

## Formation Management des risques (ISO 27005)

<b>Durée :</b>	3 jours
<b>Public :</b>	Managers, Chefs de projets
<b>Pré-requis :</b>	Avoir pris connaissance du Guide d'hygiène informatique de l'Agence Nationale de la Sécurité des Systèmes d'Information
<b>Objectifs :</b>	Implémenter la norme ISO 27005 - Gérer les risques en sécurité - Approuver des risques résiduels - Identifier des menaces, des vulnérabilités, des impacts
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	GES101581-F
<b>Note de satisfaction des participants:</b>	Pas de données disponibles

### Découvrir la norme ISO 27005

- Risque : définition, concepts associés
- Statistiques associées à la gestion du risque
- Perception du risque
- Norme ISO 27005 : contenu, méthodologie, complément du SMSI ISO 27001
- Mise en place d'une gestion des risques

### Établir le contexte

- Définition des critères d'évaluation, d'impact et d'acceptation
- Choix d'une échelle pour les critères
- Définir les champs, les limites et l'environnement du processus de gestion du risque

### Apprécier les risques

- Définition des éléments qui composent le risque
- Expression des besoins de sécurité
- Caractérisation en termes d'opportunités les menaces pesant sur le système d'information
- Confrontation des menaces aux besoins de sécurité
- Analyse et évaluation des risques : priorité et ordonnancement par rapport aux critères d'évaluation
- Appréciation des risques avec une méthode quantitative : ROSI

### Traiter les risques

- Processus de sélection et de mise en œuvre des mesures
- Détermination des modes de traitement : refus ou évitement, transfert, réduction, conservation

Formalisme par une matrice des risques

### **Accepter les risques**

Homologation de sécurité : contenu, politique  
Approbation des risques résiduels  
Gestion des risques résiduels

### **Communiquer sur les risques**

Partage d'informations sur les risques entre les différentes parties prenantes  
Réduction des incompréhensions  
Etablir un plan de communication

### **Surveiller et réexaminer du risque**

Identification des changements nécessitant une réévaluation du risque  
Identification des nouvelles menaces et vulnérabilités  
Mesure du niveau de maturité

### **Apprendre des méthodes d'analyse de risques**

OCTAVE : analyse des risques  
MEHARI (Méthode harmonisée d'analyse des risques)  
EBIOS : management des risques  
ERM  
HAZard