GROUPE PIN

Réunion du 21 janvier 2010

Certification des systèmes d'archivage numérique

Jean-Louis Pascon
Vice-Président de FEDISA

Les constats

- Des besoins en matière de validation de fonctionnement des services d'archivage pour les entreprises (Banques, Assurances, Opérateurs de télécommunication, etc.)
- Pouvoir certifier au sens de Loi
- Ne pas remettre en question les investissements déjà réalisés - notamment en matière de sécurité
- Être reconnu en France et hors de France
- Avoir une procédure disponible rapidement
- Reposer sur une méthodologie adaptée et rigoureuse

Certification/Label

- Certification : La certification est une procédure par laquelle une tierce partie, l'organisme certificateur, donne une assurance écrite qu'un système d'organisation, un processus, une personne, un produit ou un service est conforme à des exigences spécifiées dans une norme ou un référentiel.
- Label : On peut rencontrer des démarches de type « label » (hors du domaine agricole ou alimentaire) ou «contrôlé par un organisme indépendant». Elles ne constituent pas des certifications. Ces pratiques ne sont pas encadrées par des dispositions réglementaires mais sont licites tant qu'elles n'induisent pas de confusion avec une véritable certification dans l'esprit du public.

Référentiel

- Un référentiel est un document technique définissant les caractéristiques que doit présenter un produit industriel ou un service et les modalités du contrôle de la conformité à ces caractéristiques
- Un référentiel est élaboré et validé en concertation avec des représentants des diverses parties intéressées : professionnels, consommateurs ou utilisateurs, administrations concernées, etc.

Organismes certificateurs

- **Déclaration d'activité :** Déclaration auprès du Ministère chargé de l'Industrie de leur activité. Elle fait l'objet d'une publication au Journal Officiel
- **Impartialité et Compétence :** Appréciées au regard des normes en vigueur (Norme NF EN 45011)
- **Validation concertée des référentiels :** L'organisme certificateur élabore et valide chaque référentiel en concertation avec les représentants des diverses parties intéressées
- **Transparence :** Les caractéristiques essentielles contrôlées des référentiels sont publiées sous la forme d'un avis au JO

Organismes certificateurs

- Les organismes certificateurs peuvent demander à être accrédités par le Comité français d'accréditation (COFRAC). Il s'agit d'une démarche volontaire dont le but est de donner confiance au marché en attestant que l'organisme certificateur est compétent, impartial et indépendant au regard des normes européennes ou internationales pertinentes (par exemple, la norme NF EN 45011 pour les organismes certificateurs de produits industriels et de services).
- Le Comité français d'accréditation (COFRAC), créé en 1994, est une association loi 1901 à but non lucratif dont les membres représentent l'ensemble des partenaires concernés : pouvoirs publics, professionnels, laboratoires et organismes accrédités, groupements de consommateurs et utilisateurs, acheteurs publics.

Référentiels Archives

- Il existe des référentiels :
  - **OAIS :** Conceptuel, utile, mais pas d'éléments directement exploitables pour un audit
  - **MOREQ 2 :** Complet mais complexe et ne concerne que le logiciel
  - **FNTC :** Spécialisé tiers archiveurs – axé principalement sur un format assurant l'interopérabilité entre les opérateurs d'archivage
  - **AFNOR NF Z 42-013 :** Orienté conception et exploitation mais incomplet (sécurité, gestion des personnels, développement des systèmes, etc.)

Méthodes d'audit

- **TRAC : Trustworthy Repositories Audit and Certification**
- **Nestor : Network of Expertise in Long-term STOrage of Digital Resources**
- **CobiT :** Control Objectives for Information and Related Technology
- **ISO 27001 : Information security management systems**

Utiliser l'ISO 27001

- Souple grâce au SOA (Statement Of Applicability)
- Famille complète de normes (ISO 27002, ISO 27005, ISO 2701X, etc.)
- Certification reconnue mondialement (6037 sociétés certifiées dans le monde en décembre 2009)

Utiliser l'ISO 27001

- Organismes de certification déjà existants (exemple LSTI en France)
- Grande expérience des auditeurs
- Utilisation de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) pour la conception du SOA recommandée par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information)

Complet - Souple

- Pas de conflits avec les autres méthodes car pas les mêmes cibles
- Intégration possible de modèles et de normes différentes (42-013, MOREQ2, OAIS, etc.) synthétisés dans le SOA
- Convient à des structures différentes (tiers archiveurs ou structure interne à une entreprise)
- Introduction d'une métrique d'évaluation

Le travail de FedISA

- Création d'un groupe de travail regroupant experts en sécurité informatique et archivage, grands utilisateurs, opérateurs d'archivage, records managers...
- Simulation d'un audit ISO 27001 adapté à l'archivage :
  - Imaginer un archiveur type
  - Analyse EBIOS de ses risques
  - Conception du SOA de cet archiveur

Le résultat

- Un business plan réduit d'un tiers archiveur
- La définition des biens et services à protéger
- L'analyse DICT (Disponibilité, Intégrité, Confidentialité et Traçabilité)
- Des scénarios type d'attaques
- Un SOA pour ce tiers archiveur
- Un document d'aide à l'utilisation de la norme ISO 27002 dans le contexte de l'archivage numérique

Des Questions ?