Maîtrise des risques

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

conseil.dcssi@sgdn.pm.gouv.fr

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

Besoins et conformité

- La nécessité de cerner les besoins de l'organisme…
  - ✓ Ses enjeux
  - ✓ Ses objectifs « métier »
  - ✓ La valeur de son patrimoine informationnel
- …en conformité avec la réglementation applicable…
  - ✓ CNIL
  - ✓ Secret professionnel
  - ✓ Propriété intellectuelle
  - ✓ Classifié de défense
  - ✓ Réglementation sectorielle…
- …et en s'appuyant sur les normes internationales
  - ✓ Lignes directrices de l'OCDE
  - ✓ ISO 27001, ISO 17799, ISO 15408 (critères communs)…

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

Mise en perspective avec les objectifs de l'organisme

- Protéger l'organisme…
  - ✓ Préserver et valoriser l'image de marque
  - ✓ Prévenir des pertes financières
  - ✓ Garantir la continuité des activités
  - ✓ Améliorer la sécurité de l'information
  - ✓ Protéger contre les attaques informatiques
  - ✓ Assurer le respect des lois et règlements…

- …en maîtrisant les risques
  - ✓ Adopter une vision globale
  - ✓ Fournir les éléments nécessaires à la prise de décision (consensus, négociation, arbitrage, validation)
  - ✓ Faciliter la communication (implication, sensibilisation…)

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

Les apports d'une démarche structurée

- Mutualiser et pérenniser…
  - ✓ Standardiser des pratiques réutilisables et objectives
  - ✓ Instaurer un vocabulaire et un socle commun
  - ✓ Utiliser des raisonnements simples, souples et cohérents
  - ✓ Favoriser la communication entre les équipes

- …pour créer de la valeur ajoutée
  - ✓ Des résultats visibles rapidement (mise en place de mesures adaptées, augmentation de la culture de sécurité)
  - ✓ La garantie d'un niveau de service et de confiance
  - ✓ Maîtriser les dépenses et justifier les investissements de sécurité

