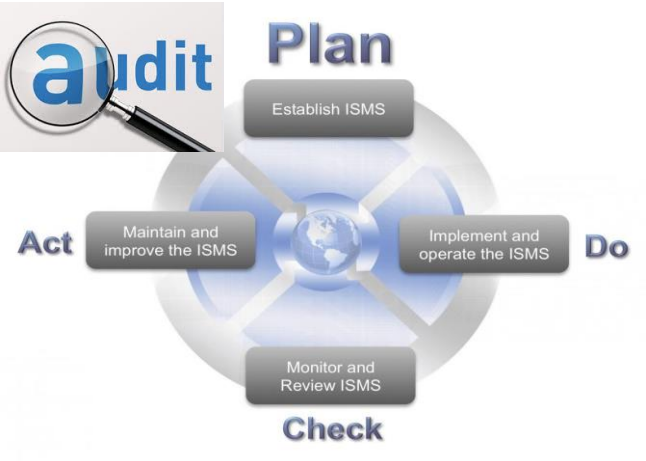
DCC CONSULTING
data center & cloud solutions



[Forum sur la Sécurité de l'Information et la Business Intelligence…

Certification ISO 27001: enjeux globaux pour les sociétés de services informatiques et les clients institutionnels]

Stéphane Jaquet – DCC Consulting, Directeur
Membre du TC215 / WG3 / CENELEC – Electrosuisse
Auditeur libre ISO 27001:2013 pour la SQS

23 Novembre 2017

Agenda

2. **Description du cadre global de la norme ISO 27001 et enjeux globaux pour les Clients, institutionnels en particulier**

3. **Les avantages d'un fournisseur de services IT et d'un éditeur logiciel certifiés ISO 27001**

2. Description du cadre global de la norme ISO 27001 et enjeux… *Définition*

La norme ISO/CEI 27001 promeut l'idée que les informations ***doivent être protégées*** *au même titre que des actifs (sensibilisation à l'échelle de toute l'entreprise), par* ***la mise en place d'un SMSI*** *(système de management de la sécurité de l'information).*

Elle permet d'identifier et de réduire au maximum ***les risques liés à la sécurité de l'information****, assure les fondements juridiques et contractuels, et* ***accroît la confiance*** *dans le cadre des relations avec les clients, les organisations publiques et dans le domaine de l'e-commerce.*

2. Description du cadre global de la norme ISO 27001 et enjeux… *La sécurité de l'information*

La sécurité de l'information

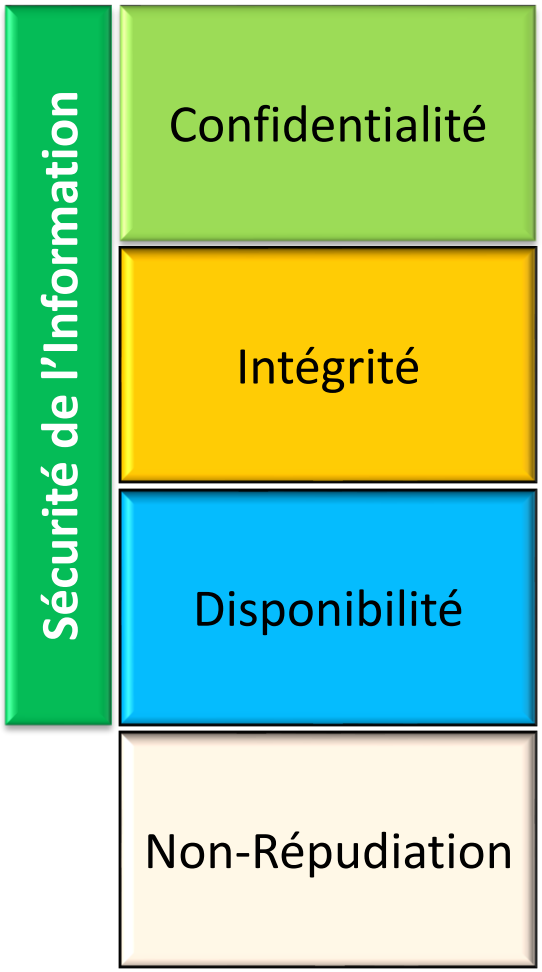
L'humain

Les processus

La technique

2. Description du cadre global de la norme ISO 27001 et enjeux… *La sécurité de l'information*

- Les trois piliers de la sécurité de l'information :



