

GR – La norme ISO-27005

UNIV-PAU / LP
Norme ISO-27005

Un consensus international

- Différents experts de différents pays au monde se sont réunis pour construire une norme sur la gestion des risques SSI : 27005
 - ISO 13335 (ancienne norme 1992)
 - EBIOS V2 (FRANCE / DCSSI / 2004)
 - AS 4360 (AUSTRALIE et NOUVELLE ZELANDE)
 - BS7799-3 (GRANDE BRETAGNE / BSI : British Standards Institute)

Norme versus Méthode

- Attention la norme ISO-27005 ne remplace pas les méthodes. Elle va permettre une uniformisation du vocabulaire et des définitions.
- Chaque méthode devra évoluer afin de devenir « compatible ISO-27005 »
- Les méthodes sont plus complètes.
 - Elles apportent des outils, des bases de connaissances beaucoup approfondis que la norme 27005.

Processus de gestion du risque

- Approche **systematique**
- Doit permettre de produire des résultats
 - **Comparables** et
 - **Reproductibles**

Composition de la norme

- 55 pages avec les annexes
- 12 chapitres
 - Les chapitres importants : de 6 à 12 : p 4 à 24
- 6 annexes (A à F) : 25 pages
 - Utiles pour la mise en œuvre de la norme
- Vient d'être traduite en Français

Les chapitres

- Chapitre 6 : Processus de gestion du risque dans sa globalité
- Chapitre 7 : Établissement du contexte
 - Périmètre de l'appréciation des risques
 - Définition des critères de base
 - Description de l'environnement
 - Organisation des processus
- Chapitre 8 : Appréciation du risque
- Chapitre 9 : Traitement du risque
- Chapitre 10 : Acceptation du risque
- Chapitre 11 : Communication du risque
- Chapitre 12 : Revue et supervision du risque

Les annexes

- **Annexe A** : Aide à la définition du périmètre du processus de gestion des risques
- **Annexe B** : Aide pour identifier et valoriser les actifs.
- **Annexe C** : Liste de menaces classées par type (Ils ont repris la liste des méthodes d'attaque d'EBIOS V2)
- **Annexe D** : Exemple de vulnérabilités et des menaces qui peuvent les exploiter (extrait des listes EBIOS)
- **Annexe E** : Exemple de méthode de calcul de risque assez simple.
- **Annexe F** : Contraintes pesant sur la réduction du risque

Certification individuelle

- Possibilité d'obtenir une certification individuelle pour la norme ISO-27005
 - Organisme de certification : LSTI
 - Plusieurs entreprises proposent la formation correspondante (2 jours et demi de formation + trois heures pour passer l'examen)