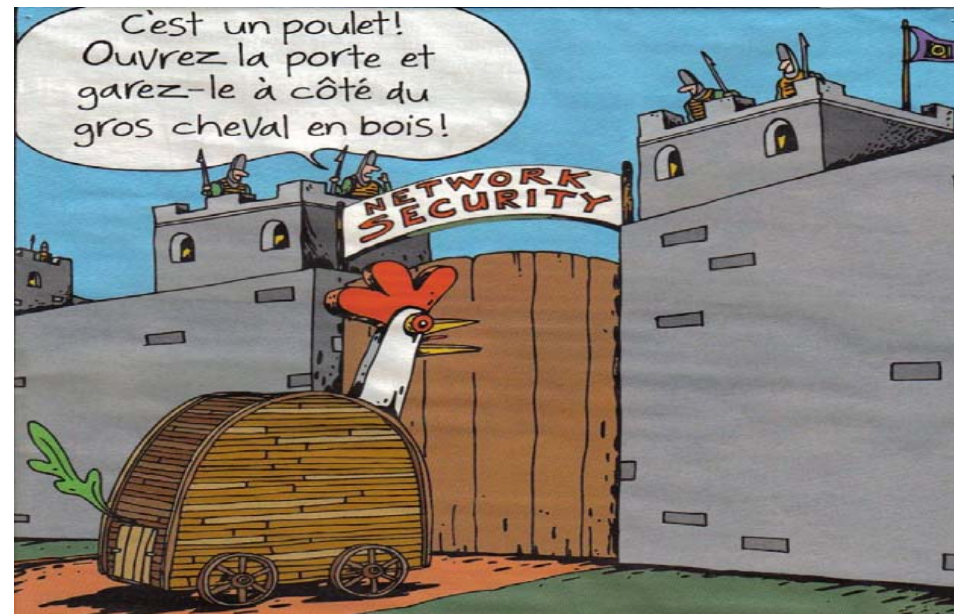


# Formation pour le CNRS « Responsable d'implémentation ISO27001 »

1. **Passage de la sécurité informatique à la sécurité des systèmes d'information puis à la sécurité de l'information.** On passe de notions plutôt techniques à des notions plutôt organisationnelles ou managériales.
  
2. **Importance croissante** des approches de conformité et développement des recours à l'évaluation et à la **certification**. La certification peut porter sur des :
  - **produits et systèmes**  
(Critères communs: IS 15403),
  - **processus**
  - **organisations**  
(par exemple IS 27001)
  - **personnes**  
(IS 27001, CISM, CISSP)





# La normalisation de la SSI

## Le WG1 Road map (extrait)

- **IS 27000** : ISMS fundamentals and vocabulary
- **IS 27001** : ISMS requirements
- **IS 27002** (17799) : Code of practice for ISM
- **IS 27003** : ISM implementation guidance
- **IS 27004** : ISM measurements
- **IS 27005** : Information security risk management
- **IS 27006** : Requirements for bodies providing audit and certification of ISMS
- **IS 27031** : ISM guidelines for telecommunications (ITU-T X.1051)
- **IS 15947** : IT intrusion detection framework
- **IS 18028** : IT Network security (parties 1 à 5)
- **IS 24762** : Guidelines for I&CT disaster recovery services
- **IS 21827** : Systems security engineering – Capability maturity model

# Caractéristiques de la formation

## → Reconnaissance internationale :

La formation « Lead implémenter » et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.

