ISO 27001: Liste des Annexes

ISO 27001 Annex A Controls

En quoi 27002 peut être utile?

- Afin de sélectionner les contrôles dans le cadre de l'implantation d'un SMSI basé sur ISO 27001 ;
- Afin d'implanter les contrôles de sécurité généralement acceptés ; ou
- Afin de développer ses propres encadrements de sécurité

ISO/IEC 27002:2013
Critères de sélection

- Les critères pour la sélection des mesures de sécurité incluent:
  - Leur pertinence selon les risques spécifiques identifiés
  - Les critères d'acceptation et le niveau de tolérance au risque de l'organisation
  - Leur coût vs la réduction de risques
  - Les exigences légales, réglementaires, d'industrie ou contractuelles applicables
  - Des facteurs non financiers (réputation, image de marque, etc.)

Facteurs clés de réussite

- Cohérence avec les objectifs d'affaires de l'organisme
- SMSI conforme à la culture de l'organisme
- Soutien et l'engagement visibles de la direction
- Bonne compréhension des exigences en matière de sécurité de l'information, d'évaluation et de gestion des risques
- Communication efficace auprès de tous
- Diffusion des lignes directrices
- Budget dévolu à la sécurité de l'information
- Mesures adéquates pour la sensibilisation, la qualification et la formation

Partie 3

ISO 27001 - Annexe A

Objectifs de contrôle et contrôles

Objectif de contrôle vs. Contrôle

- Objectif de contrôle : *But, **résultat** vers lequel tendent les actions relatives à la sécurité*

- Contrôle : ***Moyen** de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et pouvant être de nature **administrative, technique, gestionnaire ou juridique***

ISO 27001 - Annexe A
Articles 5 à 18

- Couvrent les 14 domaines suivants :
  - A.5 Politiques de sécurité de l'information
  - A.6 Organisation de la sécurité de l'information
  - A.7 Sécurité des ressources humaines
  - A.8 Gestion des actifs
  - A.9 Contrôle d'accès
  - A.10 Cryptographie
  - A.11 Sécurité physique et environnementale
  - A.12 Sécurité des opérations
  - A.13 Sécurité des communications
  - A.14 Acquisition, développement et maintenance des systèmes
  - A.15 Relations avec les fournisseurs
  - A.16 Gestion des incidents de sécurité de l'information
  - A.17 Aspects de sécurité dans la gestion de la continuité des affaires
  - A.18 Conformité

A.5 Politiques de sécurité de l'information

Objectif(s) de contrôle
• **Apporter, à la sécurité de l'information, une orientation et un soutien de de la haute-direction, conformément aux exigences métier et aux lois et règlements en vigueur.**

A.6 Organisation de la sécurité de l'information

Objectif(s) de contrôle

- **Établir un cadre de gestion afin d'initier et contrôler l'implantation et les opérations de la sécurité de l'information dans l'organisation.**
- **Assurer la sécurité de l'utilisation des technologies d'accès à distance et de mobilité**

A.7 Sécurité des ressources humaines

Objectif(s) de contrôle
• **Avant l'emploi, pendant et après :**   • **S'assurer que les employés et sous-traitants comprennent et assument les responsabilités en fonction de leur rôle.**

A.8 Gestion des actifs

Objectif(s) de contrôle
• **Identifier les actifs de l'organisation et identifier les responsables de leur protection** • **S'assurer que les informations reçoivent le niveau approprié de protection en fonction de leur importance (classification des actifs)** • **Prévenir la compromission de la « DIC » de l'information entreposée sur les médias**

A.9 Contrôle d’accès

Objectif(s) de contrôle
• **Limiter l’accès à l’information et aux facilité de traitement** • **S’assurer que seul les utilisateurs autorisés ont accès aux ressources TI** • **S’assurer que les utilisateurs protègent adéquatement leur authentifiant** • **Prévenir les accès non-autorisé aux systèmes et applications**

A.10 Cryptographie

Objectif(s) de contrôle
• **S’assurer d’une utilisation adéquate et efficace des moyens cryptographique afin de protéger l’intégrité et la confidentialité de l’information**

