HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

ISO 27002:2013
Comparatif avec la version 2005

Béatrice Joucreau

Sommaire

- Comparaison des structures
- Synthèse des changements de forme
- Synthèse des changements de fond
- Changements majeurs
  - Politique de sécurité de l'information
  - Continuité de la sécurité de l'information
  - Gestion des incidents
  - Cryptographie
- Changements mineurs
- Mesures supprimées
- Nouvelles mesures de sécurité
- Ce que ça change

Comparaison des structures

Quelques chiffres

ISO 27002:2005	ISO 27002:2013
11 chapitres (de mesures)	14 chapitres (de mesures)
39 objectifs de sécurité	35 objectifs de sécurité
133 mesures de sécurité	114 mesures de sécurité
4 chapitres avec moins de 6 mesures	4 chapitres avec moins de 6 mesures
3 chapitres à plus de 15 mesures	1 seul chapitre à 15 mesures

Comparaison des structures
Chapitres

ISO 27002:2005	ISO 27002:2013
5. Politique de sécurité	5. Politiques de sécurité de l'information
6. Organisation de la sécurité de l'information	6. Organisation de la sécurité de l'information
7. Gestion des actifs	7. Sécurité des ressources humaines
8. Sécurité liée aux ressources humaines	8. Gestion des actifs
9. Sécurité physique et environnementale	9. Contrôle d'accès
10. Gestion de l'exploitation et des télécommunications	10. Cryptographie
11. Contrôle d'accès	11. Sécurité physique et environnementale
12. Acquisition, développement et maintenance des systèmes d'information	12. Sécurité liée à l'exploitation
13. Gestion des incidents liés à la sécurité de l'information	13. Sécurité des communications
14. Gestion de la continuité de l'activité	14. Acquisition, développement et maintenance des systèmes d'information
15. Conformité	15. Relations avec les fournisseurs
	16. Gestion des incidents liés à la sécurité de l'information
	17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
	18. Conformité

Synthèse des changements de forme

- Références aux normes ISO 27000 plus nombreuses
- Structure
  - Articulation des chapitres identique : objectifs, mesures, implémentation, informations
  - Création de chapitres, déplacement de thèmes, fusion de mesures
- Reformulation de presque toutes les mesures
  - *Il convient que les procédures d'exploitation soient documentées → Il convient de documenter les procédures d'exploitation*
- Corrections de vocabulaire
- Meilleures traductions...
  - *Physical entry controls* : *Contrôle physique des accès → contrôle des accès physiques*
- ...Ou pas
  - *Code of practice for information security controls → Code de bonne pratique pour le management de la sécurité de l'information*

Synthèse des changements de fond

- Ancien chapitre 10. Gestion de l'exploitation et des télécommunications
  - 12. Sécurité liée à l'exploitation
  - 13. Sécurité des communications
  - 15. Relations avec les fournisseurs
- Ancien chapitre 12. Acquisition, développement et maintenance des systèmes d'information
  - 10. Cryptographie
  - 14. Acquisition, développement et maintenance des systèmes d'information
- Deux chapitres ont changé de sens
  - 5. Politiques de sécurité de l'information
  - 17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- 11 nouvelles mesures de sécurité
- 8 mesures de sécurité ont totalement disparu

Changements majeurs
Politiques de sécurité de l'information

- Chapitre 5 : changement de sens
- « *Politiques de sécurité de l'information*» et non plus « *politique* »
- Inclut la politique de sécurité de l'information de l'ancien chapitre 5
- Demande la déclinaison de la politique de sécurité de l'information en politiques par thème
- Remplacement de efficacité par effectivité (en français) seulement dans la 27001

Changements majeurs
Continuité de la sécurité de l'information

- Chapitre 14 → Chapitre 17
- Titre du chapitre : objectif 1 de l'ancien chapitre (en anglais)
- Changement total de l'esprit du chapitre
  - Attention portée sur la continuité de la sécurité, et non plus de l'activité
- Avant
  - Elaborer et gérer un plan de continuité d'activité
- Maintenant
  - Intégrer la sécurité dans le plan de continuité d'activité pour assurer la continuité de la sécurité en cas de sinistre
  - Redondance
  - Renvois vers les normes ISO 22301, 22313, 27031

