Catalogue de formations 2024

Continuité d'activité

et

Cybersécurité organisationnelle

HS2
Hervé Schauer Sécurité

SOMMAIRE ET CALENDRIER

Continuité d'activité

Cybersécurité organisationnelle

***Examen de certification HS2 inclus**
***Examen de certification ISC² inclus si option choisie**
* **Examen de certification ISACA inclus si option choisie**
***Examen AFNOR Certification si option choisie**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Cybersécurité organisationnelle				
Réf.	Formations	Durée	Sessions	Pages
MAJ27	Mise à jour ISO 27001 & ISO 27002	**1 J**	• 29 avril 2024 • 6 septembre 2024	**30-31**
ISO27LA***	ISO 27001 Lead Auditor	**5 J**	• 17 au 21 juin 2024 • 9 au 13 septembre 2024 • 4 au 8 novembre 2024	**32-33**
ISO27LI***	ISO 27001 Lead Implementer	**5 J**	• 26 février au 1er mars 2024 • 13 au 17 mai 2024 • 24 au 28 juin 2024 • 23 au 27 septembre 2024 • 25 au 29 novembre 2024 • 16 au 20 décembre 2024	**34-35**
IS027RM***	ISO 27005 Risk Manager	**3 J**	• 26 au 28 février 2024 • 2 au 4 avril 2024 • 3 au 5 juin 2024 • 9 au 11 septembre 2024 • 18 au 20 novembre 2024 • 16 au 18 décembre 2024	**36-37**
ISO27004	ISO27004 / Indicateurs et tableaux de bord cybersécurité	**1 J**	• 12 juin 2024 • 15 novembre 2024	**38-39**
ISO27035	ISO27035 / Gestion des incidents de sécurité	**1 J**	• 29 avril 2024 • 13 décembre 2024	**40-41**
Nos intervenants				**42-43**
Bulletin d'inscription				**44**

***Examen de certification HS2 inclus**

****Examen de certification BestCertif si option choisie**

***Examen de certification Certi-Trust si option choisie**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « RPCA »

Réf : RPCA

Objectifs

- Comprendre les fondamentaux de la Continuité d'Activité,
- Prendre en compte le contexte réglementaire et juridique,
- Connaître l'état du marché de la continuité (aspect techniques),
- Apprécier les enjeux et les risques métiers,
- Formaliser un PCA efficient,
- Évaluer le fonctionnement de mon PCA,
- Gérer une crise,
- Mettre en œuvre des stratégies de prise de fonction.

Durée & horaires

- 5 jours soit 35 heures,
- Du lundi au jeudi de 9h30 à 12h et de 13h30 à 17h30/18h00,
- Le vendredi de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne amenée à exercer la fonction de responsable du Plan de continuité d'activité :
  - RPCA,
  - Futur RPCA,
  - RSSI,
  - Assistant DSI
  - Ingénieurs sécurité assistant un RPCA,
  - Responsables de production.
- Les techniciens devenus RPCA, souhaitant obtenir une culture de management.
- Les managers confirmés manquant de la culture technique de base en matière de continuité d'activité ou ne connaissant pas les acteurs du marché.
- Toute personne amenée à assurer une fonction de correspondant local continuité d'activité ou une fonction similaire.

Pré-requis

- Aucun prérequis n'est demandé. Toutefois avoir une expérience du contexte informatique et en gestion de projet est un plus.

Méthode pédagogique

La méthode pédagogique se base sur les 4 points suivants :

- Cours orientés sur la mise en œuvre pratique de processus de continuité d'activité dans le cadre de la norme ISO 22301,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Supports

- **Support de cours au format papier et en français,**
- **Cahier d'exercices et corrections.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. La réussite à l'examen donne droit à la certification RPCA par HS2.**

Programme

Introduction - Fondamentaux de la continuité d'activité

- Interactions : RSSI, RM, Production, Direction, métiers, Services Généraux, Conformité, Juridique, RH, etc.
- Stratégies de prise de fonction du RPCA,
- Présentation de la terminologie.

Contexte réglementaire et juridique

- Panorama des référentiels du marché (lois, règlement, normes et bonnes pratiques),
- Normalisation ISO 22300 et 27000,
- Informatique et libertés, GDPR.

Aspects techniques de la continuité

- Sauvegarde & restauration,
- Réplication ou redondance,
- Réseau et télécoms.

Apprécier les enjeux et les risques métiers

- Appréciation des risques en continuité d'activité,
- Processus critiques : Bilan d'Impact sur l'Activité (BIA)

Acteurs du marché de la continuité

- Gestion des relations avec les partenaires,
- Externaliser vers un prestataire,
- Comment choisir ?

Formaliser un PCA efficient

- Projet PCA (prérequis, gouvernance, délais, livrables, etc.),
- PGC : Plan Gestion de Crise,
- PCOM : Plan de Communication (interne et externe),
- PRM : Plan de reprise métier,
- PCIT : Plan de Continuité Informatique et Télécoms,
- PRN : Plan de Retour à la Normale.
- Mon PCA fonctionne-t-il ?
- Les exercices et tests,
- L'importance du rôle d'observateur,
- Audit du PCA,
- Maintien en Condition Opérationnelle (MCO),
- Outils de gouvernance, gestion, pilotage du PCA.

Gérer une crise

- Activer tout ou partie du PCA,
- Communiquer pendant la crise,
- Assurer le retour à la normale,
- Intégrer les retours d'expérience (RETEX).

Témoignage d'un RPCA en fonction des possibilités

Examen

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « ISO 22301 Lead Auditor »

Réf : ISO22LA

Objectifs

- Comprendre le fonctionnement d'un SMCA selon l'ISO 22301,
- Comprendre le déroulement, les spécificités et les exigences d'un audit ISO 22301,
- Acquérir les compétences pour réaliser un audit interne ou un audit de certification ISO22301 en fonction de la norme ISO19011,
- Gérer une équipe d'auditeurs de SMCA,
- Comprendre la mise en œuvre d'un processus de certification ISO22301,
- Devenir auditeur ISO 22301 certifié.

Durée & horaires

- 5 jours soit 35 heures dont 2h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- RPCA
- Consultants – Auditeurs
- Chefs de Projets
- Responsables de la conformité
- Qualiticiens
- Contrôles internes

Pré-requis

- Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans
- Connaître les principes fondamentaux de la Continuité d'Activité
- RPCA

Méthode pédagogique

La méthode pédagogique se base sur les 6 points suivants :

- Cours magistral basé sur les normes ISO 19001, ISO 22301, ISO 22313, ISO 27031, ISO 31000,
- Exercices pratiques individuels et collectifs basés sur une étude de cas,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs,
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Supports

- **Support de cours au format papier et en français,**
- **Cahier d'exercices et corrections.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen HS2 22301 Lead Auditor. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Programme

Accueil des participants

- Présentation générale du cours
- Introduction aux systèmes de management
- Principes fondamentaux de la continuité d'activité.

Présentation détaillée de la norme ISO22301

- Notions de Système de Management de la Continuité d'Activité (SMCA)
- Modèle PDCA (Plan – Do – Check - Act)
- Les exigences :
  - Comprendre l'organisation et son contexte,
  - Engagement de la Direction,
  - Analyse des impacts Métier (BIA) et appréciation des risques
  - Définir les stratégies de continuité
  - Développer et mettre en œuvre les plans et procédures de continuité d'activité
  - Tests et exercices
  - Surveillance et réexamen du SMCA
  - Amélioration continue
  - Les enregistrements

Panorama des normes ISO complémentaires :

- ISO 19011
- ISO 22313
- ISO 27031
- ISO 31000
- Présentation de la continuité d'activité
- Procédures de continuité d'activité
- Exercices et tests
- Retours d'expérience sur l'audit de Plans de Continuité d'Activité (PCA)

Processus de certification ISO 23201

Présentation de la démarche d'un SMCA basé sur l'ISO 19011

- Norme ISO 19011
- Audit d'un SMCA
- Règlement de certification
- Exemples pratiques

Techniques de conduite d'entretien

Exercices de préparation à l'examen

Examen conçu, surveillé et corrigé par HS2

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « ISO 22301 Lead Implementer »

Réf : ISO22LI

Objectifs

- Comprendre la mise en œuvre d'un SMCA suivant l'ISO 22301,
- Apprendre les concepts, approches, méthodes et techniques requises pour gérer un SMCA,
- Acquérir les compétences nécessaires pour accompagner et conseiller une organisation dans l'implémentation et la gestion d'un SMCA conformément à l'ISO 22301,
- Devenir un implémenteur certifié ISO 22301

Durée & horaires

- 5 jours soit 35 heures dont 2h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Responsables en charge de la Continuité d'Activité – RPCA,
- Secrétaires généraux,
- Responsables de directions opérationnelles,
- Gestionnaires de risque,
- Chefs de projet,
- Consultants.