A.11 Sécurité physique et environnementale

Objectif(s) de contrôle
• **Prévenir les accès physiques non-autorisés et les dommages aux installations de traitement de l'information** • **Prévenir les pertes, dommages, vols et compromissions des actifs et prévenir les interruptions des opérations**

A.12 Sécurité des opérations

Objectif(s) de contrôle
• **S'assurer que les opérations informatiques sont sécuritaires** • **S'assurer que les infrastructures sont protégés contre le code-malveillant** • **S'assurer que l'information est protéger contre la perte de donnée** • **S'assurer que les évènements sont journalisés et surveillés** • **S'assurer de l'intégrité des logiciels** • **Prévenir l'exploitation des vulnérabilités techniques** • **Limiter l'impact des audits techniques**

A.13 Sécurité des communications

Objectif(s) de contrôle
• **S'assurer de la protection de l'information sur les réseaux** • **Maintenir la sécurité de l'information lors de transmission**

A.14 Acquisition, développement et maintenance des systèmes

Objectif(s) de contrôle
• **S'assurer que la protection de l'information est au cœur du cycle de vie du développement et de l'acquisition** • **Protection des données de tests**

A.15 Relations avec les fournisseurs

Objectif(s) de contrôle
• **S’assurer de la protection des actifs lors d’accès par les fournisseurs** • **Maintenir un niveau de sécurité de l’information traité par les fournisseurs**

A.16 Gestion des incidents de sécurité de l'information

Objectif(s) de contrôle
• **S'assurer d'un traitement adéquat et efficace des incidents de sécurité de l'information, incluant les communications de ces évènements**

A.17 Aspects de sécurité dans la gestion de la continuité des affaires

Objectif(s) de contrôle
• **S'assurer que la sécurité de l'information est intégré à la gestion de la continuité des affaires** • **S'assurer de la disponibilité de l'information et des capacités de traitement de l'information**

A.18 Conformité

Objectif(s) de contrôle
• **S’assurer d’éviter le non-respect des obligations légales, règlementaires et contractuelles** • **S’assurer que la sécurité est implantée et opérée en fonction de la politique de l’entreprise**

Ch. 5 : Politiques de sécurité de l'information

No	Sujet	Bonnes pratiques
5.1	**Politiques de sécurité de l'information**	
5.1.1	Politiques pour la sécurité de l'information	Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, publié et communiqué aux employés et aux tiers concernés
5.1.2	Révision des politiques de sécurité de l'information	Les politiques de sécurité de l'information doivent être révisées à intervalles fixés préalablement ou en cas de changements majeurs afin de s'assurer de leur pertinence, adéquation et efficacité

Ch. 6 : Organisation de la sécurité de l'information

No	Sujet	Bonnes pratiques
6.1	**Organisation interne**	
6.1.1	Attribution des responsabilités en matière de sécurité de l'information	Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées
6.1.2	Séparation des tâches	Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou usage non autorisé(e) des actifs de l'organisme.
6.1.3	Relations avec les autorités	Des relations appropriées doivent être mises en place avec les autorités pertinentes

Ch. 6 : Organisation de la sécurité de l'information

No	Sujet	Bonnes pratiques
6.1.4	Relations avec des groupes de spécialistes	Des contacts appropriés doivent être entretenus avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.
6.1.5	Sécurité dans la gestion de projet	La sécurité de l'information doit être adressée dans la gestion de projets peu importe le type de projet
6.2	**Appareils mobiles et télétravail**	
6.2.1	Politique sur l'utilisation d'appareils mobiles	Une politique et des mesures de sécurité doivent être adoptées pour gérer les risques introduits par l'utilisation d'appareils mobiles.
6.2.2	Politique sur la sécurité du télétravail	Une politique et des mesures de sécurité doivent être implantées afin de protéger l'information accédée, traitée ou stockée dans les sites de télétravail

Ch.7 : Sécurité des ressources humaines

No	Sujet	Bonnes pratiques
7.1	**Avant le recrutement**	
7.1.1	Sélection	Des vérifications des antécédents des postulants à un emploi doivent être réalisées conformément aux lois, aux règlements et à l'éthique et doivent être proportionnelles aux exigences d'affaires, à la classification des informations accessibles et aux risques perçus.
7.1.2	Conditions d'embauche	Les ententes contractuelles avec les employés et contractants doivent stipuler leurs obligations et celles de l'organisation en matière de sécurité de l'information.

