La déclaration d'applicabilité : comment lui donner du (bon) sens ?

Club 27001 - 20 octobre 2016

Béatrice Joucreau

HSC by Deloitte.

Définition de la déclaration d'applicabilité

- La norme ISO 27001 impose la rédaction d'une déclaration d'applicabilité (DdA)

- La déclaration d'applicabilité contient ISO 27001:2013 6.1.3.d :
  - La liste des mesures de sécurité nécessaires
  - La justification de leur insertion
  - Le fait qu'elles soient mises en œuvre ou non
  - La justification de l'exclusion de mesures de l'annexe A

Intérêt de la DdA

- Intérêt pour une organisation / un implémenteur
  - Vérifier qu'aucune mesure de sécurité importante n'a été oubliée
    - > Notamment les mesures organisationnelles
  - Avoir un inventaire des mesures déjà en place et de celles qui seront mises en place à court terme
    - > Éventuellement moyen et long terme aussi
    - > Peut servir à construire un indicateur de maturité SSI
- Intérêt pour un auditeur
  - Se faire une idée des mesures de sécurité du périmètre
  - Préparer l'audit sur site
    - > Plan d'audit, liste de questions
- Intérêt pour les parties intéressées
  - Avoir une idée du niveau de sécurité en place chez un fournisseur (par exemple)
  - Comparer les fournisseurs

Défauts fréquemment constatés

- De très nombreuses DdA ont le même contenu
  - Toutes les mesures de sécurité de l'annexe A sont sélectionnées ou presque, telles quelles
    - > Alors que pourtant, elles ne sont souvent que partiellement prévues ou mises en place
  - Aucune des mesures de l'annexe A n'est explicitée
    - > Les mesures sont sélectionnées de façon binaire
    - > Sans précision de :
      - comment elles sont ou vont être implémentées
      - quelle partie de la mesure est déjà en place et quelle partie va être mise en place

Défauts fréquemment constatés

- Certaines mesures de l'annexe A, bien que, de manière factuelle, déjà en place ou prévues, ne sont pas sélectionnées, car :
  - Leur mise en œuvre est externalisée
  - Une mesure similaire est sélectionnée

- La justification de (non)sélection est trop succincte
  - « Couvre un risque »
  - « Est une exigence de la norme ISO 27001 »
  - « Le risque couvert est accepté »

Exemple d'extrait perfectible de DdA

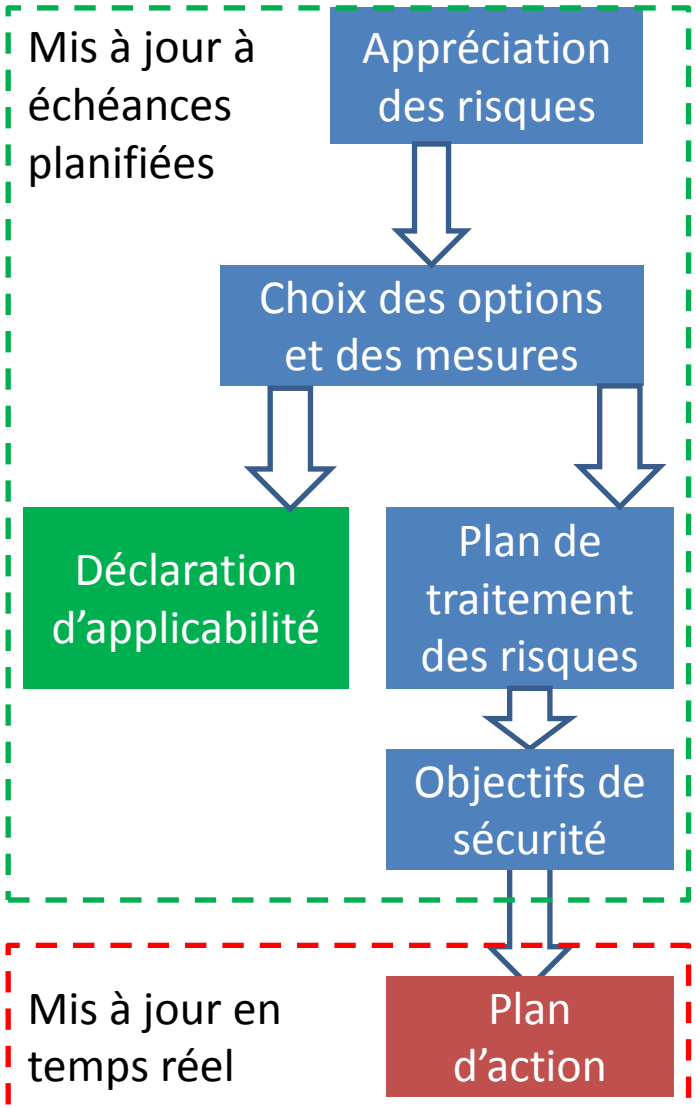
Mesure	Sélection	Implémentée	Justification
A.5.1.1 : politiques de sécurité de l'information	X	X	Déjà en place : exigence normative
A.6.2.2 : télétravail	X		Couvre un risque
A.7.1.1 : sélection des candidats			Déjà couverte par l'exigence 12.7 de PCI DSS v3.2
A .7.1.2 : Termes et conditions d'embauche	X	X	Couvre plusieurs risques
A.12.6.1 : Gestion des vulnérabilités techniques			Mesure externalisée
A.14.3 : Protection des données de test	Non	Non	Risque accepté
PCI DSS v3.2 – 12.7 : Vérification des candidatures	X	X	Exigence

