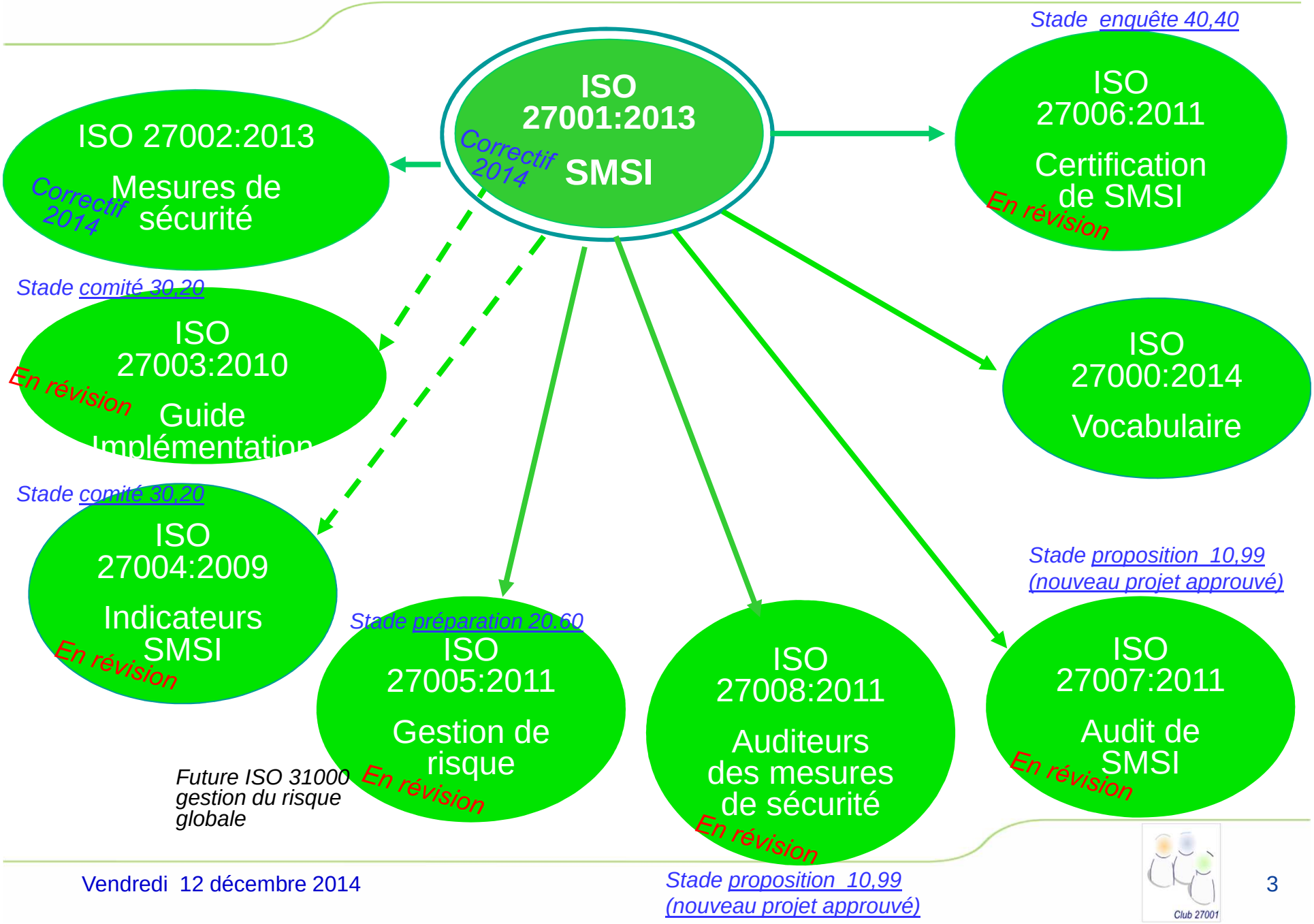
Club 27001 toulousain

12 décembre 2014

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Présentation de PCI-DSS et de son positionnement par rapport à la 270xx (Hervé Hosy, Oppida)**
- **Retour sur les normes "privacy" et lien avec la 270XX (Lionel Vodzislawsky, Celtipharm)**
- **Débat sur l'annexe A.6.1 Organisation de la SSI (animé par Jacques Sudres, C-S)**
- **Points divers :**
  - Information globale sur les renouvellements chez les différents certificateurs (Sébastien Rabaud, Scassi)
  - Conférence annuelle du Club 27001.
  - Fonctionnement du club.

ISO 2700x : une famille de normes



ISO 2700x : une famille de normes

- **ISO 27013:2012 : Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1**
  - En révision stade enquête 4040
- **ISO 27032:2012 : Lignes directrices pour la cybersécurité**
- **ISO 27035:2011 : Gestion des incidents de sécurité de l'information**
  - Révision en trois sous-parties, Stade comité 30.60
- **ISO 27014:2013 : Gouvernance de la sécurité de l'information**
- **ISO 27017 sur la sécurité du Cloud**
  - Stade enquête 40.40
- **ISO 27018:2014 : Code pratique pour la protection PII dans les nuages publics agissant comme des processeurs PII**
  - PII : Personally Identifiable Information
- **ISO 27009 sur les applications sectorielles de la 27001**
  - Stade comité 30.60

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Présentation de PCI-DSS et de son positionnement par rapport à la 270xx (Hervé Hosy, Oppida)**
- **Retour sur les normes "privacy" et lien avec la 270XX (Lionel Vodzislawsky, Celtipharm)**
- **Débat sur l'annexe A.6.1 Organisation de la SSI (animé par Jacques Sudres, C-S)**
- **Points divers :**
  - Information globale sur les renouvellements chez les différents certificateurs (Sébastien Rabaud, Scassi)
  - Conférence annuelle du Club 27001.
  - Fonctionnement du club.