Ch.7 : Sécurité des ressources humaines

No	Sujet	Bonnes pratiques
7.2	**Durant le contrat**	
7.2.1	Responsabilités de la direction	La direction doit demander aux employés et contractants d'appliquer la sécurité de l'information conformément aux politiques et procédures établies de l'organisation.
7.2.2	Sensibilisation	L'ensemble des employés et, le cas échant, les contractants, doivent suivre une sensibilisation à la sécurité et doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.
7.2.3	Processus disciplinaire	Un processus disciplinaire formel doit être élaboré pour les salariés ayant enfreint les règles de sécurité.

Ch.7 : Sécurité des ressources humaines

No	Sujet	Bonnes pratiques
7.3	**Fin ou changement du contrat**	
7.3.1	Responsabilités à la fin ou au changement du contrat	Les responsabilités en matière de sécurité de l'information qui demeurent valides après la fin ou le changement d'emploi doivent être définies, communiquées à l'employé ou au contractant et appliquées.

Ch. 8: Gestion des actifs

No	Sujet	Bonnes pratiques
8.1	**Responsabilités des actifs**	
8.1.1	Inventaire des actifs	Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré.
8.1.2	Propriétaire des actifs	Les actifs maintenus dans l'inventaire doivent avoir un propriétaire
8.1.3	Utilisation correcte	Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.
8.1.4	Restitution des actifs	Tous les employés et les contractants doivent restituer la totalité des actifs de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.

Ch. 8: Gestion des actifs

No	Sujet	Bonnes pratiques
8.2	**Classification de l'information**	
8.2.1	Critères de classification	Les informations doivent être classées en termes de valeur, d'exigences légales, de sensibilité et de criticité.
8.2.2	Marquage de l'information	Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisme.
8.2.3	Manipulation des actifs	Des procédures de manipulation des actifs doivent être élaborées et mises en œuvre conformément au plan de classification adopté par l'organisme.

Ch. 8: Gestion des actifs

No	Sujet	Bonnes pratiques
8.3	**Manipulation des supports**	
8.3.1	Gestion des supports amovibles	Des procédures doivent être mises en place pour la gestion des supports amovibles conformément au plan de classification adopté par l'organisme.
8.3.2	Mise au rebut	Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles.
8.3.3	Sécurité durant le transport	Les supports contenant des information doivent être protégés contre l'accès non-autorisé, la mauvaise utilisation ou la corruption durant le transport.

Ch. 9: Contrôle d’accès

No	Sujet	Bonnes pratiques
9.1	**Exigences d’affaires pour le contrôle d’accès**	
9.1.1	Politique de contrôle d’accès	Une politique de contrôle d’accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.
9.1..2	Accès aux réseaux et services réseaux	Les utilisateurs doivent avoir uniquement accès aux réseaux et services réseaux pour lesquels ils ont été spécifiquement reçus une autorisation.
9.2	**Gestion de l’accès des utilisateurs**	
9.2.1	Enregistrement des utilisateurs	Un processus formel d’inscription et désinscription des utilisateurs destinée à accorder et à supprimer l’accès à tous les systèmes et services d’information doit être implanté

Ch. 9: Contrôle d’accès (suite)

No	Sujet	Bonnes pratiques
9.2.2	Processus d’attribution et révocation	Un processus formel d’attribution et de révocation des droits d’accès de tous les types d’utilisateurs à tous les systèmes et services d’information doit être implanté
9.2.3	Gestion des privilèges	L’attribution et l’utilisation des privilèges doivent être restreintes et contrôlées.
9.2.4	Gestion du mot de passe utilisateur	L’attribution d’information secrète d’authentification doit être réalisée dans le cadre d’un processus formel.
9.2.5	Réexamen des droits d’accès utilisateurs	Les propriétaires d’actifs doivent réexaminer les droits d’accès des utilisateurs à intervalles réguliers
9.2.6	Révocation ou ajustement aux droits d’accès	Les droits d’accès des employés, contractants et utilisateurs tiers à l’information et aux moyens de traitement de l’information doivent être supprimés à la fin de leur période d’emploi, ou modifiés en cas de modification du contrat ou de l’accord.

