

**PSSI  
EBIOS  
ISO 27000**

**Novembre 2016**

# **Plan de la présentation**

**Introduction**

**PSSI**

**RGS V2.0**

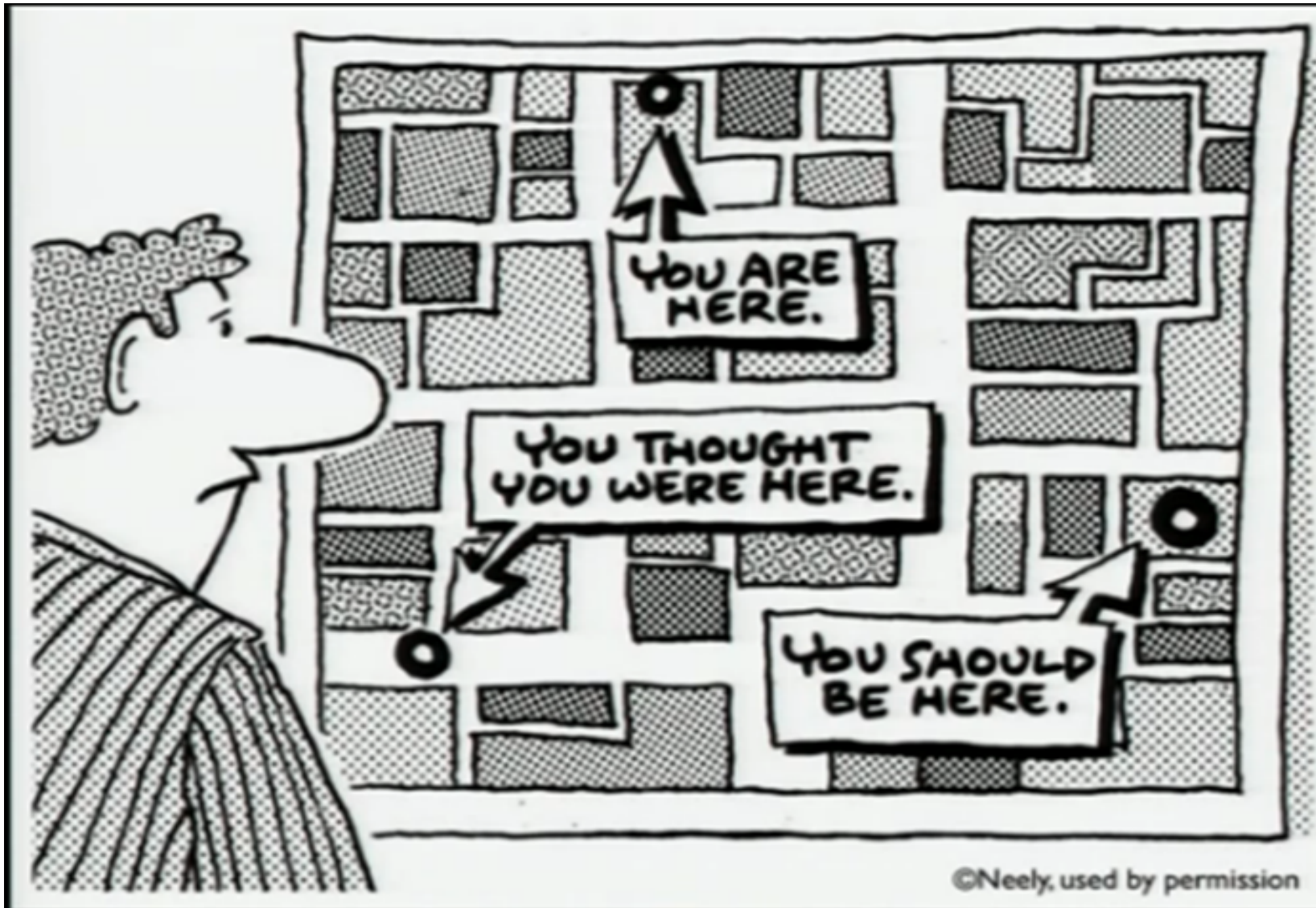
**EBIOS**

**ISO/IEC 27002:2013**

**Certification et Conformité**

# Introduction

# De la photo à l'amélioration continue













# Un peu de benchmark

Figure 1: Operator mitigation strategy assessment

		Mitigating strategy maturity	Mitigating strategy as leadership priority	Likelihood of risk increasing in 2013
1	Failure to shift the business model from minutes to bytes			
2	Disengagement from the changing customer mindset			
3	Lack of confidence on return on investment			
4	Insufficient Information to turn demand into value			
5	Lack of regulatory certainty on new market structures			
6	Failure to capitalize on new forms of connectivity			
7	Poorly managed M&A and strategic partnerships			
8	Failure to define new business metrics			
9	Lack of privacy, security and resilience			
10	Lack of organizational flexibility			
<b>Key</b> <b>High</b> <b>Low</b>				

# Allianz – survey of global business risks for 2014.

## Top 10 global business risks for 2014

	2014		2013	Rank	Trend
	1 Business interruption, supply chain risk	43%	46%	(1)	—
	2 Natural catastrophes (for example, storm, flood, quake)	33%	44%	(2)	—
	3 Fire, explosion	24%	31%	(3)	—
	4 Changes in legislation and regulation	21%	17%	(4)	—
	5 Market stagnation or decline	19%	12%	(8)	↗
	6 Loss of reputation or brand value (for example, from social media)	15%	10%	(10)	↗
	7 Intensified competition	14%	17%	(5)	↘
	8 Cyber crime, IT failures, espionage	12%	(-)	(-)	● NEW
	9 Theft, fraud, corruption	10%	(-)	(-)	● NEW
	10 Quality deficiencies, serial defects	10%	13%	(6)	↘

The third annual Allianz Risk Barometer survey was conducted among risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty (AGCS) and local Allianz entities. Figures represent the number of responses as a percentage of all survey responses (557)



**A vos claviers !**

**Trouvez, lisez et comparez le  
« Allianz Survey of Global  
Business risks » pour 2015 et  
2016 puis observez la tendance.  
Que remarquez-vous ?**



# Allianz – survey of global business risks for 2016

Top 10 Global Business Risks for 2016





# Tout en haut de l'échelle, que feriez-vous pour....?



...donner la  
direction et le  
sens qui fondent  
la base de  
légitimité de la  
sécurité...



...dans votre  
entreprise ou  
institution ?



**une PSSI !**



# I -PSSI

Document ANSSI. A l'origine, «Guide pour l'élaboration d'une PSI» version 1.1 paru en septembre 1994.

Mise à niveau en 2004 tant sur les thèmes traités que sur les documents de référence.

**Trois concepts** de base :

**Politique de sécurité** du système d'information : ensemble formalisé dans un document applicable des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques ayant pour objet la protection du SI de l'organisme.

**Principe de sécurité** : expression des orientations de sécurité nécessaires et des caractéristiques importantes de la sécurité pour l'élaboration d'une politique et en particulier des règles de sécurité la constituant.

**Règle de sécurité** : définit des exigences de sécurité pour la mise en place des moyens et sur les comportements par déclinaison des principes retenus. Se construit par déclinaison des principes dans un environnement et un contexte donnés.

# PSSI

**Quatre parties autonomes :**

**Introduction** (mise en place de la SSI dans le référentiel normatif de la SSI au sein de l'organisme et bases de légitimité)

**Méthodologie** (conduite du projet d'élaboration d'une PSSI, recommandations pour la construction des règles)

**Principes de sécurité**

**Références SSI**

# PSSI - Présentation et rôle (1/2 )

**Contexte en évolution** : dépendance croissante des organismes envers leur SI, diversification des applications, mondialisation, interconnexion, risques en extension voire nouveaux, sécurité globale.