Conséquence

- La DdA perd de son intérêt
  - En tant qu'inventaire ou état des lieux de la sécurité dans sa propre organisation
  - En tant qu'élément différenciant lors d'un audit seconde partie
  - Et en tant qu'élément engageant, facteur de confiance, transmis aux parties intéressées
- Une telle DdA semble conforme, mais son utilité est limitée

D'où provient la DdA ?

- A échéances planifiées
  - Appréciation des risques
    - > En sortie : liste de risques priorisés
  - Choix d'options de traitement puis des mesures de sécurité nécessaires
  - Élaboration d'une DdA et d'un plan de traitement des risques
  - Formulation d'objectifs de sécurité
- En temps réel
  - Conception et mise à jour d'un plan d'action



Détail du processus de construction

- Déterminer les mesures nécessaires ISO 27001:2013 6.1.3.b
  - Certaines mesures sont déjà en place
    - > Parce qu'on n'a pas attendu de mettre en place un SMSI pour faire de la sécurité
    - > A condition qu'elles aient été jugées comme étant toujours nécessaires par l'appréciation et le traitement des risques
  - D'autres répondent à un risque
  - D'autres répondent à une exigence (légale, par exemple)
  - Ces mesures sont rédigées de manière pragmatique et précise
    - > « Mettre en place un pare-feu » ou « un anti-spam »
    - > « Supprimer les accès après un départ »
    - > « Mettre en place un sas unipersonnel »
    - > « Supprimer les vidéos au bout de 3 mois »
  - **On réduit un risque avec une mesure détaillée, pas avec une mesure directement extraite de l'annexe A !**

Détail du processus de construction

- Comparer les mesures nécessaires avec celles de l'annexe A
  ISO 27001:2013 6.1.3.c
  - Pour chaque mesure de l'annexe A, indiquer si elle a été prise en compte ou non
    - La plupart des mesures détaillées sont une instanciation des mesures de l'annexe A
    - « Mettre en place un pare-feu » => A.13.1.3 « Cloisonnement des réseaux »
  - Pour vérifier qu'on n'a pas oublié tout un pan de la sécurité
  - **Une mesure de l'annexe A déjà couverte par une autre mesure (plus détaillée, ou d'un autre référentiel) doit être sélectionnée**
    - Ne pas la sélectionner est foncièrement faux et n'a aucun intérêt !
    - Cela semble alléger la DdA, mais c'est un artifice
    - « Sélectionner » une mesure signifie « la mesure est nécessaire »

Détail du processus de construction

- Justification de leur insertion ISO 27001:2013 6.1.3.d
  - Les mesures « insérées » dans la DdA celles qui sont nécessaires
    - > Sont-elles déjà existantes ?
    - > Réduisent-elles un risque ?
      - – Une mesure déjà en place mais inutile devrait être justifiée aussi
    - > Répondent-elles à une exigence ?
- Justification de l'exclusion de mesures de l'annexe A ISO 27001:2013 6.1.3.d
  - Les mesures exclues sont celles qui n'ont pas été considérées comme nécessaires
    - > Elles ne correspondent à aucune mesure pragmatique existante ou bien dans le plan de traitement des risques

Ex. 1 : Mesure existante vs mesure de l'annexe A

- L'appréciation des risques a mis en évidence :
  - L'existence de la mesure M8 : « *Tous les serveurs et postes Windows sont mis à jour au plus tard une semaine après la parution des correctifs* »
  - Les risques portant sur les systèmes UNIX sont acceptables
- Dans la DdA, faut-il sélectionner la mesure A.12.6.1 ?
  - Mesure A.12.6.1 : « *Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé* »
- Comment justifier sa (non)sélection ?

