LA METHODE EBIOS

Anas ABOU EL KALAM

I. EVOLUTION DE LA SSI

- *L'évolution de la terminologie :*
  - sécurité informatique ;
  - sécurité des systèmes d'information ;
  - sécurité de l'information ;
  - système de sécurité de l'information.

- *La SSI doit être considérée globalement*
  - en tenant compte de toutes les ressources ;
  - en étant prise en compte au plus haut niveau hiérarchique ;
  - en étant prise en compte au plus tôt dans la gestion des projets.

I. LE DEVELOPPEMENT DES METHODES SSI

- *De nouveaux besoins :*
  - formalisation, retour d'expérience
  - uniformisation, standardisation
  - qualité

- *Enrichissement des méthodes*
  - de nombreuses méthodes éprouvées approfondissent leurs bases de connaissances, développent les domaines d'application, sont complétées par des outils logiciels

- *Multiplication des méthodes*
  - adaptées à des domaines ou contextes spécifiques
  - parfois concurrentes (idées divergentes ou raisons commerciales)

I. Les méthodologies de sécurité

- *Mehari, Marion, Melisa, INCAS, CRAMM, BS7799, EBIOS, RFC 1244*

- Réalisées par des utilisateurs ayant des compétences techniques de sécurité ou des groupes de travail

- Souvent applicables par des prestataires de service sous forme
  - d'audit de sécurité
  - d'analyse de risques

- Base ➔ propositions d'actions pour améliorer la situation

ttp://www.securite.teamlog.com/publication/4/5/167/index.html

1. Généralités
2. CC et autres méthodes d'évaluation
3. La méthode EBIOS

CRITERES COMMUNS

Common Critéria for Information Security Evaluation

ISO 15408

2. Critères communs

- *But*
  - ***fournir aux utilisateurs des indications sur les produits de sécurité en terme de « degré de confiance »***
    - ⇒ Vérification analyse et teste des *fonctionnalités* de sécurité offertes par le produit,
    - ⇒ Vérification analyse et teste *processus conception* & *développement*.

Certificat délivré par DCSSI « ***atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises*** » [décret 2002-535].

2. Critères communs

- *Pays*
  - ***15 pays reconnaissent ce standard***
    - Seuls, l'Australie, Canada, France, Allemagne, RU et EU sont habilités à délivrer un certificat.
    - La Finlande, Grèce, Italie, Israël, Japon, Hollande, Norvège et l'Espagne prennent en compte les CC sans toutefois pouvoir délivrer, eux-mêmes, des certificats.
- *3 parties*
  - Introduction et modèle général
    - Concepts, Profils de Protection, Cible d'Evaluation, …
  - Exigences fonctionnelles de sécurité
    - *listes de fonctions* de sécurité à remplir
  - Exigences d'assurance de sécurité
    - techniques employées pour la vérification

2. Critères communs : PARTIE I

- définit les concepts généraux
- présente un modèle général de l'évaluation
  - évaluation de PP - *Profil de Protection*,
  - évaluation d'une ST - Security Target ou *Cible de Sécurité*
  - évaluation d'une TOE – *Cible d'Evaluation*
- *PP*
  - contient les exigences de sécurité avec la *vision utilisateur*.
    - ⇒ *indépendant de toute implémentation*.
  - contient description de la TOE, de son environnement (tech et org) d'exploitation, des menaces, ….
    - ⇒ fournit *objectifs de sécurité* & *exigences fonctionnelles* que les utilisateurs souhaitent voir intégrer dans un type de produit (e.g., firewall) ou système

2. Critères communs : PARTIE I

Tous les produits mettant en œuvre des fonctions de sécurité peuvent être évalués

- *cible d'évaluation*
  - Produit ou système soumis à une évaluation de la sécurité
    - Souvent définit par l'industriel

- *cible de sécurité*
  - spécification de besoin de sécurité
    - ⇒ un produit est évalué selon sa cible de sécurité
  - contient les exigences de sécurité avec la ***vision développeur***
    - ⇒ *inclut les spécifications* des fonctions sécurité … *(voir PP) dédiés à la cible d'évaluation*
    - ⇒ Spécifie menaces qui pèsent sur ces objectifs
    - ⇒ Spécifie mécanismes de sécurité qui seront employés.

2. Critères communs : PARTIE II

comprend l'∑ exigences fonctionnelles exprimées dans PP ou ST

exigences sont réparties suivant classes

classes décomposées en familles de composants

- *11 classes (fonctionnalités)*
  - Audit de sécurité (classe FAU)
  - Communication (classe FCO)
  - Support cryptographique (classe FDP)
  - Protection des données de l'utilisateur (classe FDP)
  - Identification et authentification (classe FIA)
  - Administration de la sécurité (classe FMT)
  - Protection de la vie privée (classe FPR)
  - Protection des fonctions de sécurité de la TOE (classe FPT)
  - Utilisation des ressources (classe FRU)
  - Accès à la TOE (classe FTA)
  - Chemins et canaux de confiance (classe FTP)

2 Critères communs : PARTIE II

- *Exemple : famille de la classe FAI*
  - FIA_AFL pour les échecs de l'authentification
  - FIA_ATD pour la définition des attributs des utilisateurs
  - FIA_SOS pour la spécification des secrets
  - FIA_UAU pour l'authentification de l'utilisateur
  - FIA_UID pour l'identification de l'utilisateur
  - FIA_USB pour le lien utilisateur-sujet

- *Exemple : composants de la famille FIA_UAU*
  - La programmation de l'authentification (FIA_UAU.1)
  - L'authentification de l'utilisateur avant toute action (FIA_UAU.2)
  - L'authentification infalsifiable (FIA_UAU.3)
  - Les mécanismes d'authentification à usage unique (FIA_UAU.4)
  - Les mécanismes d'authentification multiple (FIA_UAU.5)
  - La réauthentication (FIA_UAU.6)
  - L'authentification avec retours protégés (FIA_UAU.7)

… si l'U demande que le produit intègre des mécanismes d'auth multiples, il faudra inclure dans PP ou ST le composant FIA_UAU.5

2. Critères communs : PARTIE III

- Définit les critères d'évaluation en termes
  - d'exigences pour le développeur et
    - éléments de preuve que le développeur du produit doit fournir à l'évaluateur
  - de tâches pour l'évaluateur.
- Critères répartis en classes d'assurance puis familles de composants

- *10 classes (assurances)*
  - Évaluation d'un profil de protection (classe APE)
  - Évaluation d'une cible de sécurité (classe ASE)
  - Gestion de configuration (classe ACM)
  - Livraison et exploitation (classe ADO)
  - Développement (classe ADV)
  - Guides (classe AGD)
  - Support au cycle de vie (classe ALC)
  - Tests (classe ATE)
  - Estimation des vulnérabilités (classe AVA)
  - Maintenance de l'assurance (classe AMA)

2. Critères communs : PARTIE III

- Cette partie fournit aussi pour chaque niveau d'évaluation (EAL1 à EAL7 pour Evaluation Assurance Level) l'ensemble des composants d'assurance nécessaire à l'atteinte de ce niveau.

- *Exemple*
  - pour EAL1 : les classes ALC et AVA ne sont pas demandées.
  - pour EAL1 à EAL3 : le code source n'est pas analysé
  - à partir du niveau EAL4 : le code source est requis.
  - niveaux plus élevés : nécessité de preuves formelles pour certains critères.

3. Méthode M.E.L.I.S.A

(Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'informations)

Délégation générale à l'armement 1985.

MELISA est une méthode d'analyse de vulnérabilités qui fut mise au point par la DGA (Direction Générale des Armements) et qui a été reprise par la société CF6. http://www.cf6.fr/fr/accueil.htm

MELISA S - Confidentialité des données sensibles
MELISA P - Pérennité de fonctionnement du système
MELISA M - Sécurité micro mini informatique
MELISA. R - Sécurité réseau

http://www.securite.teamlog.com/publication/4/5/index.html

4. La méthode MARION « Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau »

- *Quoi ?*
  - méthodologie d'audit du Clusif dernière maj 1998
  - permet d'évaluer le niveau de sécurité d'une ent/se (risques) au travers de *questionnaires pondérés* donnant des *indicateurs* sous la forme de notes dans ≠ thèmes concourrant à la sécurité
  - obtenir une vision de l'entreprise auditée
    - / à un niveau jugé " correct ",
    - / aux Ent/se ayant répondu au même questionnaire

- *Comment ?*
  - niveau de sécurité évalué suivant 27 indicateurs répartis en 6 grands thèmes, chacun d'eux se voyant attribuer une note de 0 à 4,
    - niveau 3 = niveau à atteindre pour assurer sécurité correcte
  - À l'issue de cette analyse ➔ réalisation analyse de risque

4. La méthode MARION

- *Fonctionnement*
  - Questionnaires ➔ permettre d'évaluer les vulnérabilités
  - Pondération réponses ➔ évaluation indicateurs
  - *Thèmes*
    - Sécurité organisationnelle / Sécurité physique
    - Sécurité logique et exploitation / Sécurité des applis …
  - *Phases*
    - Phase 0 : préparation
      - Objectifs, champ d'action, découpage fonctionnel
    - Phase 1 : Audit des vulnérabilités
      - déroulement questionnaires recensement contraintes
    - Phase 2 : Analyse des risques
      - identification risques, impact et potentialité des risques
    - Phase 3 : Plan d'action
      - analyse moyens MEO afin atteindre niveau sécurité « correcte », tâches, degré d'amélioration à apporter, chiffrage coût mise en conformité.