Pré-requis

- Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans,
- Connaître les principes fondamentaux de la Continuité d'Activité.

Méthode pédagogique

La méthode pédagogique se base sur les 7 points suivants :

- Cours magistral basé sur les normes ISO 22301, ISO 22313, ISO 27031, ISO 31000,
- Exercices pratiques individuels et collectifs basés sur une étude de cas,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs
- Quiz pour préparation à l'examen,
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session

Supports

- Support de cours au format papier et en français,
- Cahier d'exercices et corrections.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de certification à la norme 22301 HS2 (ISO 22301 Lead Implementer). Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Programme

Introduction

- Introduction des systèmes de management,
- Principes fondamentaux de la continuité d'activité.

Présentation détaillée de la norme ISO22301

- Notions de Système de Management de la Continuité d'activité (SMCA),
- Modèle PDCA (Plan – Do – Check - Act),
- Les processus du SMCA
  - Direction,
  - Pilotage du SMCA,
  - Gestion de la conformité,
  - Gestion des impacts sur l'activité,
  - Gestion des risques,
  - Gestion des stratégies de continuité,
  - Gestion des incidents perturbateurs
  - Documentation et enregistrements,
  - Ressources, compétences et sensibilisation,
  - Surveillance et revue,
  - Gestion des actions correctives.

Panorama des normes ISO complémentaires : ISO 22313, ISO 27031, ISO 31000

Présentation des processus de continuité d'activité

- Analyse des impacts sur l'activité ou Business Impact Analysis (BIA),
- Appréciation du risque pour un SMCA sur la base de l'ISO 31000,
- Procédures de continuité d'activité,
- Exercices et tests, Retours d'expérience sur l'implémentation de Plans de Continuité d'Activité (PCA).

Mener un projet d'implémentation d'un SMCA

Convaincre la Direction

- Les étapes du projet
- Les acteurs
- Les facteurs clés de succès
- Les risques et opportunités

Intégration de l'ISO 27031 dans le SMCA

Processus de certification ISO 22301

Gestion des indicateurs

Préparation de l'examen

Examen conçu, surveillé et corrigé par HS2

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « RSSI »

Réf : RSSI

La fonction de "RSSI" est un métier transverse et multi-facettes. La formation RSSI HS2 apporte au nouveau RSSI un panorama complet des fonctions du RSSI et des attentes des organisations sur le rôle du RSSI et les connaissances indispensables à sa prise de fonction. Un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par des RSSI et des consultants expérimentés.

Objectifs

- **Acquérir les compétences indispensables à l'exercice de la fonction responsable de la sécurité des systèmes d'information, à savoir :**
  - **Enjeux de sécurité des SI dans les organisations**
  - **Connaissances techniques essentielles**
  - **Organisation de la sécurité et normes ISO27001**
  - **Politiques de sécurité, audit de sécurité et indicateurs**
  - **Méthodes d'appréciation des risques**
  - **Aspects juridiques de la sécurité des SI**
  - **Sensibilisation à la sécurité des SI et gestion des incidents**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Toute personne amenée à exercer la fonction de responsable sécurité des systèmes d'information : RSSI, futurs RSSI, RSSI adjoint, responsables sécurité opérationnelle à la production, correspondant local de sécurité des systèmes d'information**
- **Techniciens devenus RSSI, souhaitant acquérir des notions en gouvernance et management de la sécurité des SI**
- **Spécialistes de domaines transverses des systèmes d'information (qualité, audit, gestion de projets) devant compléter leurs compétences dans le domaine de la sécurité des systèmes d'information**

Pré-requis

- **Il est préférable d'avoir une expérience au sein d'une direction informatique en tant qu'informaticien ou bonne culture générale des systèmes d'information.**
- **Avoir des notions de base en sécurité appliquées au système d'information constitue un plus.**

Méthode pédagogique

- **Cette formation est proposée en mode présentiel et peut être accessible en mode distanciel via ZOOM pour les personnes qui ne peuvent ou ne veulent pas se déplacer**
- **Cours magistral dispensé à chaque fois par des experts de chaque module**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- **Dans les modules "gestion des risques" et "juridique", des exercices de contrôle des connaissances et dans les autres modules, des démonstrations ou de nombreux exemples pratiques basés sur les retours d'expérience des instructeurs et ceux de leurs clients**
- **Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges davantage concrets, en corrélation avec les attentes des stagiaires**
- **Animation par un RSSI en activité, présentant sa stratégie de prise de fonction et un retour d'expérience sur des cas concrets et détaillés de projets sécurité menés dans son organisation.**

Supports

- **Support de cours en français au format papier pour le présentiel et au format numérique pour le distanciel (sous réserve du règlement intérieur signé)**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification RSSI par HS2.**

Programme

Accueil des participants et tour de table

Enjeux de la sécurité des systèmes d'information (1 jour)

- Introduction
  - Objectifs de la cybersécurité
  - Objectifs des organisations
  - Alignement stratégique organisation / cybersécurité
  - Objectifs et organisation de la formation
- Enjeux de la cybersécurité
  - Sécurité des SI, de l'information, informatique et cybersécurité
  - Vocabulaire : critères et objectifs
  - Le critère de preuve
  - Vocabulaire : incident et risque
- Activités du RSSI
  - Le RSSI, polyvalent face aux enjeux
  - La politique de sécurité
  - Le programme de sécurité
  - Les mesures de sécurité
  - Le RSSI dans les projets
  - Le RSSI et les associations professionnelles
- Introduction à la menace cyber
  - Gérer le risque
  - Dans la peau d'un attaquant
  - Sécurité - Règles de base

Aspects techniques de la cybersécurité (1 jour)

- Introduction à la cryptographie
- Sécurité réseau
  - Principes de base du réseau
  - Attaques et mesures
  - Pare-feu et proxy
  - Architecture sécurisée
- Sécurité applicative
  - Vulnérabilités mémoire
  - Vulnérabilités web
  - Développement sécurisé
- Sécurité système
  - Principes
  - Contrôle d'accès
  - Veille sécurité
  - Mise à jour
  - Sauvegarde
  - Journalisation
  - Protection du poste de travail
  - Équipements mobiles
  - Auditer son SI

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Système de Management de la Sécurité de l'Information (normes ISO 2700x) (1/4 journée)

- Introduction à ISO 27001
- Systèmes de management et SMSI
  - Exemples de systèmes de management
  - Propriétés des systèmes de management
  - Processus du SMSI
- Introduction à ISO 27002
- Comment utiliser les normes
- Conclusion et bienfaits du SMSI ISO 27001

Politiques de sécurité (1/4 journée)

- Définitions
- Hiérarchie et utilité des politiques de sécurité
- Politiques spécifiques, organisation et exemples
- Rédaction, élaboration et mise en œuvre des politiques
- Révision des politiques
- Synthèse et éléments indispensables des politiques

Indicateurs en sécurité des SI (1/4 journée)

- Introduction et règles d'or
- Sources de collecte des indicateurs
- Spécification des indicateurs et exemples
- Indicateurs dérivés et exemples
- Risques sur les indicateurs, questions pratiques et erreurs à éviter

Audit (1/4 journée)

- Typologie des audits (technique, organisationnel, de conformité, de certification)
- Conséquences (inconvénients et objectifs)
- Vocabulaire (basé sur ISO 19011)
- Préparation à l'audit
- Considérations pratiques (formation, communication, intendance, audit à blanc, préparation)
- Démarche d'audit (ISO 19011)
- Avant l'audit, pendant l'audit, après l'audit
- Livrable
- Actions correctives entreprises et suivi
- Réception des auditeurs (maison-mère, ISO27001/HDS, ISAE3401/SOC2, Cour des Comptes, Commission bancaire, etc.)

