Solutions de normalisation innovantes et reconnues

Webinaire – BNQ

Protégez vos données et celles de vos clients : un avantage concurrentiel

Donald Chébékoué
Auditeur ISO/IEC 27001
21 juin 2023

Respecte, en tout ou en partie, l'orthographe modernisée.

Plan de la présentation

Protégez vos données et celles de vos clients :
un avantage concurrentiel

Introduction

- Services du BNQ
- Définitions
- Famille ISO/IEC 27000

Systèmes de gestion

- Norme ISO/IEC 27001
- Annexe – ISO/IEC 27002

Conclusion

- Certification ISO/IEC 27001
- Questions souvent posées sur le BNQ et la certification

Introduction

Bureau de normalisation du Québec

- **Organisme créé en 1961**
- **Unité administrative d'Investissement Québec**
- **Plus de 70 employés**

Rôle stratégique

Soutenir le **développement économique** du Québec et répondre aux **enjeux de la société** par nos services de **normalisation** et de **certification**, en proposant des solutions novatrices en matière de **qualité**, de **durabilité** et de **sécurité**.

L’offre de service du BNQ

Pour répondre aux différents besoins

Audits de certification

Élaboration de normes

Nos secteurs d’activité

Plus de 60 ans d’expertise

- Agroalimentaire
- Environnement
- Infrastructures
- Santé et mieux-être au travail
- Foresterie
- Gestion des organisations
- Protection et sureté

Croissance des entreprises du Québec

Des avantages concurrentiels

Accélérer la mise en marché d'une nouvelle technologie

Répondre aux exigences des clients

Augmenter les exportations

Démontrer la prise en charge des critères ESG

Sécurité de l’information

Définitions

SMSI : Ensemble de politiques, procédures, lignes directrices et des ressources ainsi que les activités gérées collectivement par un organisme dans le but de protéger ses actifs informationnels.

Partie intéressée ou **partie prenante** : personne ou organisme susceptible d’affecter ou d’être affecté par un changement du SMSI

Sécurité de l'information

Famille ISO/IEC 27000

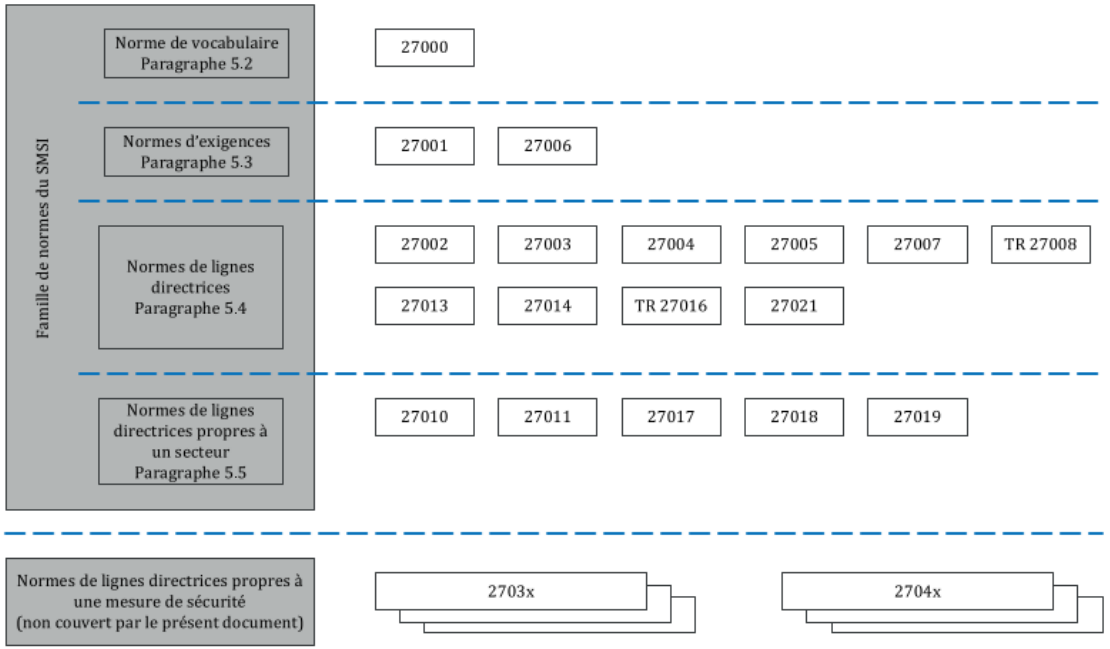


Figure 1 — Relations au sein de la famille de normes du SMSI

Source : Organisation internationale de normalisation (ISO), norme ISO/IEC 27000

Systèmes de gestion de la sécurité de l’information : ISO/IEC 27001

NORME INTERNATIONALE

ISO/IEC 27001

Troisième édition
2022-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Numéro de référence
ISO/IEC 27001:2022(F)