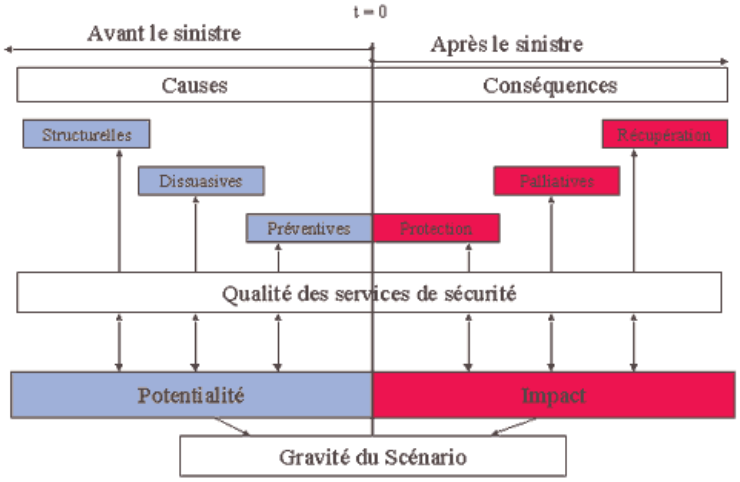
5. MEHARI : MEthode Harmonisée d'Analyse de RIsques

- *Quoi ?*
  - Méthode (du Clusif) permettant
    - ⇒ analyse rigoureuse et une évaluation quantitative des *facteurs de risque* propres à chaque situation,
    - ⇒ concilier les *objectifs stratégiques* et les nouveaux *modes de fonctionnement* de l'entreprise avec une politique de maintien des risques à un niveau convenu.
- *Idées de base ?*
  - ⇒ *analyse des vulnérabilités*
  - ⇒ lien entre *vulnérabilité* existante & *risques encourus*
  - ⇒ la présence (ou l'absence) de *mesures de sécurité* va réduire (ou non), soit la potentialité de survenance d'un sinistre, soit son impact
  - ⇒ L'interaction de ces types de mesures concoure à *réduire la gravité du risque* jusqu'au niveau choisi.

5. MEHARI

- *Comment ?*
  - Mettre à disposition des *règles*, *modes de présentation* et *schémas de décision*
  - Proposer (à une activité/entreprise) un *plan de sécurité*
    - ⇒ensemble de *mesures* permettant de pallier les failles et d'atteindre le niveau de sécurité répondant aux exigences.
- *Base*
  - Six facteurs de risque indépendants :
    - trois influant sur la *potentialité du risque*
    - trois influant sur son *impact*
  - Six types de mesures de sécurité,
    - chacun agissant sur un des facteurs de risque (structurelle, dissuasive, préventive et de protection, palliative et de récupération).

5. MEHARI



Synoptique des mesures de sécurité selon MEHARI

5. La méthode MEHARI

- *Phases*
  - ***Phase 1*** : établir *plan stratégique* de sécurité
    - ⇒ définition des *métriques* des risques & *objectifs* de sécurité,
    - ⇒ établissement d'une *politique* de sécurité,
    - ⇒ établissement d'une *charte* de management.
  - ***Phase 2*** : établissement de *plans opérationnels* de sécurité
  - ***Phase 3*** : consolidation des plans opérationnels (global).
- *Plus d'info :**
  - https://www.clusif.asso.fr/fr/production/mehari/3.asp

Comparatif des normes

Méthode	Création	Popularité	Auteur	soutien	Pays	Outils	Etat
EBIOS	**1995**	***	**DCSSI**	**Gouv**	**Fr**	**Log grat.**	
Melisa		**	DGA	Arm.	Fr		Abandonnée
Marion	1980	**	CLUSIF	Asso	Fr		Abandonnée
Mehari	1995	***	CLUSIF	Asso	Fr	L. Risicare	
Octave	1999	**	Univ	Univ	EU	L. Payant	
Cramm	1986	**	Siemens	Gouv	GB	L. Payant	
SPRINT	1995	*	ISF	Asso	GB	L. Payant	
BS 7799		***		Gouv	GB		
ISO 17799		***		Internati			
ISO 13335				Internati			
ISO 15408				Internati			
SCORE	2004		Ageris	Sec. privé	Fr	L. Payant	
CALLIO	2001		CALLIO	Sec. privé	Ca	L. Payant	
COBRA	2001		C&A	Sec. privé	GB	L. Payant	
ISAMM	2002		Evosec	Sec. privé	Be		
RA2	2000		Aexis	Sec. privé	Al	L. Payant	

EBIOS

méthode pour
l'Expression des Besoins et
l'Identification des Objectifs de
Sécurité

Vue globale

II.1 La réglementation

- Lois, décrets
  - Loi 78-17 du 06/01/78 "informatique et liberté"
  - (http://www.cnil.fr/index.php?id=301)
- Interministérielle
  - IGI 1300 du 12/03/82 "protection du secret"
- Ministérielle
- Réglementation Interne
- Les informations "classifiées de défense"
  - IGI 900 du 20/07/93
- Les informations sensibles
  - IGI 901 du 02/03/94
  - (www.ssi.gouv.fr/fr/reglementation/901/901.pdf)

✓ L'IGI 900/SGDN/SSD/DR du 20/07/93

II.2 Méthode EBIOS : Introduction

- Méthode d'analyse des risques en SSI
- Peut être appliquée pour un Système *à Concevoir* ou *Existant*
- **déterminer** les *actions* de sécurité qu'il convient d'entreprendre
- s'inspire des ITSEC (**I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria)
- *input* : CdCF (récapitule besoins)
- *output* : (objectifs de sécurité) = données pour
  - FEROS (formalisation des objectifs de sécurité).
  - l'élaboration de l'architecture fonctionnelle sécurisée

http://www.ssi.gouv.fr

I.2 Introduction

- *Cycle de vie d'une solution info*
  - *spécification des besoins* (définir ***ce que fait*** le système)
  - *conception* (définir ***comment*** on fait le système)
  - *réalisation* (***faire*** le système)
  - *utilisation* (installer et ***exploiter*** le système)

- *Spécification des besoins*
  - définir les *services* que le système doit rendre
  - déterminer le *contexte*
  - identifie les grands *choix* (stratégiques, fonctionnels...) relatifs au système
  - concrétisée par le *Cahier des Charges Fonctionnel* (CdCF)
    - objectifs stratégiques et enjeux du système à concevoir
    - *contraintes* : solutions, normes, réglementations, coûts, délais,
    - *missions* du système, *limites* du système à concevoir
    - grandes *fonctions* et *relations* avec l'extérieur
    - identification *sous systèmes* & interfaces entre ces sous-systèmes
    - …

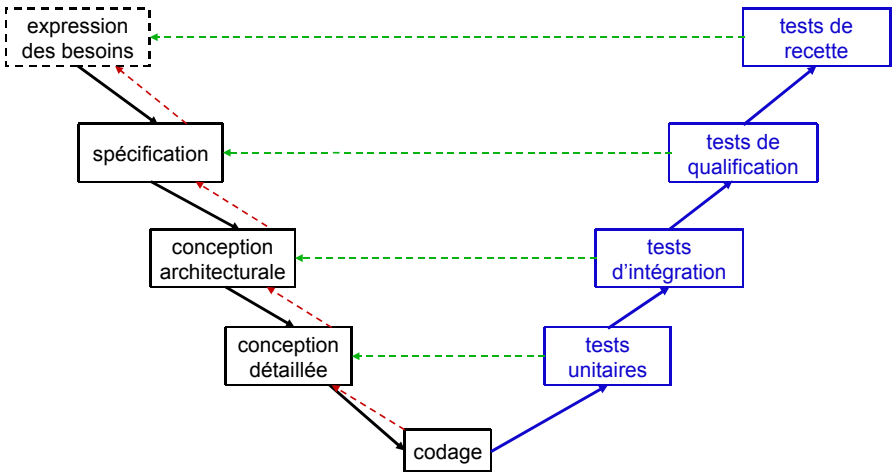
I.2 Introduction

- *Conception*
  - analyse des *besoins* exprimés par le maître d'ouvrage dans le CdCF
  - examen de *l'existant*
  - étude des *solutions*
  - bilan de *faisabilité* et le choix d'une solution
  - réponse au CdCF formalisé par *Spécifications Techniques de Besoin*

- *Réalisation*
  - Acquisition ou développement solution
  - intégration
  - Validation

- *Utilisation*
  - *installation* sur site,
  - *exploitation*,
  - *maintenance* …

I.2 Processus en V



I.2 Introduction

- *Prise en compte sécurité lors de la spécification des besoins*
  - analyser les ***enjeux*** d'un point de vue de la sécurité
    - *poids stratégique* du système pour l'organisme
    - *impact sécurité* système sur sécurité globale de l'organisme
    - *pertes maximales* que le système peut *supporter*
  - analyser le ***contexte*** dans lequel se situe le système */ sécurité*
    - *environnement* physique dans lequel va évoluer le système
    - *menaces* générales pesant sur l'organisme qui abritera le système
    - *contraintes* de sécurité auxquelles le système est soumis
  - définir les *besoins intrinsèques* de sécurité
  - déterminer les *objectifs de sécurité* pour le système

I.2 Introduction : les Objectifs de sécurité

- *résultent d'une analyse qui intègre*
  - *besoins* de sécurité initiaux,
  - *menaces* spécifiques
  - *vulnérabilités* associées aux éléments connus ou supposés
  - *choix organisationnels* retenus

- *doivent se décliner en*
  - ***mesures non techniques*** de sécurité (physique, **organisationnelle**) qui constituent les grandes lignes de la politique non technique de sécurité
  - ***mesures techniques*** de sécurité exprimant ce qui reste à couvrir par des **fonctions** techniques au sens ITSEC
    - permet d'estimer le type de fonctionnalité de sécurité que l'on désire obtenir (e.g., une classe de fonctionnalité donnée au sens ITSEC).