La **PSSI** traduit, au niveau de la direction générale de l'organisme, la dimension stratégique de l'information de son traitement, de son transport et de son archivage. La sécurité du SI porte principalement sur les composantes suivantes du patrimoine :

- Patrimoine matériel (serveurs, réseau, postes de travail,...),
- Patrimoine immatériel (programmes et informations concourant au métier),
- Informations relatives aux personnes avec lesquelles l'organisme est en relation.

La **PSSI** permet constitue un référentiel facilitant la cohérence et la pérennité des approches. Elle fournit une vision stratégique et transverse et recense les obligations de diverses natures. Enfin, elle est un bon outil de sensibilisation et d'information sur un thème complexe. Une analyse des risques spécifiques au contexte est recommandée.

# PSSI - Présentation et rôle (2/2 )

## Domaines d'application :

- Système existant ou à développer,
  - Ensemble des aspects du SI (y compris toute personne ayant accès au SI),
- Il peut donc exister plusieurs PSSI dans un même organisme. Il faut alors veiller à leur cohérence via une PSI globale.

**Lien entre PSSI et CC** (certification, Décret n° 2002-535 du 18 avril 2002).

**Lien entre PSSI et lignes directrices de l'OCDE** (29 juillet 2002). 9 principes :

Sensibilisation	Responsabilité
Réaction	Éthique
Démocratie	Évaluation des risques
Conception et mise en œuvre de la sécurité	Gestion de la sécurité
Réévaluation.	



# **PSSI - Bases de légitimité (1/7)**

**Sept rubriques :**

**Respect de la déontologie,**

**Lutte contre les menaces : accidents, erreurs et malveillances,**

**Préservation des intérêts vitaux de l'État,**

**Arsenal juridique pour la lutte contre la malveillance,**

**Préservation des intérêts particuliers de l'organisme,**

**Conformité technologique,**

**Contrôle consommériste.**

# PSSI - Bases de légitimité (2/7)

## Respect de la déontologie

**Garantie des droits de l'homme, respect de la vie privée, garantie des libertés individuelles ou publiques. Principales sources :**

### **Niveau international :**

Déclaration universelle des droits de l'homme (ONU – 1948)

Principes directeurs de l'ONU (données à caractère personnel)

Lignes directrices de l'OCDE (protection de la vie privée, flux transfrontières de données à caractère personnel)

### **Niveau de l'Union Européenne :**

Convention de sauvegarde des droits de l'homme et des libertés fondamentales (1950)

Directives du Conseil de l'Union Européenne

### **Niveau national :**

Déclaration des droits de l'homme (1789)

Loi "Informatique et Libertés"

Cybersurveillance des lieux de travail

### **Métiers :**

Codes d'éthique corporatifs

Codes d'éthiques des métiers des TI

# PSSI - Bases de légitimité (3/7)

## Gestion des risques : accidents, erreurs, défaillances et malveillances

**Obligation légale** à tous les responsables d'organismes **de lutter**, avec les moyens appropriés, **contre les accidents** divers (Décret 92-158 du 20 février 1992).

Cette obligation est en général prise en compte au niveau de la sécurité générale.

Il convient de considérer aussi les cas liés à l'utilisation du SI (en particulier les pertes de confidentialité, d'intégrité ou de disponibilité).

Les responsables d'organisme doivent donc **renforcer les contrôles de sécurité** et les inscrire comme base de légitimité partout où il existe un risque d'accident lié à l'utilisation du SI.

L'**ISO 15408** rappelle qu'une menace doit être décrite en citant l'élément menaçant (expertise, ressource, motivation), l'attaque (méthodes, vulnérabilités, opportunités) et le bien qui en est la cible.

# PSSI - Bases de légitimité (4/7)

## Préservation des intérêts vitaux de l'État

### Protection des éléments non classifiés de défense

Sécurité des SI traitant des informations sensibles (**REC 901**)

Recommandation relatives aux informations systèmes ou applications ne relevant pas du secret de défense (**REC 600**).

### Protection du secret de défense

Protection du secret et des informations concernant la défense nationale et la sûreté de l'État (**IGI 1300**)

Sécurité des SI qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées (**IGI 900**)

Protection du secret dans les rapports entre la France et les États étrangers (**II 50**)

Protection du secret de l'information pour les marchés et autres contrats (**II 2000**)

# PSSI - Bases de légitimité (5/7)

## Lutte contre la malveillance et le cybercrime

### Au niveau de l'Union Européenne :

Protection du logiciel (recommandation sur la criminalité en relation avec l'ordinateur et directive sur la protection juridique des programmes d'ordinateur)

### Au niveau national :

Les logiciels sont considérés comme des œuvres de l'esprit protégées par le Code de la propriété intellectuelle.

Des lois réglementent aussi

La divulgation non autorisée de documents techniques ou commerciaux, même après une rupture de contrat

La fraude informatique

L'interception de télécommunications.

# PSSI - Bases de légitimité (6/7)

## Préservation des intérêts particuliers de l'organisme

L'organisme peut se définir par :

Sa **mission** ou son **métier** (objectifs à exprimer)

Sa **culture** (valeurs, savoir-faire, identité commune)

Ses **orientations stratégiques** et sa **structure** (organigramme, sociogramme)

Ses **relations avec l'environnement** (contrats avec des tiers)

Ses **ressources** (humaines, juridiques, savoir-faire et ressources techniques, en particulier nécessité de confidentialité).

Si l'organisme considère qu'un de ces thèmes a un impact majeur sur sa sécurité, il le considère comme **base de légitimité** pour justifier les principes décrits dans sa PSSI.



# PSSI - Bases de légitimité (7/7)

## Conformité technologique

Contrôle étatique dans le domaine de la **cryptologie**

Contrôle des **communications** (données à caractère personnel et protection de la vie privée dans le secteur des télécommunications)

**Signature électronique** (l'écrit électronique a la même force probante que l'écrit sur support papier)

Lutte contre les **signaux parasites compromettants**.

## Contrôle consommériste

### Normalisation

Principe d'adhésion (interopérabilité), parfois caractère obligatoire

### Certification

# PSSI – Méthodologie

Partant du **référentiel de l'organisme**, validé par la Direction Générale, la première phase, validée par le comité de pilotage, permet **d'élaborer des éléments stratégiques** via une analyse des risques SSI. La deuxième phase consiste en la **sélection des principes** et en la **rédaction des règles**, elle est validée par le comité de pilotage et par la direction générale. La troisième phase permet de finaliser la **PSSI** et elle est validée par la direction générale.

Cette PSSI fournit un **cadre de référence et de cohérence**. Elle doit être complétée par un plan d'action, régulièrement mis à jour, pour en assurer la mise en œuvre.

Les suites s'orientent selon quatre thèmes :

- Déclinaison opérationnelle des **règles**
- Constitution d'une entité de **suivi et de pilotage** du plan d'action
- **Audit** de la politique de sécurité
- Mise en place d'une organisation d'**alerte** et de **veille technologique**.

# PSSI – Démarche d'élaboration (1/2)

## Finalisation et validation de la PSSI

Obtenir un **document validé** (par un comité de sécurité) après vérification de :

La cohérence des règles énoncées

L'exhaustivité de la couverture des risques

La traduction complète de l'ensemble des principes et des règles

L'applicabilité des exigences et règles au sein de l'organisme

Définir un **plan d'action**

**Diffuser la PSSI** à l'ensemble des acteurs internes et externes

Donner une large diffusion aux principes et aux règles de la PSSI

**Réexaminer la PSSI** en fonction d'événements majeurs ou au moins tous les cinq ans

# **PSSI – Démarche d'élaboration (2/2)**

## **Plan-type d'une PSSI**

### **Partie 1 Éléments stratégiques**

#### **Ch.1 Périmètre de la PSSI**

#### **Ch.2 Enjeux et orientations stratégiques**

#### **Ch.3 Aspects légaux et réglementaires**

#### **Ch.4 Échelle de besoins**

#### **Ch.5 Besoins de sécurité**

#### **Ch.6 Origine des menaces**

### **Partie 2 Règles de sécurité**

# PSSI – Principes de sécurité

Cette partie présente la **liste des principes** utiles pour l'élaboration de la PSSI.