Source : Organisation internationale de normalisation (ISO), norme ISO/IEC 27001

Normes À propos de l'ISO Actualités Participer Store

ISO/IEC 27001

Systèmes de management de la sécurité de l'information

- **Chapitre 4** Contexte de l'organisation **P**
- **Chapitre 5** Leadership **P**
- **Chapitre 6** Planification **P**
- **Chapitre 7** Supports **P, D**
- **Chapitre 8** Fonctionnement **D**
- **Chapitre 9** Évaluation de la performance **C**
- **Chapitre 10** Amélioration **A**
- **Annexe A** Référencement des mesures de sécurité de l'information **D**

Source : Organisation internationale de normalisation (ISO)

Contexte

4.1 Compréhension de l’organisation et de son contexte

4.2 Compréhension des besoins et attentes des parties intéressées

4.3 Domaine d’application du SMSI

4.4 Système de management de la sécurité de l’information

Leadership

5.1 Leadership et engagement

5.2 Politique

5.3 Rôles, responsabilités et autorités au sein de l’organisation

Planification

6.1 Actions à mettre en œuvre face aux risques et opportunités

6.2 Objectifs de sécurité de l'information et plans pour les atteindre

6.3 Planification des modifications

Supports

7.1 Ressources

7.2 Compétences

7.3 Sensibilisation

7.4 Communication

7.5 Informations documentées

Évaluation de la performance

9.1 Surveillance, mesurage, analyse et évaluation

9.2 Audit interne

9.3 Revue de direction

Amélioration

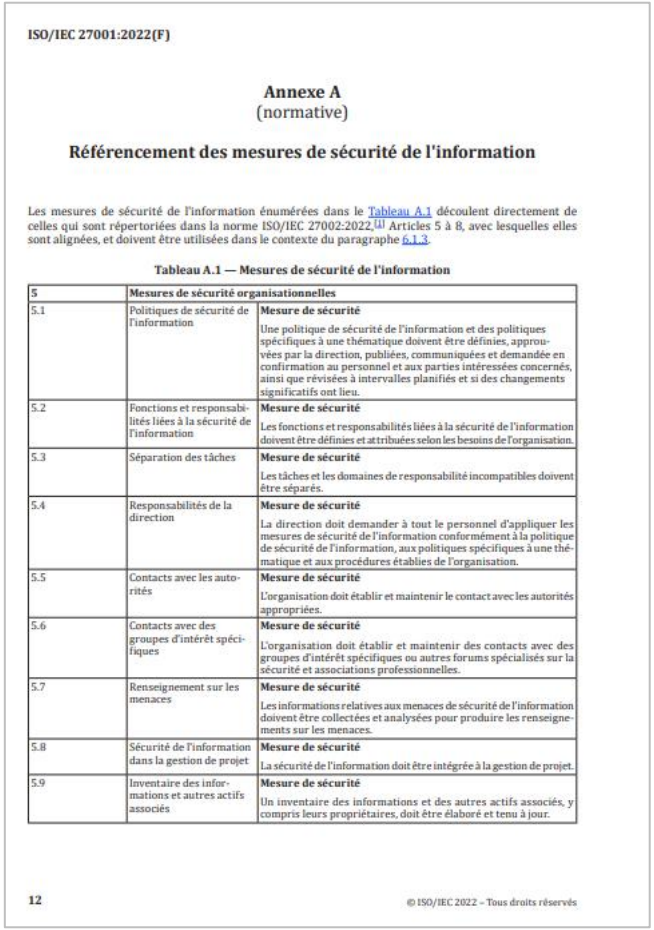
10.1 Amélioration continue

10.2 Non-conformité et action corrective

Annexe normative – Annexe A

Mesures de contrôle applicables

- **93 mesures** de contrôle
- Certaines peuvent ne pas s'appliquer à l'entreprise (**déclaration d'applicabilité**)
- En **supplément** aux contrôles organisationnels



ISO/IEC 27001:2022(F)

Annexe A
(normative)

Référencement des mesures de sécurité de l'information

Les mesures de sécurité de l'information énumérées dans le Tableau A.1 découlent directement de celles qui sont répertoriées dans la norme ISO/IEC 27002:2022,[1] Articles 5 à 8, avec lesquelles elles sont alignées, et doivent être utilisées dans le contexte du paragraphe 6.1.3.

