La Sécurité dans le Cloud

Rémi MOLLON

Équipe de Sécurité Informatique du CERN

IN2P3 École Informatique 2014

Lyon, France – 2014/07/04

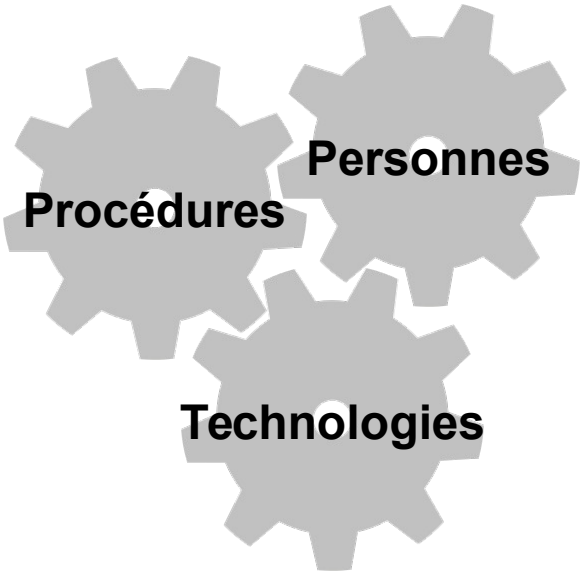
Dans le Passé...

- VMWare (Juin 2009)
  - Prise de contrôle de l'hyperviseur
- iCloud (Août 2012)
  - Perte de plusieurs comptes + effacement des données
- Dropbox (Juin 2012)
  - Vol de mot de passe et données confidentielles
- Dropbox (Octobre 2012)
  - Faille dans le client Dropbox

La Sécurité, Qu'Es Acò ?

- Une suite de produits et services (antivirus, pare-feux, authentification forte, …)
  - => NON !

- Un **processus continu**
  - Ré-évaluation régulière
  - 3 aspects :