Elle traite des **aspects organisationnels, de mise en œuvre et techniques**.

Ces principes sont présentés selon 16 domaines :

**Organisationnels** (Politique de sécurité, Organisation de la sécurité, Gestion des risques SSI, Sécurité et cycle de vie, Assurance et certification)

**Mise en œuvre** (Aspects humains, Planification de la continuité des activités, Gestion des incidents, Sensibilisation, Exploitation, Aspects physiques et environnementaux)

**Techniques** (Identification/authentification, Contrôle d'accès logique, Journalisation, Infrastructure de gestion des clés cryptographiques, Signaux compromettants)

Au sein des domaines, ils sont déclinés en règles.

# PSSI - Principes organisationnels

## Politique de sécurité

- PSI-01**    **Évolutions de la PSSI**
- PSI-02**    **Diffusion de la PSSI**
- PSI-03**    **Contrôle d'application de la PSSI**
- PSI-04**    **Protection des informations confiées à l'organisme** (dont contrats)
- PSI-05**    **Adoption d'une échelle de besoins** (D,I,C, autres)
- PSI-06**    **Critères de détermination des besoins de sécurité** (infos sensibles, vitales, stratégiques, coûteuses,...)
- PSI-07**    **Déclassification des informations**
- PSI-08**    **Surclassification des informations**
- PSI-09**    **Identification et portée de la classification d'une information**
- PSI-10**    **Définition et contrôle des habilitations**
- PSI-11**    **Critères de diffusion interne des informations**
- PSI-12**    **Critères de diffusion externe des informations**



# **PSSI - Principes de mise en œuvre**

## **Aspects humains**

**ASH-01** Notion de reconnaissance de responsabilité

**ASH-02** Clauses de sécurité dans les contrats de travail

**ASH-03** Adoption de critères de sélection du personnel travaillant sur les SI sensibles

**ASH-04** Principes généraux d'habilitation (nominative, incessible)

**ASH-05** Catégories d'habilitations

**ASH-06** Règles d'attribution et d'engagement (responsabilités)

**ASH-07** Volants de personnel (poste vital)

**ASH-08** Procédures d'habilitation pour les postes de travail sensibles

**ASH-09** Cloisonnement des postes de travail sensibles

**ASH-10** Délégation

# **PSSI – Principes techniques**

## **Identification/Authentication**

**AUT-01 Utilisation d'un même secret pour accéder à plusieurs services**

**AUT-02 Complétude des moyens d'authentification**

**AUT-03 Unicité de l'identité des utilisateurs**

**AUT-04 Délivrance et recouvrement des moyens d'authentification**

# PSSI - Références SSI

## Principaux documents de référence

**ISO 15408**

**Lignes directrices de l'OCDE**

**Codes d'éthique**

**Textes législatifs et réglementaires** (Atteintes aux personnes, atteintes aux biens, atteintes aux intérêts fondamentaux de la nation, terrorisme et atteintes à la confiance publique, atteintes à la propriété intellectuelle, disposition relatives à la cryptologie, dispositions relatives à la signature électronique)

**Autres textes au niveau national** (Protection des intérêts économiques, protection du secret, systèmes d'information, savoir-faire, cybersurveillance, etc.)

**Autres textes au niveau international** (Conseil de l'Europe, ONU)

# RGS – Référentiel général de sécurité

Le **Référentiel général de sécurité** (RGS) a été créé par l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. La version 1.0 du RGS date du 6 mai 2010, la version 2.0 est entrée en vigueur le 1<sup>er</sup> juillet 2014.

## Quelques dates

- Notification à la Commission Européenne, en application de la directive 98/34/CE, le 25 mars 2009.
- Publication du décret n°2010-112 du 2 février 2010, dit décret RGS, le 4 février 2010 au *Journal Officiel*.
- Publication le 18 mai 2010 au *Journal Officiel* de l'arrêté du 6 mai 2010, dit arrêté RGS, portant approbation de la première version du RGS.
- Annonce du 24 juin 2014 sur l'entrée en vigueur de la v.2.0 du RGS le 1<sup>er</sup> juillet.

# **RGS – Référentiel général de sécurité**

## **Documents constitutifs du RGS V1.0**

**Fonctions de sécurité (5) :** - Confidentialité, Authentification, Signature électronique, Authentification serveur, Cachet.

**Politiques de certification-type (6) :** Confidentialité, Authentification, Signature électronique, Authentification serveur, Cachet, Authentification et signature.

**Autres (3) :** Politique d'horodatage type, Variables de temps, Profils de certificats, CRLs, OCSP et algorithmes cryptographiques.

**Documents concernant l'utilisation de mécanismes cryptographiques dans les fonctions de sécurité (2) :** Mécanismes Cryptographiques, Gestion des clés cryptographiques, Authentification.

# RGS – Référentiel général de sécurité

La nouvelle version (v.2.0) a pour objectif de :

**Adapter** le Référentiel aux usages des autorités administratives, au contexte et aux nouvelles missions de l'ANSSI.

Permettre la **qualification** de nouveaux types de prestataires.

**Harmoniser** les annexes avec les nouvelles versions des **normes ETSI** correspondantes.

Corriger ou **préciser** certaines inexactitudes.

Rendre **plus lisibles** les différentes annexes.

**Référencer** les nouveaux textes de l'ANSSI.



# RGS – Référentiel général de sécurité

## Evolutions majeures du Référentiel

L'architecture générale et le contenu sont préservés.

La **première version** du RGS fixe essentiellement des règles destinées à **assurer la protection** des systèmes d'information. La **nouvelle version** intègre en complément :

- La nécessité d'assurer une **bonne hygiène informatique**
- Le besoin d'assurer la défense de ces systèmes par une surveillance visant à **détecter les attaques** et par la mise en œuvre de **réactions pré-planifiées**, notamment en cas de découverte de compromission du système. A titre d'exemple, les homologations devront prendre en compte non seulement les mesures de protection mises en place, mais aussi l'organisation et les mesures prises pour assurer cette défense.
- La nouvelle version intègre également le référentiel destinés à la **qualification des prestataires d'audit** de la sécurité des systèmes d'information

# **RGS – Référentiel général de sécurité**

## **Liste des documents constitutifs du RGS v2.0**

**Référentiel Général de Sécurité – version 2.0 – 25p.**

**RGS A1** – Règles relatives à la mise en œuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques -14p.

**RGS A2** – Politique de Certification Type « certificats électroniques de personne » - 89p.

**RGS A3** – Politique de Certification Type « certificats électroniques de services applicatifs » - 83p.

**RGS A4** – Profils de certificats /LCR/OCSP et Algorithmes Cryptographiques – 22p.

**RGS A5** – Politique d'horodatage Type – 34p.

**RGS B1** – Mécanismes cryptographiques – 63p.

**RGS B2** – Gestion des clés cryptographiques – 34p.

**RGS B3** – Authentification – 29p.

**Prestataires d'audit** de la sécurité des systèmes d'information. **Référentiel d'exigences** – 32p. **Qualification.**

# RGS – Référentiel général de sécurité

## Référentiel Général de Sécurité – Corps du RGS

Renforcer la confiance des usagers dans les services électroniques proposés par les autorités administratives

### Chapitre 1 – Mise en conformité

**Démarche en 5 étapes** (analyse des risques, objectifs de sécurité, choix et mise en œuvre des mesures, homologation de sécurité du SI, suivi opérationnel de la sécurité du SI)

Penser aussi :

- Aux clauses relatives à la **sécurité des contrats prestataires**.
- Au **facteur humain**.