Tableau A.1 — Mesures de sécurité de l'information

5	Mesures de sécurité organisationnelles	
5.1	Politiques de sécurité de l'information	**Mesure de sécurité** Une politique de sécurité de l'information et des politiques spécifiques à une thématique doivent être définies, approuvées par la direction, publiées, communiquées et demandée en confirmation au personnel et aux parties intéressées concernés, ainsi que révisées à intervalles planifiés et si des changements significatifs ont lieu.
5.2	Fonctions et responsabilités liées à la sécurité de l'information	**Mesure de sécurité** Les fonctions et responsabilités liées à la sécurité de l'information doivent être définies et attribuées selon les besoins de l'organisation.
5.3	Séparation des tâches	**Mesure de sécurité** Les tâches et les domaines de responsabilité incompatibles doivent être séparés.
5.4	Responsabilités de la direction	**Mesure de sécurité** La direction doit demander à tout le personnel d'appliquer les mesures de sécurité de l'information conformément à la politique de sécurité de l'information, aux politiques spécifiques à une thématique et aux procédures établies de l'organisation.
5.5	Contacts avec les autorités	**Mesure de sécurité** L'organisation doit établir et maintenir le contact avec les autorités appropriées.
5.6	Contacts avec des groupes d'intérêt spécifiques	**Mesure de sécurité** L'organisation doit établir et maintenir des contacts avec des groupes d'intérêt spécifiques ou autres forums spécialisés sur la sécurité et associations professionnelles.
5.7	Renseignement sur les menaces	**Mesure de sécurité** Les informations relatives aux menaces de sécurité de l'information doivent être collectées et analysées pour produire les renseignements sur les menaces.
5.8	Sécurité de l'information dans la gestion de projet	**Mesure de sécurité** La sécurité de l'information doit être intégrée à la gestion de projet.
5.9	Inventaire des informations et autres actifs associés	**Mesure de sécurité** Un inventaire des informations et des autres actifs associés, y compris leurs propriétaires, doit être élaboré et tenu à jour.

12

Source : Organisation internationale de normalisation (ISO), norme ISO/IEC 27001

Conclusion

Précisions sur le rôle du BNQ

Obtention d'une certification

Implantation de la norme

+

Audit de certification

=

Délivrance de certificat

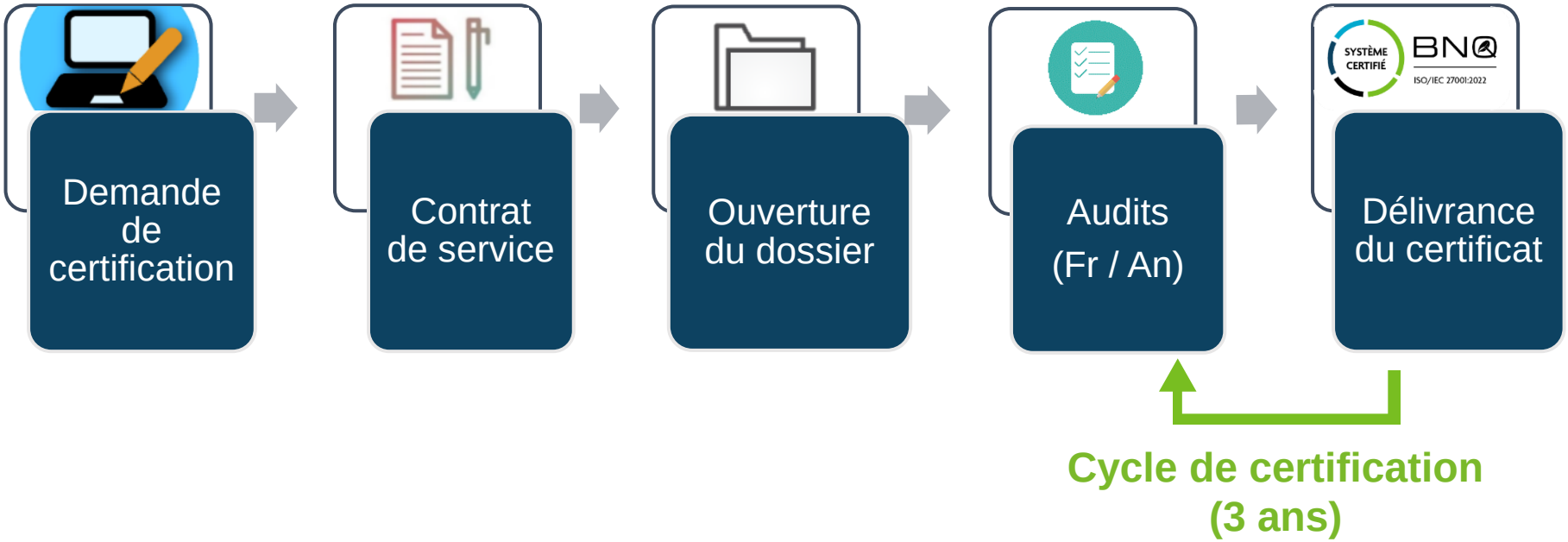
L'entreprise met en place les exigences de la norme

L'organisme de certification vérifie la conformité à la norme

SYSTÈME CERTIFIÉ BNQ ISO/IEC 27001:2022

Processus de certification

Les grandes étapes



Conclusion

Des normes et des certifications reconnues pour :

- ✓ Mettre de l’avant l’utilisation des meilleures pratiques
- ✓ Renforcer son image publique
- ✓ Meilleur positionnement sur les marchés nationaux et internationaux

BNQ
Bureau de normalisation du Québec

Votre organisme accrédité de normalisation, de certification ou de vérification

Merci.

Des questions?

SYSTÈME CERTIFIÉ

BNQ

ISO/IEC 27001:2022

Donald Chébékoué

Responsable des programmes ISO 27001 et CyberSécuritaire Canada

donald.chebekoue@bnq.qc.ca