2. Description du cadre global de la norme ISO 27001 et enjeux… *Une famille de normes*

Exigences

ISO 27001
SMSI

ISO 27006
Audit de SMSI

Guides

ISO 27000
Vocabulaire

ISO 27002
Code de bonnes pratiques

ISO 27003
Implémentation

ISO 27004
Métriques

ISO 27005
Analyse des risques

Secteurs

ISO 27034
Sécurité des Applications

2. Description du cadre global de la norme ISO 27001 et enjeux … Vue d'ensemble des normes ISO 270xx

Norme	Titre
ISO/IEC 27000	Vue d'ensemble et vocabulaire
ISO/IEC 27001	**SMSI - Exigences**
ISO/IEC 27002	**Code de bonne pratique**
ISO/IEC 27003	Lignes directrices pour la mise en œuvre du SMSI
ISO/IEC 27004	Mesurage
ISO/IEC 27005	Gestion des risques liés à la sécurité de l'information
ISO/IEC 27006	Exigences pour les organismes procédant à l'audit et à la certification
ISO/IEC 27007	Lignes directrices pour l'audit du SMSI
ISO/IEC 27008	Lignes directrices pour les auditeurs des contrôles
ISO/IEC 27010	LD - Communications intersectorielles/interorganisationnelles
ISO/IEC 27011	LD - Organismes de télécommunications

2. Description du cadre global de la norme ISO 27001 et enjeux … Vue d'ensemble des normes ISO 270xx

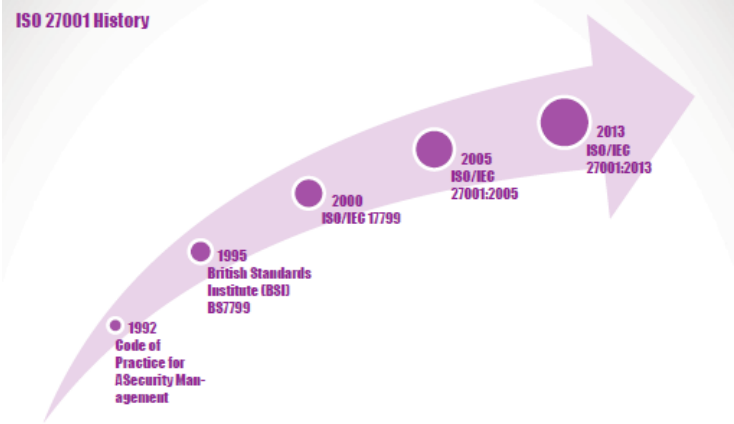
Norme	Titre
ISO/IEC 27013	LD - Mise en œuvre intégrée d'ISO 27001 et ISO 20000
ISO/IEC 27014	Gouvernance de la sécurité de l'information
ISO/IEC 27015	LD - Management de la sécurité de l'information pour les services financiers
ISO/IEC 27017	Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage (cloud services)
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
ISO/IEC 27031	LD - Préparation des TIC pour la continuité d'activité
ISO/IEC 27032	LD - Cybersécurité
ISO/IEC 27033	LD - Sécurité de réseau
ISO/IEC 27034	LD - Sécurité des applications
ISO/IEC 27035	LD - Gestion des incidents de sécurité
ISO/IEC 27037	LD - Identification, la collecte, l'acquisition et la préservation de preuves numériques
ISO/IEC 27799	Management de la sécurité de l'information relative à la santé en utilisant l'ISO 27002

2. Description du cadre global de la norme ISO 27001 et enjeux … Vue d'ensemble des normes ISO 270xx

Norme	Titre
ISO/IEC 27038	LD - Techniques de sécurité -- Spécifications concernant l'expurgation numérique
ISO/IEC 27039	LD - Techniques de sécurité -- Sélection, déploiement et opérations des systèmes de détection et prévention d'intrusion
ISO/IEC 27040	LD - Techniques de sécurité -- Sécurité de stockage
ISO/IEC 27041	LD - Techniques de sécurité -- Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident
ISO/IEC 27042	LD - Techniques de sécurité -- Lignes directrices pour l'analyse et l'interprétation des preuves numériques
ISO/IEC 27043	LD - Techniques de sécurité -- Principes et processus d'investigation sur incident