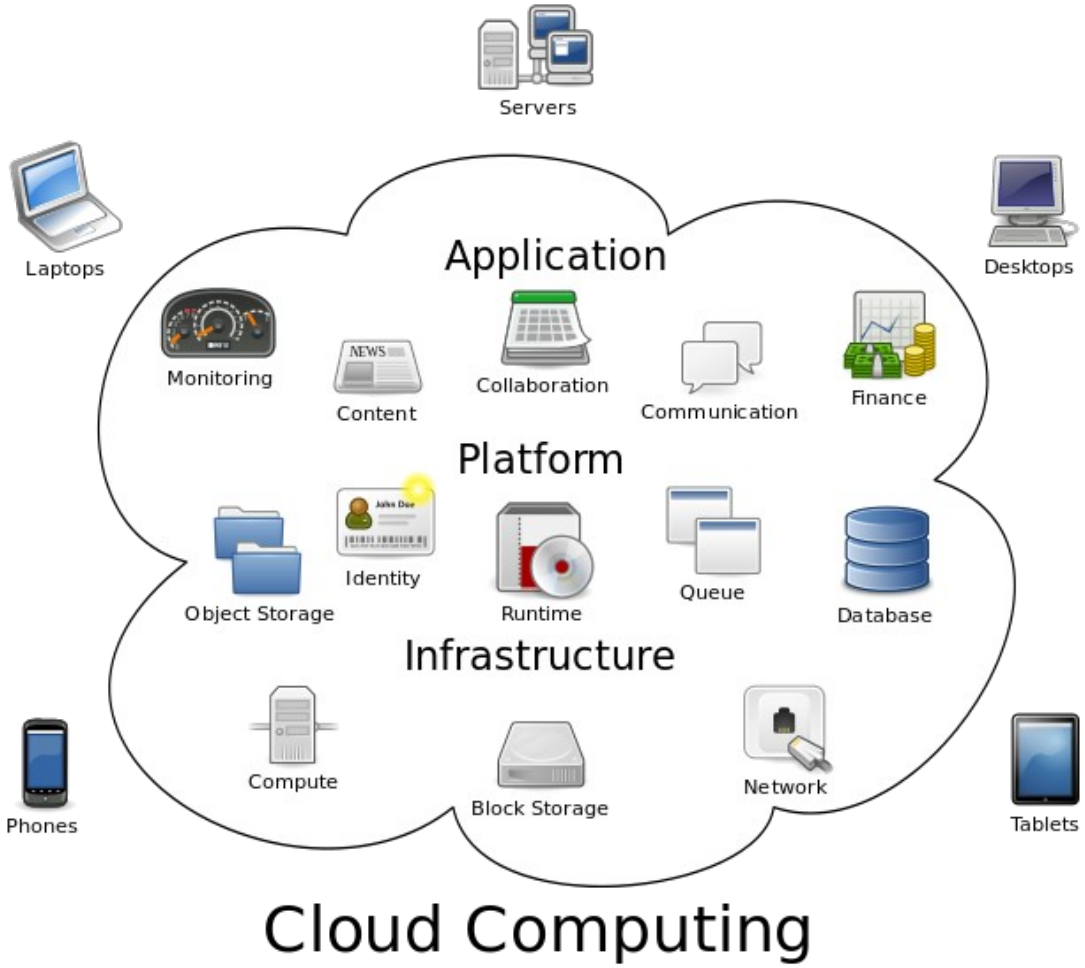


La Sécurité, Pour Qui ?

- L'équipe de sécurité informatique
  - Coordination, règles & recommandations
- Les responsables de services et administrateurs système
  - Sur leurs services/machines seulement
- Tout le monde ! Y compris les utilisateurs !

« SEC_RITY is not complete without U »

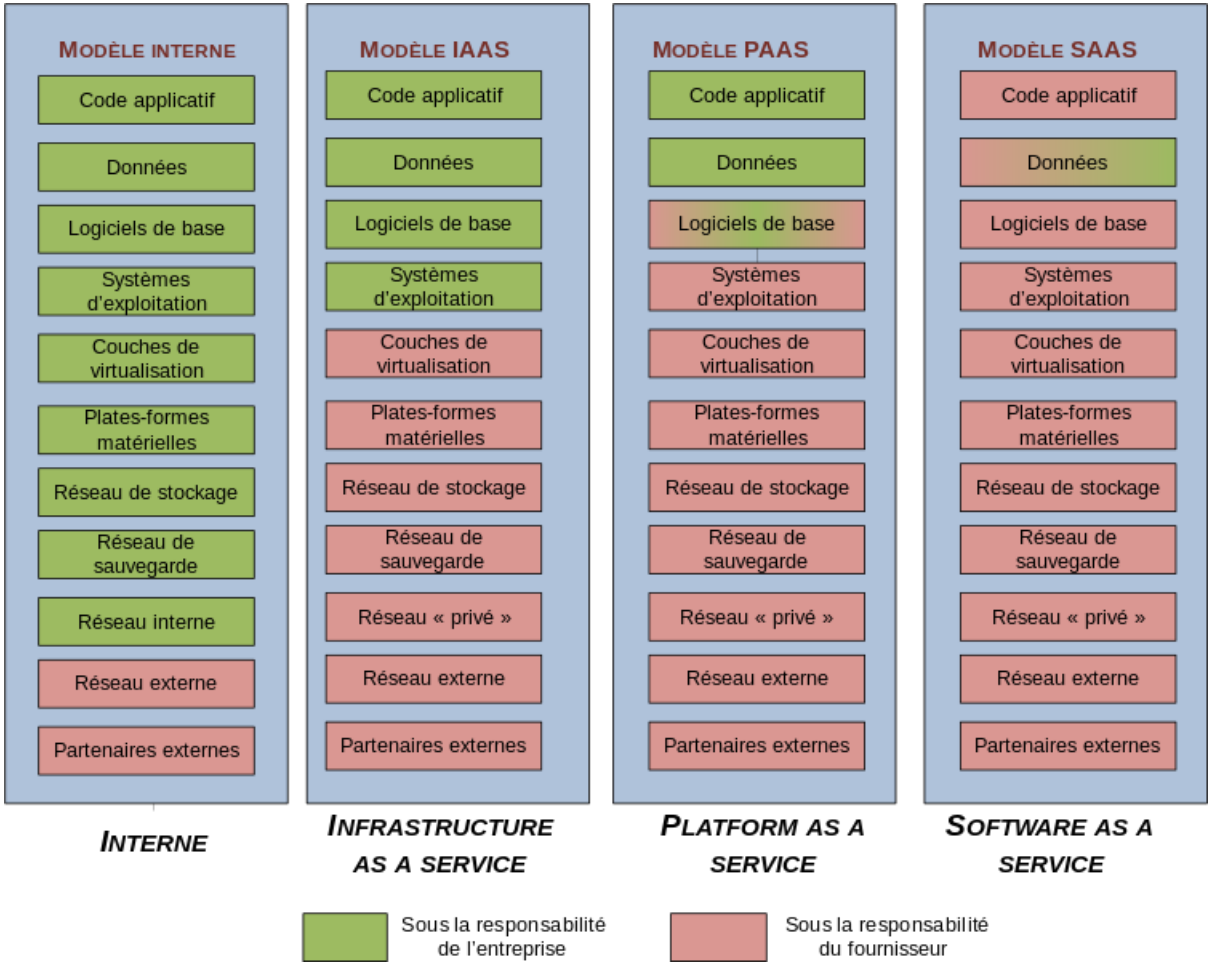
Le « Cloud Computing »