## → Durée :

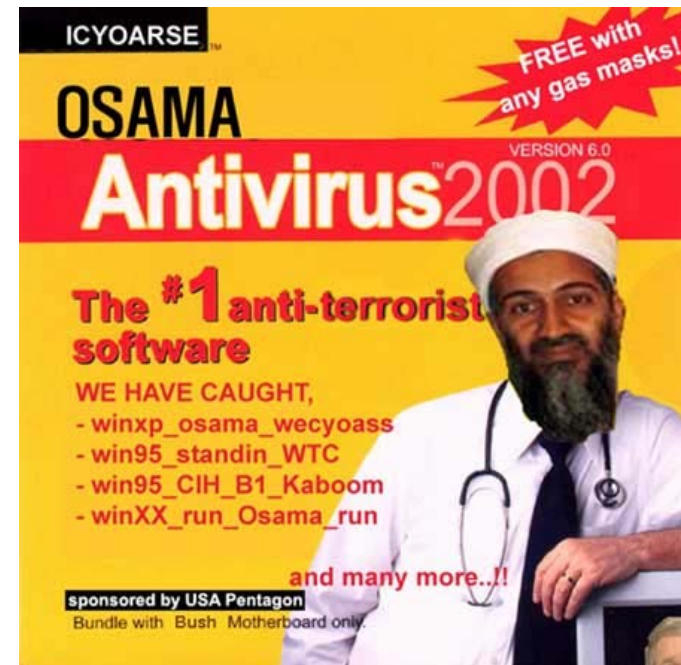
La durée est de 5 jours : 4,5 jours de cours et une demi-journée d'examen, soit un stage de 40 heures réparti en 31 heures 30 de cours, 3 heures 30 d'examen et 5 heures de travail individuel sur les exercices chez soi. Cette durée de 40 heures est nécessaire pour être conforme à la norme **IS19011:2002 7.4.4** qui spécifie cette durée pour la formation des auditeurs.

## → Quand :

début et fin de l'année 2008 en 2 groupes de 12 pers.

## → Modalités de sélection des candidats

- 24 places sont prévus (12 x 2)
- Formateurs de formateurs
- Accepter de rester en poste pour 3 ans
- S'engager à prolonger la formation en région
- Aptes à réussir l'examen et à recevoir l'agrément LSTI pour délivrer une formation diplômante



# Contenu de la formation

## → Présentation de la norme ISO 27001

- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)
- Les traces ou enregistrements
- Inventaire des actifs
- Appréciation du risque
- Traitement du risque

## → Processus de certification ISO 27001

## → Présentation de la norme ISO 27002

- Différentes catégories de mesures de sécurité
- Mesures d'ordre organisationnel
- Mesures d'ordre technique

## → Analyse de risque ISO 27005

- Introduction sur la norme ISO 27005
- Vocabulaire : risque, menace, vulnérabilité
- Processus de gestion de risque : aspects itératifs et PDCA



# Contenu de la formation

- Établissement du contexte
  - Critères de gestion de risque
  - Description de l'environnement et des contraintes
- Appréciation des risques
  - Identification des risques : actifs, menaces, vulnérabilités, conséquences, ...
  - Estimation des risques
  - Évaluation des risques
- Traitement du risque
  - Sélection des mesures de sécurité
- Acceptation du risque
- Communication du risque
- Réexamen du processus de gestion de risques et suivi des risques
- Conclusion
- ➔ **Préparation à l'audit de certification**
  - Ce que recherchent les auditeurs de certification
  - Documentation obligatoire
  - Documentation utile pour l'audit
  - Considérations pratiques
- ➔ **Préparation à l'examen**

# Les normes IS 2700x

## IS 27000 : principes et vocabulaire

**Principes** : présentation de la famille des normes de la série 2700x.

**Elles sont liées à l'ISMS (Information Security Management System).**

Des normes techniques y sont rattachées

- 13335 TR 3 à 5,
- 15947 TR sur les principes de la détection d'intrusion,
- 18028 sur la sécurité des réseaux,
- 18043 sur la gestion de la détection d'intrusion,
- 18044 TR sur la gestion d'incident
- 24762 sur la continuité – disaster recovery services).

*GRAVE ! ...  
On a une intrusion  
sur notre serveur !*



Par ailleurs, la norme donne les **définitions** des termes liés à la série 2700x.

