18 septembre 2013

Comparatif de la nouvelle ISO27002:2013 avec la version 2005

Claire CARRE, manager chez Solucom

solucom
management & IT consulting

ISO 27002:2013 : quels apports et quelles perspectives ?

- Qu’est-ce qui a changé ?
- La norme v2013 permet-elle de traiter les limites de la norme actuelle ?
- Quels impacts sur la gouvernance Sécurité ?

Une 1ère bonne nouvelle ☺

La disparition des mesures qu'on n'a jamais su utiliser !

Sécurité de la documentation système
Il convient de protéger la documentation système contre les accès non autorisés.

Fuite d'informations
Toute possibilité de fuite d'informations doit être empêchée.

Système d'autorisation concernant les moyens de traitement de l'information
Il convient de définir et de mettre en œuvre un système de gestion des autorisations pour chaque nouveau moyen de traitement de l'information

Mesures contre le code mobile
Lorsque l'utilisation de code mobile est autorisée, la configuration doit garantir que le code mobile fonctionne selon une politique de sécurité clairement définie et tout code mobile non autorisé doit être bloqué.

Avant / après

Étude menée sur la version REVISED text for FDIS 27002

27002:2005

- 11 chapitres
- 39 objectifs
- 133 mesures

27002:2013

- 14 chapitres
- 35 objectifs
- 113 mesures

Qu'en est-il de la structure de la norme ?

Au niveau de la structure des chapitres [1/2]

Plus de cohérence sur les sujets traités au sein des chapitres
Une meilleure adéquation entre les chapitres et les acteurs de la DSI

27002:2005	27002:2013
	5. Information security policies
	6. Organization of information security
	7. Human resources security
	8. Asset management
	9. Access control
	10. Cryptography
5. Security policy	11. Physical and environmental security
6. Organization of information security	12. Operations security
7. Asset management	13. Communications security
8. Human resources security	14. System acquisition, development and maintenance
9. Physical and environmental security	15. Supplier relationships
10. Communications and operations management	16. Information security incident management
11. Access control	17. Information security aspects of business continuity management
12. Information systems acquisition, development and maintenance	18. Compliance
13. Information security incident management	
14. Business continuity management	
15. Compliance	

Au niveau de la structure des chapitres [2/2]

Les nouveaux chapitres sont principalement constitués de mesures issues d'autres chapitres

Le chapitre ***Information system acquisition, development and maintenance*** est scindé en 2 pour mieux mettre en évidence la sujet de la cryptographie

- **System acquisition, development and maintenance**
- **Cryptography**

Le chapitre ***Communications and Operations Management*** est coupé en 3 chapitres, clarifiant les périmètres de responsabilités d'acteurs bien distincts

- **Operations security**
- **Communications security**
- **Supplier relationships**

Au niveau des objectifs de sécurité

Les objectifs sont formulés de manière plus synthétique,
ce qui offre une plus grande souplesse dans l'implémentation

27002:2005	27002:2013
Responsibility for assets **Objective**: To achieve and maintain appropriate protection of organizational assets. All assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets..	**Objective**: To identify organizational assets and define appropriate protection responsibilities.
Information systems audit considerations **Objective**: To maximize the effectiveness of and to minimize interference to/from the information systems audit process. There should be controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.	**Objective**: To minimise the impact of audit activities on operational systems.

Au niveau des mesures de sécurité

Globalement, les modifications sont plutôt mineures
mais de nombreuses mesures ont été déplacées

 6 nouvelles mesures

 26 mesures supprimées

 29 mesures modifiées

27002:2005	27002:2013

Learning from information security incidents

- Réduction des contraintes liées à la mesure : les paramètres à analyser lors d'un incident de sécurité ne sont pas spécifiés

There should be mechanisms in place to enable the **types, volumes, and costs of information security incidents** to be quantified and monitored.

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Secure log-on procedures

- Modification du périmètre de la mesure : la sécurisation des accès est cadrée par la politique de contrôle des accès

Access to operating systems should be controlled by a secure log-on procedure.

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

Security requirements analysis and specification

- Simplification de la formulation de la mesure

Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Et sur le fond ?