Ch. 9: Contrôle d’accès (suite)

No	Sujet	Bonnes pratiques
9.3	**Responsabilités des utilisateurs**	
9.3.1	Utilisation du mot de passe	Il doit être exigé des utilisateurs qu’ils respectent les pratiques de l’organisation dans l’utilisation d’information secrète d’authentification.
9.4	**Contrôle d’accès aux systèmes et applications**	
9.4.1	Restriction d’accès à l’information	L’accès aux informations et aux fonctions applicatives des systèmes doit être restreint conformément à la politique de contrôle d’accès.
9.4.2	Ouverture de session sécurisée	Lors que requis par la politique de contrôle d’accès, l’accès aux systèmes et aux applications doit être soumis à une procédure sécurisée d’ouverture de session.

Ch. 9: Contrôle d’accès (suite)

No	Sujet	Bonnes pratiques
9.4.3	Système de gestion des mots de passe	Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité.
9.4.4	Emploi des utilitaires système	L’emploi des programmes utilitaires permettant de contourner les mesures d’un système ou d’une application doit être limité et contrôlé étroitement.
9.4.5	Contrôle d’accès au code source	L’accès au code source du programme doit être restreint.

Ch. 10: Cryptographie

No	Sujet	Bonnes pratiques
10.1	**Contrôles cryptographiques**	
10.1.1	Politique d'utilisation de contrôles cryptographiques	Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.
10.1.2	Gestion des clés	Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et implantée tout au long de leur cycle de vie.

Ch. 11: Sécurité physique et environnementale

No	Sujet	Bonnes pratiques
11.1	**Zones sécurisées**	
11.1.1	Périmètre de sécurité physique	Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité
11.1.2	Contrôles d'accès physiques	Les zones sécurisées doivent être protégées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité est admis.
11.1.3	Sécurisation des bureaux, salles et équipements	Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements.

Ch. 11: Sécurité physique et environnementale (suite)

No	Sujet	Bonnes pratiques
11.1.4	Protection contre les menaces extérieures et environnementales	Des mesures de protection physique contre les désastres naturels, les attaques ou les accidents doivent être conçues et appliquées.
11.1.5	Travail dans les zones sécurisées	Des procédures encadrant le travail en zone sécurisée doivent être conçues et appliquées.
11.1.6	Zones d'accès public, de livraison et de chargement	Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

Ch. 11: Sécurité physique et environnementale (suite)

No	Sujet	Bonnes pratiques
11.2	**Équipements**	
11.2.1	Choix de l'emplacement	Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.
11.2.2	Services généraux	Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux.
11.2.3	Sécurité du câblage	Les câbles électriques ou de télécommunications transportant des contre toute interception d'information ou dommage.
11.2.4	Maintenance du matériel	Le matériel doit être entretenu correctement pour garantir sa disponibilité permanente et son intégrité.

Ch. 11: Sécurité physique et environnementale (suite)

No	Sujet	Bonnes pratiques
11.2.5	Sortie d'un actif	Un matériel, des informations ou des logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.
11.2.6	Sécurité du matériel hors des locaux	La sécurité doit être appliquée au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.
11.2.7	Mise au rebut ou recyclage sécurisé du matériel	Tout le matériel contenant des supports de stockage doit être vérifié pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.