*Et si on organisait une  
manifestation sur la  
voie publique ? ...*





# Les normes IS 2700x

## IS 27001 (ISMS Requirements)

Référence aux principes de l'OCDE et à l'approche qualité (Roue de Deming, Plan, Do, Check, Act).

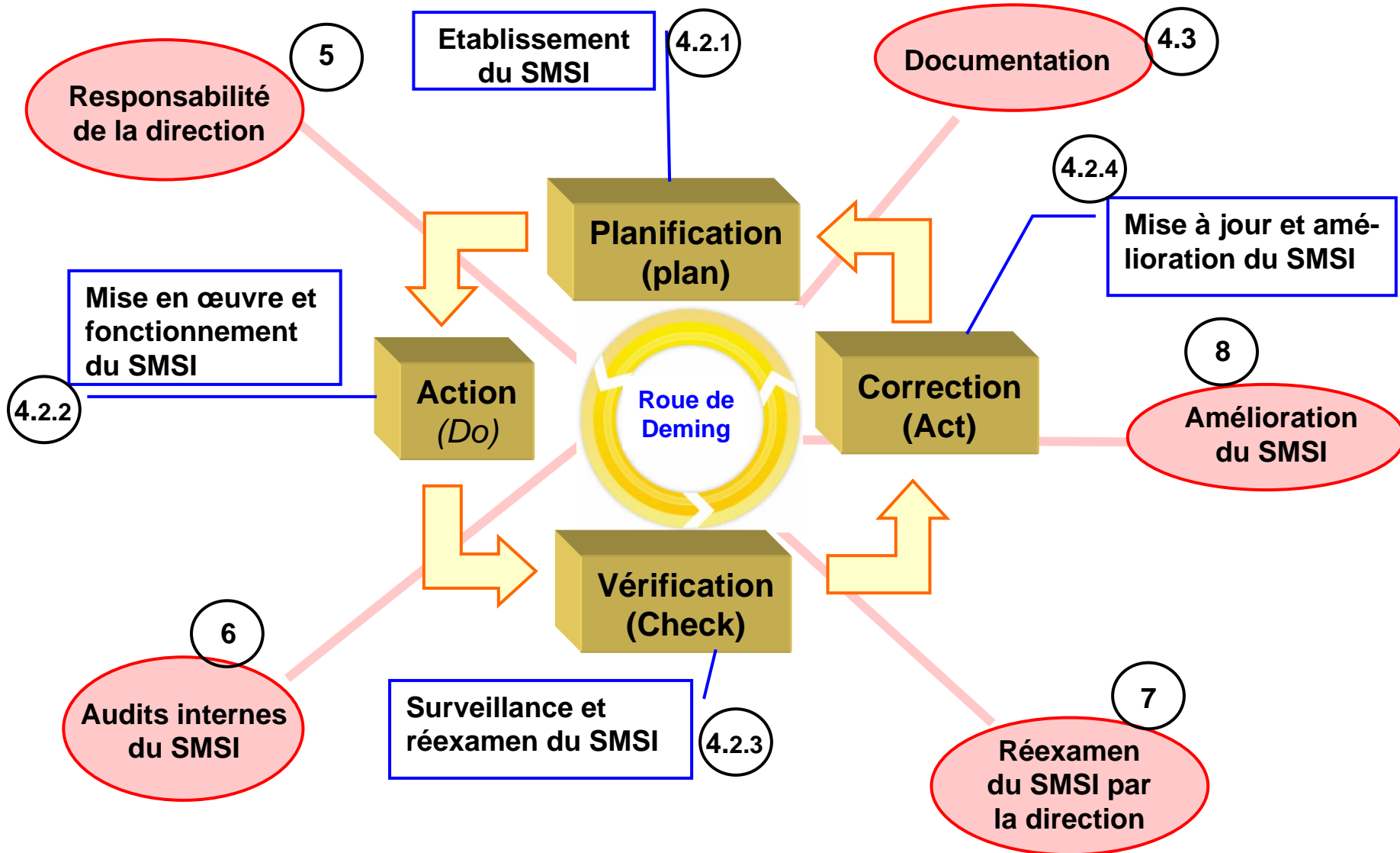
- **Le chapitre 4** mentionne les étapes (établir l'ISMS, le mettre en oeuvre et l'exploiter, le contrôler et le réviser, le maintenir et l'améliorer). Il décrit aussi les exigences en matière de documents.
- **Le chapitre 5** affirme la responsabilité managériale
- **Le chapitre 6** décrit l'organisation des contrôles internes
- **Le chapitre 7** traite de la révision, sous responsabilité managériale, de l'ISMS
- **Le chapitre 8** porte sur l'amélioration de l'ISMS