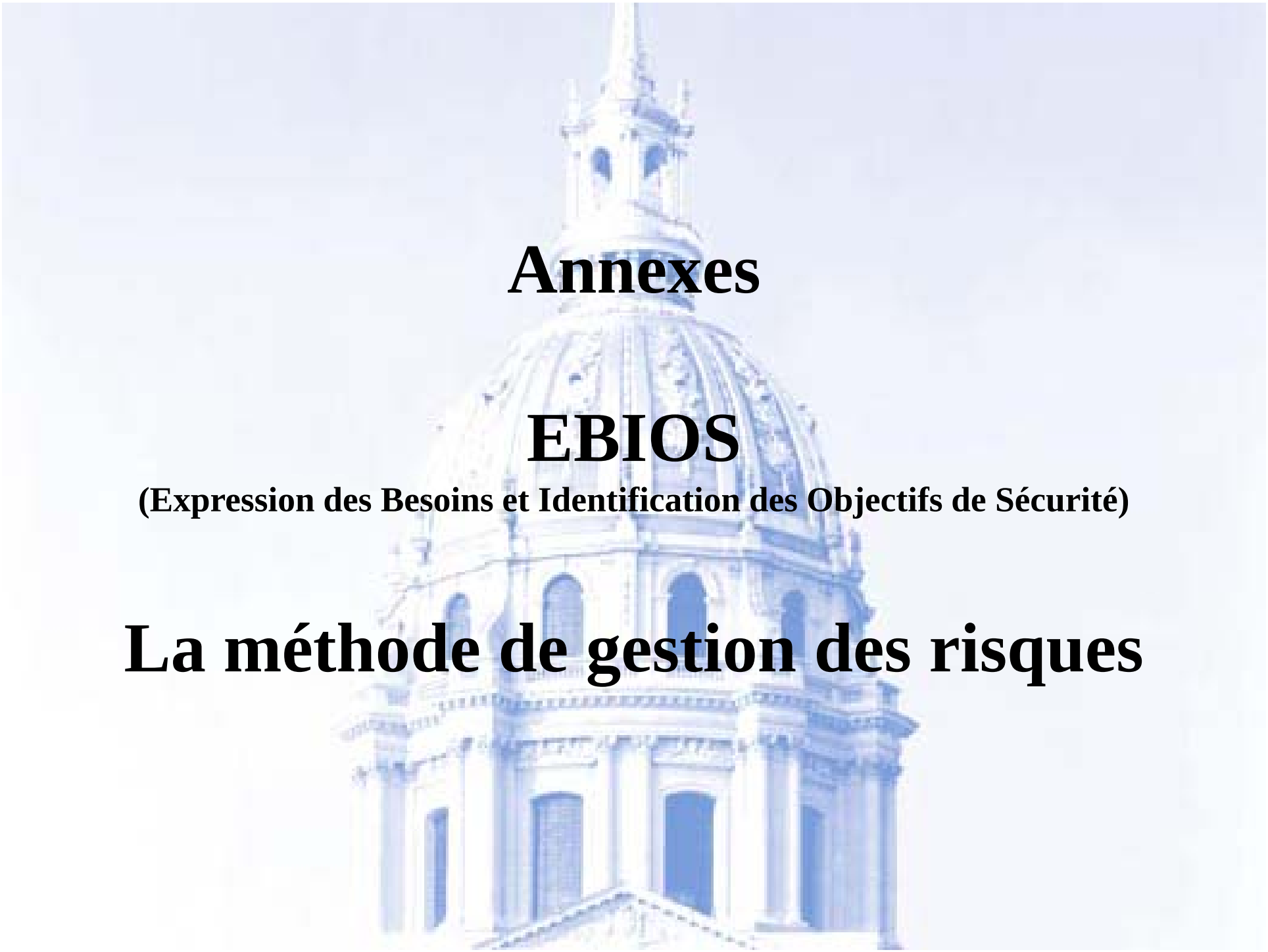
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Coût de la démarche

- Une approche modulaire selon les enjeux et le sujet étudié…
  - ✓ En survol ou détaillée
  - ✓ Globale ou focalisée
  - ✓ Premiers pas ou capitalisation d'expériences

- …pour des résultats adaptés
  - ✓ Une note de stratégie de sécurité (exemple : 4-8 h.j)
  - ✓ Une politique de sécurité (exemple : 20-50 h.j)
  - ✓ Un cahier des charges (exemple : 10-20 h.j)
  - ✓ Un plan d'action, un référentiel d'audit, des tableaux de bord…

(les charges dépendent de nombreux facteurs tels que le périmètre étudié, sa complexité, le nombre de personnes impliquées…)



Annexes

EBIOS

(Expression des Besoins et Identification des Objectifs de Sécurité)

La méthode de gestion des risques

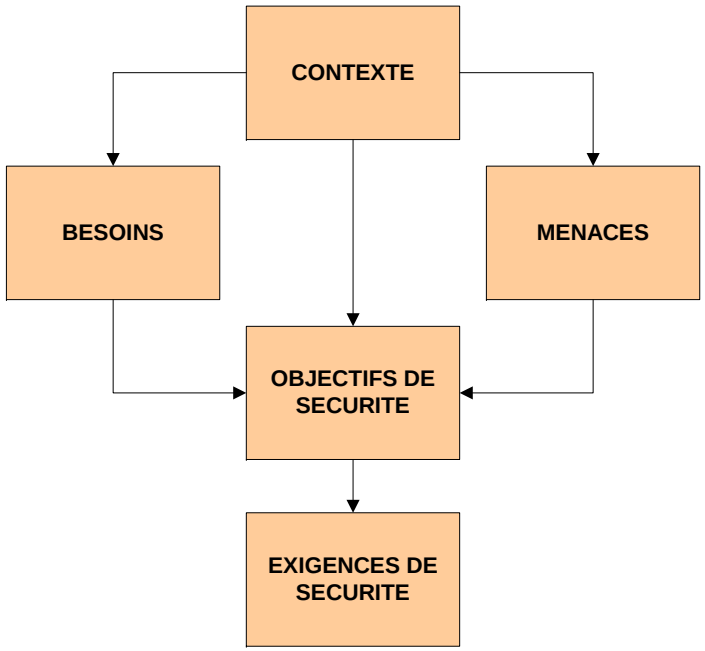
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Les utilisateurs de la méthode

