
Club 27001-Toulouse

Synthèse des réunions du Club 27001 Parisien

Réunion du 1er Juin 2007

Réunions du Club 27001 Parisien

Synthèse globale

- **Quatre réunions se sont tenues à Paris**
 - ✓ 26 Octobre 2006
 - ✓ 14 décembre 2006
 - ✓ 15 février 2007
 - ✓ 19 avril 2007

- **Les participants**
 - ✓ Des représentants de grandes entreprises
 - ✓ Des représentants d'organismes publics
 - ✓ Des consultants provenant du monde SSI et du monde normatif
 - ✓ Des représentants de sociétés de service

Réunions du Club 27001 Parisien

Réunion du 26 Octobre 2006 (23 présents)

□ Présentation

- ✓ Présentation détaillée de la norme et du processus de certification (Alexandre Fernandez et Hervé Schauer)
(cf site ISO 27001)

□ Points remarquables de la réunion

- ✓ Ne pas confondre audit de certification et accompagnement vers la certification
- ✓ Panorama des normes 27000
 - Certaines sont obligatoires pour une certification : 27001 et 27006
 - Autres sont des guides
- ✓ Présentation des principales limites

Réunions du Club 27001 Parisien

Réunion du 26 Octobre 2006

□ Questions

- ✓ L'impact financier des risques peut-il être évalué ?
- ✓ Comment ce fait-il que l'on puisse publier la 27001 avant la 27005 ?
- ✓ Quelle est la valeur de la 27001 ?

Réunions du Club 27001 Parisien

Réunion du 26 Octobre 2006

- Décisions actées par les participants, à l'unanimité :
 - ✓ Le groupe doit rester ouvert - tout le monde doit pouvoir y venir.
 - ✓ Pas de cotisation obligatoire.
 - ✓ Fréquence des réunions : 2 mois.
 - ✓ Il n'est pas souhaité le rapprochement ou la constitution d'une association à ce stade.
 - ✓ L'anglais n'est pas interdit pour animer des présentations.
 - ✓ Signature d'un NDA pour chaque personne participant aux réunions afin d'éviter la divulgation d'informations confidentielles éventuellement communiquées par les participants. Chaque personne pouvant demander si elle le souhaite que telle ou telle information ne figure pas au compte-rendu.
 - ✓ Le compte-rendu sera publié sur le site et diffusé aux membres de la liste.
 - ✓ La publication des présentations est laissée à l'appréciation de chaque orateur.

Réunions du Club 27001 Parisien

Réunion du 14 décembre 2006 (19 présents)

□ Présentation

- ✓ la certification ISO 27001 chez British Telecom par Richard JONES (cf site ISO 27001)
- ✓ 15 certif (UK), 10 ailleurs, 1 en cours en France

□ Points remarquables de la démarche BT

- ✓ Objectifs
 - Offrir une alternative à l'audit SAS 70
 - Prouver le bon niveau de maîtrise de la sécurité
- ✓ Définir le périmètre des certifications
 - Activités de 5 pers à activités de 200 personnes

Réunions du Club 27001 Parisien

Réunion du 14 décembre 2006 (19 présents)

□ Points remarquables de la démarche BT (suite)

- ✓ Les difficultés majeures
 - Définir le périmètre
 - Identifier les actifs
 - Définir et organiser la collecte des preuves
 - Mesurer l'efficacité du SMSI
 - Implémenter les mesures de sécurité concernant les personnes
- ✓ La charge de mise en œuvre
 - 0,5 à 1 pers /projet (de 6 mois à 2 ans)
 - Outillage interne

Réunions du Club 27001 Parisien

Réunion du 14 décembre 2006

- Questions principales à BT
 - ✓ Combien d'organismes certificateurs ? (3)
 - ✓ Comment gérer autant de certificats ?
 - ✓ Comment sont gérés les prestations ou fournitures faites par des entités BT non certifiées et qui entrent dans le périmètre de la certification ?

- Intérêt de la certification ISO 27001 : tour de table
 - ✓ Conseil en SSI : pas de demande de la part des clients
 - ✓ Domaine bancaire: certification pas envisagée à court terme
 - ✓ Industriels : écueil → organisations internes
 - ✓ Organismes publics : aucun intérêt pour la certification mais intérêt pour la démarche SMSI

Réunions du Club 27001 Parisien

Réunion du 15 février 2007 : 1ère présentation

□ Présentation

- ✓ Orange : l'expérience d'une mise en conformité à SARBANES-OXLEY (Claude Serre)
- ✓ Quels référentiels utiliser ?
 - Pour le système de management de la qualité : ISO 9001 et 14000,
 - Pour la sécurité l'ISO 27002 et ISO 27001 .

□ Conclusion du présentateur:

- ✓ quand un CAC intervient dans une entreprise certifiée ISO 27001, son niveau de confiance est plus élevé ;
- ✓ il faut garder une couverture de sécurité suffisante tout en réduisant le nombre de mesures de sécurité ;
- ✓ l'overdose de mesures nuit au bon fonctionnement de l'entreprise .

Réunions du Club Iso27001 Parisien

Réunion du 15 février 2007 : 2ème présentation

□ Présentation

- ✓ NTT Europe On-line (NTTEO) (Neil WHEELWRIGHT et Robert STEGGLES)
- ✓ Certification globale ISO 27001 de l'ensemble de ses entités et activités européennes couvrant : le Royaume-Uni, la France, l'Allemagne, l'Espagne et les Pays-Bas.
- ✓ Objectif : répondre à la demande de clients

□ Points remarquables

- ✓ L'engagement de la direction générale
- ✓ Le périmètre
- ✓ Les objectifs : choisis et mesurables
- ✓ Les livrables : Déclaration d'applicabilité, plan de traitement du risque, registre des risques.
- ✓ La publicité : interne et externe

Réunions du Club 27001 Parisien

Réunion du 19 avril 2007

□ Présentation

- ✓ Opportunités de mutualisation entre ISO 27001 et ITIL (Alexandre Fernandez)

□ Points remarquables

- ✓ Périmètre SMSI plus vaste
- ✓ Attention au vocabulaire et aux similitudes
- ✓ Interprétations différentes

ITIL	ISO 27001
Orienté business	Orienté confiance
Système informatique	Système d'information
Pas de certification	Certification possible
Bonnes pratiques	Exigences obligatoires

- ✓ Volonté des entreprises : mutualiser l'approche d'analyse de risques (projets, opérationnel, système d'information)

Réunions du Club 27001 Parisien

Sujets identifiés

- ❑ Expériences d'implémentation de SMSI
- ❑ Comment faire un levier de l'ISO27001 ? Qu'est-ce que la norme peut apporter ? comment éviter d'aller dans le mur ?
- ❑ Réflexion autour de l'IT Management : la cross certification ? le positionnement de la ISO 27001 par rapport aux autres référentiels 20000, sorbanes Oxley ,contrôle interne,...
- ❑ Mariage de l'analyse de risque avec l'ISO 27001
- ❑ Développer un cas pratique, servant d'exemple type pour expliquer et sensibiliser
- ❑ Les métriques d'un SMSI
- ❑ La gestion documentaire du SMSI
- ❑ Retours d'expérience sur des points plus particuliers (Risk Assesment, tableaux de bord, ...)
- ❑ Les approches et solutions de gestion des enregistrements du SMSI (audit, preuve, ...)
- ❑ Les impacts de la certification sur le processus de formation des utilisateurs

VII. Questions