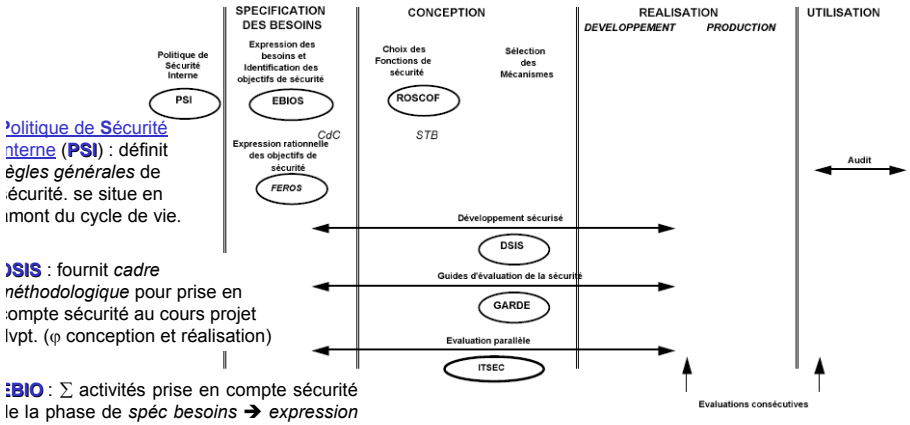
I.2 Introduction

- *Prise en compte sécurité lors de la Conception*
  - **choisir** les *fonctions* de sécurité répondant aux objectifs de sécurité
  - **sélectionner** ou spécifier les *mécanismes* associés
  - consolider la *politique de sécurité technique* du système
  - définir la *politique d'administration* de la sécurité
  - définir, le cas échéant : mode dégradé, *plan sauvegarde* et *plan secours*

- *Prise en compte sécurité lors de la Réalisation*
  - **Réaliser** (soit même) ou se procurer (produit marché) *mécanismes séc*
  - les **intégrer** avec les autres éléments du système
  - effectuer une **analyse** de *vulnérabilité* résiduelle.

- *Prise en compte sécurité lors de la Réalisation*
  - **installer** puis **configurer** *mécanismes sécurité* sur site d'exploitation
  - **validation** de la *sécurisation globale* du système
  - **formation** des futurs responsables de la sécurité du système.
  - administration, test,sauvegarde, audit

I.2 Introduction : phases & docs



Politique de Sécurité interne (**PSI**) : définit *règles générales* de sécurité. se situe en amont du cycle de vie.

DSIS : fournit *cadre méthodologique* pour prise en compte sécurité au cours projet dvpt. (φ conception et réalisation)

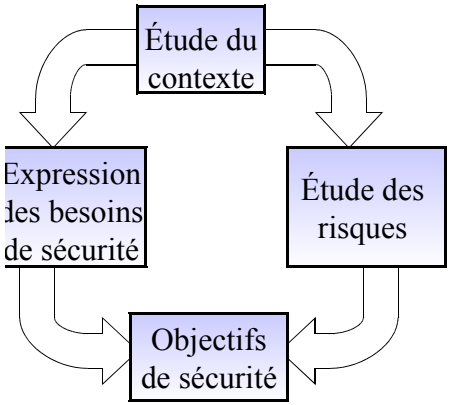
EBIOS : ∑ activités prise en compte sécurité de la phase de *spéc besoins* ➔ *expression objectifs* sécurité

Fiche d'**E**xpression **R**ationnelle des **O**bjectifs de **S**écurité (**FEROS**) : *formalisation objectifs* de sécurité

Réalisation des **O**bjectifs de **S**écurité par le **C**h**O**ix des **F**onctions (**ROSCOF**) : guide concepteur dans *choix fonctions* sécurité répondant aux objectifs. (φ conception après expression objectifs)

Guides d'**A**ide à la **R**é**D**action des fournitures pour l'**E**valuation (**GARDE**) : pour *évaluation ITSEC*

I.2 Démarche EBIOS



EBIOS suit une démarche naturelle et applicable par le futur utilisateur qui permet de:

- responsabiliser les acteurs
- formaliser un raisonnement
- analyser un système existant
- rationaliser les objectifs de sécurité au sens des ITSEC ou des CC

- *besoins de sécurité*
  - associés aux *fonctions* et *informations* du système, porteuses d'exigences de sécurité (i.e., sensibles), identifiées dans l'étude du contexte
  - exprimés en terme de dispon, intégrité, confidentialité
  - exprimés par utilisateurs & responsables du système qui représentent leurs exigences en matière de sécurité.

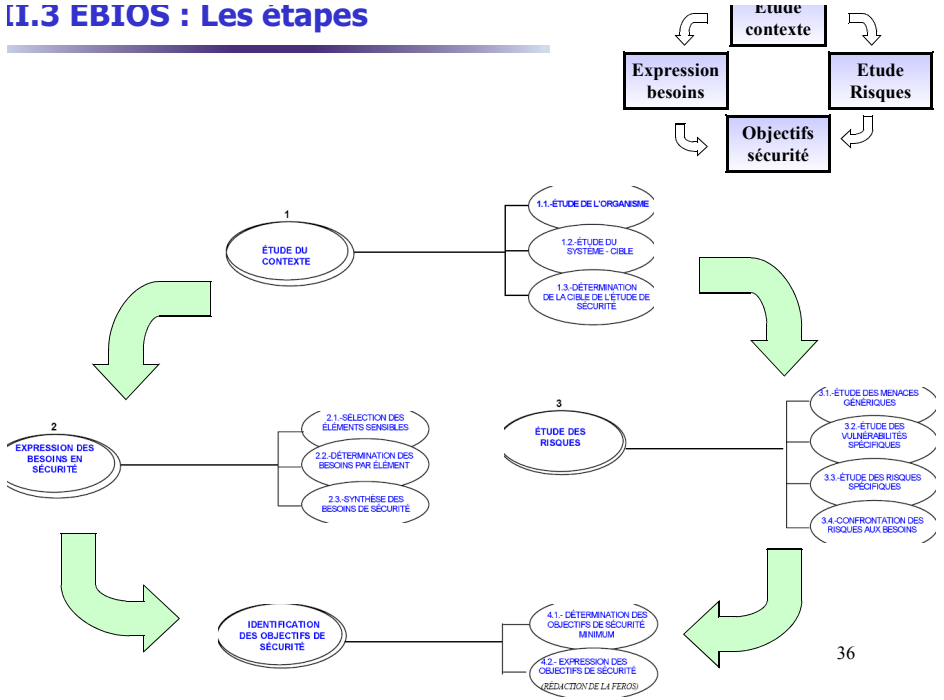
- *Etude des risques*
  - détermination des *vulnérabilités* spécifiques au système
    - caractérisées par *faisabilité* ou *probabilité* de réalisation
  - sélection *menaces* pertinentes (exhaustives, impact sur syst, ..)
  - asso (menaces, vulnérabilités) ⟹ identification risques

- *objectifs de sécurité*
  - Se déduisent de :
    - confrontation risques ← → besoins de sécurité
    - prise en compte des contraintes (e.g., réglementation)
  - Comprennent
    - mesures non-techniques (e.g., organisationnelles),
    - mesures techniques (e.g., fonctions de sécurité).

EBIOS

méthode pour
l'Expression des Besoins et
l'Identification des Objectifs de Sécurité

Les étapes



Plan

3. La méthode EBIOS

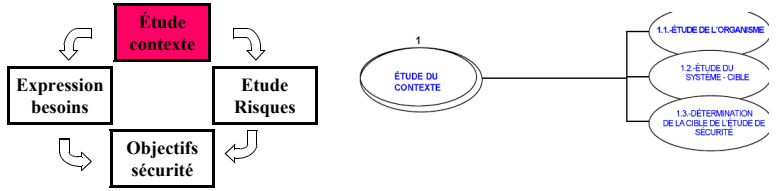
3.1 Étude du contexte

3.2 Expression des besoins de sécurité

3.3 Analyse des risques

3.4 Identification des objectifs de sécurité

I.3 Etape I : Contexte



But :

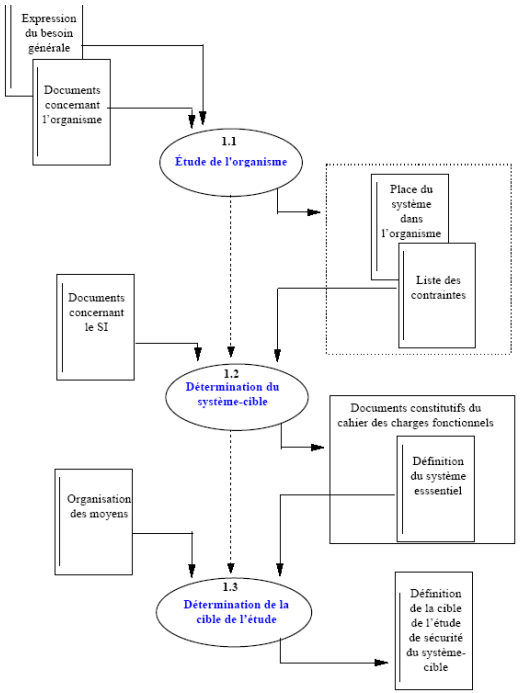
- identifier *globalement* ***système-cible***
  - Prise de connaissance du domaine à étudier
  - situer ***système-cible*** dans son environnement
  - ➔ déterminer *précisément* la ***cible de l'étude***
- Préciser : enjeux, contexte, missions / services, moyens
- *Réunir les informations nécessaires à la planification de l'étude*

- Résultat
  - le champ d'investigation de l'étude est clairement délimité,
  - les obligations et les contraintes sont recensées et
  - les sujets à traiter sont connus

I.3 Etape I : Contexte

Trois activités

- *Étude de l'organisme*
- *Étude du système cible*
- *Détermination de la cible de l'étude*