Gestion de risques (1/2 journée)

- Méthodologies d'appréciation des risques (ISO27001, EBIOS, Mehari)
- Vocabulaire
- Identification et valorisation d'actifs
- Menace, source des risques, vulnérabilités
- Analyse de risque
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Évaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)
- Notion de risque résiduel
- Acceptation du risque

Aspects juridiques de la SSI (1/2 journée)

- Focus sur 3 obligations générales de protection du SI
  - Un bref panorama des obligations de SSI
  - LPM et OIV
  - NIS, OSE et FSN
  - RGPD
- Synthèse des principales règles de la SSI au sein des organisations
  - Détecter les incidents
  - Journaliser les activités
  - Encadrer les usages dans les organisations
  - Contractualiser avec les prestataires
- Le volet pénal : réagir aux atteintes à la sécurité des systèmes d'information
  - L'importance de la gestion de crise
  - La qualification des faits de cybercriminalité

Sensibilisation à la sécurité des SI (1h)

- Mesure de sécurité
- Programme de sensibilisation
- Objectif de la sensibilisation
- Moyens de sensibilisation et vecteurs de communication
- Sources d'information
- Conseils
- Rappel des objectifs
- Coûts
- Évaluation

Gestion des incidents en sécurité des SI (1h)

- Définitions
- Exemples d'incidents liés à la sécurité

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- Objectifs de la gestion des incidents liés à la SSI
- Étapes de la gestion d'un incident
  - Préparation, identification et analyse, confinement, endiguement, éradication, recouvrement, retour d'expérience
- Erreurs à éviter
- Outils
- Ressources

Acheter des prestations en sécurité des SI (1h)

- Contexte et objectifs
- Acheter la SSI
  - Définition
  - Le service achats
  - Le processus achats
  - Avant / pendant
  - Après
  - Augmentez votre pouvoir d'achat

Examen (1h30)

Témoignage et retour d'expérience d'un RSSI (1h30)

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « Security by Design »

Réf : SECUBYDESIGN

La maîtrise de la gestion de projet informatique associée aux risques numériques est une dimension essentielle aux systèmes d'information. Ainsi l'intégration réussie de la cybersécurité est une étape clef afin de mener à bien les projets informatiques. Cela amène à mettre en perspectives les enjeux classiques de la gestion de projet notamment en termes de coût/délai/performance, au service d'un métier, avec un contexte où il est souvent nécessaire de composer avec une infogérance, le cloud, la règlementation et les bonnes pratiques en matière de sécurité des systèmes d'information.

La présente formation apporte une vision pragmatique de la sécurité applicable aux projets informatiques. Le retour d'expérience proposé en matière de sécurité et de gestion de projet donnera des clés facilitant le pilotage du projet et la conception d'une sécurité intégrée.

Objectifs

- **Faciliter la prise en compte de la sécurité dans vos projets informatiques**
- **Fiabiliser votre gestion de projets informatiques**
- **Contribuer à niveau de confiance acceptable du SI**
- **Maîtriser les risques liés à la sous-traitance et à l'externalisation**

Durée & horaires

- **2 jours soit 14 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Toute personne qui est ou envisage de mener un projet informatique**
- **DSI, RSSI, chef de projet, responsable opérationnel**
- **Responsable métier, gestionnaire de contrat, gestionnaire de risque**
- **Consultant**

Pré-requis

- **Cette formation ne nécessite pas de pré-requis particulier.**

Méthode pédagogique

- **Cours magistral avec de nombreux exemples anonymisés**
- **Exercices de mise en œuvre**
- **Mises en situation**
- **Support de cours au format papier en français**
- **Certificat attestant de la participation à la formation**

Supports

- **Support de cours au format papier en français**
- **Extraits de documents pratiques : charte informatique, fiches de traitement, etc.**
- **Certificat attestant de la participation à la formation**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Module 1 : Introduction à la sécurité des systèmes d'information

- Le contexte
- Une étude de cas
- Un quizz

Module 2 : Principes de sécurité des systèmes d'information

- Des architectures sécurisées
- Une administration sécurisée des SI
- La sécurité de l'infrastructure
- La sécurisation des développements logiciels et applicatifs : DevSecOps, SDLC, OWASP, CWE, etc
- Les fondamentaux de la cryptographie

Module 3 : Sécurité des systèmes d'information et projet informatique

- Pourquoi intégrer la sécurité dans vos projets ?
- Les rôles et les responsabilités SSI dans les projets
- Les étapes SSI dans les projets : approche Agile intégrée, ISO 27034, etc
- Quelques aspects juridiques et règlementaires : NIS, LPM, RGPD, etc
- La maîtrise des risques : EBIOS RM, MEHARI, etc
- Une étude de cas
- Une sous-traitance maîtrisée : maintien en conditions opérationnelles et de sécurité (MCO-MCS), plan d'assurance sécurité (PAS), référentiel Cloud, etc
- La documentation SSI
- Les audits de sécurité : infrastructure et applications

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

« Préparation au CISSP »

Réf : CISSP

Le CISSP (Certified Information Systems Security Professional) est la certification en sécurité des systèmes d'information proposée depuis 1989 par l'(ISC)² (International Information Systems Security Certification Consortium). C'est l'une des certifications professionnelles les plus reconnues dans le monde. Elle s'appuie sur le CBK (Common Body of Knowledge), tronc commun de connaissances composé de 8 domaines couvrant tous les aspects de la sécurité des systèmes d'information.

La formation CISSP d'HS2 est au format "boot camp" : c'est un entrainement intensif dont l'objectif est de préparer à l'examen de certification CISSP de l'ISC². Afin de tirer un maximum de bénéfices de cette formation, les participants devront être dans la phase finale de leur préparation, le boot camp étant la dernière ligne droite avant la certification. Ils devront notamment avoir lu le CBK officiel ("Official ISC² Guide to the CISSP Exam" (ISC)² Press). La formation s'articule autour des 8 domaines du CBK : pour chacun, les concepts fondamentaux sont d'abord brièvement expliqués, puis les stagiaires sont soumis à des séries de questions auxquelles ils répondent de façon anonyme à l'aide d'un boîtier électronique individuel. Les résultats de chaque question sont ensuite analysés avec les formateurs. Cette méthode permet au stagiaire de "s'imprégner" de l'esprit CISSP et de maximiser ses chances de réussite.

Objectifs

- **Préparer sereinement les participants à l'examen de certification CISSP de l'ISC²**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Professionnels de la sécurité souhaitant valoriser leurs expériences**
- **Personnes souhaitant acquérir une certification en sécurité reconnue au niveau mondial**

Pré-requis

- **Avoir lu le CBK ("Official ISC² Guide to the CISSP Exam - (ISC)² Press).**

Méthode pédagogique

- **Rappels des points clés à connaitre dans chacun des domaines**
- **Séries de questions ciblées permettant de valider les connaissances**
- **Séries de questions aléatoires visant à mettre les stagiaires en conditions d'examen**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Supports

- **Support de cours au format papier en anglais**
- **Diapositives en anglais à l'écran, avec explications en français par les formateurs**
- **Livre CBK officiel de l'(ISC)² envoyé sur demande, uniquement après réception des documents de confirmation d'inscription.**
- **Livre de révision officiel de l'(ISC)² comprenant :**
  - **Des fiches de révision**
  - **Des questions d'entrainement**
  - **Un examen blanc complet**
- **Questions d'entrainement en anglais**
- **Boîtier électronique individuel pour répondre aux questions**
- **Certificat (ISC)² attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Examen de certification CISSP de l'(ISC)² à passer dans un centre PearsonVue (www.pearsonvue.com). HS2 est partenaire officiel de l'(ISC)² en France et au Luxembourg et est autorisée à vendre l'examen CISSP dans ces deux pays.**

Programme

Lundi

- **Matin :** Accueil et introduction au CISSP
- **Après-midi :** Information Security & Risk Management

Mardi

- **Matin :** Assets Security
- **Après-midi :** Security Architecture & Engineering

Mercredi

- **Matin :** Identity & Access Management
- **Après-midi :** Security Operations

Jeudi

- **Matin :** Security Assessment and Testing
- **Après-midi :** Software Development Security

Vendredi

- **Matin :** Software Development Security + Communication & Network Security
- **Après-midi :** Communication & Network Security

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

« Préparation au CCSP »

Réf : CCSP

La certification CCSP, créée en 2015 par l'(ISC)² en partenariat avec le CSA (Cloud Security Alliance), est l'une des certifications les plus reconnues dans le domaine du cloud computing. C'est la certification "soeur" du CISSP, entièrement focalisée sur les problématiques liées à l'infonuagique. Elle s'appuie sur le CCSP CBK (Common Body of Knowledge), tronc commun de connaissances composé de 6 domaines couvrant tous les aspects de la sécurité du Cloud.

La formation CCSP d'HS2 est au format "boot camp" : c'est un entrainement intensif dont l'objectif est de préparer à l'examen de certification CCSP de l'(ISC)². Afin de tirer un maximum de bénéfices de cette formation, les participants devront être dans la phase finale de leur préparation, le boot camp étant la dernière ligne droite avant la certification. Ils devront notamment avoir lu le CBK officiel (« Official (ISC)² Guide to the CSSP CBK », Sybex). La formation s'articule autour des 6 domaines du CCSP : pour chacun, les concepts fondamentaux sont d'abord brièvement expliqués, puis les stagiaires sont soumis à des séries de questions auxquelles ils répondent de façon anonyme à l'aide d'une application en ligne similaire à celle de l'examen réel. Les résultats de chaque question sont ensuite analysés avec les formateurs. Cette méthode permet au stagiaire de « s'imprégner » de l'esprit CCSP et de maximiser ses chances de réussite.

