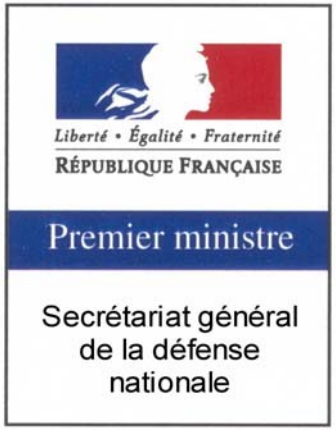

Retour d'expérience sur la méthode EBIOS®

Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil

Cyril Demonceaux
conseil.dcssi@sgdn.pm.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Pourquoi homologuer ?

- Pour garantir la protection des informations conformément à la réglementation

  « Tout système d'information traitant des informations classifiées doit faire l'objet d'une décision d'emploi formelle. Cette décision s'appuie sur l'homologation de sécurité » (IGI 1300)

- Pour être en mesure d'apporter la preuve que l'on a respecté la loi
  - ✓ pour la protection des informations classifiées de défense
  - ✓ pour la protection des informations nominatives

- Pour attester de son niveau de sécurité vis-à-vis de ses partenaires (organismes tiers, clients, OTAN…)

- **<u>Pour mettre en place une approche globale de gestion de risques</u>**
  - ✓ le patrimoine informationnel doit être protégé
  - ✓ obtenir une vision cohérente en termes
    - ➢ des responsabilités
    - ➢ de place de la SSI dans le système d'information
    - ➢ de coûts et de priorités

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Sur quelle base homologuer ?

Quelles sont mes intentions ?

Comment y répondre ?

Comment les faire appliquer ?

Comment vérifier mes choix ?

EBIOS
différents livrables
différentes approches

FEROS
de haut niveau

FEROS
détaillée

Cible de sécurité
système

PSSI

AUDITS

Dossier d'homologation

Les conditions du succès - Avant l'étude

- Impliquer l'organisme
  - ✓ La démarche doit être portée par la direction
    - ➢ Motivation de l'ensemble acteurs de l'organisme
  - ✓ Sensibiliser l'organisme à l'intérêt d'une homologation
    - ➢ Nécessité d'une gestion globale des risques
  - ✓ Définir un chef de projet

- Mettre en place une stratégie d'homologation
  - ✓ Définir le niveau de maturité SSI de l'organisme
  - ✓ Identifier l'autorité d'homologation
    - ➢ Assistée d'une commission d'homologation
  - ✓ Constituer un dossier de sécurité
    - ➢ Définir les livrables
    - ➢ Définir le périmètre de l'étude

Les conditions du succès – Pendant l'étude

- Constituer un groupe de travail à chaque étape
  - ✓ Identifier les bons acteurs
  - ✓ Sensibiliser les acteurs
  - ✓ Nommer un leader
    - ➢ Arriver à un consensus ou trancher
- Être force de proposition
- Collecter les informations
- Faire valider chaque étape par la commission d'homologation
  - ✓ Adapter les livrables aux destinataires
  - ✓ Implique la direction tout au long de la réalisation du dossier de sécurité
  - ✓ Facilite l'homologation

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

FEROS de haut niveau - Quelles sont mes intentions ?

- Présenter les caractéristiques de l'organisme
  - ✓ Les domaines d'activité, les contraintes, les références réglementaires
- Définir les grandes lignes du système
  - ✓ Lister les processus critiques et le patrimoine informationnel à protéger
  - ✓ Identifier les entités de haut niveau supportant les processus critiques
- Exprimer des besoins de sécurité par processus et information critiques
- Formaliser des menaces de haut niveau
  - ✓ Déterminer les pans de la sécurité à étudier
  - ✓ Risques organisationnelles
- Cahier des charges SSI
  - ✓ Document contractuel fourni à la MOE

FEROS détaillée – Réponse de la MOE

- Piloter, superviser la sécurité du système

- Spécifier le système
  - ✓ Enrichir les entités du système sur la base des spécifications fonctionnelles
  - ✓ Lister les solutions de sécurité pressenties sur le système
    - ➢ Prendre en compte les produits de sécurité

- Formuler les scénarios de risques
  - ✓ Identification des nouvelles vulnérabilités
  - ✓ Rédaction de scénarios de risque adaptés au contexte

- Rédiger les objectifs de sécurité
  - ✓ Plan de traitement des risques
    - ➢ Couverture des risques et des éléments du contexte

Cible de sécurité - Réponse de la MOE

- Déterminer les exigences de sécurité fonctionnelles
  - ✓ La MOE doit être force de proposition
  - ✓ Définir un ensemble d'exigences de sécurité à partir
    - ➢ d'exigences issues de la base de connaissances EBIOS (PSSI, ISO 15408, ISO 17799)
    - ➢ de solutions définies par l'industriel / DJS
    - ➢ de mesures existantes dans l'organisme
  - ✓ Les exigences doivent être spécifiques au contexte de l'étude

- Justifier clairement la couverture des objectifs de sécurité
  - ✓ Identification des risques résiduels
    - ➢ Couverture des risques
    - ➢ RTE / DVR de l'audit / expertise / évaluation des produits de sécurité
  - ✓ Validation par la commission d'homologation

PSSI - Réponse de la MOE

- Appliquer concrètement la gestion de risques du SI
- Respecter les PES d'installation et de configuration des produits de sécurité
- Affiner les exigences de sécurité fonctionnelles de la cible de sécurité
  - ✓ Rédiger une PSSI
    - Chapitrage du guide PSSI
  - ✓ Rédiger les procédures d'exploitation de sécurité
    - Par site
    - Par type d'acteur
- Rédaction du contrat de fonctionnement

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

En conclusion

- Les pièges à éviter
  - ✓ Débuter trop tard
  - ✓ Pas d'architecture claire
  - ✓ Pas de validation formelle de la direction
  - ✓ Pas de chef de projet
  - ✓ Laisser les documents dans l'armoire forte !

- EBIOS permet
  - ✓ de rédiger un dossier de sécurité SSI dans le cadre d'une homologation
  - ✓ de contribuer à des démarches SSI globales : schéma directeur, politique de sécurité, tableaux de bord…
  - ✓ d'impliquer tous les acteurs et d'effectuer des arbitrages
  - ✓ de réaliser une traçabilité de la démarche