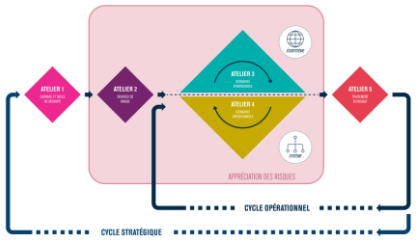


Références

- ☐ **PRENDRE LA MESURE DU RISQUE NUMÉRIQUE**
- ☐ **COMPRENDRE LE RISQUE NUMÉRIQUE ET S'ORGANISER**
  - ■ Étape 1 Définir un cadre de gouvernance du risque numérique
  - ■ Étape 2 Comprendre son activité numérique
  - ■ Étape 3 Connaître son seuil d'acceptation des risques
  - ■ Étape 4 Construire ses pires scénarios de risque
  - ■ Étape 5 Définir sa stratégie de sécurité numérique et de valorisation
  - ■ Étape 6 Mettre en place des polices d'assurance adaptées
- ☐ **BÂTIR SON SOCLE DE SÉCURITÉ**
  - ■ Étape 7 Placer l'humain au centre du jeu
  - ■ Étape 8 Homologuer ses services numériques critiques
  - ■ Étape 9 Bâtir sa protection
  - ■ Étape 10 Orienter sa défense et anticiper sa réaction
  - ■ Étape 11 Faire preuve de résilience en cas de cyberattaque
- ☐ **PILOTER SON RISQUE NUMÉRIQUE ET VALORISER SA CYBERSÉCURITÉ**
  - ■ Étape 12 Connaissance : de la veille à l'analyse
  - ■ Étape 13 Engagement : de l'adhésion à l'action
  - ■ Étape 14 Agilité : l'amélioration continue et la performance
  - ■ Étape 15 Valorisation : la cybersécurité, un avantage compétitif

ATELIER 1 – CADRAGE ET SOCLE DE SÉCURITÉ

a. définir le cadre de l'étude ;
b. définir le périmètre métier et technique de l'objet étudié ;
c. identifier les événements redoutés et évaluer leur niveau de gravité ;
d. déterminer le socle de sécurité.

ATELIER 2 – SOURCES DE RISQUE

a. identifier les sources de risque et les objectifs visés ;
b. évaluer les couples SR/OV ;
c. sélectionner les couples SR/OV jugés prioritaires pour poursuivre l'analyse.

ATELIER 3 – SCÉNARIOS STRATÉGIQUES

a. construire la cartographie de menace numérique de l'écosystème et sélectionner les parties prenantes critiques ;
b. élaborer des scénarios stratégiques ;
c. définir des mesures de sécurité sur l'écosystème.

ATELIER 4 – SCÉNARIOS OPÉRATIONNELS

a. élaborer les scénarios opérationnels ;
b. évaluer leur vraisemblance.

ATELIER 5 – TRAITEMENT DU RISQUE

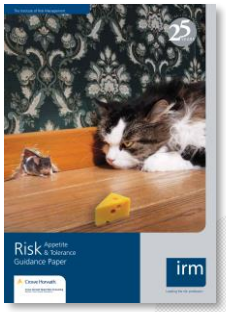
a. réaliser la synthèse des scénarios de risque ;
b. définir la stratégie de traitement du risque et les mesures de sécurité ;
c. évaluer et documenter les risques résiduels ;
d. mettre en place le cadre de suivi des risques.

Powered by CONIX

Synthèse des Références

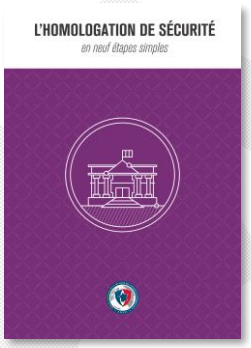
Gouvernance de la cybersécurité

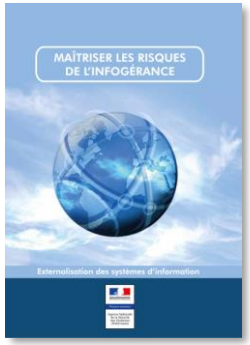
Appétence au risque



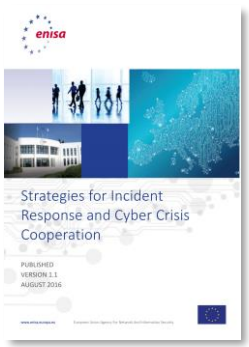
Cyberassurance

Guides ANSSI associés





Dispositif de maîtrise du risque cyber & Stratégie de cyberdéfense



Continuité d'activité & Résilience