### Chapitre 2 – Etapes de la mise en conformité

Référence à la norme **ISO/IEC 27005**

Domaines DIC avec ajout de l'**authentification** et de la **traçabilité**.

Importance du **suivi opérationnel**.

# **RGS – Référentiel général de sécurité**

## **Référentiel Général de Sécurité – Corps du RGS**

**Chapitre 3** – Règles relatives à la cryptographie et à la protection des échanges électroniques (et annexes B1, B2, B3)

- Certificats électroniques 3 niveaux (\*, \*\*, \*\*\*), 2 niveaux si à double usage.
- Confidentialité 3 niveaux (\*, \*\*, \*\*\*)
- ANSSI autorité racine de l'IGC/A.

**Chapitre 4** – Règles relatives aux accusés d'enregistrement et aux accusés de réception (A2, A3, A5, B1, B2)

**Chapitre 5** – Qualification des produits de sécurité et des prestataires de services de confiance

Elle peut être élémentaire (QE), standard (QS) ou renforcée (QR)

Qualification des prestataires de confiance (PSCO). Concerne les services de certification électronique et d'horodatage ainsi que l'audit de la sécurité des SI.

**Chapitre 6** – Validation des certificats par l'Etat.

# **RGS – Référentiel général de sécurité**

## **Référentiel Général de Sécurité – Corps du RGS**

### **Chapitre 7 – Recommandations relatives à l'application du référentiel**

- Organisation : responsabilités, système de management, politique de sécurité.
- Implication des instances décisionnelles.
- Adapter l'effort de protection aux enjeux.
- Adopter une démarche globale.
- Informer et sensibiliser le personnel.
- Prendre en compte la sécurité dans les contrats et les achats.
- Prendre en compte la sécurité dans les projets d'externalisation et d'informatique en nuage.
- Mettre en place des mécanismes de défense des systèmes d'information.
- Utiliser les produits et prestataires labellisés pour leur sécurité.
- Elaborer des plans de traitement d'incidents ainsi que de continuité et de reprise d'activité.
- Procéder à des audits réguliers de la sécurité du SI.
- Réaliser une veille sur les menaces et les vulnérabilités.
- Favoriser l'interopérabilité.

# **RGS – Référentiel général de sécurité**

## **Référentiel Général de Sécurité – Corps du RGS**

**Chapitre 8** – Transition entre la première et la deuxième version du RGS.

**Chapitre 9** – Liste des annexes du RGS

- Annexes de type A sur l'utilisation de certificats électroniques
- Annexes de type B sur l'utilisation de mécanismes cryptographiques
- Référentiel d'exigences applicables aux prestataires d'audit de la SSI.

**Chapitre 10** – Références documentaires

- Références réglementaires
- Références techniques

# RGS – Référentiel général de sécurité

## Référentiel Général de Sécurité – Annexe B3

### Authentification – version de janvier 2010

#### Notions sur l'**authentification**

- vérification de l'identité d'une entité, donc toujours combinée à une identification
- Ce que l'on sait, ce que l'on a, ce que l'on est, ce que l'on sait faire
- Les états : initial, connexion, session authentifiée, déconnexion
- Distinction entre l'authentification de machines et l'authentification de personnes
- Cas du mot de passe à usage unique

#### **Règles et recommandations** concernant les mécanismes d'authentification

# **RGS – Référentiel général de sécurité**

## **L'homologation de sécurité en neuf étapes simples**

### **Présentation de la stratégie d'homologation**

#### **Etape 1 – Quel système d'information homologuer et pourquoi ?**

##### **Référentiel applicable :**

- IGI 1300 (informations classifiées de défense)
- RGS (échanges entre autorité administrative et usager ou entre autorités administratives)
- PSSIE (Politique de Sécurité des Systèmes d'Information de l'Etat) pour les systèmes des administrations de l'Etat

##### **Périmètre :**

- Eléments fonctionnels et d'organisation
- Eléments techniques
- Périmètre géographique et physique

##### **Questions :**

- Eléments non maîtrisés ? Doivent de préférence faire l'objet d'une labellisation de sécurité (qualification ou à défaut certification)



# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 2 – Quel type de démarche mettre en œuvre ?

Estimer les **enjeux** et en déduire la profondeur de la démarche

**Annexe 1** - Estimation rapide du **besoin de sécurité** d'un système d'information (15 questions ; si plus de 2 « je ne sais pas », se faire aider ; niveau faible, moyen ou fort)

**Annexe 2** – Estimation rapide du **niveau de maturité** d'un organisme (1 question, niveau élémentaire ; 5 questions, niveau moyen ; 7 questions, niveau avancé)

4 types de démarche (par croisement des deux niveaux) :

**Pianissimo** : démarche autonome

**Mezzo-piano** : démarche autonome approfondie

**Mezzo-forte** : démarche assistée approfondie (assistance conseil externe)

**Forte** : hors-champ du guide

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 3 – Qui contribue à la démarche ?

**Autorité d'homologation** : personne physique qui prononce l'homologation de sécurité (niveau de direction de l'organisme)

**Commission d'homologation** : assiste l'autorité d'homologation. Sa taille et sa composition dépendent du système et des enjeux.

Les **acteurs** de l'homologation

- Maîtrise d'ouvrage
- RSSI
- Responsable d'exploitation du système
- Les prestataires
- Les systèmes interconnectés

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 4 – Comment s'organise-t-on... ?

**Contenu du dossier d'homologation** : varie selon le type de démarche. (**Stratégie d'homologation**, référentiel de sécurité, **risques identifiés et objectifs de sécurité**, politique de sécurité des systèmes d'information, **procédures d'exploitation sécurisée du système**, journal de bord de l'homologation, certificats de qualification des produits ou prestataires, résultats d'audits, **liste des risques résiduels, décision d'homologation**) Avec **compléments** pour les **systèmes déjà en service** (tableau de bord des incidents et de leur résolution, résultats d'audits intermédiaires, journal des évolutions du système)

**Planning** : en amont, lié à celui du projet. Les échéances des étapes de la démarche d'homologation doivent figurer dans le planning (dont début et fin de l'analyse de risques, remise des différents documents du dossier, réunions de la commission, audits éventuels).

**Questions** : nécessité d'un audit (autorité d'homologation)

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 5 - Risques pesant sur le système (1/2)

**Analyse de risques** (combinaison d'un élément redouté et d'un scénario de menaces) : L'analyse peut être simplifiée pour le niveau pianissimo, pour les autres niveaux, méthode éprouvée à privilégier.

**Pianissimo** : Liste des menaces courantes en annexe 4. Conserver celles pertinentes. Pour chacune, biens essentiels pouvant être affectés. Impact DIC pour chaque lien, fournit un scénario de risque. Hiérarchiser les scénarios (probabilité, impact). Si un impact très fort apparaît, l'étape 2 est à revoir, envisager une démarche plus élevée.

**Mezzo-piano, mezzo-forte** : **EBIOS 2010**, via l'autorité d'homologation, **FEROS**.

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 6 – La réalité correspond-elle à l'analyse ?

Mesure de l'écart entre les résultats de l'étude et la réalité. Selon le niveau de la démarche, de vérification peu formelle à audit complet. Trace écrite nécessaire. Eventuel rapport d'audit intégré au dossier d'homologation.

**Pianissimo** : Audit technique optionnel.

**Piano** : Audit formalisé recommandé sur les parties les moins maîtrisées.

**Mezzo-forte** : Audit technique du système d'information fortement recommandé.

Les audits sont à mener sur un périmètre soigneusement défini selon le référentiel ANSSI d'exigences relatif aux prestataires d'audit de la sécurité des systèmes d'information. Dans certains cas, des **tests d'intrusion** peuvent être effectués.