Le respect des clauses de ces chapitres est indispensable dans le cadre d'une certification.

**En Annexe C**, tableau de correspondance entre cette norme et les normes IS9001:2000 (qualité) et IS 14000:2005 environnement)

# Les normes IS 2700x

## ISO 27001: 5 chapitres qui construisent le SMSI





# Les normes IS 2700x

## IS 27002 : historique

A l'origine de cette norme, on trouve la **BS 7799**, standard britannique développé à la fin des années 90 et qui s'est imposé outre-Manche.

C'est un document en deux parties :

**BS 7799 Part 1** : Code of Practice for information security management,

**BS 7799 Part 2** : Specification for information security management.

Normalisation de la BS :

- Une première tentative a eu lieu en 1995 et a abouti à un échec.
- Une seconde tentative en 2000 (fast-track) a vu le vote de l'IS 17799 qui ne reprend que la partie 1 de la BS 7799.

Cette norme a été révisée et la nouvelle version est parue mi-2005 sous le nom de 17799:2005 devenu depuis le début de l'année **ISO 27002**.

Cette version présente mieux les mesures, les conseils de mise en oeuvre et l'environnement (control, implementation guidance, others).



# Les normes IS 2700x

## IS 27002 : Contenu

**Les premiers chapitre** décrivent les grands principes (définir les exigences de sécurité, les références des mesures, les facteurs critiques de réussite, etc.)

**Le chapitre 5** décrit le contenu d'une PSSI, « document issu de la Direction de l'entreprise » et insiste sur le fait qu'elle doit être diffusée sous une forme accessible et compréhensible par ses destinataires.

**Le chapitre 6** traite de l'organisation de la SSI « une structure transverse permet de coordonner les mesures de sécurité (analyse des risques, sensibilité de l'information, incidents ..) »

**Les derniers chapitres** traitent :

- De la classification et du contrôle (ch. 7)
- De la sécurité du personnel (ch. 8),
- De la sécurité physique et environnementale (ch. 9),
- De la gestion des tâches et des communications (ch. 10),
- Du contrôle d'accès (ch. 11)
- Du développement et maintenance des systèmes (ch. 12)
- De la gestion des incidents de sécurité (ch. 13)
- De la gestion de la continuité (ch. 14 )
- Enfin le dernier chapitre traite de la conformité (ch. 15)



# Les normes IS 2700x

## IS 27005 (Information security risk management)

- **Processus de gestion du risque** en sécurité de l'information (identifier, estimer les niveaux de risque, évaluer les risques, traiter les risques, accepter les risques, communiquer, superviser et réviser).
- Identification des **actifs**, des **menaces**, des **vulnérabilités**, des **impacts/conséquences**, des **mesures existantes ou planifiées**.
- **Traitement du risque** : après évaluation, évitement, transfert, réduction, acceptation.

Annexe A : Champ et limites du processus de gestion du risque.

Annexe B : Identification et évaluation des actifs, évaluation d'impact.

Annexe C : Types de menaces (accidentelles, environnementales ou volontaires).