Objectifs

- **Préparer sereinement les participants à l'examen de certification CCSP de l'ISC²**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Architecte**
- **Administrateur**
- **Manager sécurité**
- **Ingénieur sécurité**
- **Chef de projet**
- **Consultant en sécurité**
- **Toute personne souhaitant valoriser ses expériences dans le domaine du Cloud**

Pré-requis

- **Avoir lu le CBK ("Official (ISC)² Guide to the CCSP CBK" - Sybex).**

Méthode pédagogique

- **Rappels des points clés à connaitre dans chacun des domaines**
- **Séries de questions ciblées permettant de valider les connaissances**
- **Séries de questions aléatoires visant à mettre les stagiaires en conditions d'examen**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Supports

- **Support de cours au format papier en anglais**
- **Diapositives en anglais à l'écran, avec explications en français par les formateurs**
- **Livre CCSP CBK officiel de l'(ISC)² envoyé sur demande, uniquement après réception des documents de confirmation d'inscription.**
- **Livre de révision officiel de l'(ISC)² comprenant :**
  - **Des fiches de révision**
  - **Des questions d'entrainement**
  - **Un examen blanc complet**
- **Questions d'entrainement en anglais**
- **Ordinateur mise à disposition pendant la formation pour répondre aux questions**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Examen de certification CCSP de l'(ISC)² à passer dans un centre PearsonVue (www.pearsonvue.com). HS2 est partenaire officiel de l'(ISC)² en France et au Luxembourg et est autorisée à vendre l'examen CCSP dans ces deux pays.**

Programme

Accueil et introduction au CCSP

Domaine 1. Architectural Concepts & Design Requirements :
- Rappel des fondamentaux
- Test d'entrainement

Domaine 2. Cloud Data Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 3. Cloud Platform & Infrastructure Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 4. Cloud Application Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 5. Operations
- Rappel des fondamentaux
- Test d'entrainement

Domaine 6. Legal and Compliance
- Rappel des fondamentaux
- Test d'entrainement

Entrainement final

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

« Préparation au CISA »

Réf : CISA

Le CISA (Certified Information Systems Auditor) est la certification internationale des auditeurs des systèmes d'information. Cette certification est régulièrement exigée auprès des auditeurs informatiques et sécurité. Elle est éditée par l'association internationale des auditeurs informatiques ISACA (http://www.isaca.org/).

La formation CISA d'HS2 est au format "boot camp" : c'est un entraînement intensif dont l'objectif est de réussir l'examen. La formation s'articule autour des thèmes du CISA : la pratique de l'audit SI; la gouvernance des SI; l'acquisition et l'implantation des SI; l'exploitation et la gestion des SI; l'audit de l'informatique et des opérations, l'audit des infrastructures et des réseaux, la sécurité des actifs informationnels, et le contexte de l'examen (QCM, typologie de questions).

Objectifs

- **Préparer sereinement les participants à l'examen de certification CISA de l'ISACA**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Consultants en organisation, consultants en systèmes d'information, consultants en sécurité.**
- **Auditeurs**
- **Informaticiens**
- **Responsables informatiques**
- **Chefs de projets, urbanistes, managers**

Pré-requis

- **Connaissance générale de l'informatique, de ses modes d'organisation et de son fonctionnement.**
- **Connaissance des principes généraux des processus SI et des principes de base de la technologie des SI et des réseaux.**
- **Avoir lu le CRM (CISA Review Manuel" ou "Manuel de préparation au CISA" officiel de l'ISACA) est un plus**

Méthode pédagogique

- **Cours magistraux par des consultants certifiés CISA**
- **Exercices pratiques par des questions à l'issue de chaque exposé**
- **Examen blanc de 100 questions et explications à chaque mauvaise réponse**

Supports

- **Support de cours en français au format papier**
- **Certificat attestant de la participation à la formation**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Examen de certification CISA de l'ISACA à passer dans un centre PearsonVue (www.pearsonvue.com). HS2 est partenaire officiel de l'ISACA en France et est autorisée à vendre l'examen CISA en package avec la formation.**

Programme

Le stage est organisé sur 5 journées de révision des 5 thématiques de la certification CISA associées à des séries de questions illustratives.

Les 5 domaines abordés (repris dans le CRM et le support de cours) :

- **Le processus d'audit des SI :** méthodologie d'audit, normes, référentiels, la réalisation de l'audit, les techniques d'auto-évaluation.
- **La gouvernance et la gestion des SI :** Pratique de stratégie et de gouvernance SI, politiques et procédures, pratique de la gestion des SI, organisation et comitologie, gestion de la continuité des opérations.
- **L'acquisition, la conception et l'implantation des SI :** la gestion de projet, l'audit des études et du développement, les pratiques de maintenance, contrôle applicatifs.
- **L'exploitation, l'entretien et le soutien des SI :** l'audit de la fonction information et des opérations, l'audit des infrastructures et des réseaux.
- **La protection des actifs informationnels :** audit de sécurité, gestion des accès, sécurité des réseaux, audit de management de la sécurité, sécurité physique, sécurité organisationnelle.

Le stage se termine lors de la dernière journée par un exposé de pratiques pour se préparer et passer l'examen (QCM de 4 heures).
Cet exposé est suivi d'un un examen blanc (2 heures) de 100 questions suivies d'une revue des réponses des stagiaires.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Formation « Homologation de la SSI : RGS, IGI1300, LPM, PSSIE »

Réf : SECUHOMOL

La démarche d'homologation de sécurité des systèmes d'informations s'est imposée dans de multiples référentiels gouvernementaux. Cette approche permet d'expliciter les besoins de sécurité d'un système, d'en évaluer la protection effective et de faire accepter les risques résiduels par une autorité adaptée.

C'est autour de ce cœur méthodologique, que les différents référentiels (RGS, II901, IGI1300, LPM, PSSIE) développent leurs spécificités…

Objectifs

- **Se familiariser avec les différents référentiels gouvernementaux de sécurité de l'information et leurs limites**
- **Mettre en œuvre une démarche d'homologation de sécurité**
- **Fournir les clés pour approfondir les différents cadres réglementaires**
- **Aborder la mise en place d'une organisation de gestion de la sécurité dans la durée**

Durée & Horaires

- **2 jours soit 14 heures**
- **9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participants

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Responsables de mise en conformité au RGS v2**
- **Toute personne ayant la nécessité de connaître et comprendre le Référentiel Général de Sécurité**
  - **Agents au sein des autorités administratives**
  - **Prestataires d'hébergement**
  - **Consultants accompagnant à la conformité**
  - **Fournisseurs de services aux autorités administratives**
- **Agents des ministères, rectorats/préfectures, mairies/collectivités territoriales, établissements publics...**

Pré-requis

Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- **Cours magistral avec échanges interactifs**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Programme

Panorama des référentiels SSI étatiques

- Principes de certification/qualification
- Objectifs de l'homologation
- Démarche d'homologation
  - Analyse de risque
  - Mise en œuvre des mesures de sécurité
- Plan de traitement des risques
- Conformité
- IGI1300
- PSSIE
- LPM
- II901
- Cryptographie RGS
  - Audits d'homologation
  - Acte d'homologation
- Dossier d'homologation
- Comité et autorité d'homologation
- Revue et maintien dans la durée
- Stratégies de mise en œuvre
  - Pour nouveau système
  - Pour système existant

Formation « Gestion de crise cyber »

Réf : SECUCRISE

Les méthodes proactives demeurent limitées et tout un chacun est confronté un jour à une crise due à des incidents informatiques ou un problème de sécurité. Il faut donc maîtriser cette réaction d'urgence et savoir y faire face.

Objectifs

- Apprendre à mettre en place une organisation adaptée pour répondre efficacement aux situations de crise
- Apprendre à élaborer une communication cohérente en période de crise
- Apprendre à éviter les pièges induits par les situations de crise
- Tester votre gestion de crise SSI.

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Directeur ou responsable des systèmes d'information
- Responsable de la sécurité des systèmes d'information
- Responsable de la gestion de crise
- Responsable des astreintes
- Responsable de la gestion des incidents

Pré-requis

- Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.