- Exemples d'organismes utilisateurs ou clients
  - ✓ Ministères (systématiquement dans certains, encouragé partout ailleurs)
  - ✓ L'ensemble des ministères et industriels dès lors qu'un système traite des informations classifiées de défense
  - ✓ Aéroports de Paris (ADP)
  - ✓ Agences sanitaires
  - ✓ Caisse nationale d'assurance maladie (CNAM)
  - ✓ Centre national d'études spatiales (CNES)
  - ✓ Commissariat à l'énergie atomique (CEA)
  - ✓ Conseil de l'Union européenne
  - ✓ France Télécom
  - ✓ GIE cartes bancaires
  - ✓ Michelin
- Exemples de prestataires (par ordre alphabétique)
  - ✓ ALCATEL CIT
  - ✓ ALGORIEL
  - ✓ AQL
  - ✓ DICTAO
  - ✓ EADS
  - ✓ FIDENS
  - ✓ MISIS
  - ✓ ON-X / EDELWEB
  - ✓ OPPIDA
  - ✓ ORASYS
  - ✓ TEAMLOG
  - ✓ TELINDUS / CF6
  - ✓ THALES SECURITY SYSTEMS
  - ✓ XP-CONSEIL

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

Les apports de chaque étape



- Étude du contexte
  - ✓ Vision globale et explicite du système étudié, des enjeux, des contraintes et référentiels applicables
- Expression des besoins
  - ✓ Positionnement des éléments à protéger (patrimoine informationnel) en terme de disponibilité, intégrité, confidentialité… et mise en évidence des impacts en cas de sinistre
- Étude des menaces
  - ✓ Recensement des scénarios pouvant porter atteinte aux composants (techniques ou non) du SI
- Identification des objectifs de sécurité
  - ✓ Mise en évidence des risques réels et expression de la volonté de les traiter en cohérence avec le contexte particulier de l'organisme
- Détermination des exigences de sécurité
  - ✓ Spécification des mesures concrètes à mettre en œuvre pour traiter les risques sur la base d'une négociation argumentée

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

Les résultats de la méthode

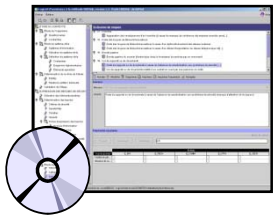
EBIOS

- Schéma directeur
- Note de stratégie
- Politique de sécurité
- Cahier des charges
- Plan d'action
- Tableaux de bord
- Référentiel d'audit
- Négociation & arbitrage
- Responsabiliser les acteurs

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

L'outillage et les services

- Les guides
  - ✓ La méthode et ses bases de connaissances (5 sections), ses meilleures pratiques expliquant comment utiliser EBIOS selon le contexte
  - ✓ Des plaquettes et un mémento synthétiques



- Le logiciel libre
  - ✓ Gratuit, disponible sur demande ou en téléchargement
  - ✓ Plus de 2000 cédéroms envoyés dans 50 pays
- Les traductions

  - ✓ L'ensemble du référentiel est disponible gratuitement en français, en anglais, en allemand et en espagnol
- Les compétences
  - ✓ Les formations au CFSSI pour les agents de l'administration (formation de 2 jours, formation de formateurs de 5 jours, formations ad-hoc)
  - ✓ La formation en ligne sur la gestion des risques (en cours)
  - ✓ La labellisation de personnes (en cours d'élaboration)

- Le Club EBIOS
  - ✓ 75 experts du secteur public et du secteur privé, français et étrangers