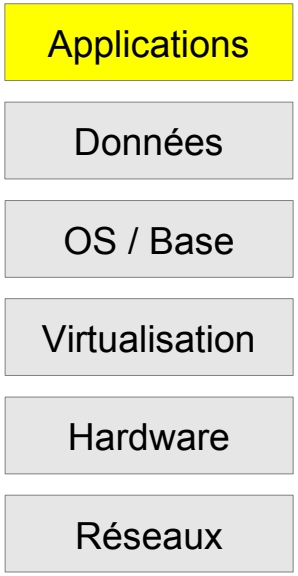
Les Motivations

- Nouvelle approche plus dynamique
  - Évolutivité des services
  - Mutualisation des ressources
  - Réduction des coûts
- Et la sécurité !?
  - Séparation des services
  - Isolation/Virtualisation
  - Liste de normes

Les Différents Modèles



Couche « Code Applicatif »



- Mauvaise configuration
  - Authentification / Autorisations
- Mauvais design/implémentation
  - Buffer overflow, divers injections, validation des entrées, ...
  - Voir les recommandations OWASP
- Contrôle complet par les utilisateurs (sauf SaaS)
  - Applications malicieuses

Couche « Données »

Applications

Données

OS / Base

Virtualisation

Hardware

Réseaux

- Perte de contrôle des données
  - Position géographique
  - Qualité de stockage
- Confidentialité
  - Chiffrement et gestion des clés
- Non-interopérabilité entre les fournisseurs
  - Norme « Cloud Data Management Interface »

Couche « OS & Base »

Applications

Données

OS / Base

Virtualisation

Hardware

Réseaux

- Configuration par défaut
  - Mots de passe
- Mises à jour
- Applications inutiles
- Gestion des logs systèmes
  - Traçabilité
  - Responsabilité ?

Couche « Virtualisation »

- « Faux » sentiment d'isolation
  - Co-hébergement de VMs
  - Attaques matérielles ou logicielles
  - Potentielles vulnerabilités
- Introspection des Vms
  - e.g. Xen Access

Applications

Données

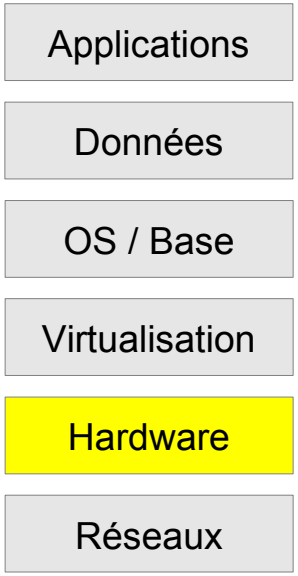
OS / Base

Virtualisation

Hardware

Réseaux

Couche « Hardware »



- Vulnérabilités
  - e.g. IPMI
- Pas d'accès physique
  - Temps d'intervention ?
- Pannes
  - Arrêt du service
  - Perte de données

Couche « Réseaux »