Supports

- Support de cours au format papier en français
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

Programme

Module 1 : Gestion de crise cyber

- Exemple de crises cyber
- Cas concret détaillé d'une crise cyber "rançongiciel"
  - Pourquoi est-ce la principale crainte des organisations ?
  - Quel est l'état d'un système d'information et d'une organisation après le déclenchement d'un rançongiciel ?
  - Description d'une chronologie classique : l'attaque, le constat, la réaction, le suivi et la sortie de crise

Module 2 : Dispositif de crise et les spécificités d'une cyber-attaque

- Vocabulaire : Investigation/Inforensic, Plan de défense, Assainissement, Durcissement, Reconstruction, Main courante, etc.
- Les spécificités d'une crise cyber
- Qu'est-ce qu'un dispositif de gestion de crise cyber ?
- Organisations types
- Processus de la crise : la montée en crise, le lancement, les points de situation, la sortie de crise
- Outillage
- Facteurs humains et gestion du stress
- Logistique et communication
- Cyber-assurance
- Mise en situation : qualification et premier plan d'actions

Module 3 : Observation & Investigation

- Comprendre pour mieux agir
- Plan d'investigation : vecteurs d'intrusion/patient 0, de propagation, mécanismes de persistance
- Responsabilité de l'investigation
- Posture d'observation
- Actions clefs de l'investigation
- Outillage du plan d'investigation
- Interactions inter et intra cellules de crise
- Mises en situations : définir une posture, mobiliser les ressources, établir un plan d'investigation

Module 4 : Défense & Surveillance

- Plan de défense
- Responsabilité de la défense
- Remédiation
- Reconstruction
- Durcissement
- Surveillance de circonstance et surveillance long terme
- Mises en situation : évaluer les impacts, établir un plan de défense, construire l'organisation nécessaire

Module 5 : Sortie de crise… et l'après crise

- Critères de sortie de crise
- Analyse de la cause primaire ("root cause analysis")
- Construction du RETEX
- Plan d'actions post-crise
- Retour en mode projet et en "RUN"
- S'entraîner / exercices de crise
- Mises en situation : construction un plan d'actions post-crise, acter une sortie de crise, établir un RETEX

Synthèse : les clefs de la gestion de crise cyber

Mise en situation complète

Formation « EBIOS 2018 Risk Manager »

Réf : EBIOS2018

EBIOS Risk Manager est une méthode de gestion des risques conçue par l'ANSSI et publiée en octobre 2018 (nous appellerons cette méthode EBIOS RM ou EBIOS2018 pour éviter de la confondre avec EBIOS2010). Cette nouvelle méthode combine une démarche conformité afin de se focaliser sur un panel réduit de risques, tout en approfondissant ceux-ci, et met l'accent sur les risques liés aux parties prenantes et à l'externalisation. Elle est recommandée par l'ANSSI pour les appréciations des risques orientées projet et SMSI, avec l'objectif de remplacer la méthode EBIOS2010 et ses cas d'usages.

Objectifs

- **Fournir aux participants l'ensemble des éléments pour pouvoir, par la suite être autonome dans la réalisation d'une analyse des risques selon la méthodologie EBIOS 2018 Risk Manager.**
- **Présenter le vocabulaire et les différents ateliers qui composent la méthode.**

Durée & horaires

- **3 jours soit 21 heures**
- **Deux premiers jours : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Dernier jour : de 09h30 à 12h et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 20 participants**

Public visé

- **Personne souhaitant découvrir, comprendre ou mettre en pratique la méthode EBIOS2018**
- **RSSI**
- **Consultants en sécurité, y compris ceux connaissant d'autres méthodes comme ISO27005 ou EBIOS2010**

Pré-requis

- **La connaissance préalable de la gestion des risques en cybersécurité est nécessaire, par exemple avoir suivi une formation Mehari, EBIOS 2010, ou ISO27005 Risk Manager.**
- **Une base en sécurité des systèmes d'information est requise (sécurité des réseaux, sécurité des systèmes, etc), par exemple avoir suivi la formation SECUCYBER.**

Méthode pédagogique

- **Cours magistral théorique via le déroulé d'un cas fictif**
- **Exercice pratique : mise en application des concepts préalablement enseignés. Déroulement de la méthode sur un cas d'étude.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification EBIOS 2018 Risk Manager par HS2. En option, il est possible d'acheter l'examen EBIOS Risk Manager d'AFNOR Certification.**

Programme

Les bases de la gestion de risques

- Objectif de la gestion de risque
- Les principales normes en gestion de risques (ISO 27005, MEHARI, etc.)
- Présentation de la méthodologie EBIOS RM (historique, évolution, concepts)
- Les notions essentielles (risques, gravité, vraisemblance, etc.)

Atelier 1 : socle de sécurité

- Identification du cadre et périmètre de l'analyse de risque
- Étude des événements redoutés et valorisation de leur gravité
- Identification des principaux référentiels composant le socle de sécurité

Atelier 2 : sources de risque

- Identification des sources de risques et des objectifs visés
- Évaluation de la pertinence des couples SR/OV
- Sélection des couples les plus pertinents

Atelier 3 : scénarios stratégiques

- Élaboration de la cartographie de l'écosystème et sélection des parties prenantes critiques
- Élaboration des scénarios stratégiques
- Définition des mesures de sécurité existantes

Atelier 4 : scénarios opérationnels

- Élaboration des scénarios opérationnels
- Évaluation de leur vraisemblance

Atelier 5 : traitement du risque

- Réalisation de la synthèse des scénarios de risque
- Définition de la stratégie de traitement de risque et définition du Plan d'Amélioration Continue de la Sécurité (PACS)
- Évaluation des risques résiduels
- Mise en place du cadre du suivi des risques

Examen HS2

Formation « Essentiels ISO27001 & ISO27002 »

Réf : ESS27

La norme ISO27001 est la référence internationale en termes de système de management de la sécurité de l'information (SMSI). Les projets de mise en conformité se multipliant, une connaissance des éléments fondamentaux pour la mise en œuvre et la gestion d'un SMSI est nécessaire. Par ailleurs, la norme ISO27001 décrit une approche pragmatique de la gestion de la sécurité de l'information avec le choix de mesures de sécurité découlant d'une appréciation des risques. Elle s'appuie sur le guide ISO27002 pour fournir des recommandations sur le choix et l'implémentation des mesures de sécurité.

Objectifs

- **Être capable de présenter la norme ISO27001, les processus de sécurité qui lui sont associés et le projet de mise en conformité**
- **Maîtriser la corrélation entre ISO27001 et ISO27002**
- **Savoir sélectionner les mesures de sécurité**

Durée & horaires

- **2 jours soit 14 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information :**
  - **RSSI et à leurs équipes**
  - **Personnes responsables de services opérationnels**
  - **DSI et leurs équipes**
  - **Responsables méthodes et qualité**

Pré-requis

- **Aucun pré-requis n'est demandé. Toutefois, avoir une expérience en informatique et en sécurité est un plus.**

Méthode pédagogique

Cours magistral basé sur les normes.

Supports

- **Support de cours au format papier en français**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Introduction aux systèmes de management

- Management de la SSI
- Historique des normes ISO27
- Panorama des normes ISO27
- Présentation détaillée de la norme ISO27001
- Gestion des risques
- Mesures de sécurité
  - Présentation de la norme ISO27002
  - Gestion des mesures de sécurité
  - Implémentation des mesures de sécurité et PDCA
  - Documentation des mesures de sécurité
  - Audit des mesures de sécurité
  - Autres référentiels de mesures de sécurité
- Certification ISO27001

Formation « Mise à jour ISO27001 & ISO27002 »

Réf : MAJ27

La norme ISO27001 est la référence internationale en termes de système de management de la sécurité de l'information (SMSI). La norme ISO27001 décrit une approche pragmatique de la gestion de la sécurité de l'information avec le choix de mesures de sécurité découlant d'une appréciation des risques. Elle s'appuie sur le guide ISO27002 pour fournir des recommandations sur le choix et l'implémentation des mesures de sécurité.

2022 est l'année de la publication d'une importante mise à jour de la norme ISO27002 et donc en conséquence de l'Annexe A de la norme ISO 27001. Les changements contenus dans ces nouvelles versions impactent forcément un SMSI existant mais également toute démarche de gestion de la Cybersécurité.

