les mesures de contrôle figurant dans la norme ISO/CEI 27002:

- Lorsque les divers éléments de la structure d'une mesure (décrite dans le présent paragraphe) sont identiques, seule une référence à la mesure correspondante de la norme ISO/CEI 27002 est fournie.
- Lorsque la mesure de contrôle requiert d'autres conseils et informations dans le contexte de la protection des IIP, des conseils supplémentaires figurent dans les paragraphes intitulés "Conseils pour la protection des IIP" et "Autres informations concernant la protection des IIP". Ces conseils sont aussi désignés par l'expression "Conseils de mise en œuvre pour la protection des IIP".
- La numérotation des articles de la présente spécification reproduit celle des articles correspondants de la norme ISO/CEI 27002.

L'Annexe A établit un ensemble de mesures propres à la protection des IIP. Elle suit le format de la norme ISO/CEI 27002, qui contient la définition de chaque mesure suivie de la finalité de la mesure et de conseils et autres informations pouvant s'avérer pertinents.

NOTE – L'Annexe B fournit les correspondances entre la présente spécification (Rec. UIT-T X.1058 (2026) | ISO/CEI 29151:2026) et son édition précédente (Rec. UIT-T X.1058 (2017) | ISO/CEI 29151:2017).

Le Tableau 1 donne l'emplacement, dans la norme ISO/CEI 27002, des conseils propres à la protection des IIP et autres informations concernant la mise en œuvre des mesures de contrôle.

Tableau 1 – Emplacement dans la norme ISO/CEI 27002 des conseils propres à la protection des IIP (appelées DCP dans la norme ISO/CEI 27002) et autres informations concernant la mise en œuvre des mesures de contrôle (appelées "mesures de sécurité" dans la norme ISO/CEI 27002)

Numéro de la mesure dans la norme ISO/CEI 27002	Nom de la mesure dans la norme ISO/CEI 27002	Remarques
Article 5 – Mesures de sécurité organisationnelles		
5.1	Politiques de sécurité de l'information	Contient des conseils supplémentaires concernant la protection des IIP.
5.2	Fonctions et responsabilités liées à la sécurité de l'information	Contient des conseils supplémentaires concernant la protection des IIP.
5.3	Séparation des tâches	Contient des conseils supplémentaires concernant la protection des IIP.
5.4	Responsabilité de la direction	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.5	Contacts avec les autorités	Contient des conseils supplémentaires concernant la protection des IIP.
5.6	Contacts avec des groupes d'intérêt spécifiques	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.7*	Renseignements sur les menaces	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.8	Sécurité de l'information dans la gestion de projet	Contient des conseils supplémentaires et d'autres informations concernant la protection des IIP.
5.9	Inventaire des informations et autres actifs associés	Contient des conseils supplémentaires concernant la protection des IIP.
5.10	Utilisation correcte des informations et autres actifs associés	Contient des conseils supplémentaires concernant la protection des IIP.
5.11	Restitution des actifs	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.12	Classification des informations	Contient des conseils supplémentaires concernant la protection des IIP.
5.13	Marquage des informations	Contient des conseils supplémentaires concernant la protection des IIP.
5.14	Transfert des informations	Contient des conseils supplémentaires concernant la protection des IIP.
5.15	Contrôle d'accès	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.16	Gestion des identités	Contient des conseils supplémentaires concernant la protection des IIP.
5.17	Informations d'authentification	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.18	Droits d'accès	Contient des conseils supplémentaires et d'autres informations concernant la protection des IIP.
5.19	Sécurité de l'information dans les relations avec les fournisseurs	Contient des conseils supplémentaires et d'autres informations concernant la protection des IIP.
5.20	La sécurité de l'information dans les accords conclus avec les fournisseurs	Contient des conseils supplémentaires concernant la protection des IIP.
5.21	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.22	Surveillance, révision et gestion des changements des services fournisseurs	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.23*	Sécurité de l'information dans l'utilisation de services en nuage	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.

Tableau 1 – Emplacement dans la norme ISO/CEI 27002 des conseils propres à la protection des IIP (appelées DCP dans la norme ISO/CEI 27002) et autres informations concernant la mise en œuvre des mesures de contrôle (appelées "mesures de sécurité" dans la norme ISO/CEI 27002)

Numéro de la mesure dans la norme ISO/CEI 27002	Nom de la mesure dans la norme ISO/CEI 27002	Remarques
5.24	Planification et préparation de la gestion des incidents de sécurité de l'information	Contient des conseils supplémentaires concernant la protection des IIP.
5.25	Évaluation des événements de sécurité de l'information et prise de décision	Contient des conseils supplémentaires concernant la protection des IIP.
5.26	Réponse aux incidents de sécurité de l'information	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.27	Tirer des enseignements des incidents de sécurité de l'information	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.28	Collecte des preuves	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.29	Sécurité de l'information pendant une perturbation	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.30*	Préparation des TIC pour la continuité d'activité	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.31	Exigences légales, statutaires, réglementaires et contractuelles	Contient des conseils supplémentaires concernant la protection des IIP.
5.32	Droits de propriété intellectuelle	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.33	Protection des enregistrements	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.34	Protection de la vie privée et des DCP	Contient des conseils supplémentaires concernant la protection des IIP.
5.35	Révision indépendante de la sécurité de l'information	Contient des conseils supplémentaires et d'autres informations concernant la protection des IIP.
5.36	Conformité aux politiques, règles et normes de sécurité de l'information	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
5.37	Procédures d'exploitation documentées	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
Article 6 – Mesures de sécurité applicables aux personnes		
6.1	Sélection des candidats	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
6.2	Termes et conditions du contrat de travail	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
6.3	Sensibilisation, enseignement et formation en sécurité de l'information	Contient des conseils supplémentaires concernant la protection des IIP.
6.4	Processus disciplinaire	Contient des conseils supplémentaires concernant la protection des IIP.
6.5	Responsabilité après la fin ou le changement d'un emploi	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.
6.6	Accords de confidentialité ou de non-divulgaration	Contient des conseils supplémentaires concernant la protection des IIP.
6.7	Travail à distance	Contient des conseils supplémentaires concernant la protection des IIP.
6.8	Déclaration des événements de sécurité de l'information	Ne contient aucun conseil supplémentaire ou autre information concernant la protection des IIP.