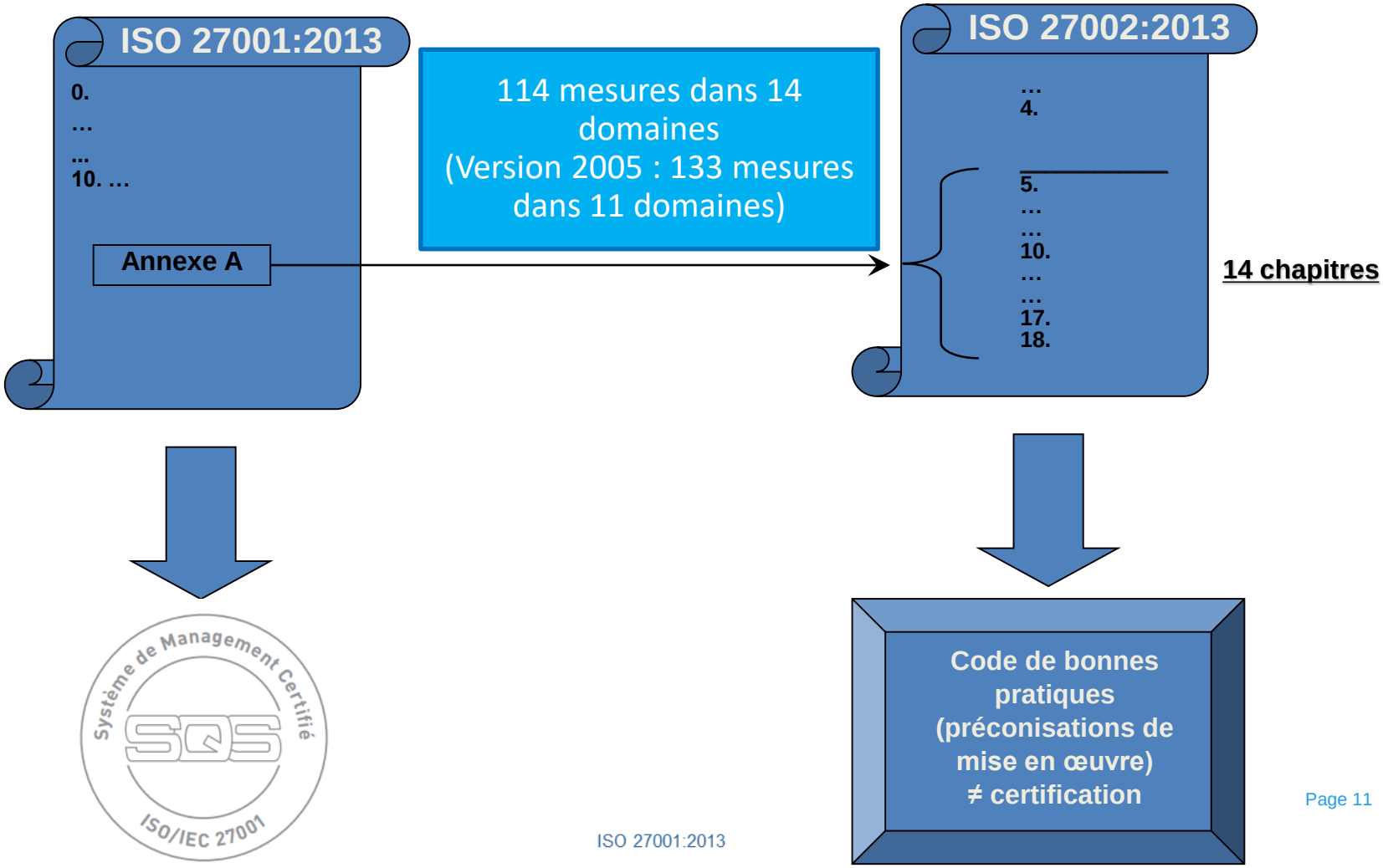
2. Description du cadre global de la norme ISO 27001 et enjeux… *Historique*

- En 1995, le standard britannique "BS 7799" créé par BSI définit des mesures de sécurité détaillées