Ex. 1 : Mesure existante vs mesure de l'annexe A

- Mauvaises façon de faire
  - A.12.6.1 sélectionnée, et déjà en place grâce à M8
  - Ou bien A.12.6.1 non sélectionnée car couverte par M8
    - > Est faux puisque la correspondance n'est que partielle
      - – Seuls les systèmes Windows sont mis à jour
    - > Ne permet pas de se rendre compte qu'on oublie les systèmes UNIX

- Bonne façon de faire

Mesure	Nécessaire	Existante	Justification / Détail de l'implémentation
M8 : […]	Oui	Oui	Déjà en place Couvre le risque R42
A.12.6.1 : […]	Partiellement	Oui	Partiellement en place par le biais de M8, qui couvre le risque R42 sur les systèmes Windows . Les risques couvrant les systèmes UNIX sont acceptés.

Ex. 2 : Externalisation d'une mesure

- L'appréciation a mis en évidence :
  - Un risque relatif aux vulnérabilités systèmes, non acceptable
- Le plan de traitement des risques précise :
  - Ce risque sera partagé
  - L'application des correctifs de sécurité sera sous-traitée à un infogérant : tous les serveurs Windows externalisés seront mis à jour au plus tard une semaine après la parution des correctifs
- Dans la DdA, faut-il sélectionner la mesure A.12.6.1 ?
- Comment justifier sa (non)sélection ?

Ex. 2 : Externalisation d'une mesure

- Mauvaise façon de faire
  - Ne pas sélectionner la mesure A.12.6.1 car elle serait sous-traitée
    - > Si une mesure est sous-traitée, elle doit faire l'objet de clauses de sécurité dans les contrats. Comment identifier ces clauses si la mesure correspondante est exclue ?
    - > La vraisemblance du risque ne peut pas diminuer car l'infogérant ne procèdera pas à l'application des correctifs
    - > Les conséquences du risque ne sont pas partagées puisque l'implémenteur ne pourra pas se retourner contre l'infogérant
- Bonne façon de faire

Mesure	Nécessaire	Existante	Justification / Détail de l'implémentation
A.12.6.1 : […]	Oui	Non	Couvre le risque R42. Tous les serveurs Windows seront mis à jour par l'infogérant au plus tard une semaine après la parution des correctifs
A.15.1.1 à A.15.1.2 : […]	Oui	Non	Permet de partager le risque R42. Externalisation de la mesure A.12.6.1

Et les exigences des parties intéressées ?

- Est-il possible de ne pas sélectionner dans la DdA les mesures correspondant à leurs exigences ?
  - Les exigences des parties intéressées doivent être inventoriées ISO 27001:2013 4.2.b
  - Les objectifs de sécurité doivent prendre en compte les exigences applicables ISO 27001:2013 6.2.c
    - > Mais peuvent être nuancés en fonction des éléments de contexte interne et externe
  - Ils sont implicitement inclus dans les mesures ISO 27001:2013 6.2.c
  - **Donc les exigences des parties intéressées prises en compte doivent être sélectionnées dans la DdA**
    - > Si une exigence de partie intéressée est exclue, la justification provient du contexte

Les caractéristiques d'une DdA sensée

- Correcte
  - Sans contradictions
- Complète
  - Sans exclusion artificielle de mesures
- Exacte et précise
  - En différenciant les mesures partiellement et totalement implémentées
  - En s'autorisant la sélection partielle d'une mesure pour réduire un risque
  - En précisant explicitement quels risques ou exigences sont couverts par les mesures sélectionnées

Exemple simplifié de DdA sensée

Mesure	Nécessaire	Existante	Justification / Détail de l'implémentation
A.5.1.1 : politiques de sécurité de l'information	Oui	Oui	Déjà en place : politique de classification (A.8.2.1), politique cryptographique (A.10.1.1).
A.8.2.1 : Classification des informations	Oui	Partiellement	Couvre le risque R12. Partiellement en place car ne prend pas encore en compte les exigences légales.
A.7.1.1 : sélection des candidats	Partiellement	Partiellement	Nécessaire uniquement sur le périmètre PCI DSS. L'exigence 12.7 de PCI DSS v3.2 couvrira ce risque, et n'est en place que pour une partie du personnel.
A .7.1.2 Termes et conditions d'embauche	Oui	Oui	Couvre le risque R09.
A.12.6.1 : Gestion des vulnérabilités techniques	Partiellement	Non	Couvre le risque R42 induit par l'absence de veille sur les systèmes Windows. Cette mesure sera externalisée. Les risques couvrant les systèmes UNIX sont acceptés.
A.15.1.2	Oui	Non	Couvre le risque R42 avec la mesure A.12.6.1, car celle-ci sera externalisée.
PCI DSS v3.2 – 12.7 : Vérification des candidatures	Oui	Partiellement	Exigence des clients. La vérification n'est effectuée que sur les développeurs pour le moment.

Questions

- ?