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 7 - Quelles mesures de sécurité mettre en œuvre pour couvrir ces risques ?

**Traitement du risque** : Eviter, réduire, assumer, transférer. Plusieurs choix possibles pour un même risque.

**Mise en œuvre des mesures** : Elles peuvent être techniques, organisationnelles ou juridiques. Elles sont décidées par l'autorité d'homologation sur proposition de la commission.

**Définition du plan d'action** : Les risques résiduels sont identifiés dans le plan d'action. Celui-ci indique les vulnérabilités éventuelles, leur degré, l'action correctrice envisagée, le pilote désigné et l'échéance associé.

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### Etape 8 – Comment réaliser la décision d'homologation ?

**Accepter les risques résiduels** : l'autorité d'homologation signe une attestation formelle autorisant la mise en service du système d'information, du point de vue de la sécurité. Si problème, **APE** (Autorisation Provisoire d'Emploi)

**Périmètre** : géographique et physique, fonctionnel et organisationnel, technique, référentiel réglementaire, pièces du dossier.

**Conditions d'exploitation** et plan d'action.

**Durée** : 5 ans avec revue annuelle. Si risques résiduels nombreux ou très nombreux, trois ans, voire un an.

**Conditions de suspension ou de retrait** : modification du contexte

# RGS – Référentiel général de sécurité

## L'homologation de sécurité en neuf étapes simples

### 9 – Qu'est-il prévu pour continuer d'améliorer la sécurité ?

**Procédure de révision périodique** de l'homologation par la commission.

**Plan d'action** pour traiter les **risques résiduels**

**Veille technologique** pour identifier les **nouvelles vulnérabilités** qui apparaissent. En cas de fort impact sur le système, relancer le processus d'homologation.

En **conclusion**, un ensemble de **conseils** pratiques (généraux, avant et pendant l'étude) est fourni.

**Quatre annexes** : estimation rapide du besoin de sécurité, estimation rapide de la maturité, liste de documents du dossier d'homologation (20), liste de menaces (issues de la base EBIOS)



# Méthode EBIOS

Méthode créée en 1995 et maintenue depuis par le **SCSSI** devenu la **DCSSI** puis l'**ANSSI**.

Depuis 2000, **convergence** vers **les principales normes** internationales du domaine : ISO 15408, ISO 31000 et Guide ISO 73, ISO série 2700x... En 2003, création d'un **Club utilisateurs** et mise à jour des bases de connaissances.

Prise en compte d'approches issues de la qualité (ISO 9000) comme la « roue de Deming » : **PDCA** (Plan, Do, Check, Act) ou Planifier, Mettre en œuvre, Vérifier et Améliorer.

Parution d'une **nouvelle version en 2010**, compatible avec le **RGS**. La **présentation d'EBIOS sur le site de l'ANSSI** se compose de :

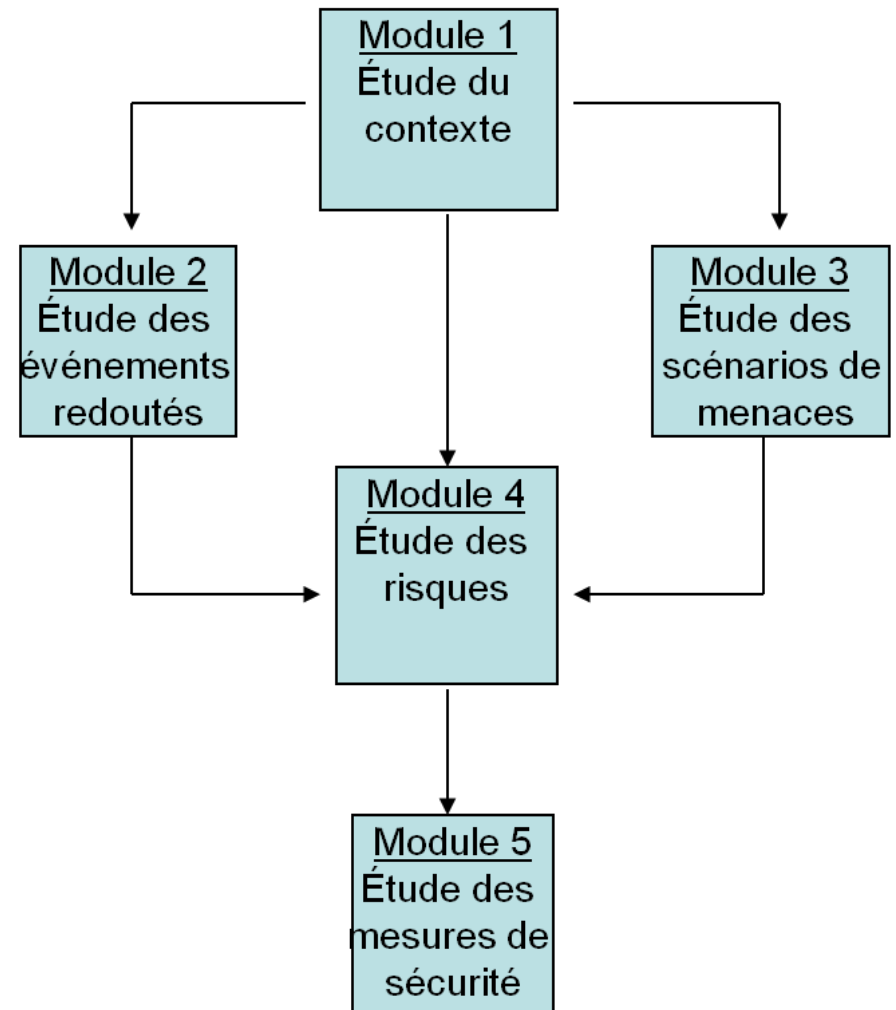
**Guides** : Méthodologie, Base de connaissances, Etude de cas (Archimed), Plaquette méthode, Plaquette RSSI.  
**Logiciel**.

# Les étapes d'EBIOS

Une méthode de gestion des risques **souple** permettant une présentation hiérarchique des risques pesant sur le patrimoine informationnel.

Elle permet de déterminer les **biens essentiels** et les **biens supports** associés,

La démarche est **itérative** : il est fait appel plusieurs fois à chaque module pour une amélioration progressive du contenu et la démarche globale est aussi tenue à jour de manière continue (PDCA).



# Étude du contexte

Délimiter et décrire le **périmètre** de l'étude.

Définir les **métriques**.

