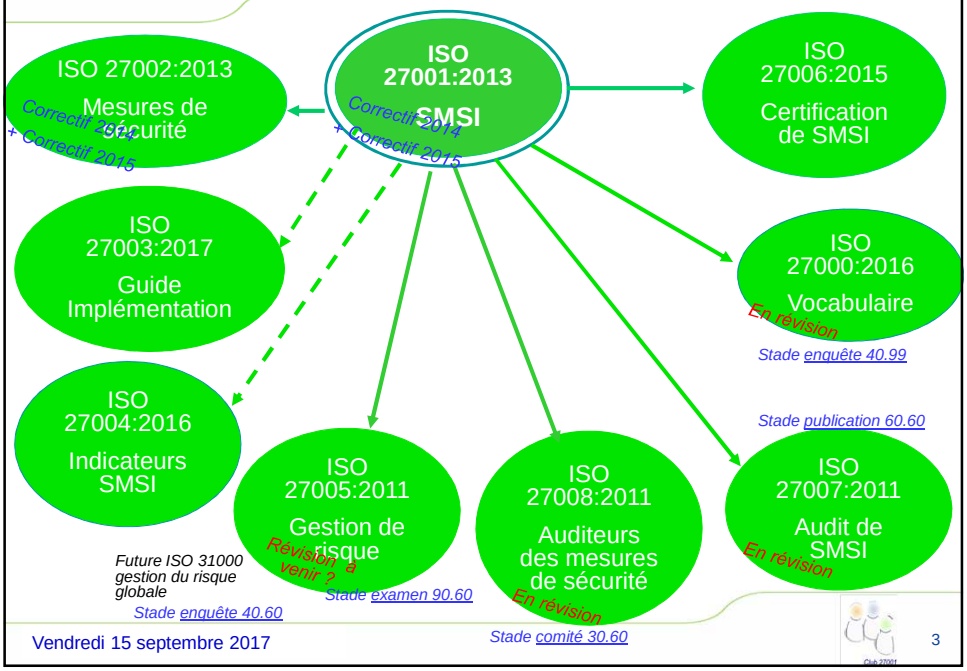
Club 27001 toulousain
15 septembre 2017

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Stratégie nationale cybersécurité et activités de l'ANSSI (Yves Jussot, ANSSI, référent région Occitanie)**
- **Sécurité des objets connectés du point de vue de l'attaquant (Arnaud Courty, ON-X)**
- **Discussion autour du chapitre A.8.3 de l'ISO 27002 (Animée par Jacques Sudres, C-S)**
- **Points divers**

ISO 2700x : une famille de normes



ISO 2700x : une famille de normes

- **ISO 27013:2015 : Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1**
- **ISO 27032:2012 : Lignes directrices pour la cybersécurité**
- **ISO 27035:2016 : Gestion des incidents de sécurité de l'information**
  - Partie 1: Principes de la gestion des incidents
  - Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents
- **ISO 27014:2013 : Gouvernance de la sécurité de l'information**
- **ISO 27017:2015 Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27001 pour les services de nuage**
- **ISO 27018:2014 : Code pratique pour la protection PII dans les nuages publics agissant comme des processeurs PII**
  - PII : Personally Identifiable Information
- **ISO 27009:2016 sur les applications sectorielles de la 27001**
  - En révision : stade proposition 10.99

Ordre du jour

- Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)
- **Stratégie nationale cybersécurité et activités de l'ANSSI (Yves Jussot, ANSSI, référent région Occitanie)**
- Sécurité des objets connectés du point de vue de l'attaquant (Arnaud Courty, ON-X)
- Discussion autour du chapitre A.8.3 de l'ISO 27002 (Animée par Jacques Sudres, C-S)
- Points divers

Ordre du jour

- Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)
- Stratégie nationale cybersécurité et activités de l'ANSSI (Yves Jussot, ANSSI, référent région Occitanie)
- **Sécurité des objets connectés du point de vue de l'attaquant (Arnaud Courty, ON-X)**
- Discussion autour du chapitre A.8.3 de l'ISO 27002 (Animée par Jacques Sudres, C-S)
- Points divers

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Stratégie nationale cybersécurité et activités de l'ANSSI (Yves Jussot, ANSSI, référent région Occitanie)**
- **Sécurité des objets connectés du point de vue de l'attaquant (Arnaud Courty, ON-X)**
- **Discussion autour du chapitre A.8.3 de l'ISO 27002 (Animée par Jacques Sudres, C-S)**
- **Points divers**

Objectifs et mesures de l'Iso 27001:2013

- A.5 : Politiques de sécurité
- A.6 : Organisation
- A.7 : RH
- **A.8 : Gestion des actifs**
  - A.8.3 Manipulation des supports
    - A.8.3.1 Gestion des supports amovibles
    - A.8.3.2 Mise au rebut des supports
    - A.8.3.3 Transfert physique des supports
- A.9 : Contrôle d'accès
- A.10 : Cryptographie
- A.11 : Sécurité physique et environnementale
- A.12 : Sécurité en exploitation
- A.13 : Sécurité des communications
- A.14 : Acquisition, développement et maintenance des SI
- A.15 : Relations fournisseurs
- A.16 : Gestion d'incidents
- A.17 : Continuité d'activité
- A.18 : Conformité