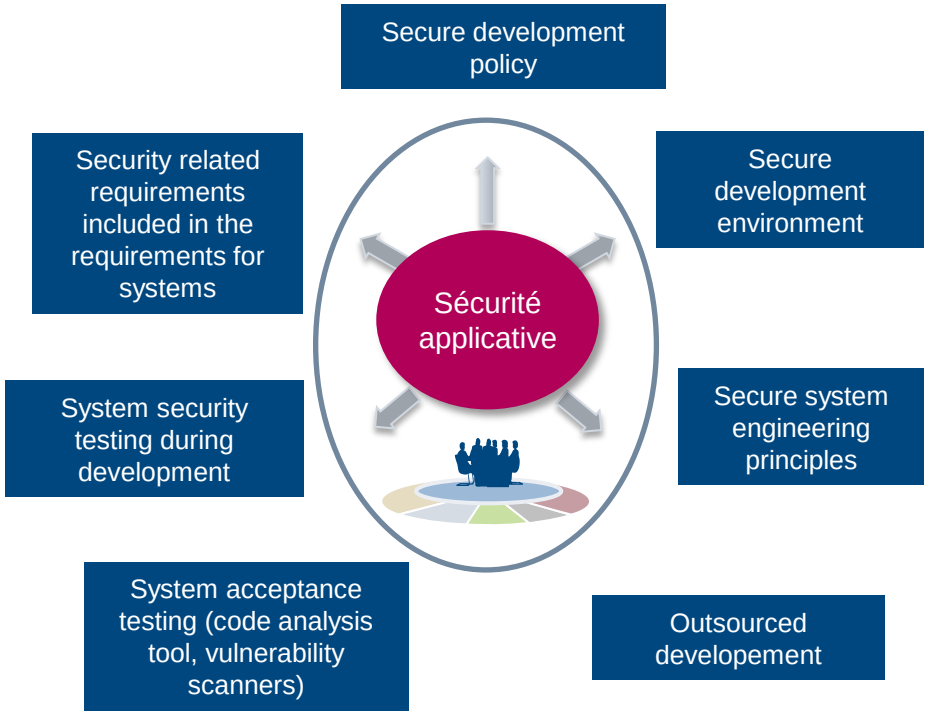
Les big bang [1/3]

System acquisition, development and maintenance

14

- La norme demande de prendre en compte la sécurité dans la gestion de projet, quels que soient les types de projets (chapitre *organization of information security*)
- Les exigences sont plus générales et s'appliquent mieux à toute sorte de projet de développement
  - suppression de l'objectif « *correct processing in applications* » (validation des données en entrée et en sortie, intégrité des messages, etc.)
- Les mesures font un focus sur les applications sensibles: sur les réseaux publics et gérant des transactions
- Les bonnes pratiques de sécurité applicative sont renforcées
- Le sujet de la gestion des données de tests est abordé dans ce chapitre et non plus dans « *operations et communication management* »

Objective: to ensure that information security is designed and implemented within the developement lifecycle of information systems



Et sur le fond ?

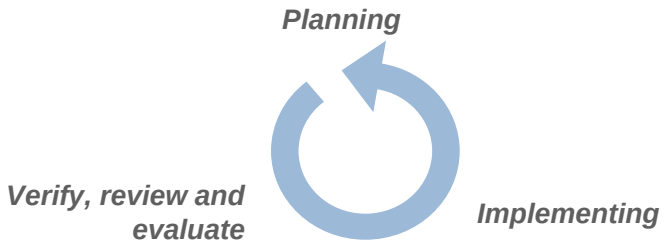
Les big bang [2/3]

Information security aspects of business continuity management

17

- La norme traite maintenant de la continuité de la sécurité de l'information et non de la continuité business !
  - Les mesures sont organisées selon une logique PDCA
- Un objectif de sécurité complémentaire « *redundancies* » concerne la disponibilité des « *information processing facilities* »
  - Une unique mesure demande de mettre en place de la redondance des composants ou des architectures pour répondre aux exigences de disponibilité
- Une note indique que les informations sur le *business continuity management* sont disponibles dans les normes ISO 22301, 27301, 22313

Objective: Information security continuity should be embedded in the organization's business continuity management systems



Et sur le fond ?