Changements majeurs
Gestion des incidents

- N'est plus dans la norme ISO 27001
- Chapitre 13 → Chapitre 16
- Fusion des deux objectifs en un seul
- Deux points ajoutés
- Ce qui manquait, du fait que c'était dans l'ISO 27001
  - Traitement des incidents conformément aux procédures
- Ce qui manquait, alors que ce n'était pas dans l'ISO 27001
  - Appréciation des événements liés à la sécurité : gravité
  - Classement d'événement en incident, et hiérarchisation

Changements majeurs
Cryptographie

- Mis à part dans un chapitre spécifique (12.3 → 10)
- Modification de l'objectif
  - On ne parle plus d'utiliser des moyens cryptographiques pour protéger l'information
  - On garantit l'utilisation correcte et efficace de la cryptographie
  - Car l'utilisation de cryptographie s'est banalisée
  - Et car son utilisation n'apporte pas de sécurité si ce n'est pas bien fait
- Politique de gestion des clés
  - Avant : politique pour favoriser l'utilisation de techniques cryptographiques
  - Maintenant : politique sur l'utilisation, la protection et la durée de vie des clés
  - Dans la 27002 : ajout de l'objectif « authentification »
  - Mais il faut toujours consulter un spécialiste. Pas de référence à d'autres normes
- Gestion des clés
  - Suppression de l'explication de la différence entre algo symétrique / asymétrique

Changements mineurs

- Gestion des accès : plus présenté par strate. Permet une utilisation plus large
- *« Faites appel à un spécialiste »* (11.1.4 protection contre les menaces externes et environnementales)
- Définition différente du télétravail : inclut toutes les formes de travail effectué en dehors des locaux → moins restrictif pour la France
- Sélection des candidats plus restrictive : les tiers et contractants ne sont plus concernés
- Chapitre spécifique à la gestion des fournisseurs
- Modification de « *gestion du mot de passe* » en « *Gestion des informations secrètes d'authentification* » → permet d'intégrer les PKI
- Modification de « *commerce électronique* » en « *services d'application* »

Mesures supprimées : exemples

- Redondantes, ou fusionnées avec d'autres mesures
  - Ex : bon fonctionnement des applications
  - Ex : contrôle d'accès réseau
- Correspondant à des exigences de l'IS27001:2013
  - Implication de la direction vis-à-vis de la sécurité de l'information
  - Coordination de la sécurité de l'information
- Prises en compte dans l'appréciation des risques
  - Identification des risques provenant des tiers
  - Protection des outils d'audit du système d'information
- Purement supprimées
  - Fuite d'information
  - Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information

Nouvelles mesures de sécurité

Utilisateurs

Maîtrise de la gestion des accès utilisateur

Restrictions liées à l'installation de logiciels

Projets

Sécurité de l'information dans la gestion de projet

Principes d'ingénierie de la sécurité des systèmes

Environnement de développement sécurisé

Phase de test de la sécurité du système

Événements de sécurité

Incidents

Appréciation des événements liés à la sécurité de l'information et prise de décision
Réponse aux incidents liés à la sécurité de l'information

Continuité de la sécurité

Mise en œuvre de la continuité de la sécurité de l'information
Disponibilités des moyens de traitement de l'information

Fournisseurs

Chaîne d'approvisionnement des produits et des services informatiques

→ Renvoie à la clause de l'ISO 27001:2013
« S'assurer que les processus externalisés sont définis et contrôlés »

Ce que ça change

- Moins de guidage pour l'implémentation
  - Se référer à d'autres normes (ou à des spécialistes)
- Changements d'interprétation
  - Secrets d'authentification
  - Télétravail
- Des mesures obscures sont clarifiées
  - Commerce électronique
- Ou supprimées
  - Fuite d'information

- Le plus gros changement : refaire la DdA

Merci

- Questions ?