Activité I.1 : Etude de l'organisme

Données en Entrée : Plan stratégique, bilan d'activité, charte sécurité

Données Sortie : place système dans organisation, liste contraintes

PRESENTATION ORGANISATION

Savoir faire : recueil éléments stratégiques

- missions (service/destinataire),
- métiers (techniques, savoir faire employé)
- valeurs (principes, étique)
- axes stratégiques (lignes directrices/évolution ➔ enjeux)

ORGANISATION GENERALE

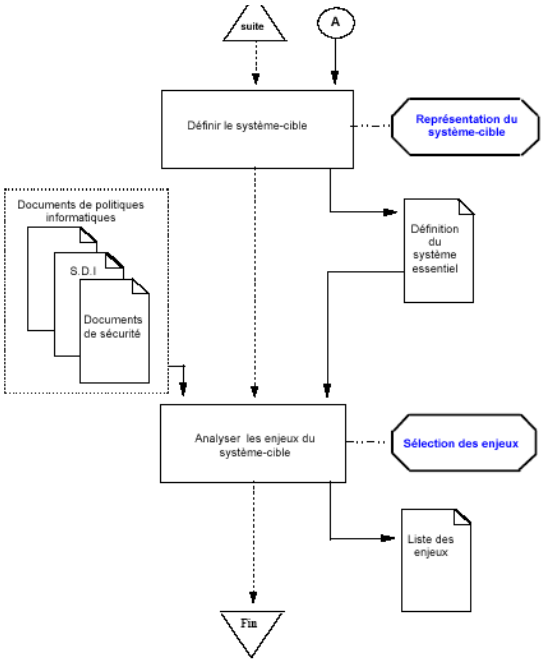
- Structure (divisionnelle / fonctionnelle ou matricielle)
- Organigramme (structure ➔ liaison subordination, dépendances)

CONTRAINTES

- ***Stratégiques*** : évolution possibles structures/orientations
- ***Territoriales*** : dispersion des sites
- ***Conjoncturelles*** : continuité service même si grèves/crises
- ***Structurelle*** : e.g., structure internationale ➔ concilier exigences propres à chaque nation
- obligations ***légales*** et réglementaires
- relatives au ***personnel*** : sensibilisation sécurité, confid.
- d'ordre ***calendaire*** : réorganisation service, nouvelle politique
- d'ordre ***budgétaire*** : mesures sécurité préconisées ont coût qui peut être important

Activité I.2 : Etude du système cible

Dynamique



Activité I.2 : Etude Système Cible

Données en Entrée : ***relations*** entre domaines d'***activité*** du SI, liens inter-domaines, évolution, priorités, évaluation risques stratégiques

Données Sortie : ***Architecture*** conceptuelle du SI, relations ***fonctionnelles*** avec système-cible, Définition du "système essentiel" du système-cible, Sélection enjeux

ELEMENTS à faire : ***fonctions, informations***, enjeux

- contribution du système-cible aux missions du SI de l'organisme
- description générale du système-cible (fonctions, traitements, produits),
- relations fonctionnelles avec le système-cible
- enjeux du système-cible au sein du SI

Caractérisation architecture conceptuelle du SI

- DÉCOUPAGE EN DOMAINES FONCTIONNELS
  - fonctions : opérationnelles, de support, de contrôle
- REPRÉSENTATION DES RELATIONS INTER-DOMAINES
  - interactions entre activités : objets supports de l'information, traitements, moyens

Activité I.2 : Etude Système Cible

Représentation du système-cible dans le SI :

- DESCRIPTION FONCTIONNELLE DU SYSTÈME-CIBLE
  - préciser pr **fonction** : résultats attendus, activités à réaliser, entités manipulée
- CARACTÉRISATION PROCESSUS
  - contraintes informationnelles et organisationnelles : relations, interactions, flux, …

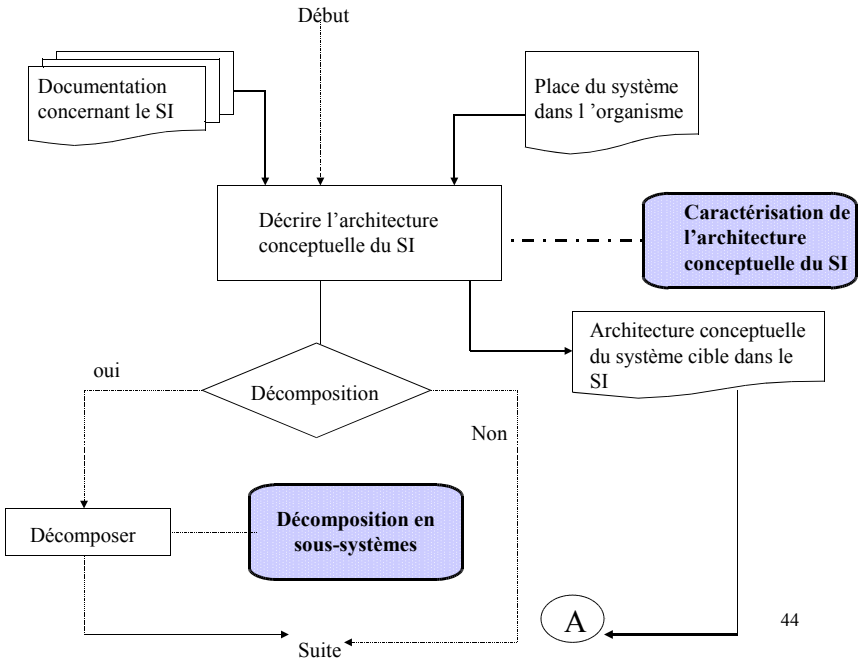
Sélection des enjeux du système-cible

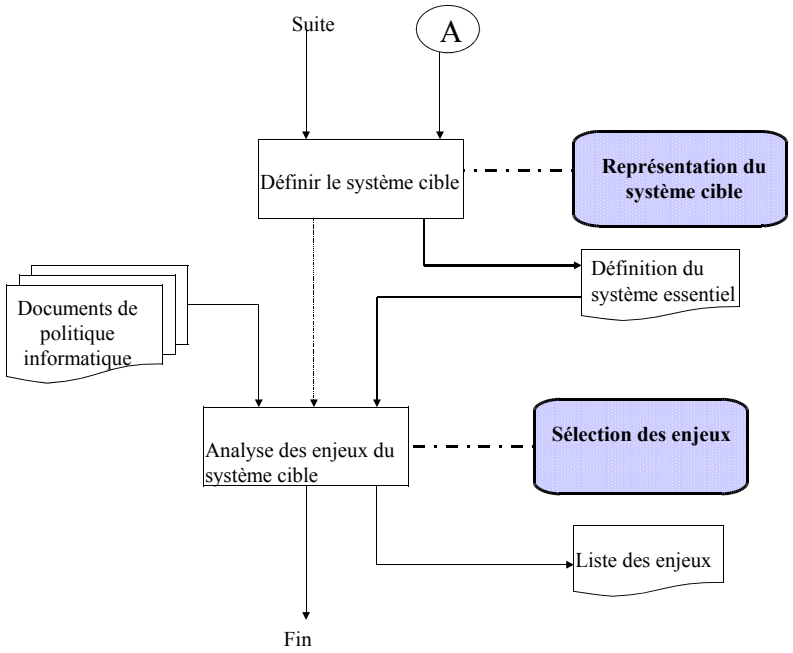
1- EVALUATION DES ENJEUX DE POLITIQUE GÉNÉRALE DU SI
   - scénarii d'évolution du SI : cibles organisa.&physiques à moyen&long terme, améliorations, rentabilité, ...

2 - RECUEIL ÉLÉMENTS DE POLITIQUE DE SÉCURITÉ DU SI
   - priorités, résultats, consignes

3- IDENTIFICATION DES CONTRAINTES
   - d'antériorité, réglementaires, financières, temps, relatives aux méthodes, tech.

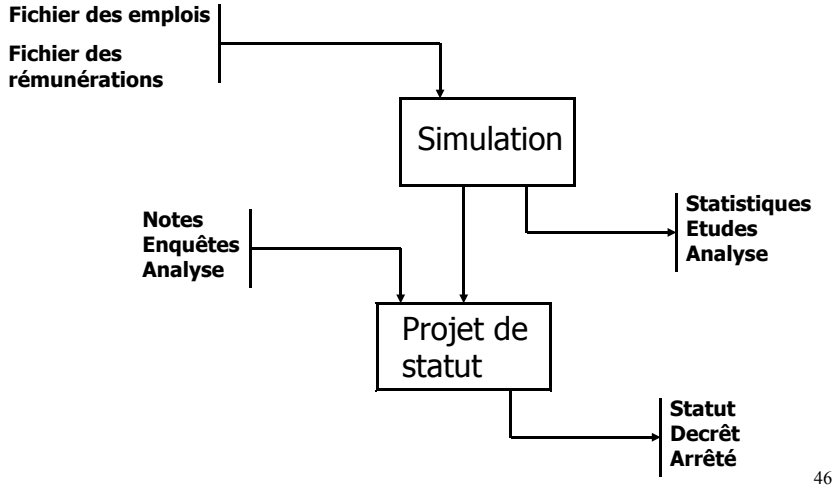
4- IDENTIFICATION DES EXIGENCES GÉNÉRALES
   - Exigences techniques :fichiers, architecture, progiciels, matériel, réseau, …
   - Exigences organisationnelles ;
   - Exploitation : délais, fourniture résultat, services, suivi, plan secours
   - Gestion des développements : outils, organisation à mettre en place
   - …