Les big bang [3/3]

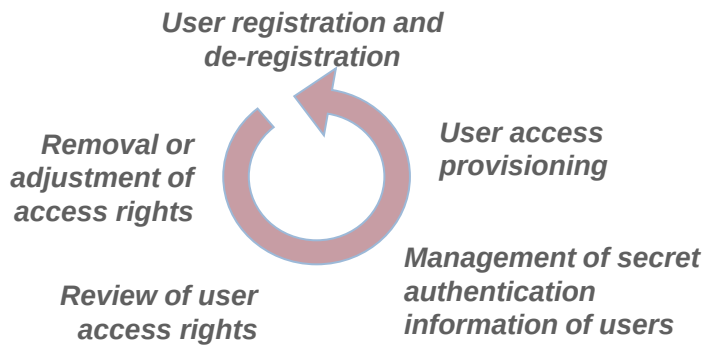
Access control

9

- Le chapitre se concentre sur la gestion des accès des utilisateurs et sur l'accès aux applications et aux systèmes
  - Suppression du contrôle d'accès réseau
  - Suppression du contrôle d'accès à l'OS
  - Suppression du télétravail

  ➔ 25 → 14 mesures
- Le cycle de vie des habilitations est plus complet
- La gestion du mot de passe est élargie à la gestion des « *secret authentication* »
- Un focus spécifique est fait sur l'accès au code source

Objective: to ensure authorized user access and to prevent unauthorized access to systems and services



Et sur le fond ?

Les petites nouveautés [1/2]

Organization of information

6

- Suppression des éléments liés à la sécurité des « *external parties* »
  - Ces points sont partiellement repris dans le chapitre « *supplier relationships* »
- Intégration d'un objectif relatif aux « *mobile devices* » et au télétravail

Asset management

8

- Tous les sujets relatifs à la gestion des biens sont regroupés au sein de ce chapitre, ce qui inclut :
  - « *Return of assets* » issu du chapitre « *human resource security* »
  - « *Media handling* » issu du chapitre « *operations and communication management* »

Information security incident management

16

- Ajout de quelques précisions dans la gestion des incidents
  - Une phase de « *assessment of and decision on information security events* » pour décider si les évènements sont considérés comme des incidents de sécurité
  - Une phase de traitement « *response to information security incidents* »
- La phase d'apprentissage suite à l'analyse des incidents est assouplie : il n'est plus nécessaire d'évaluer le type, le volume et les coûts des incidents

Et sur le fond ?

Les petites nouveautés [2/2]

Operations security

12

- Ce chapitre conserve les mesures propres à l'exploitation
  - *Operational procedures and responsibilities*
  - *Protection from malware*
  - *Back up*
  - *Logging and monitoring*
- Il est complété par quelques mesures issues d'autres chapitres
  - *Control of operational software*
  - *Technical vulnerability management*
  - *Information systems audit considerations*

Communications Security

13

- Ce chapitre concentre tous les mesures liées au réseau
- Il reprend :
  - Celles issues du chapitre « *operation and communication management* » : « *network security management* » et « *exchange of information* »
  - Celles issues du chapitre « *access control* » en ne conservant que la mesure « *segregation of networks* »

Supplier relationships

15

- Ce chapitre concentre toutes les mesures liées à la gestion des fournisseurs, en remplaçant la notion de « *third party* » par « *supplier* »
- Une nouvelle mesure est ajoutée sur le report des exigences de sécurité sur la chaine de sous-traitance
- La mesure sur « *identification of risks related to external parties* » a été supprimée

Et sur le fond ?

Circulez, y a rien à voir ! [1/2]

Information security policies

5

- Au lieu d'une politique de sécurité unique, la norme fait maintenant référence à un ensemble de politiques à plusieurs niveaux
  - Une « *Information security policy* » qui décrit les objectifs et les principes de sécurité
  - Des « *topic-specific policies* »

Human resource security

7

- Les tiers ne font plus partie des cibles de ce chapitre
  - Les « *contractors* » sont toujours adressés
- Les sujets « *return of assets* » et « *removal of access rights* » sont maintenant traités respectivement dans les chapitres « *asset management* » et « *access control* »

Cryptography

10

- Peu de modifications
- Une précision est apportée sur la gestion des clés tout au long du cycle de vie (génération, stockage, archivage, etc.)

Et sur le fond ?

Circulez, y a rien à voir ! [2/2]

Physical and environmental security

11

- Conservation de toutes les mesures, certaines sont légèrement reformulées
- Ajout des 2 mesures sur « *unattended user equipement* » et « *clear desk and clear screen policy* » issues du chapitre « *access control* »

Compliance

18

- Conservation de toutes les mesures, sauf de l'objectif « *information systems audits considerations* », qui est repris dans le chapitre « *operation security* »

ISO 27002:2013 : quels apports et quelles perspectives ?

- Qu’est-ce qui a changé ?
- La norme 2013 permet-elle de traiter les limites de la norme actuelle ?
- Quels impacts sur la gouvernance Sécurité ?