Objectifs

- **Découvrir les mises à jour 27001 & 27002**
- **Se préparer à la migration du SMSI en 2022**
- **Comprendre les apports des nouvelles versions des normes pour lancer un projet de SMSI**
- **Appréhender l'usage de la nouvelle 27702 pour vos audits ou vos politiques de sécurité**

Durée & horaires

- **1 jour soit 7 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personne qui souhaite prendre connaissance des nouveautés des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information, préparer l'évolution de son SMSI pour maintenir sa certification :**
  - **RSSI et à leurs équipes**
  - **Personnes responsables de services opérationnels**
  - **DSI et leurs équipes**
  - **Responsables méthodes et qualité**

Pré-requis

- **Avoir suivi une formation Lead Implementer ou Lead Auditor 27001 ou maîtriser les normes 27001-27002 en version 2013/2017**

Méthode pédagogique

Cours magistral basé sur les normes, exercices de mises en situation.

Supports

- **Support de cours au format papier en français**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation, éligible au CP2 d'ISC2**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Les nouveautés :

- Amendements de la norme ISO27001 : l'Annexe A
- Une nouvelle vision « processus » de l'ISO27002:2022
  - La nouvelle organisation des 93 mesures
  - Les attributs : intérêt et usages
  - Les nouvelles mesures
- L'impact sur la documentation SSI
  - PSSI et les politiques associées
  - Déclaration d'applicabilité
  - Gestion du SMSI : suivi de projets, manuel, modèles documentaires.
  - Points de contrôle : Indicateurs, activité de surveillance, programme d'audit interne
- Evolution des processus du SMSI
  - Appréciation des risques
  - Plan de traitement des risques
  - Audit Interne
  - Surveillance
- Stratégies de migration d'un SMSI
  - Approche par la DdA
  - Approche par Processus
- Etudes de cas :
  - Faire évoluer les mesures de sécurité existantes
  - Communiquer sur ces évolutions
    - Acteurs du SMSI
    - Clients et partenaires
- Gestion de la relation avec l'organisme de certification
  - Gérer les audits intermédiaires
  - Bascule sur les nouvelles versions
- Evolutions des autres normes 27x
  - ISO 27005
  - ISO 27006
  - ISO 27701

Formation « ISO 27001 Lead Auditor »

Réf : ISO27LA

Objectifs

- Apprendre à auditer sur la norme ISO27001 et les guides associés
- Devenir auditeur ou responsable d'équipe d'audit pour les systèmes de management de la sécurité de l'information (SMSI)
- Disposer de la vision auditeur vis-à-vis de la norme ISO 27001,
- Intégrer le modèle PDCA lors des activités d'audits,
- Auditer les différentes catégories de mesures de sécurité (Annexe A de l'ISO27001 / ISO27002) et conduire un audit de SMSI et ses entretiens en maîtrisant les notions de non-conformités majeures ou mineures.

Durée & horaires

- 5 jours soit 35 heures réparties en 31h30 de cours, 3h30 de travail individuel sur les exercices le soir et 3h00 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- La formation s'adresse à tous ceux amenés à conduire des audits d'un SMSI et plus généralement un audit dans le domaine de la cybersécurité, donc :
  - les membres des équipes de contrôle interne,
  - des équipes sécurité ou des équipes d'audit,
  - les auditeurs d'autres systèmes de management comme les qualiticiens,
  - les auditeurs externes réalisant des audits conseil (appelés également pré-audits ou audit à blanc) pour leurs clients,
  - ceux souhaitant devenir auditeur de conformité ISO27001, et ceux devant être audités et devant comprendre l'état d'esprit de l'auditeur.

Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, la connaissance des systèmes de management dans un autre domaine, la qualité par exemple, est un plus. La notion de SMSI (ISO 27001) et la réalisation d'audits de systèmes de management (ISO 19011) seront explicitées lors de la formation. Cependant la lecture des normes ISO 27001 et ISO 19011 avant la formation est recommandée. Les 133 mesures de sécurité sont rapidement survolées et ne seront pas acquises à l'issue de cette formation, leur maîtrise demandant des bases solides en informatique.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur les normes ISO27001, ISO19011, et plus succinctement les normes ISO27002, ISO17021, ISO27006 et ISO27007.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.
- Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous auditeurs de SMSI

- **Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des cas réels d'audit anonymisés et un jeu de rôle auditeur / audité.**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification HS2 ISO 27001 Lead Auditor. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation. En option, il est possible d'acheter les examens de certification Certi-Trust, BestCertif CPF ou BestCertif COFRAC.**

Programme

Accueil des participants et tour de table

Introduction à la sécurité des systèmes d'information

Introduction au système de management

- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

Présentation détaillée de la norme ISO 27001 pour l'auditeur

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

Relations entre les éléments structurants du SMSI

- Principaux processus d'un SMSI

Processus de certification ISO27001

- Certification et accréditation
- Autorités d'accréditation
- Organismes de certification
- Normes ISO17021 et ISO27006
- Règlement de certification

Présentation de la norme ISO 27002

- Objectifs et usage de la norme
- Exigences de l'ISO 27001
- Auditer une mesure de sécurité
- Présentation des mesures de sécurité
- Exemple d'audit de mesures de sécurité

Présentation de la démarche d'audit de la norme ISO19011

- Principes de l'audit
- Types d'audit
- Programme d'audit
- Démarche d'audit
- Avant l'audit
- Audit d'étape 1
- Audit d'étape 2
- Après l'audit
- Auditeur et Responsable d'équipe d'audit

Présentation de la démarche d'audit SMSI

- Application ISO17021, ISO27006 et ISO19001 à un SMSI
- Critères d'audit
- Déroulement d'un audit
- Constats d'audit et fiches d'écart
- Conduite d'entretiens
- Réunion de clôture
- Rapport d'audit

Examen de certification conçu, surveillé et corrigé par HS2

Formation « ISO 27001 Lead Implementer »

Réf : ISO27LI

Objectifs

- Apprendre à mettre en œuvre la norme ISO27001 et les guides associés
- Apprendre à utiliser concrètement les normes, avec des exemples pour que chacun puisse les utiliser chez lui ou chez ses clients : les processus à mettre en place, le dimensionnement et l'organisation du projet, etc

Durée & horaires

- 5 jours soit 35 heures réparties en 31h30 de cours, 3h30 de travail individuel sur les exercices le soir et 3h00 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Personnes devant mettre en œuvre un SMSI à tous les niveaux, du management à l'opérationnel :
  - RSSI et à leurs équipes
  - Personnes responsables de services opérationnels
  - DSI et leurs équipes
  - Responsables méthodes et qualité
  - Consultants et aux personnes en reconversion souhaitant mettre en œuvre l'ISO27001
- Personnes devant participer à l'implémentation de la norme en vue d'une certification ISO27001 ou une certification HDS (Hébergeur de Données de Santé)

Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, avoir une expérience en informatique et en sécurité est un plus.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur la norme ISO27001, et plus succinctement les normes ISO27002, ISO27003, ISO2004 et ISO27005.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.
- Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous implémenteurs de SMSI
- Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des études de cas : périmètre, politique, procédures, plan projet, suivi et réunions, traitement des risques, surveillance et indicateurs. Ces exercices permettent également de se préparer à l'examen de certification.
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification HS2 ISO 27001 Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h30 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas. En option, il est possible d'acheter les examens de certification Certi-Trust, BestCertif CPF ou BestCertif COFRAC.**

Programme

Accueil des participants et tour de table

Introduction à la sécurité des systèmes d'information

Introduction au système de management
- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

Présentation détaillée de la norme ISO 27001
- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

Présentation de la norme ISO 27002
- Différentes catégories de mesures de sécurité
- Mesures d'ordre organisationnel / technique
- Implémentation d'une mesure de sécurité selon le modèle PDCA

Panorama des normes complémentaires
- ISO27017, ISO27018, ISO27025

Processus dans un SMSI
- Processus support
- Gestion des exigences légales et réglementaires
- Gestion des risques
- Implémentation et suivi des mesures de sécurité
- Gestion des incidents
- Gestion documentaire
- Évaluation de la performance

La gestion des risques et la norme ISO 27005
- Vocabulaire : risque, menace, vulnérabilité, etc.
- Critères de gestion de risque
- Appréciation des risques, acceptation du risque, communication du risque
- Déclaration d'applicabilité (DdA/SoA)
- Réexamen du processus de gestion de risques et suivi des facteurs de risques

Gestion des exigences légales et réglementaires
- Protéger les données à caractère personnelles
- Outils de veille juridique
- Gestion des engagements contractuels
- Gestion des fournisseurs et prestataires
- Contractualiser la sécurité

L'évaluation des performances
- Surveillance au quotidien
- Indicateurs et norme ISO 27004
- Audit interne
- Revue de Direction

Projet SMSI
- Conviction la direction
- Étapes du projet
- Acteurs
- Facteurs clés de réussite et d'échec
- Processus de certification ISO27001

Certification ISO27001
- Accréditation
- Normes ISO19011 et ISO27007
- Normes ISO17021 et ISO27006
- Règlement de certification