Exemple

Représentation des fonctions

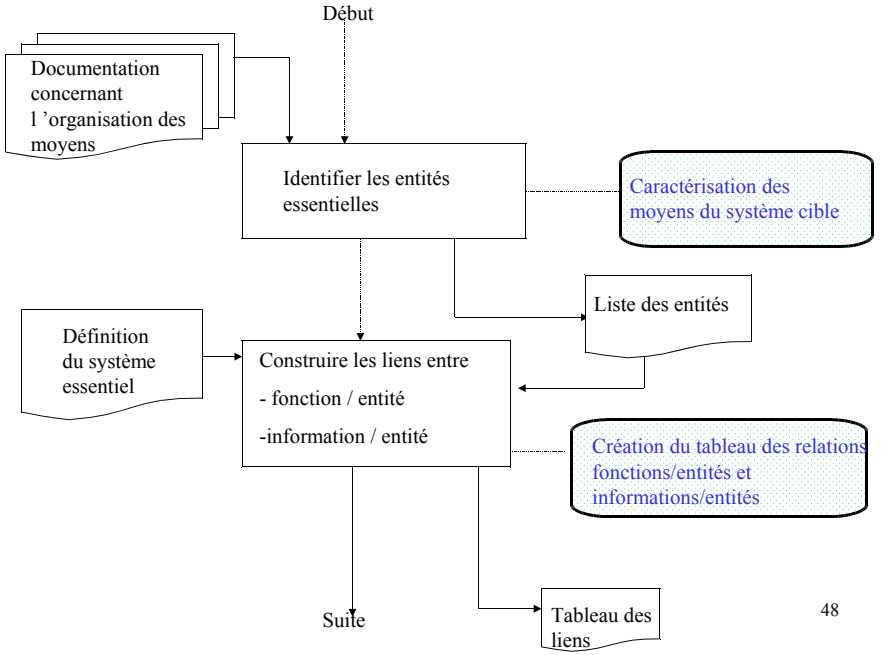


Activité I.3 : Détermination de la cible de l'étude

- *But*
  - déterminer entités sur lesquelles s'appuient réalisation mesures sécurité
- *Quoi ?*
  - faire l'inventaire des entités et les décrire
  - déterminer pour chaque fonction et information essentielles, les entités qui concourent à leur réalisation
    - Tableau des liens entités/fonctions & entités/infos

- *Caractérisation des moyens de la cible de l'étude*
  - profiler les moyens qui permettront réalisation ces fonctions
  - moyens sont caractérisés par entités techniques & non tech.
  - types d'entités ➔ mieux identifier menaces & vulnérabilités
  - entités : Matériels, logiciels, réseaux, personnels, site, organisations

I.Etude du contexte-> 1.3.Détermination de la *cible de l 'étude*



Activité I.3 : Détermination de la cible de l'étude

- *Création tableau Fonctions / Entités et Informations / Entités*
  - liens < fonctions, entités qui contribuent à leur réalisation >
  - liens < infos, entités qui concourent au traitement des infos >

Entités / Fonctions	Matériels		Logiciels			Réseaux	Sites		Personnels		Organisations	
	M1	M2	L1	L2	L3	R1	S1	S2	P1	P2	O1	O2
Fonction 1		+			+	+		+		+	+	
	+		+		+		+			+		+
Fonction n	+			+		+	+		+	+		+

Exemple

Relation entre *informations* sensibles et *entités*

Entité / Information	Matériel			Logiciels			Réseaux			Personnel		
	Serveur	Station	...	OS	Appli.	...	Ethernet	X25	...	Admin.	Ingénieurs	Dévs
Messagerie												
Edition de plans												
.....												

Étude du Contexte : récapitulatif

Objectifs

- *Prise de connaissance du domaine à étudier*
- *Préciser les enjeux du système pour l'organisme*
- *Réunir les informations nécessaires à la planification de l'étude*

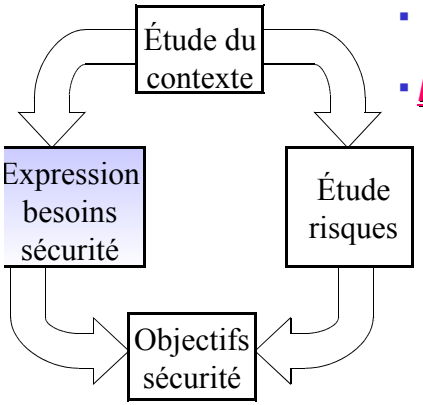
Résultat *Contraintes et Cible de sécurité connus*

Actions

- *Étude de l'organisme*
- *Étude du système cible*
- *Détermination de la cible de l'étude*

Plan

Etape 2 : Besoins



- ***sensibilité*** fonctions et informations
- ***besoins*** de sécurité
  - associés aux objets sensibles et aux fonctions essentielles de cible étude
  - exprimés par U fonctionnels en termes de C D I
  - quantifiés par leurs impacts sur org.

2. Expression des besoins de sécurité (2/4)

Objectifs	• *Sélectionner les fonctions essentielles et les informations sensibles* • *Faire exprimer les utilisateurs sur les besoins en D, I, C, NR*
Résultat	*Liste validée des besoins de sécurité*

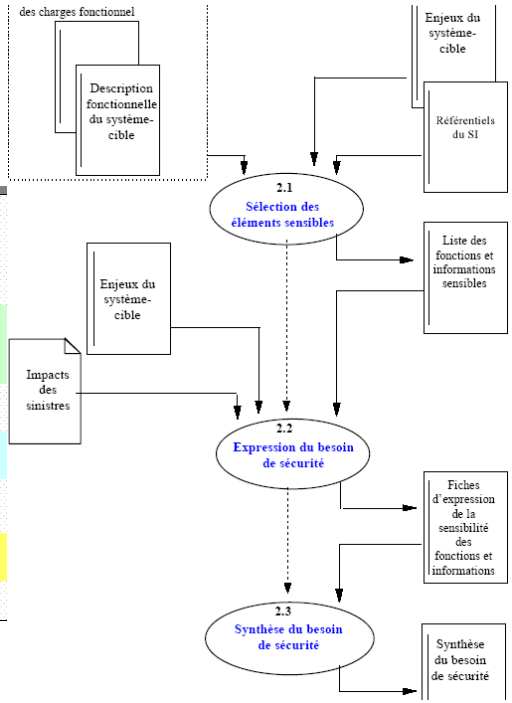
Actions

- *Sélection des fonctions et des informations essentielles*
- *Expression des besoins sécurité des fonctions et informations sensibles*
- *Synthèse du besoin de sécurité*

Etape II : Besoins

Trois activités

- *Sélection info&fnct sensibles*
- *Expression besoins sécurité*
- *Synthèse besoins sécurité*



Activité II.1 : Sélection éléments sensibles

- *DE* : système essentiel, enjeux système-cible
- *DS* : Liste fctns et infos sensibles ; Fiches d'expression besoins de sécurité
- *responsable* ➔ indique informations qui présentent caractère de sensibilité
- *User* ➔ exprimer appréciation sensibilité dns fiches "expres. besoins de sécurité"

- *A. Détermination des éléments sensibles*

  « sensibilité » ≡ exigence de séc caractérisée par besoin de C I D »
  - SÉLECTION INFOS SENSIBLES
  - SÉLECTION FCTNS SENSIBLES
    - entités : Matériels, logiciels, réseaux, personnels, site, organisations

- *B. Création des fiches expression des besoins de sécurité*
  - Recueil besoins réalisé au moyen de questionnaires remis aux Users
  - besoins associés à infos et fonctions s'expriment selon des critères de CID
  - Pour chacun des 3 critères DIC, étudier événements (sinistres) et examiner impact
    - l'impact s'exprime sur une échelle de 0 (aucun impact) à 4 (impact extrême)

Activité II.2 : Expression besoins sécurité

- *Comment ?*
  - proposer aux *Users* une fiche expression des besoins pour *chaque information* ou *chaque fonction* qu'ils manipulent
  - ***Les besoins de sécurité sont indépendants des risques encourus et des moyens de sécurité mis en oeuvre.***
    - Ils représentent donc une valeur *intrinsèque* de la sensibilité des infos, des fonctions ou des sous-fonctions.
  - Exemple (domaine militaire) :
    - attribuer une valeur de confidentialité à documents ➔ les classifier (secret défense, confidentiel défense...)

Fonction/Informations essentiels

Information	• *Classifiées : secret défense* • *Vitales : mission de l'organisme* • *Nominatives : loi informatique et liberté* • *Stratégiques : contrats/accords* • *Coûteuses : délai / coût*
Fonction	• *mission impossible suite dégradation fcnt* • *traitement secret*

Exemple de la sensibilité des objets

Fonction/Information sensible / Sinistres		.....	Image de marque	Infraction aux lois	Pertes financières	.....	Besoin de sécurité	Commentaires
D	Inaccessibilité							
	Destruction							
I	Modif. Accidentelle							
	Modif. Délibérée							
C	Divulg. Interne							
	Divulg. Externe							

Notation d'évaluation d'impact

- *Exemple Notation (C & I) dans domaine militaire*
  - 4 : Atteintes qui, exploitées peuvent directement paralyser …
  - 3 : Atteintes qui peut créer préjudice ou peut faciliter réalisation actions graves
  - 2 : Atteintes qui peut créer préjudice peu grave
  - 1 : Atteinte ne risquant pas de provoquer gêne notable dans le fonctionnement