Ch. 11: Sécurité physique et environnementale (suite)

No	Sujet	Bonnes pratiques
11.2.8	Matériel utilisateur laissé sans surveillance	Les utilisateurs doivent s'assurer que le matériel laissé sans surveillance est protégé
11.2.9	Politique de bureau propre et écran vide	Une politique du bureau propre pour les documents papier et les supports de stockage amovible et une politique de l'écran vide doivent également être adoptées

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.1	**Procédures et responsabilités liées aux opérations**	
12.1.1	Procédures opérationnelles documentées	Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.
12.1.2	Gestion des changements	Les changements apportés à l'organisation, aux processus d'affaires, aux installations de traitement de l'information et aux systèmes qui affectent la sécurité de l'information doivent être contrôlés.
12.1.3	Dimensionnement	L'utilisation des ressources doit être surveillée et ajustée au plus près, et des projections doivent être faites sur les dimensionnements futurs pour assurer les performances requises par le système.

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.1.4	Séparation des environnements de développement, d'essai et de production	Les environnements de développement, d'essai et de production doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement de production.
12.2	**Protection contre les codes malveillants**	
12.2.1	Mesures contre les codes malveillants	Des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants doivent être implantées, combinées à une sensibilisation appropriée des utilisateurs.
12.3	**Sauvegarde**	
12.3.1	Copies de sauvegarde	Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.4	**Journalisation et surveillance**	
12.4.1	Journaux d'audit	Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité de l'information doivent être produits, conservés et régulièrement révisés.
12.4.2	Protection des informations journalisées	Les équipements de journalisation et les informations journalisées doivent être protégés contre le sabotage et les accès non autorisés.
12.4.3	Journal administrateur et journal d'opérations	Les activités de l'administrateur système et de l'opérateur système doivent être journalisées et les journaux doivent être protégés et régulièrement révisés.

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.4.4	Synchronisation des horloges	Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps précise et préalablement définie.
12.5	**Contrôle des logiciels d'exploitation**	
12.5.1	Installation de logiciel sur les systèmes d'exploitation	Des procédures doivent être implantées afin de contrôler l'installation de logiciel sur les systèmes d'exploitation. .

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.6	**Gestion des vulnérabilités techniques**	
12.6.1	Gestion des vulnérabilités	L'information concernant les vulnérabilités techniques des systèmes d'information utilisés doivent être obtenus rapidement, l'exposition de l'organisation à ces vulnérabilités évaluée et les mesures appropriées prises afin de mitiger les risques associés.
12.6.2	Restriction à l'installation de logiciel	Des règles encadrant l'installation de logiciel par les utilisateurs doivent être établies et implantées.

Ch. 12: Sécurité des opérations

No	Sujet	Bonnes pratiques
12.7	**Considérations liés à l'audit des systèmes d'information**	
12.7.1	Contrôles de l'audit des systèmes d'information	Les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation doivent être soigneusement planifiées et convenues afin de minimiser le risque de perturbation des processus d'affaires.

Ch. 13: Sécurité des communications

No	Sujet	Bonnes pratiques
13.1	**Gestion de la sécurité réseau**	
13.1.1	Mesures sur les réseaux	Les réseaux doivent être gérés et contrôlés afin de protéger l'information dans les systèmes et applications
13.1.2	Sécurité des services réseaux	Les mécanismes de sécurité, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis à l'interne ou impartis
13.1.3	Cloisonnement des réseaux	Les groupes de services, utilisateurs et systèmes d'information doivent être ségrégés sur les réseaux

Ch. 13: Sécurité des communications

No	Sujet	Bonnes pratiques
13.2	**Transfert d'information**	
13.2.1	Politiques et procédures d'échange d'information	Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tous types d'équipements de télécommunication.
13.2.2	Accords	Des accords doivent être conclus pour l'échange d'informations entre l'organisme et les parties externes.
13.2.3	Messagerie électronique	Les informations liées à la messagerie électronique doivent être protégées de manière adéquate.
13.2.4	Engagement de confidentialité	Les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme, doivent être identifiées et réexaminées régulièrement.