Examen de certification conçu, surveillé et corrigé par HS2

Formation « ISO 27005 Risk Manager »

Réf : ISO27RM

Une fois que les bonnes pratiques ont été appliquées, la sécurité des systèmes d'information a besoin d'être ajustée aux besoins et au contexte de chaque organisme. Partant de ce constat, les experts en sécurité ont placé la gestion des risques au cœur des processus de gestion de la cybersécurité. Aujourd'hui, systèmes de management, homologations, et RGPD sont basés par une approche sur le risque, de même que de nombreuses certifications (ISO27001, HDS, PCI-DSS, ISO22301, etc). La gestion des risques reste pourtant une démarche parfois d'abord difficile et qui conditionne souvent la réussite du système de management ou du projet associé.
La norme ISO27005 est la méthode de gestion des risques en sécurité de l'information reconnue internationalement, et un des principaux guides de la série des normes ISO27001. ISO 27005 est pragmatique, elle vise la gestion des risques dans la durée, et elle impose la prise de responsabilité par le propriétaire du risque, généralement la direction générale. Elle est la méthode préconisée pour toute appréciation des risques dans le cadre d'un SMSI (Système de Management de la Sécurité de l'Information). Elle peut être également utilisée pour l'appréciation des risques imposée en plus du BIA (Business Impact Analysis) dans un SMCA (Système de Management de la Continuité d'Activité) et dans beaucoup d'autres cadres.

Objectifs

- **Acquérir une compréhension globale des concepts, de la norme, des méthodes et des techniques de gestion des risques**
- **Apprendre à mettre en œuvre la méthode ISO 27005 dans son contexte**
- **Appliquer la méthode ISO27005 avec efficacité là où celle-ci accorde de la liberté à l'implémenteur**
- **Maîtriser le processus de gestion des risques et son cycle de vie**
- **Savoir apprécier les risques et présenter ses propositions de traitement aux propriétaires des risques**

Durée & horaires

- **3 jours soit 21 heures réparties en 2,5 jours de cours et 0,5 d'examen.**
- **Deux premiers jours : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Dernier jour : de 09h30 à 12h et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Consultants**
- **RSSI**
- **Chefs d projet**
- **Toute personnes devant réaliser des appréciations des risques en cybersécurité**

Pré-requis

- **Pour assister à cette formation, il est recommandé de posséder des connaissances en informatique.**

Méthode pédagogique

La méthode pédagogique se base sur les cinq points suivants :

- **Approche du sujet de manière interactive où les stagiaires remplissent un tableur édité par l'instructeur et déroulent la méthode sans la connaître**
- **Cours magistral basé sur la norme ISO 27005**

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

- **Des exemples et études de cas tirés de cas réels**
- **Des exercices réalisés individuellement**
- **Mise en œuvre d'une appréciation des risques et d'un traitement des risques sur une étude de cas, en groupe, à l'aide d'un tableur**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**
- **Clef USB permettant de conserver le travail réalisé durant la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de certification HS2 ISO 27005 Risk Manager. L'examen est composé de deux parties : un QCM avec la norme sous les yeux et une étude de cas permettant de vérifier la capacité d'application pratique de la méthode. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation. En option, il est possible d'acheter les examens de certification Certi-Trust, BestCertif CPF ou BestCertif COFRAC.**

Programme

Introduction

- Normes ISO270XX
- ISO 27005 et les autres méthodes dont Ebios, Mehari, etc
- Vocabulaire du management du risque selon l'ISO 27005

Présentation interactive du vocabulaire fondamental et de l'approche empirique du management du risque avec la participation active des stagiaires à un exemple concret

- Identification et valorisation d'actifs
- Menaces et vulnérabilités
- Identification du risque et formulation sous forme de scénarios
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Évaluation des risques
- Différents traitements du risque
- Acceptation des risques
- Notion de risque résiduel

Norme ISO 27005

- Introduction
- Gestion du processus de management du risque
- Cycle de vie du projet et amélioration continue (modèle PDCA)
- Établissement du contexte
- Identification des risques
- Estimation des risques
- Évaluation des risques
- Traitement du risque
- Acceptation du risque
- Surveillance et réexamen des facteurs de risque
- Communication du risque

Exercices

Mise en situation : étude de cas

- Réalisation d'une appréciation de risque complète sur ordinateur
- Travail de groupe
- Simulation d'entretien avec un responsable de processus métier
- Présentation orale des résultats par le meilleur groupe
- Revue des résultats présentés

Examen de certification conçu, surveillé et corrigé par HS2

Formation
« ISO27004 / Indicateurs et tableaux de bord cybersécurité »

Réf : ISO27004

Que ce soit un avion ou un organisme, il est toujours possible de conduire celui-ci avec peu d'informations, mais cela sera moins efficace, voire dangereux. Dans le cas de la gestion de la sécurité de l'information, le pilotage d'une telle activité consiste à prendre des décisions et ce à plusieurs niveaux. Ce peut être la décision de modifier une fréquence de scan antivirus ou encore, à un niveau plus stratégique, l'arbitrage en faveur d'une redistribution des budgets.

Si elles ne relèvent pas du même niveau d'arbitrage, ces décisions ont ceci en commun qu'elles se font de façon plus éclairée si elles sont prises en fonction d'informations fiables et pertinentes. La prise de décision est d'autant meilleure qu'elle peut s'appuyer sur des indicateurs concrets et pertinents.

Les indicateurs stratégiques, regroupés en tableaux de bord, permettent de répondre à ce besoin d'information. Pour ce faire ils doivent être adaptés au profil du lecteur et aux décisions qui sont attendues de lui. En ce sens, les tableaux de bord sont à rapprocher des principes de communication dont la finalité est d'obtenir une action de la cible de cette communication.

Un tableau de bord pertinent se doit également d'être réaliste, ce qui implique que son coût soit maitrisé et en rapport avec les enjeux qu'il permet d'arbitrer. L'objectif étant, non pas de construire des indicateurs trop complexes et coûteux à produire, ce qui contribuerait à consommer de la valeur plutôt qu'à sécuriser celle-ci…

Objectifs

- Comprendre ce qu'est un indicateur, ce en quoi il est nécessaire à une gestion efficace de la sécurité de l'information, comment en faire un outil de communication vis-à-vis de toutes les parties prenantes, comment mettre en place des tableaux de bord adaptés à un contexte
- Savoir concevoir des indicateurs pertinents et réalistes dans le contexte de son organisme
- Savoir concevoir des indicateurs conformes aux exigences de la norme ou du référentiel suivi
- Savoir tirer des informations utiles des indicateurs en produisant des tableaux de bord pour surveiller et améliorer un SMSI, pour prouver sa conformité et améliorer la SSI, et pour communiquer

Durée & horaires

- 1 jour soit 7 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Personnes chargées de concevoir des indicateurs sécurité, de les produire, ou de présenter des tableaux de bord.
- Personnes chargées de déployer des indicateurs sécurité
  - RSSI et équipes du RSSI
  - Consultants en sécurité
  - Ingénieurs sécurité.
- Personnes chargées de produire des indicateurs de sécurité
  - Ingénieur de production informatique
  - Chef de projet métier

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Pré-requis

- **Avoir suivi la formation "Essentiels ISO27001/ISO27002" ou la formation "RSSI"**
- **ou avoir suivi une formation plus complète à l'ISO27001 comme "ISO27001 Lead Implementer"**
- **ou avoir une connaissance de la SSI et une maîtrise de l'ISO27001 ou des systèmes de management en général**
- **ou être déjà RSSI ou consultant sécurité avec une expérience**

Méthode pédagogique

- **Cours magistral avec des exemples pratiques issus de l'expérience des formateurs.**
- **Exercices pratiques individuels de mise en œuvre d'indicateurs.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

- Introduction
  - Qu'est-ce qu'un indicateur ?
  - Vocabulaire
- Indicateurs : pourquoi mesurer une activité ?
  - Peut-on piloter sans instruments ?
  - Quelle valeur ajoutée
- Points à mesurer dans le domaine de la SSI
  - Efficience de la sécurité
  - Coût de la sécurité, ou de l'absence de sécurité
  - Conformité aux normes, référentiels, exigences, réglementations
- Approches pour gérer les indicateurs :
  - Travaux issus du monde de la sécurité : ANSSI, ISO, CLUSIF, CIGREF
  - Techniques de communication au service des indicateurs
  - Coût des indicateurs
- Démarche de mise en œuvre
  - Vue d'ensemble
  - Concevoir ses indicateurs
    - Définir ses besoins et ses finalités
    - Définir les moyens de production
  - Produire ses indicateurs
  - Communiquer ses indicateurs
  - Auditer ses indicateurs
- Conseils pratiques
  - Principaux indicateurs à mettre en place
    - Pour un Système d'Information
    - Pour un SMSI
  - Exemples
  - Erreurs à éviter
  - Identifier les solutions simples et efficaces (« quick wins »)
- Présentation de la norme ISO 27004
  - Raison d'être de la norme
  - Processus de mise en œuvre
  - Quels indicateurs pour quel usage
- Exercices

Formation « Gestion des incidents de sécurité / ISO27035 »

Réf : ISO27035

La gestion des incidents de sécurité dans un délai court et leur prise en compte dans la gestion des risques et l'amélioration continue sont imposés par l'ISO 27001. Le processus de gestion des incidents de sécurité est un processus fondamental pour le succès d'une bonne organisation de la sécurité des systèmes d'information. Un guide, la norme ISO27035, explicite en détail comme organiser ce processus.