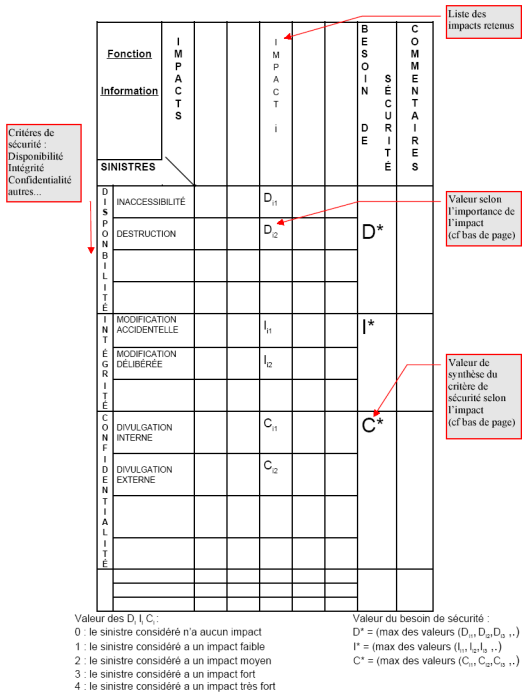
- *Exemple Notation pour une organisation*
  - Niveau 4 : toucher pérennité de l'organisme
  - Niveau 3 : modification importante de la structure/capacité
  - Niveau 2 : diminuer la capacité de l'organisme
  - Niveau 1 : provoquer une gène dans le fonctionnement
  - Niveau 0 : ne provoque pas une gène notable

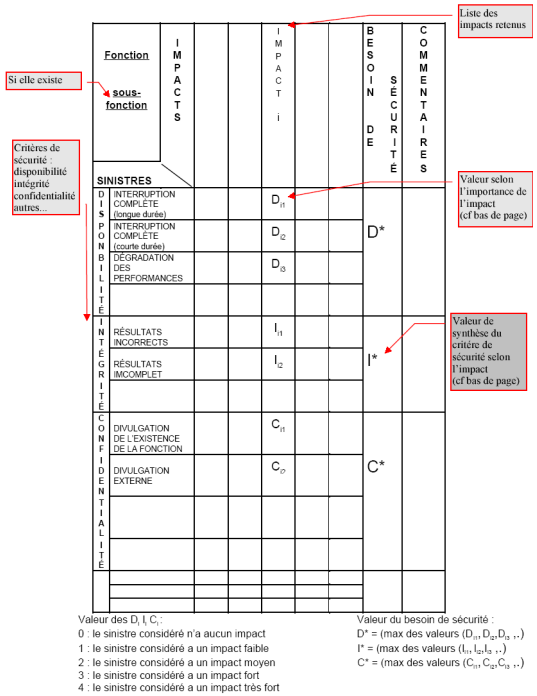
Exemple d'échelle d'évaluation des sensibilités

- « 0 » la perte du critère est sans conséquence pour l'organisme
- « 1 » La perte du critère entraînerait des conséquences défavorables aux intérêts de l'organisme,
- « 2 » La perte du critère entraînerait des conséquences dommageables aux intérêts de l'organisme,
- « 3 » La perte du critère entraînerait des conséquences graves aux intérêts de l'organisme,
- « 4 » La perte du critère entraînerait des conséquences exceptionnellement graves aux intérêts de l'organisme

Activité II.3 : Synthèse besoins sécurité

- ***But***
  - Affecter, pour chaque information et/ou sous-fonction, la valeur finale de sensibilité qui résulte de la synthèse des valeurs attribuées par les utilisateurs.
  - L'auditeur reporte les valeurs de sensibilité déterminées par les utilisateurs sur la fiche "synthèse des besoins de sécurité" et détermine la valeur considérée comme la synthèse.

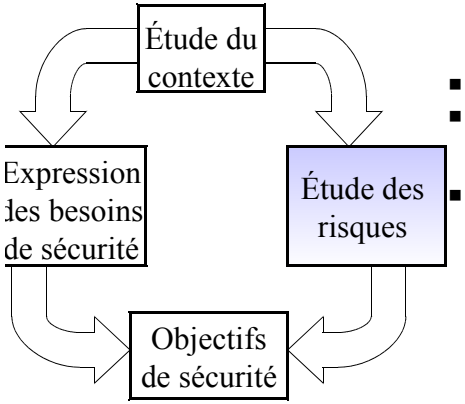




Plan

3. La méthode EBIOS

3. Risques



- Quelles sont les menaces ?
- Quelles sont les risques qui peuvent réellement affecter l'organisme ?
- Activités de l'étape

Étude des risques (3/4)

Objectifs	*Déterminer les risques qui doivent être couverts par les objectifs de sécurité de la cible de l'étude*
Résultat	*Liste validée des risques retenus*

Actions

- *Étude des menaces génériques*
- *Étude des vulnérabilités spécifiques*
- *Analyse des risques spécifiques*
- *Confrontation des besoins de sécurité aux risques spécifiques*

3.1 Étude des menaces génériques

Les menaces sont sélectionnées à partir d'une liste de menaces génériques relatives à des thèmes :

- Accidents physiques
- Événements naturels
- Pertes des services essentiels
- Perturbations dues aux rayonnements
- Compromission des informations
- Défaillance technique
- Agression physique
- Fraude
- Compromission des fonctions
- Erreurs

3.1 Exemple de sélection de menaces génériques

Thème	menace	Cause		Origine			
		Accidentelle	Délibérée	Ludique	Avide	Stratégique	Terroriste
III Pertes de service	Défaillance de la climatisation	x					
	Perte d'alimentation électrique	x	x				x
	Perte de moyens de télécom.	x					
VIII Actions illicites	Piégeage de matériel		x			x	
	Piégeage de logiciel		x			x	
	Abus de droit		x	x			
	Usurpation de droit		x	x			
	Fraude		x		x		

3.1 Étude de l'impact de la menace

*Évaluer les impacts des menaces sur la cible de l'étude en affectant une valeur en terme de **sévérité** (gravité)*

Une sévérité s'exprime sur une échelle de 0 à 4 où :

- 0 : la menace n'entraîne aucune conséquence
- 1 : la menace implique une conséquence faible
- 2 : équivaut à une perte moyenne
- 3 : signifie une perte importante
- 4 : correspond à une perte complète.

3.1 Exemple de sévérité des menaces pertinentes

Menace	Sévérité			Commentaires
	D	I	C	
10.Défaillance de la climatisation	2	0	0	Local aéré
11.Perte d'alimentation électrique	1	0	0	Groupe électrogène disponible
12.Perte de moyens de télécom.	4	0	0	Mission essentielle
30.Piégeage de matériel				
33.Piégeage de logiciel				
39.Abus de droit				
40.Usurpation de droit				
42.Fraude				

3.2 Etude des Vulnérabilités spécifiques

Définition *Une vulnérabilité est une "**caractéristique**" du système qui peut être exploitée par une menace*

Menace 33
- Possibilité de créer ou modifier des commandes systèmes
- Possibilité d'implanter des programmes pirates
- Possibilité de modifier ou changer les applicatifs
- Possibilité d'existence de fonctions cachées

Menace 18
- Matériel ayant des éléments permettant l'écoute passive (câblage, prises de connexion...)

3.2 Caractérisation des vulnérabilités

❖ Les vulnérabilités sont caractérisées par leur ***faisabilité*** ou leur ***probabilité***.

- La faisabilité caractérise les vulnérabilités associées aux menaces délibérées (intentionnelles)
- La probabilité caractérise les vulnérabilités associées aux menaces accidentelles

Faisabilité (F)

0: menace infaisable
0.25: nécessité de moyens très importants des connaissances pointues
0.5: nécessité d'un certain niveau d'expertise ou matériel spécifique
0.75: réalisable avec moyens standards et connaissance de base
1: menace réalisable par tout public

Probabilité (P)

0: menace improbable
0.25: menace faiblement probable
0.5: menace moyennement probable
0.75: menace fortement probable
1: la menace est certaine

3.2 Liste des vulnérabilités associée à la menace 33

Menace n°33	*Libellé de la vulnérabilité*	*Mat & Log*	*Réseau interne*	*Site*	*Personnel utilisateur*	*Personnel développeur*	*Organisation*
Piégeage de logiciel	*Possibilité de modifier les applicatifs*	0.5	0.25				
	Possibilité d'implanter des programmes pirates	0.75	0.5				
	Possibilité d'existence de fonctions cachées introduite en phase de conception	0.5	0.25				
	Personnel manipulable				0.25	0.75	
	Facilité de pénétrer dans les locaux			0.5			
	Absence de consigne de sécurité						0.75

3.3 Analyse des risques spécifiques

- Un risque est considéré comme une menace associée à un ensemble de vulnérabilités qui permettent sa réalisation.
- Il est caractérisé par son :
  - *impact* direct en (D, I, C) issu de la *menace* et
  - une *faisabilité / probabilité* issue des *vulnérabilités* retenues
- Chaque risque, ainsi caractérisé doit être explicité clairement. C'est l'objet de la fiche des risques spécifiques, qui synthétise, pour le système-cible, l'ensemble des risques spécifiques qui le concernent.

3.3 Analyse des risques spécifiques

- Exemple :
  - Infection par virus provoquée par une disquette d'origine douteuse amené par le personnel.
  - Piégeage logiciel fait par le personnel d'entretien en dehors des heures ouvrables.
- Les vulnérabilités exploitées se trouvent dans la fiche des vulnérabilités spécifiques.
- Un risque est référencé par son numéro de menace, et par un numéro d'ordre dans la menace si cela est nécessaire.