Ch. 14 : Acquisition, développement et maintenance

No	Sujet	Bonnes pratiques
14.1	**Exigences de sécurité des systèmes d'information**	
14.1.1	Analyse et spécifications des exigences	Les exigences relatives à la sécurité de l'information doivent être incluses dans les exigences des nouveaux systèmes d'information ou les améliorations apportées aux systèmes d'information existants
14.1.2	Sécurité des services applicatifs sur les réseaux publics	L'information liée aux services applicatifs transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les litiges contractuels et la divulgation et la modification non autorisées.
14.1.3	Protection des services transactionnels	Les informations liées aux services applicatifs transactionnels doivent être protégées pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.

Ch. 14 : Acquisition, développement et maintenance

No	Sujet	Bonnes pratiques
14.2	**Sécurité des processus de développement et soutien**	
14.2.1	Politique de développement sécuritaire	Des règles pour le développement sécuritaire des applications et systèmes doivent être établies et appliqués aux développements internes à l'organisation
14.2.2	Procédures de contrôle des modifications	Les changements aux systèmes dans le cycle de développement doivent être contrôlés par des procédures formelles de contrôle des changements.
14.2.3	Réexamen technique des applications après modification du système d'exploitation	Lorsque des systèmes d'exploitation sont changés, les applications d'affaires critiques doivent être revues et testées pour s'assurer qu'il n'y a pas d'impact négatif sur les opérations ou la sécurité.

Ch. 14 : Acquisition, développement et maintenance

No	Sujet	Bonnes pratiques
14.2.4	Restrictions relatives à la modification des progiciels	La modification des progiciels ne doit pas être encouragée, doit être limitée aux changements nécessaires et être contrôlée de manière stricte.
14.2.5	Principes d'ingénierie sécuritaire	Des principes pour l'ingénierie sécuritaire des systèmes doivent être établis, documentés, maintenus et appliqués à toutes les initiatives d'implantation de systèmes d'information.

Ch. 14 : Acquisition, développement et maintenance

No	Sujet	Bonnes pratiques
14.2.6	Protection des environnements de développement	L'organisation doit établir et protéger adéquatement les environnements de développement sécuritaire pour les efforts de développement et d'intégration de systèmes qui couvrent l'ensemble du cycle de développement.
14.2.7	Externalisation du développement logiciel	Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme.
14.2.8	Essais des fonctions de sécurité	Les fonctions de sécurité doivent être testées durant le développement.

Ch. 14 : Acquisition, développement et maintenance

No	Sujet	Bonnes pratiques
14.2.9	Acceptation des systèmes	Des tests d'acceptation et les critères y étant reliés doivent être établis pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.
14.3	**Données d'essai**	
14.3.1	Protection des données d'essai	Les données d'essai doivent être soigneusement sélectionnées, protégées et contrôlées

Ch. 15 : Relations avec les fournisseurs

No	Sujet	Bonnes pratiques
15.1	**Sécurité de l'information dans les relations avec les fournisseurs**	
15.1.1	Politique de gestion de la sécurité de l'information avec les fournisseurs	Les exigences de sécurité de l'information pour adresser les risques associés à l'accès d'un fournisseur aux actifs de l'organisation doivent être convenues avec le fournisseur et documentées.
15.1.2	Sécurité dans les accords avec les fournisseurs	Toutes les exigences de sécurité de l'information pertinentes doivent être établies et convenues avec chaque fournisseur qui peut accéder, traiter, stocker, communiquer ou fournir de l'infrastructure technologique pour l'information de l'organisation.
15.1.3	Sécurité de la chaine d'appro-visionnement	Les ententes avec les fournisseurs doivent inclure les exigences permettant d'adresser les risques associés à la chaine d'approvisionnement des services d'information et de communication.

Ch. 15 : Relations avec les fournisseurs

No	Sujet	Bonnes pratiques
15.2	**Gestion de la prestation de services des fournisseurs**	
15.2.1	Surveillance et examen	Les organisations doivent régulièrement surveiller, contrôler et auditer la prestation de services des fournisseurs.
15.2.2	Gestion des changements dans la prestation de services	Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.