- En 1998, le BSI introduit le SMSI
- En 2000, ISO édite la norme ISO/CEI 17799:2000 (codes des bonnes pratiques issues de la BS 7799)
- ***En 2005, deux normes sont éditées :***
  - ISO/CEI 17799:2005 qui remanie les domaines et objectifs
  - ISO/CEI 27001:2005 qui introduit la notion de SMSI et offre la possibilité de certification
- En 2007, ISO 27002 remplace ISO/IEC 17799
- ***En 2013, ISO révise les normes ISO/CEI 27001:2013 et ISO/CEI 27002:2013 et les adapte pour répondre à un mode opérationnel***

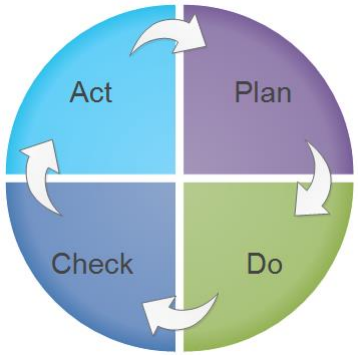
2. Description du cadre global de la norme ISO 27001 et enjeux… *Contenu de la norme*



2. Description du cadre global de la norme ISO 27001 et enjeux… *Contenu de la norme*

Procédures selon 27001 (chap. 4 à 10)

- 4 - Contexte de l'organisation
- 5 - Leadership
- 6 - Planification
- 7 - Support
- 8 - Fonctionnement
- 9 - Evaluation des performances
- 10 - Amélioration



Contrôles selon 27001 - Annexe A

- 5 - POSI - Politiques de sécurité de l'information
- 6 - Organisation de la sécurité de l'information
- 7 - Sécurité des ressources humaines
- 8 - Gestion des actifs
- 9 - Contrôle d'accès
- 10 - Cryptographie
- 11 - Sécurité physique et environnementale
- 12 - Sécurité liée à l'exploitation
- 13 - Sécurité des communications
- 14 - Acquisition, développement et maintenance des systèmes d'information
- 15 - Relations avec les fournisseurs
- 16 - Gestion des incidents liés à la sécurité de l'information
- 17 - Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- 18 - Conformité

2. Description du cadre global de la norme ISO 27001 et enjeux… *Les mythes liés à ISO 27001…*

- *"C'est un job purement pour l'informatique (ou l'IT)" !*
- *"Il s'agit d'écrire des politiques et des procédures"*
- *"ISO 27001 ne fera que rendre notre travail plus difficile"*
- *"Il sera mis en œuvre en 2 mois"*
- *"Nous le faisons seulement pour la certification".*

3. Les avantages d'un fournisseur de services IT et d'un éditeur logiciel certifiés ISO 27001… (1/2)

1. S’adresser à tous les types d’organismes (flexibilité, **agilité**)
2. Améliorer la **confiance** des parties intéressées en assurant la **conformité à leurs exigences**
3. Améliorer l'avantage marketing (image et crédibilité) en obtenant la certification ISO 27001
4. Réduire les **dépenses** liées aux **incidents** liés à la sécurité de l'information (Meilleure maîtrise des risques)
5. **Améliorer l'organisation interne** en définissant mieux les responsabilités et les devoirs
6. **Garantir une pérennité de fonctionnement de l’organisme** par l’engagement formel de la Direction à atteindre des objectifs et à **améliorer la sécurité de l’organisation elle-même** et **des parties prenantes concernées**.

ISO 27001:2013

3. Les avantages d'un fournisseur de services IT et d'un éditeur logiciel certifiés ISO 27001… (2/2)

1. Intégrer la **sécurité de l'information** aux **processus métier** pour un **meilleur alignement**
2. **Améliorer les décisions** en les basant sur les données du système de gestion de la sécurité de l'information
3. Créer une culture **d'amélioration continue** de la sécurité de l'information -> Le niveau de sécurité de l'organisme croît
4. **Impliquer les employés** et les **autres parties intéressées** dans l'amélioration de la sécurité de l'information
5. **Suivre l'évolution des risques** initialement identifiés, les mesures prises et les risques nouveaux ou mis à jour, afin de mesurer l'efficacité des mesures prises (cycles de 3 ans)
6. Faciliter les échanges. ISO 27001 est un référentiel international.

Questions?

DCC CONSULTING SàRL
data center & cloud solutions

Merci de votre attention!