Annexe D : Vulnérabilités et méthodes d'évaluation des vulnérabilités.

Annexe E : Approches d'évaluation du risque en sécurité de l'information

## IS 27005 (Information security risk management)

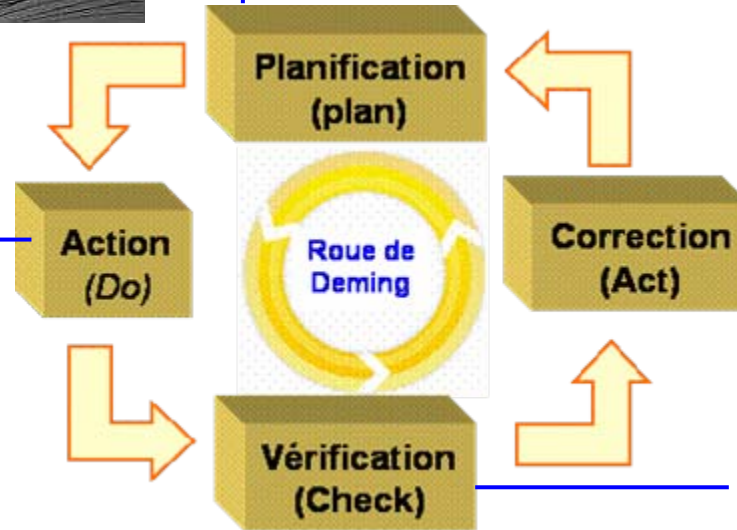


- Identifier les risques
- Quantifier chaque risque par rapport
  - aux conséquences que sa matérialisation pourrait avoir sur l'activité
  - à sa probabilité d'occurrence (*likelihood*)
- Identifier les actions appropriées pour réduire les risques identifiés à un niveau acceptable

- Rectifier le traitement du risque à la lumière des événements et des changements de circonstances
- Améliorer le processus de gestion du risque

- Implémenter les actions pour réduire les risques
- Eduquer la direction et le personnel sur les risques et les actions prises pour les atténuer

Surveiller et réexaminer les résultats, l'efficacité et l'efficience du processus



# Vos contacts FSD

<b>Protection du patrimoine scientifique</b>	<b>Jean-Luc Toffart</b> Courriel : <a href="mailto:jean-luc.toffart@cnrs-dir.fr">jean-luc.toffart@cnrs-dir.fr</a> tél : 01 44 96 41 5
<b>Sécurité des systèmes d'information</b>	<b>Robert Longeon</b> Courriel : <a href="mailto:robert.longeon@cnrs-dir.fr">robert.longeon@cnrs-dir.fr</a> tél : 01 44 96 48 76  + <i>François MORRIS</i> Courriel : <a href="mailto:francois.morris@impmc.jussieu.fr">francois.morris@impmc.jussieu.fr</a> tél : 01 44 27 37 85
<b>Missions à l'étranger – Formations - Habilitations</b>	<b>Josiane Pauchont</b> Courriel : <a href="mailto:josiane.pauchont@cnrs-dir.fr">josiane.pauchont@cnrs-dir.fr</a> tél : 01 44 96 41 84
<b>Secrétariat technique</b>	<b>Christine Pierre</b> Courriel : <a href="mailto:christine.pierre@cnrs-dir.fr">christine.pierre@cnrs-dir.fr</a> tél : 01 44 96 41 85
<b>Le Fonctionnaire de Sécurité de Défense</b>	<b>Joseph Illand</b> Courriel : <a href="mailto:joseph.illand@cnrs-dir.fr">joseph.illand@cnrs-dir.fr</a> tél : 01 44 96 41 88



**Site Web :** <http://www.sg.cnrs.fr/FSD/default.htm>

**Courriel :** [Fonc-Def-Sec@cnrs-dir.fr](mailto:Fonc-Def-Sec@cnrs-dir.fr)