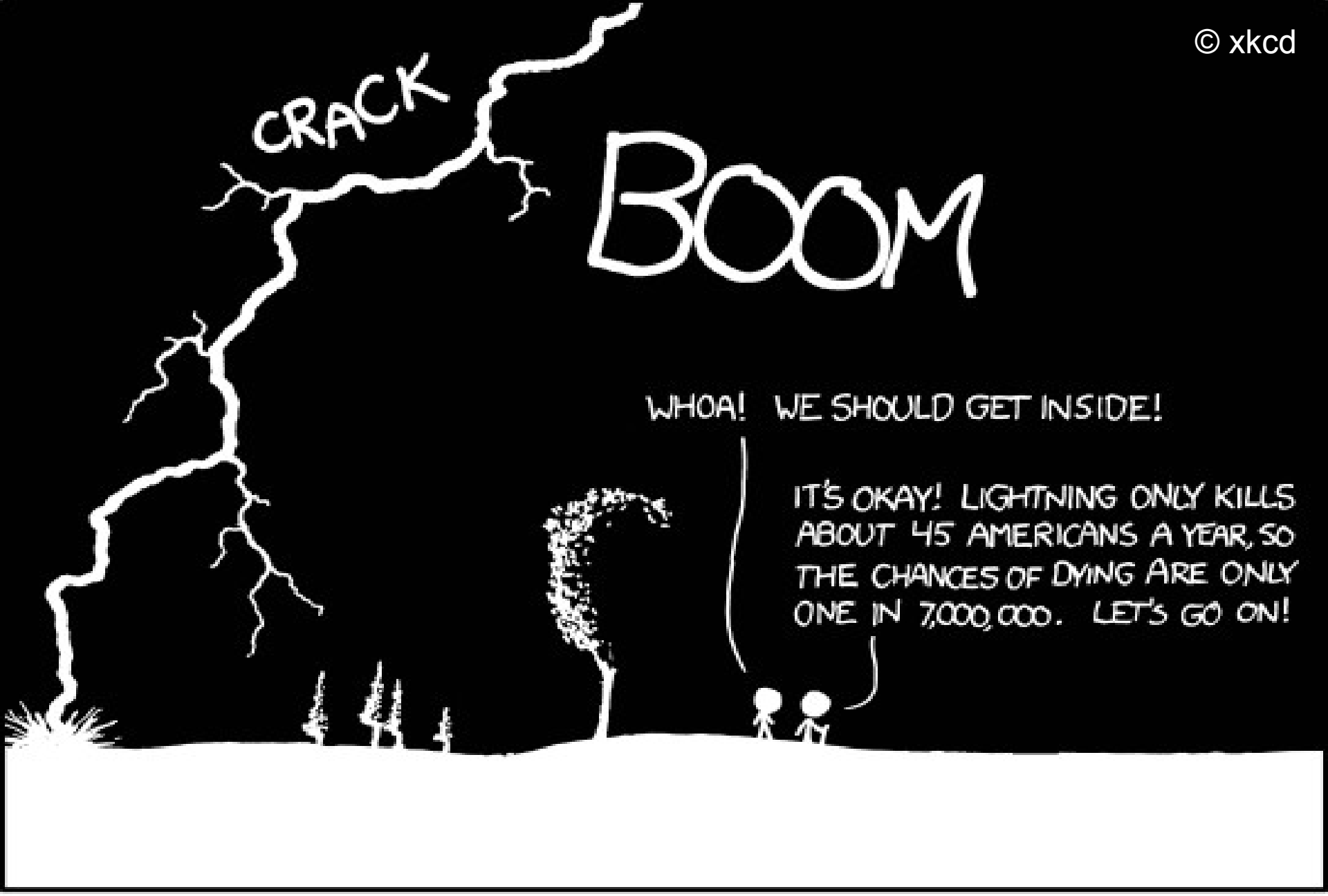
- Applications
- Données
- OS / Base
- Virtualisation
- Hardware
- Réseaux

- Disparition de réseau « interne »
  - Partagé entre les clients
  - Attaques niveau réseau facilitées
  - Possibilité de VLANs
- Bande passante partagée
  - Limitations / Quotas

Évaluation des Risques

$$Risque = \frac{Conséquences \times Probabilité}{Mesures\ de\ Protection}$$

- Lister et qualifier les risques
  - « Business-oriented »
  - Part de subjectivité
  - Implication de la direction
- Investissements sur les risques les plus importants en priorité



THE ANNUAL DEATH RATE AMONG PEOPLE WHO KNOW THAT STATISTIC IS ONE IN SIX.

Service Level Agreement

- Accords utilisateurs / fournisseurs
  - Utilisateur(s) privilégié(s)
  - Conformité(s) réglementaire(s)
  - Emplacement des données
  - Ségrégation des données
  - Restauration
  - Support
  - Efficacité