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Présentation de PCI-DSS et de son positionnement par rapport à la 270xx (Hervé Hosy, Oppida)**
- **Retour sur les normes "privacy" et lien avec la 270XX (Lionel Vodzislawsky, Celtipharm)**
- **Débat sur l'annexe A.6.1 Organisation de la SSI (animé par Jacques Sudres, C-S)**
- **Points divers :**
  - Information globale sur les renouvellements chez les différents certificateurs (Sébastien Rabaud, Scassi)
  - Conférence annuelle du Club 27001.
  - Fonctionnement du club.

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Présentation de PCI-DSS et de son positionnement par rapport à la 270xx (Hervé Hosy, Oppida)**
- **Retour sur les normes "privacy" et lien avec la 270XX (Lionel Vodzislawsky, Celtipharm)**
- **Débat sur l'annexe A.6.1 Organisation de la SSI (animé par Jacques Sudres, C-S)**
- **Points divers :**
  - Information globale sur les renouvellements chez les différents certificateurs (Sébastien Rabaud, Scassi)
  - Conférence annuelle du Club 27001.
  - Fonctionnement du club.

Objectifs et mesures de l'Iso 27001:2013

- A.5 : Politiques de sécurité
- A.6 : Organisation
  - A.6.1 Organisation Interne
    - A.6.1.1 Fonctions et responsabilités
    - A.6.1.5 SSI dans la gestion de projet
- A.7 : RH
- A.8 : Gestion des actifs
- 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.6.1.1 Fonctions et responsabilités liées à la Sécurité de l'Information

- **Mesure : Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information**
  - Préconisation b) : Il convient d'affecter une entité responsable à chaque actif ou processus et de documenter ses responsabilité s dans le détail
- **Comment affectez vous l'entité responsable ?**
  - Comme avant, la DSI est responsable de tous les actifs
  - Je « force la main » des métiers (et je m'assois sur la préconisation d) qui demande à ce que les personnes désignées soient compétentes)
  - J'ai fait des réunions avec les métiers pour identifier les personnes compétentes et favorisé le dialogue
  - J'ai montré aux métiers que ces responsabilités permettaient aussi de se valoriser auprès de leurs clients (interne sou externes)
  - …

A.6.1.5 La sécurité de l'information dans la gestion de projet

- **Mesure : Il convient de traiter la sécurité de l'information dans la gestion de projets, quel que soit le type de projet**
  - Préconisation c) : La sécurité de l'information doit être intégrée à toutes les phases de la méthodologie de projet appliquée
- **Comment intégrez vous la SSI dans la méthodologie de projet ?**
  - La méthodo… quoi ? Je ne sais pas, les projets sont externalisés, je ne m'en occupe pas, c'est le problème du sous traitant
  - Une fois le projet terminé, on fait un dossier de sécurité et je le signe (mieux, on nomme un RSSI projet dont le principal job est de le signer)
  - Je travaille pour la Défense, on suit le GISSIP
  - Les objectifs de sécurité ? On utilise toujours les mêmes depuis 5 ans, de toute façon la DSI n'a qu'à sécuriser l'infrastructure.
  - Chaque projet est staffé avec un RSSI compétent, il fait une analyse de risque dès le début et il suit toutes les mesures
  - …

Ordre du jour

- **Point sur l'évolution des normes (Claire Albouy-Cossard, CNAMTS)**
- **Présentation de PCI-DSS et de son positionnement par rapport à la 270xx (Hervé Hosy, Oppida)**
- **Retour sur les normes "privacy" et lien avec la 270XX (Lionel Vodzislawsky, Celtipharm)**
- **Débat sur l'annexe A.6.1 Organisation de la SSI (animé par Jacques Sudres, C-S)**
- **Points divers :**
  - Information globale sur les renouvellements chez les différents certificateurs (Sébastien Rabaud, Scassi)
  - Conférence annuelle du Club 27001.
  - Fonctionnement du club.

Conférence annuelle du Club 27001

- **Huitième conférence "SMSI et normes ISO 27001"**
- **Date : 24 mars 2015**
  - Lieu : Espace Saint Martin, Paris
  - Appel à communication
    - Les présentations feront de 35 à 45 minutes et seront en français ou en anglais.
    - 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
    - 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. Le comité de programme sera sensible à l'aspect pratique des propositions.

- **Vendredi 30 janvier ou 27 février ?**
  - Lieu : ???
  - Sujets ???
    - 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, ...)
    - Sécurité des objets connectés
    - Comparaison des méthodes d'analyse de risques
    - …