L'ISO 27017 et 27018

Présentation réalisée par François Lorek

Agenda

- Présentation
- Petit rappel historique du Cloud
- Les différents types de normes ISO JTC1 SC27
- ISO 27017 c'est quoi et pourquoi faire ?
- ISO 27018 c'est quoi et pourquoi faire ?
- Questions / Réponses

Présentation de l’intervenant

François Lorek

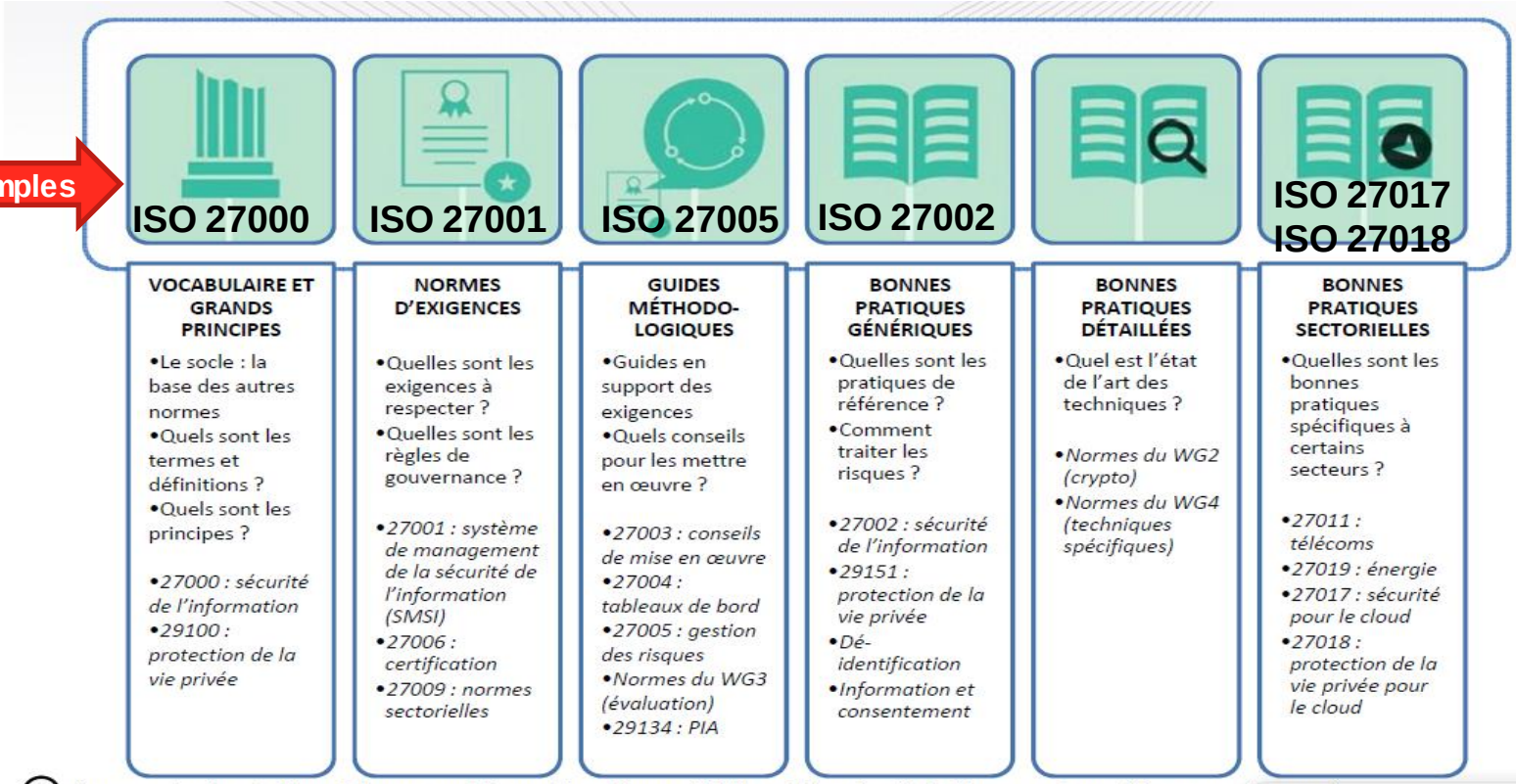
- Auditeur certifié ISO 9001, ISO 20000-1, ISO 22301, ISO 27001 et CSA Star Certification
- 20 ans d’expérience dans le conseil aux entreprises
- Expert en système de management intégré et Cyber-risques, habilité confidentiel défense
- Plus de 50 missions d’audit intégré, et plus de 500 jours d’audits de certification depuis 2008
- Expert français en normalisation auprès de l’AFNOR et de l’ISO, membre des commissions de normalisation sur la sécurité de l’information, les services informatiques, la qualité, le risk management, la sécurité et la résilience et sur la compliance
- Vice convenor ISO/JTC1/SC27/WG4 et représentant WG1/WG4 au sein de la délégation française