A.8.3.1 Gestion des supports amovibles

- **Mesure : Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l'organisme**
  - Préconisation de mise en œuvre : Il convient de rendre impossible toute récupération du contenu. Il convient si nécessaire et réalisable d'exiger une autorisation pour le retrait des supports…… Il convient de n'activer le support que si nécessaire… Il convient de transférer les données sur un support neuf avant qu'elles ne deviennent illisibles…
- **Gérez vous vos supports amovibles de façon conforme**
  - Bien sûr : Pas de plan de classification, comme ça je ne suis pas embêté.
  - C'est quoi un support amovible ?
  - Il y a une politique, mais personne ne la suit
  - Oui, nous avons des outils de traçabilité de tous les supports amovibles, avec mise en cache de ce qui est exporté, des listes blanches de supports etc…

A.8.2.2 Mise au rebut des supports

- **Mesure : Il convient de procéder à une mise au rebut sécurisée des supports qui ne servent plus, en suivant des procédures formelles**
  - Préconisation de mise en œuvre : Il convient que les procédures formelles de mise au rebut sécurisée réduisent au minimum le risque des fuites d'information confidentielle vers des personnes non autorisées. Ces procédures doivent être proportionnelles à la sensibilité de l'information…
- **Comment mettez vous au rebut vos supports?**
  - J'efface ma clef USB quand elle est pleine.
  - Tout est stocké sur le réseau, dans la messagerie ou dans le « cloud », on ne met rien sur des supports amovibles
  - Toutes nos clefs et disques durs sont étiquetés en fonction de la sensibilité et sont broyés dès que plus utilisés
  - …

A.8.3.3 Transfert physique des supports

- **Mesure : Il convient de protéger les supports contenant de l'information contre les accès non autorisés, l'utilisation frauduleuse ou l'altération lors du transport**
- Préconisation de mise en œuvre : Il convient de que le transporteur soit fiable. Il convient d'établir la liste des coursiers autorisés. Il convient que l'emballage choisi soit suffisant… Il convient de conserver les journaux identifiant le support…ainsi que les dates et heures…
- **Avez-vous des procédures de transfert?**
  - Oui, c'est le secrétariat qui s'en occupe, mais je ne sais pas comment
  - On envoie tout par la Poste, dans des enveloppes fermées
  - Pas besoin, on envoie tout par Internet.
  - Tous nos envois se font sous double enveloppe plastifiée, en valeur déclarée, avec du « scotch bleu » partout, on fait signer des ABB' et on tient à jour des inventaires même pour le courrier standard, les convoyeurs sont habilités, même l'ANSSI prend exemple sur nous.
  - …

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Stratégie nationale cybersécurité et activités de l'ANSSI (Yves Jussot, ANSSI, référent région Occitanie)**
- **Sécurité des objets connectés du point de vue de l'attaquant (Arnaud Courty, ON-X)**
- **Discussion autour du chapitre A.8.3 de l'ISO 27002 (Animée par Jacques Sudres, C-S)**
- **Points divers**

Prochaine conférence annuelle du Club 27001 : 28/03/2017
Appel à communication

- **Contenu des soumissions à envoyer à conference@club-27001.fr :**
  - Nom de l'auteur, biographie et affiliation
  - Synopsis d'une page maximum de l'intervention avec un plan de celle-ci
  - Format libre

- **Calendrier**
  - 15 janvier 2018 : date limite de réception des soumissions
  - 18 janvier 2018 : réunion du comité de programme
  - 25 janvier 2018 : notification aux auteurs et publication du pré-programme
  - 15 février 2018 : publication du programme définitif
  - 21 mars 2018 : réception des présentations
  - 28 mars 2018 : conférence

Prochaine conférence annuelle du Club 27001 : 28/03/2017
Appel à communication

- **La conférence annuelle du Club 27001 privilégie les retours d'expérience dans l'utilisation des normes de la série ISO 27000, qu'il s'agisse de la mise en œuvre d'une des normes, leur usage y compris sans certification, les difficultés rencontrées et les intérêts perçus.**

- **Les propositions doivent faire part d'un retour d'expérience pratique, et ne doivent pas être la présentation d'une offre de service, d'un produit ou plus généralement d'une solution commerciale.**

- **35 à 45 minutes en français ou en anglais.**

Prochaines réunions

- **Vendredi 15 décembre ?**
  - Lieu : ?
  - Sujets : ?
    - SMI intégrés 27001 (Stéphane Jourdain (Kéops), Pierre Darphin (Cegedim), Charlotte Renun, Scassi)
    - PSSI-E, 901 (SI sensibles), PSSI MCAS : intégration dans les PSSI => réunion complète ? ON-X, CS, G. Trouessin, Apsys, MSA, etc.
    - Homologations : défense, RGS, etc. (accréditation / certification / agrément ?) ON-X, CS, G. Trouessin, Apsys, MSA, etc.
    - Séance analyse de risques complète
    - Retour d'expérience 27001 (Stéphane Jourdain, Kéops)
    - PSSI
    - Positionnement de 27001 vis-à-vis d'autres référentiels tels que RGS, PCI-DSS, ISAE3402, HDS…
    - Adéquation ou pas des standards actuels de la sécurité (27001 en particulier), alors qu'ils sont loin d'être matures en termes d'implémentation, face aux évolutions des modèles informatiques (Méthodes Agile, DevOps, Cloud Computing, BYOD, ...)