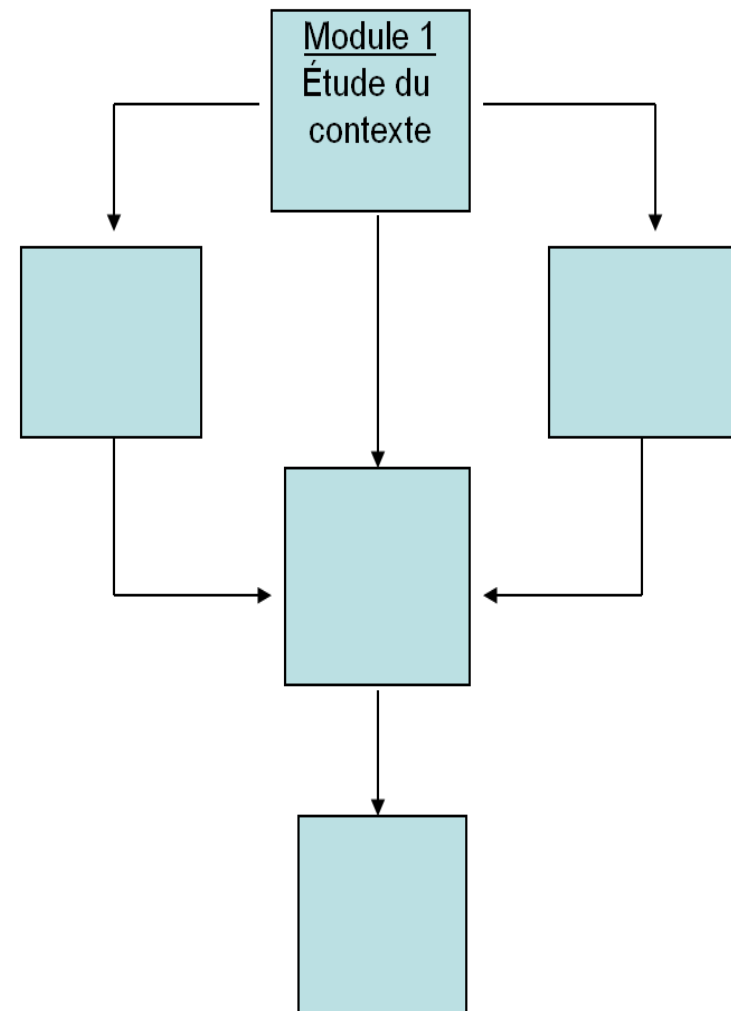
Identifier les **biens essentiels** et les **biens supports**.

## Activités :

Définir le **cadre** de la gestion des risques.

Préparer les **métriques**.

Identifier les **biens**.



# Expression des besoins

**Apprécier** les risques.

Estimer les besoins de sécurité des **biens essentiels**.

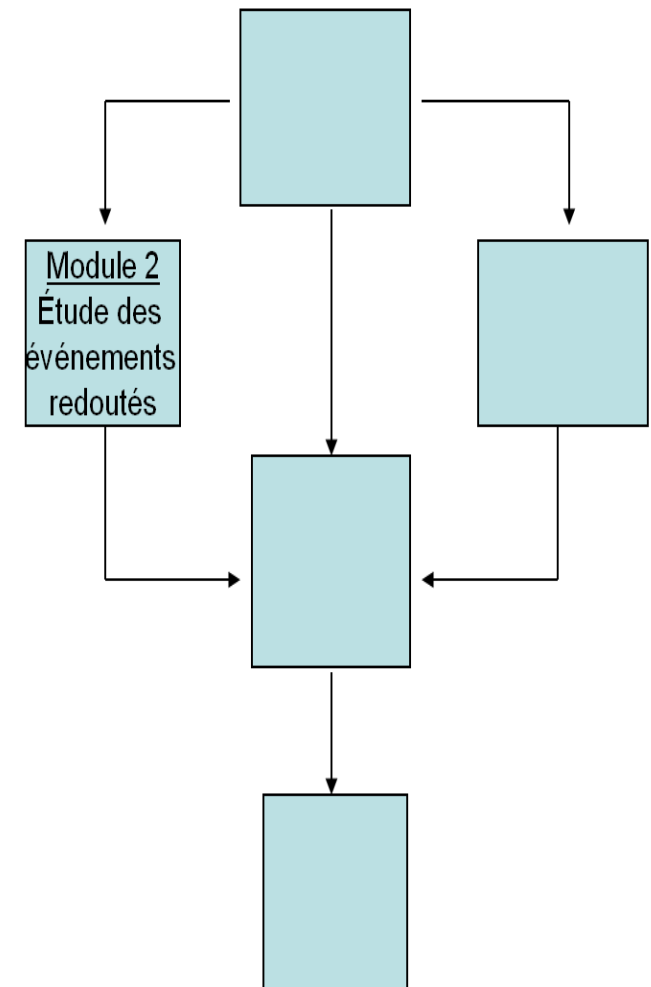
Mettre en évidence les **sources de menaces**.

Recenser les éventuelles mesures de sécurité existantes.

**Identifier**, expliciter et **positionner** les **événements redoutés** en terme de gravité et de vraisemblance.

**Activités :**

Apprécier les **événements redoutés**.



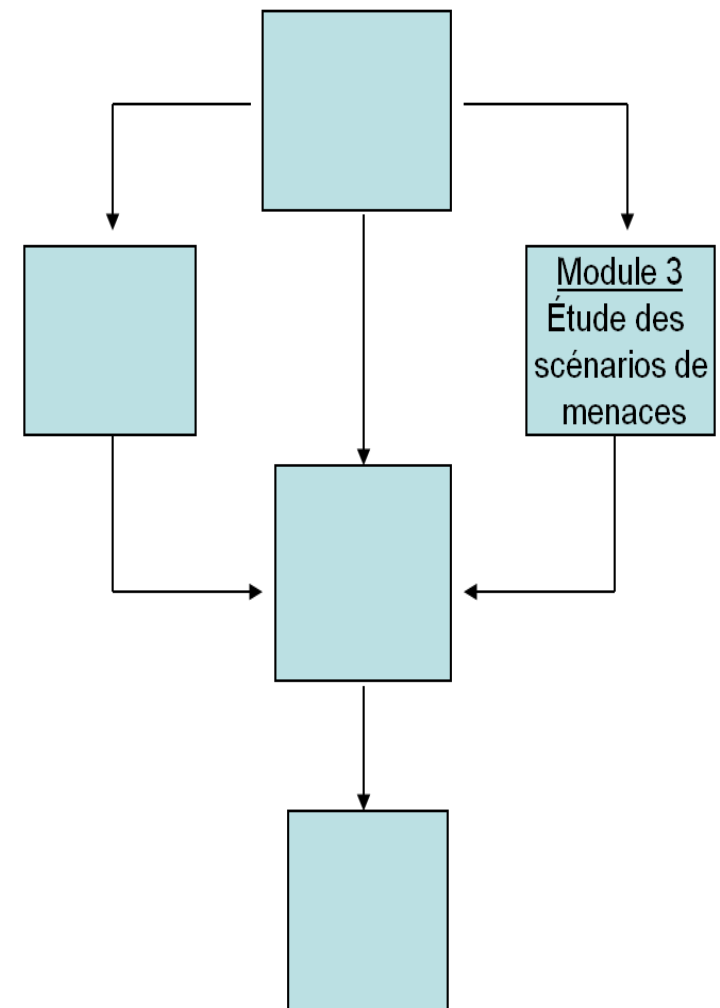
# Étude des menaces

**Identifier et estimer les scénarios** pouvant engendrer les événements redoutés.

Étudier les **menaces** que peuvent générer les sources de menaces et les **vulnérabilités** exploitables des biens supports.

**Activités :**

Apprécier les **scénarios** de menaces.



# Identification des objectifs

Mettre en évidence les **risques** pesant sur l'organisme par confrontation des événements redoutés aux scénarios de menaces.