Normes ISO/IEC

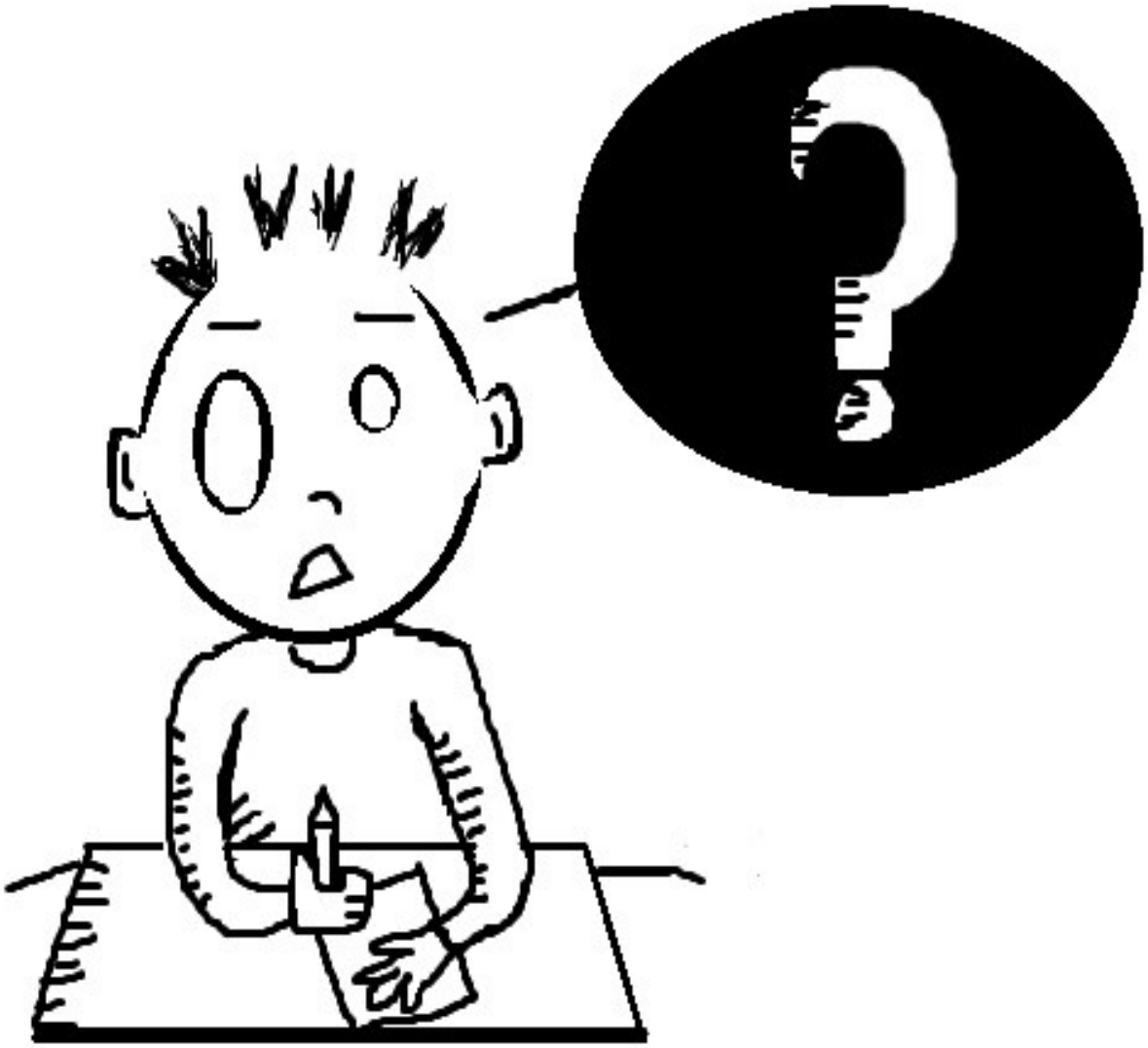
- **ISO 7498-2 :** Identification, autorisations, confidentialité, disponibilité, non-répudiation
- **ISO 27001 :** Gestion des risques liés à la sécurité de l'information
- **ISO 27002 :** Code de bonne pratique pour la sécurité de l'information
- **ISO 27017 (draft) :** Basé sur ISO 27002 pour le Cloud Computing
- **ISO 27018 (draft) :** Code de bonne pratique pour la protection des données personnelles pour les fournisseurs Cloud publics

Cadre Légal

- Basé sur le SLA
  - Engagements contractuels du fournisseur
  - Indemnisation en cas de non-respect
- Attention à l'international
  - Lois différentes en fonctions de pays
  - Confidentialité, utilisation, activités illégales
  - Poursuites juridiques compliquées

Conclusions

- Évaluation des risques importante
- Infrastructures Cloud attractives
  - Grande quantités de données et services
- Normes spécifiques en cours d'élaboration
- Cloud Security Alliance
  - Formations, certifications, conférences



QUESTIONS