L'historique du Cloud en quelques dates

- 2008 : Création du Cloud Security Alliance (Cloud Security Matrix)
- 2010 : Création du Sous Comité 38 à l'ISO
- 2011 : Publication de la NIST 800-145 (Définition du Cloud Computing)
- 2014 : Publication de l'ISO 27018 1ère édition
- 2015 : Publication de l'ISO 27017 1ère édition

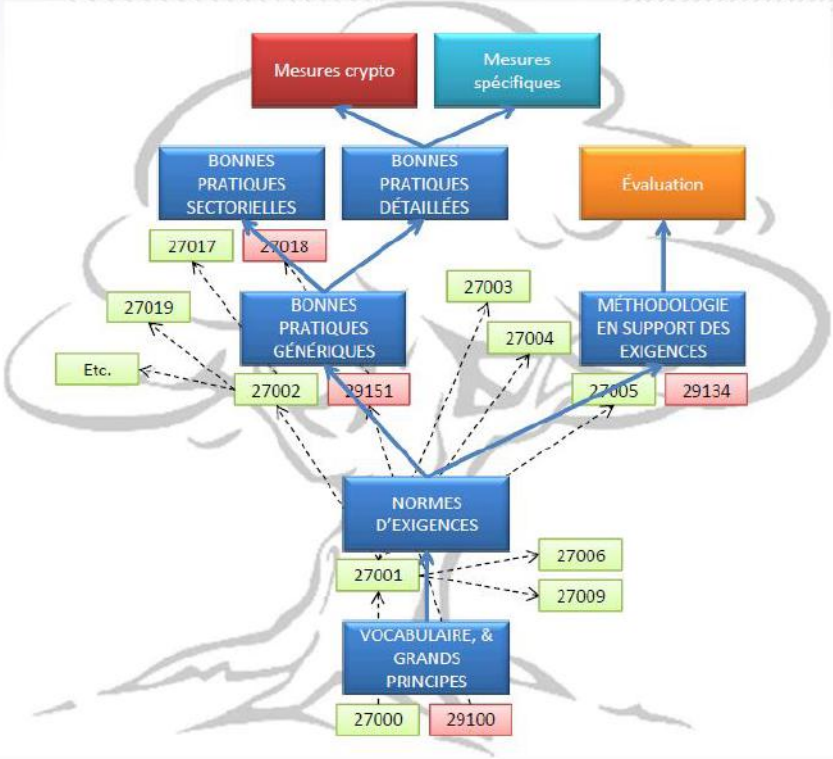
Différents types de normes à l'ISO/JTC1/SC27

Exemples



[images adaptées de Marco Galtarossa, anbileru adaleru, Thomas Helbig et Christopher Holm-Hansen sur https://thenounproject.com]

L'arbre des normes du l'ISO/JTC1/SC27



Légende :

- TYPES
- WG1
- WG2
- WG3
- WG4
- WG5

CNIL.

https://www.cnil.fr/

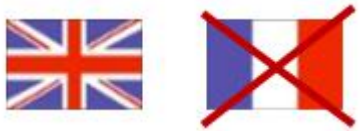
ISO 27017 (1ère Edition le 15 décembre 2015)

- Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

A quoi sert l'ISO 27017 ?

- Fournir un guide de bonnes pratiques spécifiques aux services de cloud computing
- L'ISO/IEC 27017 (Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services en nuage) est un catalogue de bonnes pratiques pour les contrôles de sécurité adapté aux services en nuage
- Ces bonnes pratiques sont additionnelles à celles de l'ISO/IEC 27002 sur la sécurité de l'information, dans le cas où on s'inscrit dans le cadre de l'ISO/IEC 27001
- Elle intègre des bonnes pratiques et techniques et organisationnelles
- Le recours à la norme ISO/IEC 27017 peut être utile dans une procédure de mise en conformité dans le contexte spécifique du cloud

ISO 27018 (1ère Edition le 1er août 2014)



- Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

A quoi sert l'ISO 27018 ?

- Fournir un guide de bonnes pratiques spécifiques aux services de cloud computing
- L'ISO/IEC 27018 (Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII) est un catalogue de bonnes pratiques de protection de la vie privée pour les fournisseurs de services de cloud computing
- Ces bonnes pratiques sont additionnelles à celles de l'ISO/IEC 27002 sur la sécurité de l'information, dans le cas où on s'inscrit dans le cadre de l'ISO/IEC 27001
- Elle intègre des bonnes pratiques et techniques et juridiques
- Le recours à la norme ISO/IEC 27018 peut être utile dans une procédure de mise en conformité dans le contexte spécifique du cloud

Sommaire de la norme ISO 27017

Sommaire de la norme ISO 27018

Standard BS ISO/IEC27018

Pour plus d'information sur les référentiels ISO 27017 & ISO 27018

N'hésitez pas

Contactez - Nous

T : +33 1 55 34 11 40