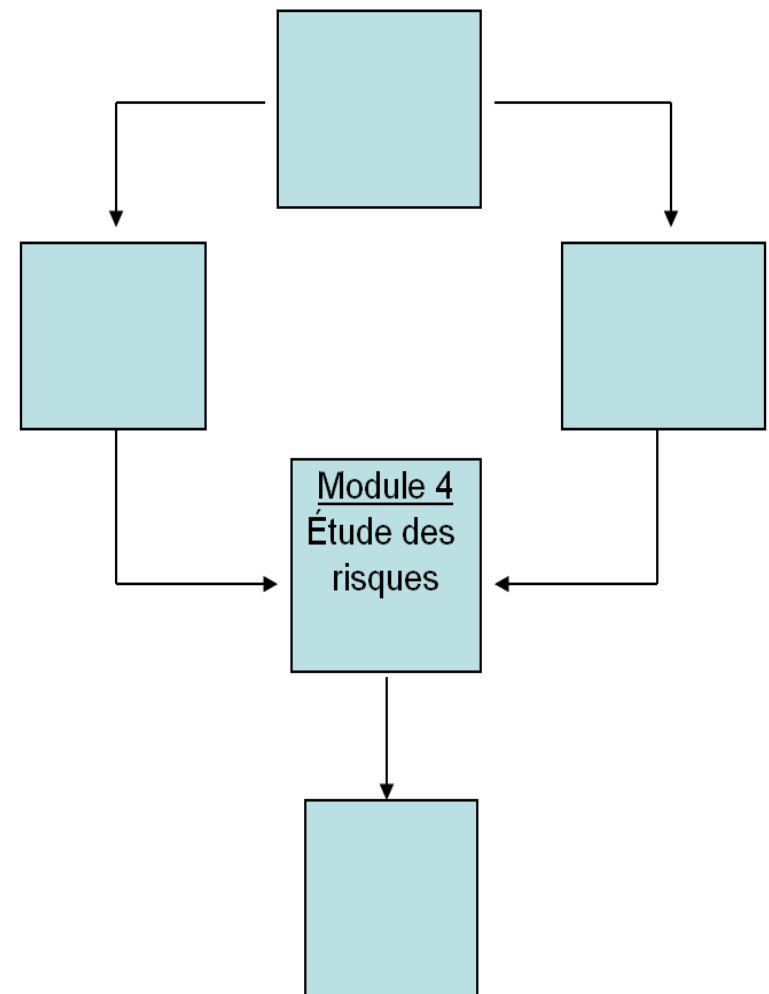
**Estimer et évaluer les risques.**

**Identifier les objectifs de sécurité.**

**Activités :**

**Apprécier les risques.**

**Identifier les objectifs de sécurité.**



# Exigences de sécurité

**Spécifier les mesures de sécurité** à mettre en œuvre.

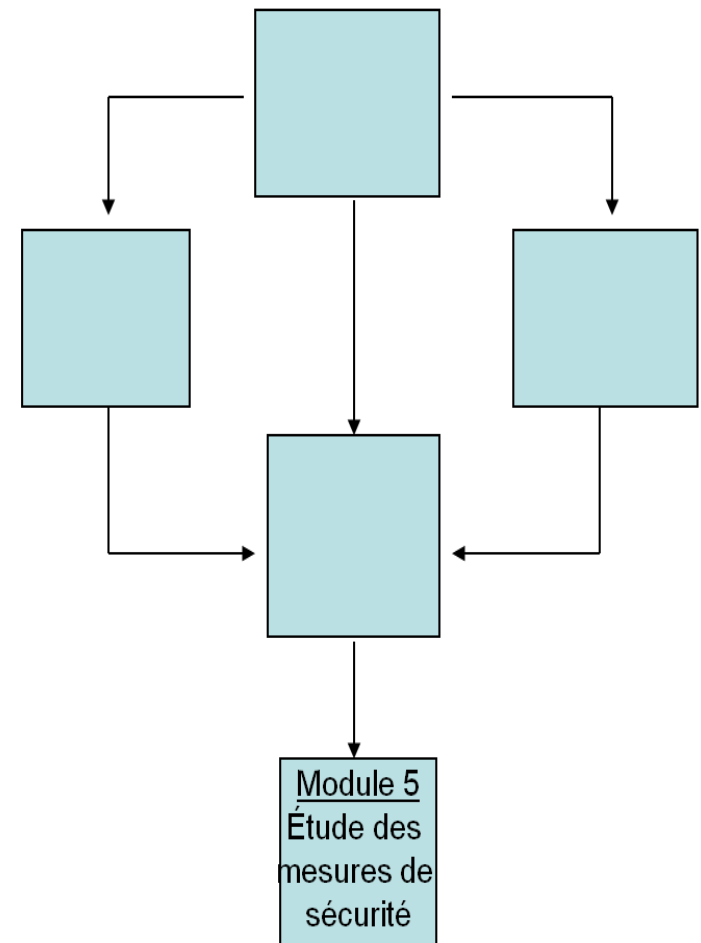
Planifier la **mise en œuvre** des mesures.

**Valider le traitement des risques** et les **risques résiduels**.

**Activités :**

**Formaliser** les mesures de sécurité à mettre en œuvre.

**Mettre en œuvre** les mesures de sécurité.



# Résultats d'EBIOS

Le but premier d'EBIOS est d'identifier des objectifs et des exigences de sécurité suite à une analyse de risques.

En utilisant les résultats des différentes étapes, on peut obtenir comme résultat :

- une **politique de sécurité**, un **plan de sécurité**, un **schéma directeur SSI**,
- des **spécifications** pour une **MOA**,
- une **FEROS** (Fiche d'Expression Rationnelle des Objectifs de Sécurité),
- un **profil de protection** au sens de l'**ISO 15408**.

EBIOS permet aussi de contribuer à des démarches globales, il facilite l'implication et la responsabilisation des acteurs.

Il fournit aussi un langage, une approche cohérente et est compatible avec les principales normes internationales.



# Logiciel EBIOS

Un **logiciel** associé à **EBIOS** est disponible et gratuitement téléchargeable sur le site de l'ANSSI. Il correspond à la **mise en œuvre de la méthode** et permet :

- de **consigner les résultats** des études,
- de **préparer des documents de synthèse** (FEROS, PSSI, note stratégique de SSI...).
- de **personnaliser les bases de connaissances** liées à la méthode.

Noter l'existence d'un produit développé par la société **Fidens**.

# ISO 27002:2013 - Historique

## Origine

A l'origine de cette norme, on trouve la **BS 7799**, standard britannique développé au début des années 1990 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*.

Une première tentative de normalisation à l'ISO 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.

Elle est devenue l'ISO/CEI 27002 en juillet 2007.

Elle est entrée en révision (conjointement avec l'ISO/CEI 27001) en 2008.

La nouvelle version est parue en octobre 2013.

# ISO 27002:2013 - Champ

## Code of practice for information security management

**Champ** : L'**information** est un actif important qu'il convient de **protéger** de façon appropriée quelle que soit sa **forme** (écrite ou orale, électronique ou visuelle,...) ou son **support**.

La **sécurité de l'information** traite **au moins les trois aspects** suivants :

**Confidentialité** : S'assurer que l'information n'est accessible que par ceux qui y sont autorisés.

**Intégrité** : Préserver la pertinence et la complétude des informations et des moyens de traitement.

**Disponibilité** : S'assurer que les utilisateurs autorisés ont accès aux informations et aux supports associés quand il le faut.

# ISO 27002:2013 – Principes

## Les Principes

### Définir les exigences de sécurité : Trois sources

Environnement légal, réglementaire et contractuel,  
Évaluation des risques,  
Références internes à l'entreprise.

### Choisir les références des contrôles :

Au plan **législatif** (droits d'auteur, traces, protection des données et informations nominatives).

En tant que **documents internes de bonne pratique** (politique de sécurité, définition des responsabilités, plans de formation et de sensibilisation, recensement des incidents de sécurité, plans de continuité de l'activité).

Quatorze chapitres de recommandations.

# ISO 27002:2013 – Ch. 5 et 6

## Ch.5 Politiques de sécurité de l'information

Définition des politiques de sécurité,  
Revue des politiques de sécurité.

## Ch.6 Organisation de la sécurité de l'information

Rôles et responsabilités,  
Séparation des tâches,  
Contacts avec les autorités,  
Contacts avec les groupes d'intérêt spécifiques,  
Sécurité de l'information en gestion de projet,  
Dispositifs mobiles et télétravail.