3.2 Analyse des vulnérabilités spécifiques

R33	Libellé du risque	F
1	Un informaticien développeur a introduit une fonction cachée dans les applicatifs	0.5x0.75=0.375
2	Un informaticien développeur a introduit une fonction cachée dans les logiciels réseau	0.25x0.75=0.187
3	Le personnel utilisateur modifie les applicatifs	0.25x0.5=0.125
4	Un membre du service implante des programmes pirates	0.75x0.75=0.562
5	Un intrus pénètre dans le site pour implanter des programmes pirates	0.75x0.5x0.75= 0.281

3.2 Liste des vulnérabilités associée à la menace 33

Menace n°33	*Libellé de la vulnérabilité*	*Mat & Log*	*Réseau interne*	*Site*	*Personnel utilisateur*	*Personnel développeur*	*Organisation*
Piégeage de logiciel	*Possibilité de modifier les applicatifs*	0.5	0.25				
	Possibilité d'implanter des programmes pirates	0.75	0.5				
	Possibilité d'existence de fonctions cachées introduite en phase de conception	0.5	0.25				
	Personnel manipulable				0.25	0.75	
	Facilité de pénétrer dans les locaux			0.5			
	Absence de consigne de sécurité						0.75

Un informaticien développeur a introduit une fonction cachée dans les applicatifs

3.2 Liste des vulnérabilités associée à la menace 33

Menace n°33	*Libellé de la vulnérabilité*	*Mat & Log*	*Réseau interne*	*Site*	*Personnel utilisateur*	*Personnel développeur*	*Organisation*
Piégeage de logiciel	*Possibilité de modifier les applicatifs*	0.5	0.25				
	Possibilité d'implanter des programmes pirates	0.75	0.5				
	Possibilité d'existence de fonctions cachées introduite en phase de conception	0.5	0.25				
	Personnel manipulable				0.25	0.75	
	Facilité de pénétrer dans les locaux			0.5			
	Absence de consigne de sécurité						0.75

Un informaticien développeur a introduit une fonction cachée dans les logiciels réseau

3.3 Analyse des risques spécifiques

Synthétiser *pour le système cible l'ensemble des* ***risques spécifiques*** *qui le concernent*

N° menace	N° risque	Libellé du risque	D (Impact menace)	I	C	F/P (vulnérabilité)
10		la centrale de clim. Tombe en panne	2	0	0	25%
22		Un utilisateur du CECP diffuse une information sensible par le réseau RTC	0	0	3	12.5%

3.4 Confrontation des risques aux besoins

Le but de cette activité est de retenir les risques qui sont véritablement susceptibles de porter une atteinte aux fonctions ou aux informations sensibles.
La sélection s'effectue par la mise en relation des risques spécifiques avec les besoins de sécurité, pour mettre en évidence l'impact final de la réalisation d'un risque.

Actions :
- détermination pour chaque fonction et info de la liste des risques qui les concernent
- confrontation des risques aux fonctions et informations.
- réflexion qui est menée lors de cette activité sert également à orienter la décision de partage entre les mesures techniques et non-techniques.

3.4 Confrontation des risques aux besoins

La synthèse s'effectue par la rédaction de la liste des risques retenus pour le système cible, classés en catégories représentatives de leur gravité.
Les besoins de sécurité ont été exprimés pour les fonctions et les info. La confrontation des besoins aux risques consiste à déterminer les liens directs entre les menaces d'une part et les fonctions et informations d'autre part.

Fonction K				Besoin (sensibilité) **D I C**		
Menaces	Impact (sévérité)			Impact final		
	D	**I**	**C**	**D**	**I**	**C**
Menace_ i						

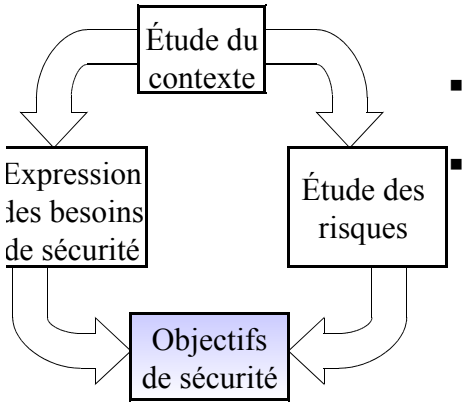
3.4 Exemple de confrontation des risques aux besoins

- Si une sévérité est nulle, alors l'impact réel est nul
- Si une sévérité est non nulle, alors l'impact réel est égal à la sensibilité

Fonction K				Sensibilité **3 2 0**		
Menaces	Sévérité			Impact final		
	D	**I**	**C**	**D**	**I**	**C**
Défaillance de la clim	2	0	0	3	0	0
Un utilisateur du CECP diffuse une …….	0	0	3	0	0	0

Plan

4. Identification objectifs de sécurité



- Que peut faire l'organisme pour que son système soit mieux sécurisé?
- Activités de l'étape

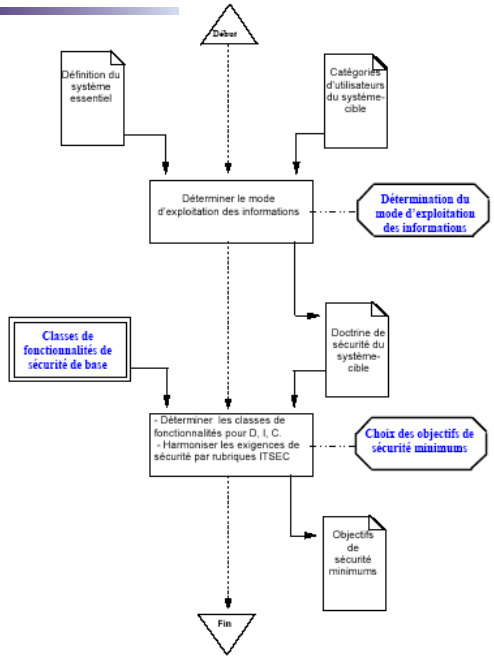
4.Identification des objectifs de sécurité (4/4)

Objectifs	*exprimer ce que doit réaliser la cible de l'étude pour que le système-cible fonctionne de manière sécurisé.*
DE	Listes besoins sécurité / risques /contraintes
Résultat	*Rédaction de la FEROS/Liste des objectifs de sécurité*

Actions

- *choix des fonctionnalités de base en fonction de la politique de sécurité de l'information et du mode d'exploitation du système,*
- *sélection des objectifs de sécurité pour le système comprenant*
  - *fonctionnalités techniques complémentaires*
  - *choix des contre-mesures non techniques,*
  - *prise en compte des contraintes/enjeux.*

Activités



4.1 Choix du mode d'exploitation des informations

Le mode d'exploitation des informations consiste à indiquer comment le système traite, transmet ou conserve des informations de sensibilités différentes pour des utilisateurs de catégories différentes.

- *Catégorie 1: Le mode d'exploitation **exclusif***
  - *Tous U ont même niveau + besoin commun d'en connaître*
- *Catégorie 2: Le mode d'exploitation **dominant***
  - *Tous U ont même niveau + n'ont pas tous besoin commun d'en connaître*
- *Catégorie 3: Le mode d'exploitation du système **multi-niveaux***
  - *U ne sont pas tous habilitées + n'ont pas tous besoin commun d'en connaître*

4.1 Choix du mode d'exploitation des informations

choix du mode d'exploitation s'effectue après avoir déterminé si :

- les types de sensibilité des infos (CDI) correspondent à des classifications et
- si notions d'habilitation existent.

Il convient ensuite de se reporter aux tableaux suivants pour trouver le type du mode d'exploitation.

Sans besoin d'en connaître ou équivalent

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	1	3	3	3
2	1	1	3	3
3	1	1	1	3
4	1	1	1	1

Avec besoin d'en connaître ou équivalent

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	2	3	3	3
2	2	2	3	3
3	2	2	2	3
4	2	2	2	2

Avec mention de catégorie

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	3	3	3	3
+ catégorie	2	3	3	3
2	3	3	3	3
+ catégorie	2	2	3	3
3	3	3	3	3
+ catégorie	2	2	2	3
4	3	3	3	3
+ catégorie	2	2	2	2

4.2 Expression des objectifs de sécurité

but : expression complète objectifs de sécurité de la cible de l'étude.

- s'appuient sur les objectifs de sécurité minimums et prennent en compte les risques et les contraintes.

4.1. Tableaux page 54 (Techniques)

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	1	3	3	3
2	1	1	3	3
3	1	1	1	3
4	1	1	1	1

Sans besoin d'en connaître

Si sensibilité d'une info C=4 et si tous les users doivent accéder alors habilitation =4

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	2	3	3	3
2	2	2	3	3
3	2	2	2	3
4	2	2	2	2

Avec besoin d'en connaître

Classification maximum des informations

Niveau d'habilitation minimum des utilisateurs	1	2	3	4
0	3	3	3	3
1	2	3	3	3
2	2	2	3	3
3	2	2	2	3
4	2	2	2	2

Habilitation

	D	I	C
Administrateur	4	4	2
Utilisateur	2	1	4

Sensibilité

	D	I	C
Courrier élect.	4	2	2
Compte rendu	2	3	3

Classe de fonctionnalité pour la C = F-B1, I=F-IN, D=F-Q2

Choix d'une classe de fonctionnalité pour la confidentialité

Habilitation administrateur = 2
Sensibilité compte rendu = 3

Habilitation minimum des personnels	Mode d'exploitation	Classification maximmum des informations 1	2	3	4
0	1	-	-	-	-
	2	-	-	-	-
	3	F-C2	F-C2	F-B1	F-B3
1	1	Néant	-	-	-
	2	F-C2	-	-	-
	3	F-C2	F-C2	F-B1	F-B2
2	1	Néant	Néant	-	-
	2	F-C2	F-C2	-	-
	3	F-C2	F-C2	F-B1	F-B2
3	1	Néant	Néant	Néant	-
	2	F-C2	F-C2	F-C2	-
	3	F-C2	F-C2	F-B1	F-B2
4	1	Néant	Néant	Néant	F-C2
	2	F-C2	F-C2	F-C2	F-C2
	3	F-C2	F-C2	F-B1	F-B1

