
phosforea
my learning experience

Gérer ses risques avec EBIOS

phosforea
my learning experience

Principe général

- Il ne faut pas confondre la gestion des risques avec l'appréciation des risques

1. Gestion des risques = ensemble de processus
2. Appréciation des risques = un des processus de la gestion des risque

Références

- Norme ISO31000, clause 4.4.1 : mise en œuvre du cadre organisationnel de management du risque
  1. Définir un calendrier et une stratégie appropriés
  2. Appliquer la politique et le processus de management du risques aux processus organisationnels
  3. Se conformer aux obligations légales et réglementaires
  4. Communiquer et se concerter avec les parties prenantes …
  5. …

Démarche de mise en oeuvre

phosforea
my learning experience

Présentation de la démarche

phosforea
my learning experience

1. Obtenir un mandat de la direction et son engagement

- ISO31000, clause 4.2 - Il convient que la direction :
  1. Définissent et approuve la politique de management du risque
  2. S'assure que la culture de l'organisme et sa politique sont en phase
  3. Détermine des indicateurs de performance
  4. …
  5. S'assure que les ressources nécessaires sont allouées
  6. Communique à l'ensemble des parties prenantes

2. Nommer un responsable

- Ses responsabilités
  1. Planifier les activités
  2. Gérer l'équipe de gestion des risques
  3. Rédiger les rapports d'appréciation des risques
  4. Gérer les communication et la sensibilisation du risque avec les parties prenantes
  5. Assurer le suivi des recommandations

phosforea
my learning experience

3. Définir les responsabilités

Direction	• Approuve le risque et mène les arbitrages … est resp. des risques
Finances	• Participe à l'analyse des coûts et suit le budget
RH	• Participe à l'élaboration des plans de formation/sensibilisation • Contribue au recrutement des personnels
Sécurité	• Révélateur des risques : identifie et propose des mesures appropriées
DSI	• Met en place et exploite les mesures de sécurité IT
Juridique	• Identifie les exigences légales et règlementaires
Marketing/comm.	• Etudie les impacts sur la réputation de l'entreprise
Qualité	• Assure la conformité du programme de gestion des risques

4. Choisir une méthodologie d'analyse des risques

- Compatible ISO27001 … et ISO27005

5. Déterminer les ressources nécessaires

- Selon l'ISO27001, clause 5.2.1 et l'ISO31000, clause 4.3.5 – L'organisme doit déterminer et fournir les ressources nécessaires pour :
  - Effectuer l'évaluation des risques et établir un plan de traitement des risques
  - Définir et mettre en œuvre les politiques et les mesures de sécurité sélectionnées
  - Effectuer des examens et surveiller le processus de gestion des risques

6. Planifier les activités

- Etape essentielle au succès des projets d'appréciation des risques
- Préférable de faire coïncider l'élaboration du PdTR avec celle du budget d'organisme
- Participation active et obligatoire des parties prenantes

phosforea
my learning experience

7. Etablir la politique de management des risques

- Proche de la politique du SMSI ou PSI
  1. Objectifs et engagement de la direction
  2. La gouvernance : responsabilités et comitologies
  3. Le domaine d'application
  4. Cadre légal et réglementaire
  5. L'appétence aux risques

Plus d’informations

phosforea
my learning experience

Outillage / Références

- Les différents documents relatifs à la méthode EBIOS (guide méthodologique, étude de cas, base de connaissance…) sont disponibles à l'adresse suivante :
  - http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

- Un logiciel permettant l'enregistrement de toutes les données d'analyse de risque est également disponible :
  - https://adullact.net/projects/ebios2010/

- Un fichier excel est à votre disposition dans l'onglet « RESSOURCES » pour vous aider à réaliser vos analyses de risque

phosforea
my learning experience

Fin du module

Ce module est à présent terminé, vous pouvez retourner sur votre tableau de bord.

phosforea
my learning experience