En synthèse

Plus de cohérence des sujets abordés au sein de chaque chapitre

Plus de lisibilité pour les acteurs hors périmètre sécurité

Des objectifs de sécurité plus clairs

Suppression des mesures obsolètes et ajout de quelques nouvelles mesures

Pas de révolution, mais des évolutions qui vont dans le bon sens

MAIS… 

Des points qui ne sont toujours pas traités [1/2]

Certaines mesures sont encore peu auditables

- « *system administrator and system operator activities should be logged and the logs protected and regularly reviewed* »
  ➔ 3 points de contrôle en 1

Certaines mesures restent trop macroscopiques pour constituer des « bonnes » pratiques de sécurité

- « *networks should be managed and controlled to protect information in systems and applications* »
- « *groups of information services, users and information systems should be segregated on networks* »
  ➔ se décline en nombreux sous-points

Certaines mesures « de base » ne sont pas prises en compte

- Durcissement des postes de travail / des terminaux
- Durcissement des socles
- Réseaux sans fil…

Des points qui ne sont toujours pas traités [2/2]

Les nouvelles menaces (cybercriminalité) et les réponses associées ne sont pas développées explicitement

Même si ces sujets peuvent être extrapolés dans certaines mesures, pas de mentions explicites de :

- La surveillance / corrélation des évènements de sécurité (logique SOC)
- La sécurisation de l'administration (seulement la gestion des comptes à privilège et les logs des actions des administrateurs)
- La sécurisation des accès à l'entreprise, notamment depuis Internet
- Les dispositifs de réaction en cas de cyber-attaques (logique CERT)

Les (r)évolutions technologiques ne sont pas non plus explicitement prises en compte

- La virtualisation n'est pas traitée explicitement
  - Même si on peut décliner les mesures existantes dans un contexte virtualisé
    - Ex: mesures sur le cloisonnement, mesures sur la résilience, etc.

  ➔ il manque peut-être une mesure sur la définition des règles de sécurité dans un contexte virtualisé

- Le cloud n'est pas traité explicitement
  - Même si le sujet peut être vu dans le chapitre « *supplier relationships* »

Et par rapport au guide de l'hygiène informatique de l'ANSSI ?

Les deux référentiels apparaissent comme plutôt complémentaires

Plus global : traite les aspects d'organisation et de gouvernance, et de toutes les thématiques sécurité

Ne traite pas de certaines mesures techniques assez précises : sécurisation des équipements terminaux, protection vis-à-vis d'Internet, surveillance…

Plus en lien avec l'implémentation des mesures à un instant T

Ne traite pas des aspects de prise en compte de la sécurité dans les projets (pas de logique d'amélioration liée à la sécurisation des projets)

ISO 27002:2013 : quels apports et quelles perspectives ?

- Qu’est-ce qui a changé ?
- La norme 2013 permet-elle de traiter les limites de la norme actuelle ?
- Quels impacts sur la gouvernance Sécurité ?

Quels impacts sur les projets de certification ISO 27001 ?

Pour les projets de certification en cours, la nouvelle norme va faciliter l'appropriation par les acteurs de la DSI qui sont impliqués dans les projets

Pour les certifications existantes, la migration vers ce nouveau référentiel devrait avoir un impact limité

- Beaucoup de mesures restent identiques ou proches
- La norme ISO 27001:2013 incite à compléter la DDA avec des mesures complémentaires, ce qui permet de conserver les « anciennes » mesures si nécessaire
- Néanmoins, une mise à jour de la DDA sera nécessaire

➔ Le plus gros des efforts devrait porter sur le volet **« prise en compte de la sécurité dans les projets et les développements »** …

… et finalement, ça tombe bien puisque ça reste souvent le **point noir des SMSI** qui sont déjà matures

Une norme qui reste « l'esperanto » de la sécurité

Flexibilité dans la mise en œuvre

- La nouvelle version de la norme ISO 27002 reste donc une liste de mesures de sécurité, ne détaillant pas l'ensemble des caractéristiques de mise en œuvre.
  Comme précédemment et c'est aussi cela qui a fait son succès !

Démarche pérenne

- Sa stabilité dans le temps et son caractère « indépendant des technologies » en font un outil utile dans la durée

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Claire CARRE

Responsable de département

Tel : +33 (0)1 49 03 26 85

Mobile : +33 (0)6 10 99 01 97

Mail : claire.carre@solucom.fr