# ISO 27002:2013 – Ch. 7

## Ch.7 Sécurité en ressources humaines

**Avant emploi** (Screening, conditions d'emploi)

**Pendant emploi** (Responsabilités managériales, sensibilisation et formation, processus disciplinaire)

**Fin ou changement d'emploi** (responsabilités)

# ISO 27002:2013 – Ch. 8

## Ch.8 Gestion des actifs/biens

**Responsabilités** concernant les **biens/actifs** (inventaire, détermination d'un **propriétaire**, utilisation acceptable, restitution)

**Classification** de l'information (classification de l'information, étiquetage, manipulation)

Gestion des **supports** (supports amovibles, fin de vie, transport)

.

# ISO 27002:2013 – Ch. 9 et 10

## Ch.9 Contrôle d'accès

**Exigences business** (politique de contrôle d'accès, accès aux réseaux et aux services réseaux)

**Gestion des accès utilisateurs** (enregistrement et désenregistrement, allocations, gestion d'accès privilégiés, gestion d'information secrètes d'authentification, revue de droits, ajustement ou suppression de droits)

**Responsabilités des utilisateurs** (utilisation d'informations secrètes)  
**Contrôle d'accès aux applications et systèmes** (restriction d'accès, procédures sûres de log-on, système de gestion de mots de passe, utilisation de programmes à privilège, contrôle d'accès aux programmes source)

## Ch.10 Cryptographie

**Politique** sur l'utilisation de moyens cryptographiques,

**Gestion de clé.**



# ISO 27002:2013 – Ch. 11

## Ch.11 Sécurité physique et environnementale

### Aires de sécurité

Périmètre de sécurité physique,  
Mesures d'**accès physiques**,  
Sécurisation des **bureaux, pièces et installations**,  
Protection contre les **menaces externes et environnementales**,  
Travail dans des aires de sécurité,  
**Aires de livraison ou d'expéditions**.

### Équipement

Protection de site et d'équipement,  
Soutien aux **infrastructures**,  
Sécurité du **câblage**,  
Maintenance de l'équipement,  
Enlèvement, mise au rebut,  
Sécurité des biens et équipements hors-sites,  
Enlèvement ou réutilisation sûre d'équipement,  
Équipement non surveillé,  
Politiques de **bureau net** et d'écran de veille.

# ISO 27002:2013 – Ch. 12

## Ch.12 Sécurité opérationnelle

**Responsabilités et procédures opérationnelles** (procédures documentées, changement de management, capacité du management, séparation des environnements de développement, de tests et opérationnels)

**Protection contre les malwares,**

**Backup,**

**Supervision et enregistrement d'événements,**

**Contrôle des logiciels opérationnels,**

**Gestion des vulnérabilités techniques,**

**Considérations sur l'audit des systèmes d'information.**

# ISO 27002:2013 – Ch. 13

## Ch.13 Sécurité des communications

### Gestion de la sécurité des réseaux

Réseaux,  
Services,  
**Séparation** des réseaux.

### Transfert d'informations

**Politique et procédures,**  
Accords sur les transferts d'informations,

**Messagerie électronique,**  
Accords de confidentialité.

# ISO 27002:2013 – Ch. 14

## Ch.14 Acquisition, développement et maintenance de systèmes

### Exigences de sécurité sur les systèmes d'information

**Analyse et spécification d'exigences** en sécurité de l'information,  
Sécurisation de services applicatifs sur les réseaux publics,  
Protection des transactions dans les services applicatifs.

### Sécurité dans les processus de développement et de soutien

Procédures de contrôle lors des **changements de systèmes**,  
Revue technique des applications après changement de plateforme opérationnelle,  
Restrictions sur les changements de packages logiciels,  
Principes d'ingénierie de systèmes sûrs,  
Environnement sûr de développement,  
**Développement externalisé**,  
Test de sécurité des systèmes,  
Test d'acceptation de systèmes.

### Données de test

# ISO 27002:2013 – Ch. 15

## Ch.15 Relations avec les fournisseurs

### Sécurité de l'information dans les relations avec les fournisseurs

Politique de sécurité de l'information pour les relations avec les fournisseurs,  
Traitement de la sécurité dans les accords avec les fournisseurs,  
Technologie de communication et de l'information pour la **supply chain**.

### Gestion de la fourniture de service

Supervision et revue des services fournisseurs,  
Gestion des changements dans les services de fournisseurs

Considérer aussi l'**ISO/CEI 27036** (*Information security for supplier relationships*) en 4 parties.

# ISO 27002:2013 – Ch. 16

## Ch.16 Gestion d'incident en sécurité de l'information

**Responsabilités et procédures,**  
**Rapports d'événements** en sécurité de l'information,  
Rapport sur des faiblesses en sécurité de l'information,  
Estimation et décision suite à des événements de sécurité de l'information,  
**Réponse** à des incidents de sécurité de l'information,  
**Leçon à tirer** des incidents de sécurité de l'information,  
Gestion des preuves.

Noter l'existence d'**autres normes** sur ce thème comme l'**ISO/CEI 27035**.

# ISO 27002:2013 – Ch. 17

## Ch.17 Gestion de la continuité en sécurité de l'information

### Continuité de la sécurité de l'information

**Planification** de la continuité,

**Mise en œuvre** de la continuité de la sécurité de l'information,

**Vérification**, revue et évaluation de la continuité en sécurité de l'information.

### Redondances

Disponibilité de ressources de traitements de l'information.

Sur ce thème, on dispose aussi de l'**ISO/IEC 27031** et surtout de l'**ISO 22301**, issue du TC 223 sur la sécurité sociétale et du citoyen.

# ISO 27002:2013 – Ch. 18

## Ch.18 Conformité

### Conformité aux contraintes légales et contractuelles

Identification des **exigences légales et contractuelles** applicables

Droits en matière de **propriété intellectuelle**

Protection des **enregistrements**

**Privacy** et protection des informations d'identification personnelle (PII)

Réglementation sur les **mesures cryptographiques**

### Revue de sécurité de l'information

Revue indépendante de la sécurité de l'information

Conformité avec les politiques et normes de sécurité

Revue de conformité technique



# Certification et conformité

De nombreuses **méthodes d'évaluation** existent dans différents pays (France : EBIOS, MARION, MEHARI ; Grande Bretagne : CRAMM ; USA : Octave, COBRA, FIPS,...). On note aussi une tendance à l'apparition de **normes** traitant de la sécurité de l'information.

Cette évolution tend à faire passer la responsabilité de la **sécurité de l'information** de la direction informatique à la **direction générale** (globalité, transversalité) et à poser la question des « **propriétaires** » de l'information.

Elle tend aussi à faire définir des **niveaux de sensibilité de l'information**, lesquels facilitent ensuite l'évaluation de la sécurité des informations selon divers critères (Disponibilité, Intégrité, Confidentialité mais aussi Traçabilité, Imputabilité, Non-Répudiation,...)

# Certification et conformité

La **certification** est aussi en évolution. A l'origine, on trouve essentiellement une approche qualité et la vérification par un **tiers de confiance** de la conformité à un référentiel (par exemple **ISO 9000**), lequel tiers certifie ensuite cette conformité..

L'**ISO 27001**, en lien avec l'**ISO 27002**, fait apparaître un schéma (et une approche) voisin de la **qualité**. Elle correspond à de nombreux besoins, en particulier sur la communication en matière de sécurité et peut se révéler suffisamment rapide et d'un coût modéré.

Enfin, la certification tend à pouvoir porter sur **des produits ou des systèmes** (**Critères Communs** – ISO/CEI 15408 ou **CSPN** – Certification de Sécurité de Premier Niveau en France) , des organisations ou des individus.

Notons en particulier le cas de la norme **ITIL/ISO 20000**, de la norme **ISO 28000** sur la *supply chain* et de l'**ISO 26000** sur la responsabilité sociétale (cette dernière ne conduisant pas en principe à une certification).