Choix d'une classe de fonctionnalité pour l'intégrité

Habilitation administrateur = 4
Sensibilité compte rendu = 3

Habilitation minimum des personnels	Mode d'exploitation	Classification maximmum des informations 1	2	3	4
0	1	-	-	-	-
	2	-	-	-	-
	3	F-IN	F-IN	F-IN	F-J3
1	1	Néant	-	-	-
	2	F-IN	-	-	-
	3	F-IN	F-IN	F-IN	F-J2
2	1	Néant	Néant	-	-
	2	F-IN	F-IN	-	-
	3	F-IN	F-IN	F-IN	F-J2
3	1	Néant	Néant	Néant	-
	2	F-IN	F-IN	F-IN	-
	3	F-IN	F-IN	F-IN	F-J2
4	1	Néant	Néant	Néant	F-IN
	2	F-IN	F-IN	F-IN	F-IN
	3	F-IN	F-IN	F-IN	F-J1

Choix d'une classe de fonctionnalité pour la Disponibilité

Habilitation administrateur = 4
Sensibilité compte rendu = 2

Habilitation minimum des personnels	Mode d'exploitation	Classification maximmum des informations 1	2	3	4
0	1	-	-	-	-
	2	-	-	-	-
	3	Néant	Néant	F-P1	F-P3
1	1	Néant	-	-	-
	2	F-Q2	-	-	-
	3	F-Q2	F-Q2	F-P1	F-P2
2	1	Néant	Néant	-	-
	2	F-Q2	F-Q2	-	-
	3	F-Q2	F-Q2	F-P1	F-P2
3	1	Néant	Néant	Néant	-
	2	F-Q2	F-Q2	F-Q2	-
	3	F-Q2	F-Q2	F-P1	F-P2
4	1	Néant	Néant	Néant	F-Q2
	2	F-Q2	F-Q2	F-Q2	F-Q2
	3	F-Q2	F-Q2	F-P1	F-P1

Synthèse des classes de fonctionnalités F-IN et F-C2

Objectif

Il s'agit de la synthèse des classes de fonctionnalités F-IN et F-C2, qui concerne les systèmes pour lesquels il y a des exigences élevées d'intégrité pour les données et les programmes et un besoin de contrôle d'accès discrétionnaire, en rendant les utilisateurs individuellement responsables de leurs actions à travers des procédures d'identification, l'audit des événements relatifs à la sécurité et l'isolation des ressources. [fusion de F-IN et F-C2]

Identification et authentification

Le système doit identifier et authentifier de façon unique les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre le système et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies…….. [extrait de F-IN]

Contrôle d'accès

Le système doit pouvoir distinguer et administrer les droits d'accès des utilisateurs, des rôles et des processus aux objets désignés explicitement (le terme rôle désigne des utilisateurs qui ont des attributs spéciaux). Il doit être possible de restreindre l'accès des utilisateurs à ces objets d'une façon telle que cet accès ne soit possible que par l'intermédiaire de processus établis spécialement……..

2.2.2 Politique de sécurité des systèmes d'informations

litique de sécurité Repose sur :

ermination des informations et des processus à protéger
ermination des menaces et de leur impact.
ermination d 'un niveau acceptable de risque.

La politique de sécurité définit

les mesures à prendre, les structures et l'organisation à mettre en place.

Que devons nous protéger?
Contre qui? Comment?

4.1 Choix du mode d'exploitation des informations

Définir politique de droit d'accès

Exemple

objet / sujets	Info1	Info2	Info3	fonction 1	fonction 2
Catégorie 1	lire	lire écrire		exécuter	
Catégorie 2			modifier		exécuter

4.1 Choix du mode d'exploitation des informations

Définir politique de droit d'accès

Exemple

objet / sujets	Info1	Info2	Info3	fonction 1	fonction 2
Catégorie 1	lire	lire écrire		exécuter	
Catégorie 2			modifier		exécuter

2.2 L'ÉTUDE EBIOS® CONCRÈTEMENT

- La durée est très variable, elle dépend de :
  - la maîtrise de la méthode
  - l'outillage (logiciel)
  - la complexité du système à étudier
  - la disponibilité des différents acteurs
- Le groupe de travail est composé de :
  - responsables
  - informaticiens
  - utilisateurs
- Après ?
  - FEROS, spécifications détaillées et mise en œuvre
  - Schéma directeur en SSI
  - Politique de sécurité des systèmes d'informations
  - ….

2.2.1 FEROS

Fiche d'Expression Rationnelle des objectifs de sécurité

N°150 SGDN/DISSI/SCSSI, 10 Février 1991

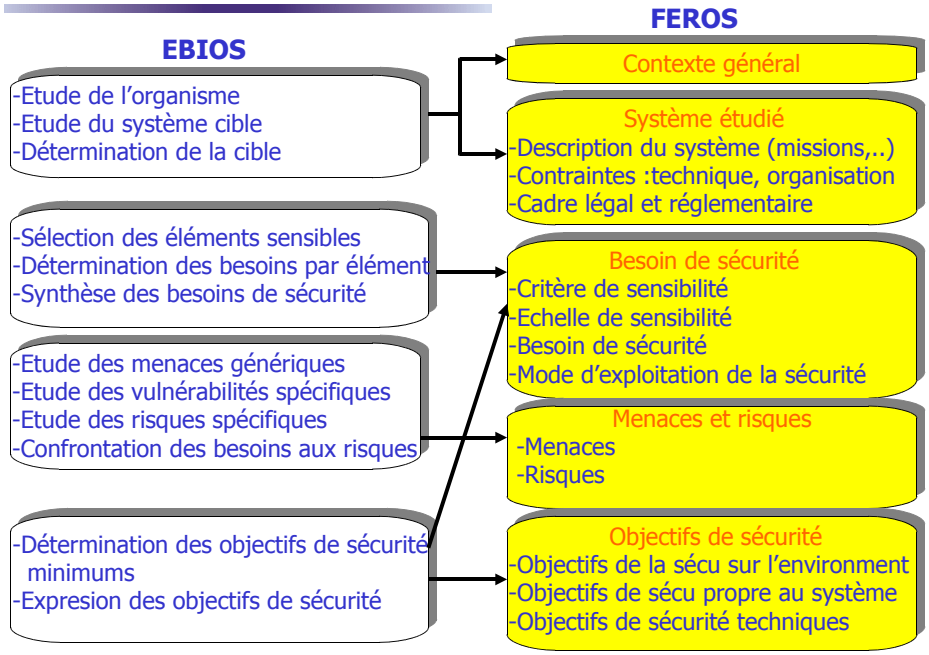
http://www.ssi.gouv.fr/fr/confiance/methodes.html

2.2.1 FEROS

- Elle est de la responsabilité du futur utilisateur
  la FEROS est signée par une haute autorité
- Elle permet une réflexion de sécurité dès le stade de la conception

  Il faut l'avis des divers utilisateurs pour la remplir

2.2.1 Plan d'une FEROS

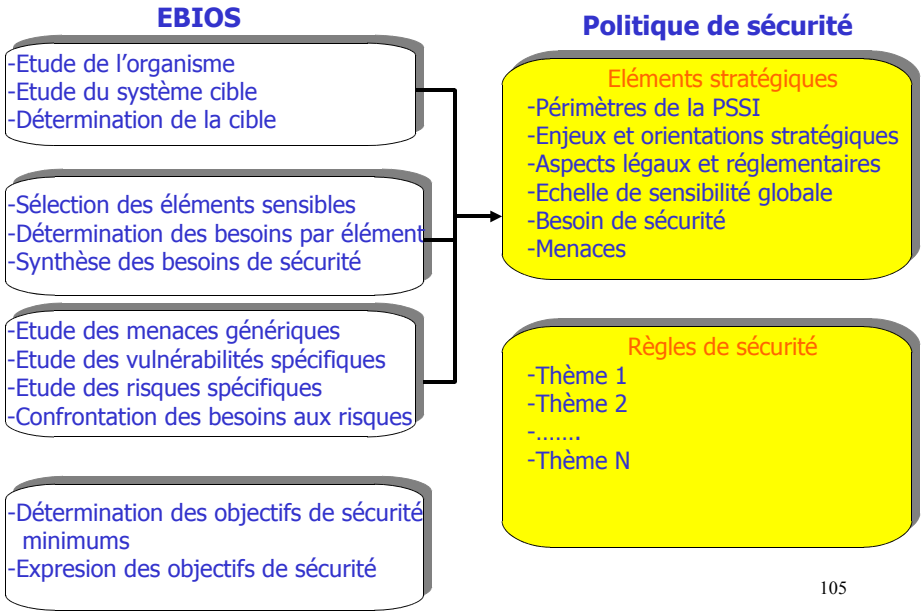


2.2.2 Comment élaborer une PSSI en utilisant EBIOS ?

Une solution efficace pour élaborer une PSSI consiste à :

- Organiser le projet PSSI,
- Réaliser une étude EBIOS globale,
-Extraire les données nécessaires de l'étude EBIOS (contexte, expression objectifs de sécurité, étude des menaces génériques),
- Réaliser les dernières tâches évoquées dans le guide PSSI :
  -choix des principes de sécurité,
  - élaboration des règles de sécurité,
  - élaboration des notes de synthèse,
  - finalisation et validation de la PSSI,
  - élaboration et validation du plan d'action.

2.2.2 Schéma d'illustration



2.2.3 Schéma directeur en SSI

- Le Schéma directeur est un modèle. Il permet :

- Une « vision » des menaces et des vulnérabilités et donc du risque.
- De mettre en évidence les éléments du système d 'information pour agir à moindre coût sur le niveau du risque global.
- Il faut avoir des objectifs pour élaborer un modèle

- **Le " modèle " est l'expression de l'ensemble des besoins de sécurité dans le cadre "d'un existant" et compte tenu de contraintes** (budget,postes, qualification du personnel, réglementation, etc.).

2.2.3 Schéma d'illustration