Objectifs

- **Comprendre et savoir mettre en œuvre concrètement dans son SMSI le processus de gestion des incidents de sécurité et une équipe de réponse aux incidents de sécurité (Information Security Incident Response Team : ISIRT)**
- **Comprendre et savoir gérer les interactions du processus de gestion des incidents de sécurité avec les autres processus dans son organisme, par exemple savoir différencier incident informatique et incident de sécurité.**
- **Apprendre à organiser son processus de gestion des incidents de sécurité.**

Durée & horaires

- **1 jour soit 7 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **DSI**
- **Personnes chargées de gérer les incidents de sécurité ;**
- **Personnes chargées de gérer les incidents au sens ITIL/ISO 20000 ;**
- **Responsables de la mise en place d'un SMSI.**

Pré-requis

- **Cette formation ne demande pas de pré-requis particuliers.**

Méthode pédagogique

- **Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.**

Supports

- **Support de cours au format papier en français**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

- Introduction
  - Contexte, Enjeux et ISO27001, Vocabulaire
- Norme ISO 27035
  - Concepts
  - Objectifs
  - Bienfaits de l'approche structurée
  - Phases de la gestion d'incident
- Planification et préparatifs (Planning and preparation)
  - Principales activités d'une équipe de réponse aux incidents de sécurité (ISIRT)
  - Politique de gestion des incidents de sécurité
  - Interactions avec d'autres éférentiels ou d'autres politiques
  - Modélisation du système de gestion des incidents de sécurité
  - Procédures
  - Mise en œuvre de son ISIRT
  - Support technique et opérationnel
  - Formation et sensibilisation
  - Test de sons système de gestion des incidents de sécurité)
- Détection et rapport d'activité (Detection and reporting)
  - Activités de l'équipe opérationnelle de détection des incidents de sécurité de l'information
  - Détection d'évènements
  - Rapport d'activité sur les événements
- Appréciation et prise de décision (Assessment and decision)
  - Activités de l'équipe opérationnelle d'analyse des incidents de sécurité
  - Analyse immédiate et décision initiale
  - Appréciation et confirmation de l'incident
- Réponses (Responses)
  - Principales activités d'une équipe opérationnelle de réponse aux incidents de sécurité
  - Réponse immédiate
  - Réponse à posteriori
  - Situation de crise
  - Analyse Inforensique
  - Communication
  - Escalade
  - Journalisation de l'activité et changement
- Mise à profit de l'expérience ('Lessons Learnt')
  - Principales activités d'amélioration de l'ISIRT
  - Analyse Inforensique approfondie
  - Retours d'expérience
  - Identification et amélioration
- Mise en pratique
  - Documentation
  - Exemple d'incidents de sécurité de l'information
  - Catégories d'incidents de sécurité
  - Méthodes de classement ou de typologie d'incidents de sécurité
  - Enregistrement des évènements de sécurité
  - Fiche de déclaration des évènements de sécurité
- Aspects légaux et réglementaires de la gestion d'incidents

Nos Intervenants
Formations en continuité d'activité et cybersécurité organisationnelle

Jean-Luc Austin dispense la formation : CISA

Tony Belot dispense les formations :
RSSI - ISO27LA - ISO27LI - ISO27RM

William Bourgeois dispense les formations : ISO27LA - ISO27LI

Matthieu Caron dispense les formations : CISSP - CCSP

Lucien Caumartin dispense la formation : ISO27LA

Thierry Chiofalo dispense la formation : ISO27004

François Coupez dispense la formation : RSSI

Mathieu Couturier dispense la formation : SECUCRISE

Sabine Dacruz Mangeot dispense la formation : SECUPROJET

Amélie Deleuze dispense la formation : RSSI

Alexandre Fernandez-Toro dispense les formations : ISO27LA - ISO27LI

Etienne Gérain dispense les formations : EBIOS2018 - ISO27RM

Jordan Hordé dispense les formations :
ISO27LA - ISO27LI - ISO27RM - EBIOS2018

Anthony Hubbard dispense les formations :
RSSI - ISO27LA - ISO27LI - ISO27035

Emmanuel Jouffin dispense la formation : RSSI

Morgane Nguyen dispense la formation : IS027035

Giuliano IPPOLITI dispense la formation :

CCSP

Thomas Le Poëtvin dispense les formations :

RSSI - EBIOS2018 - ISO27LA - ISO27LI - ISO27RM

Julien Levrard dispense la formation :

ISO27LI

Alexandre Magloire dispense les formations :

SECUHOMOL- EBIOS2018 - ISO27LI

Elisabeth Manca dispense les formations :

RSSI - ISO27LI

Baptiste Maulion dispense les formations :

ISO22LA - ISO22LI

Morgane Nguyen dispense la formation :

ISO27035

Vincent Nguyen dispense les formations :

SECUCRISE - ISO27035

Paul Pennaneac'h dispense les formations :

RSSI - SECUHOMOL - ISO27LI

Matthieu Renard dispense la formation :

EBIOS2018

Stéphanie Ruelle dispense la formation :

EBIOS2018

Hervé Schauer dispense les formations :

ISO22LI - ISO22LA

Matthieu Schipman dispense les formations :

RSSI - CISSP

Thomas Seyrat dispense la formation :

RSSI

Mikaël Smaha dispense les formations :

EBIOS2018 - ISO27RM - ISO27LI

Alphonsine Yacoubou-Djima dispense les formations :

ESS27 - ISO27LA - ISO27LI

HS2
Hervé Schauer Sécurité

Bulletin d'inscription

Merci de retourner ce bulletin soit par courrier à HS2 – 10, rue des Poissonniers – 92200 Neuilly-sur-Seine –
Soit par courriel à formation@hs2.fr

Responsable Formation

Nom et Prénom : .....
Fonction : ..... Société : .....
Adresse : .....
Code postal : ..... Ville : .....
Tél. : ..... E-mail : .....

Souhaite inscrire la ou les personne(s) suivante(s) au(x) stage(s) mentionné(s) :

• Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

• Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

• Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

Adresse de facturation (si différente)

Société : ..... Adresse : .....
Code postal : ..... Ville : .....
Nom du correspondant : ..... Tél. : .....
E-mail : .....
N° de TVA intracommunautaire .....

Établissez-vous des bons de commande avec des références à reporter sur notre facture ? oui ❍ non ❍
Si oui, l'inscription sera confirmée uniquement à réception de votre bon de commande.

Demande de subrogation via votre OPCO* : oui ❍ non ❍
*Dans le cas d'une subrogation de paiement via votre OPCO, l'inscription sera confirmée uniquement à réception du contrat ou de l'accord de prise en charge de votre OPCO et de notre convention de formation signée et tamponnée

Date :
Cachet et signature de l'employeur

Convention de formation : pour chacune des sessions proposées, une convention de formation est disponible sur simple demande.
Attention, la prise en compte de votre demande d'inscription sera effective uniquement à réception d'un mail de confirmation par nos services.
Pour tout renseignement complémentaire, vous pouvez contacter le service formation par mail à formation@hs2.fr ou par téléphone au +33 974 774 390.

Retrouvez-nous sur notre site : **www.hs2.fr**

Renseignement / inscription à nos formations, n'hésitez pas à nous contacter :

Lynda Benchikh / Elisa Keller / Estelle Dubois

☎ +33 (0)974 774 390

formation@hs2.fr

Déclaration d'activité enregistrée sous le numéro 11922236092
auprès du préfet de région d'Ile-de-France

Pour nous contacter :

☎ +33 (0)974 774 390 / +33 (0)644 014 072

formation@hs2.fr

Pour nous suivre :

@HS2formation

@HS2formation

@HS2formation

Datadock Organisme Référencé

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : **ACTIONS DE FORMATIONS**