Ch. 16 : Gestion des incidents de sécurité de l'information

No	Sujet	Bonnes pratiques
16.1	**Gestion des incidents de sécurité de l'information et améliorations**	
16.1.1	Responsabilités et procédures	Les responsabilités de la gestion et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.
16.1.2	Processus de signalement	Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.
16.1.3	Remontée de failles de sécurité par les employés	Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Ch. 16 : Gestion des incidents de sécurité de l'information

No	Sujet	Bonnes pratiques
16.1.4	Évaluation et décision	Les événements liés à la sécurité de l'information doivent être évalués afin de décider s'ils constituent des incidents de sécurité.
16.1.5	Procédures de traitement	Les incidents de sécurité de l'information doivent être traités conformément aux procédures établies
16.1.6	Post-mortem et améliorations	Les connaissances acquises lors de la résolution d'incidents de sécurité doivent être utilisées afin de réduire la probabilité d'occurrence ou l'impact de d'incidents éventuels.
16.1.7	Collecte de preuve	L'organisation doit définir et appliquer des procédures pour l'identification, la collecte, l'acquisition et la préservation d'information pouvant servir d'éléments de preuve.

Ch. 17 : Aspects de sécurité de la gestion de la continuité des affaires

No	Sujet	Bonnes pratiques
17.1	**Continuité de la sécurité de l'information**	
17.1.1	Planification de la continuité de la sécurité de l'information	L'organisation doit déterminer ses exigences de sécurité de l'information et la continuité de la gestion de la sécurité de l'information advenant une situation de crise ou un désastre.
17.1.2	Implantation de processus, procédures et contrôles	L'organisation doit établir, documenter, implanter et maintenir des processus, procédures et contrôles afin d'assurer le niveau de continuité exigé de la sécurité de l'information durant une situation de crise ou un désastre

Ch. 17 : Aspects de sécurité de la gestion de la continuité des affaires

No	Sujet	Bonnes pratiques
17.1.3	Vérification régulière	L'organisation doit vérifier les contrôles de continuité de la sécurité de l'information à intervalles régulières afin de s'assurer qu'ils sont valides et efficaces durant une situation de crise ou un désastre.
17.2	**Redondance**	
17.2.1	Disponibilité des installations de traitement des informations	Les installations de traitement des informations doivent être implantées avec une redondance suffisante pour satisfaire les exigences de disponibilité.

Ch. 18 : Conformité

No	Sujet	Bonnes pratiques
18.1	**Conformité aux exigences légales et contractuelles**	
18.1.1	Identification des exigences	Pour chaque système d'information et pour l'organisme, toutes les exigences légales, réglementaires et contractuelles en vigueur doivent être définies, documentées et mises à jour, ainsi que l'approche utilisée par l'organisme pour satisfaire à ces exigences.
18.1.2	Droits de propriété intellectuelle	Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.

Ch. 18 : Conformité

No	Sujet	Bonnes pratiques
18.1.3	Protection des enregistrements de l'organisme	Les enregistrements importants doivent être protégés contre la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.
18.1.4	Protection des données relatives à la vie privée	La protection et la confidentialité des données doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.
18.1.5	Réglementation relative aux mesures cryptographiques	Les mesures cryptographiques doivent être utilisées conformément aux accords, lois et réglementations applicables.

Ch. 18 : Conformité (suite)

No	Sujet	Bonnes pratiques
18.2	**Réexamen de sécurité de l'information**	
18.2.1	Réexamen indépendant de la sécurité de l'information	L'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire les objectifs de contrôles, contrôles, politiques, processus et procédures de sécurité de l'information) doit être réexaminée de manière indépendant à intervalles réguliers ou lors de changements majeurs.
18.2.2	Conformité avec les politiques et les normes de sécurité	Les gestionnaires doivent régulièrement s'assurer de la conformité du traitement de l'information et des procédures de leur champ de responsabilité aux politiques, standards et autres exigences de sécurité de l'information.
18.2.3	Vérification de la conformité technique	Les systèmes d'information doivent être régulièrement examinés pour vérifier leur conformité aux politiques et standards de sécurité de l'information de l'organisation.