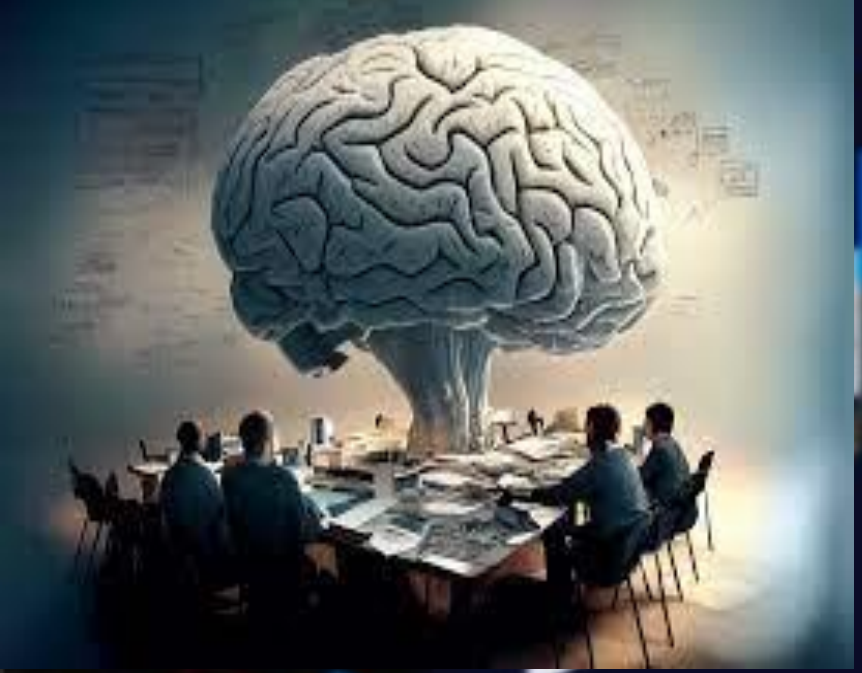


FORMATIONS CERTIFIANTES

CATALOGUE 2023-2024

POURQUOI SE CERTIFIER ?

L’expérience est un atout indéniable, mais comment démontrer vos connaissances et compétences auprès d’employeurs ?

GRACE A LA CERTIFICATION !

De nos jours, il est primordial d’être capable de rallier à son diplôme un métier ; Ainsi, En obtenant une certification, vous démontrez votre expertise et prouvez votre capacité à vous différencier des autres sur le marché du travail de plus en plus concurrentiel d’aujourd’hui.

La certification apporte de la crédibilité à votre curriculum vitae, ce qui vous ouvre d’importantes possibilités d’évolution de carrière.
C’est un facteur clé de succès pour obtenir des opportunités d’emploi mieux rémunérées et une reconnaissance accrue.

Avantages :

- ❑ Amélioration de l’employabilité et de meilleures opportunités d’emploi.
- ❑ Emplois mieux rémunérés avec en prime augmentation de salaires
- ❑ Reconnaissance de carrière au sein de l’entreprise et auprès de ses pairs
- ❑ Accroissement de la crédibilité et de la notoriété
- ❑ Permet de booster des carrières et etre plus compétitif

TABLE INDEX DES FORMATIONS CERTIFIANTES

REFERENCE	INTITULE DE LA FORMATION	ORGANISME DE CERTIFICATION	PARTENAIRE TECHNIQUE
INFORMATIQUE & CYBERSECURITE			
ISO 27000			
SI-ILA	ISO 27001:2022 LA : systèmes de management de la sécurité de l'information	**ISO**	**GROUP SOFT SARL**
SI-IRM	ISO 27005:2022 RM : préconisations pour la gestion des risques liés à la sécurité de l'information		

PROGRAMMES DÉTAILLÉS DES FORMATIONS CERTIFIANTES

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-ILA**	Intitulé de la formation certifiante **: ISO 27001:2022 LA : systèmes de management de la sécurité de l'information**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agréé Pearson VUE)*	**Responsable pédagogique :** Expert en management de la sécurité certifié ISO 27001 de JFN

Description et objectifs :

Face à l'essor de la cybercriminalité et à l'émergence constante de nouvelles menaces, il peut paraître difficile, voire impossible, de gérer les cyber-risques. ISO/IEC 27001 aide les organisations à prendre conscience des risques et à identifier et traiter de manière proactive les lacunes. c'est la norme la plus connue au monde en matière de systèmes de management de la sécurité de l'information (SMSI).

Elle définit les exigences auxquelles un SMSI doit répondre. elle fournit aux entreprises de toutes tailles, quel que soit leur secteur d'activité, des lignes directrices pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information. Elle octroie également la conformité à ISO/IEC 27001 qui signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette Norme internationale.

ISO/IEC 27001 préconise une approche holistique de la sécurité de l'information, fondée sur des procédures de contrôle applicables aux personnes, aux politiques et aux technologies. Un système de management de la sécurité de l'information mis en œuvre conformément à cette norme est un outil à l'appui de la gestion des risques, de la cyber-résilience et de l'excellence opérationnelle.

ISO/IEC 27001 Introduction

La formation d'introduction à la norme ISO/IEC 27001 vous permettra d'appréhender les concepts fondamentaux d'un Système de management de la sécurité de l'information ; de comprendre l'importance d'un Système de management de la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement. L'objectif est de :

Connaître les concepts, approches, méthodes et techniques permettant de mettre en œuvre un Système de management de la sécurité de l'information

Comprendre les éléments fondamentaux d'un Système de management de la sécurité de l'information

Cible :

Les personnes intéressées par le management de la sécurité de l'information

Les personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information

Programme : Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001

.

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-ILA**	Intitulé de la formation certifiante **: ISO 27001:2022 LA : systèmes de management de la sécurité de l'information**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en management de la sécurité certifié ISO 27001 de JFN

ISO/IEC 27001:2022 Foundation

La formation ISO/IEC 27001:2022 Foundation vous permettra d'appréhender les éléments fondamentaux pour mettre en œuvre et gérer un SMSI, selon la norme ISO/IEC 27001:2022. Durant cette formation, vous apprendrez les différents modules d'un SMSI, la politique SMSI, les procédures, la mesure de la performance, l'engagement de la direction, l'audit interne, la revue de la direction et l'amélioration continue. L'objectif est de :

Comprendre les éléments et le fonctionnement d'un Système de management de la sécurité de l'information

Comprendre la corrélation entre la norme ISO/IEC 27001:2022 et ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres réglementaires

Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management de la sécurité de l'information

Cible :

Toute personne impliquée dans le management de la sécurité de l'information
Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information
Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

Programme :

Leçon 1 : Introduction aux concepts du Système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/IEC 27001:2022
Leçon 2 : Exigences relatives au Système de management de la sécurité de l'information et examen de certification.

ISO/IEC 27001 Lead Implementer

Les menaces et les attaques contre la sécurité de l'information augmentent et s'améliorent constamment. La meilleure forme de défense contre elles est la mise en œuvre et le management appropriés des mesures et des bonnes pratiques en matière de sécurité de l'information. La formation ISO/IEC 27001 Lead Implementer permet aux participants d'acquérir les connaissances nécessaires pour aider une organisation à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un SMSI.

Cette formation est conçue pour préparer les participants à la mise en œuvre d'un SMSI basé sur la norme ISO/IEC 27001. Elle vise à fournir une compréhension complète des bonnes pratiques d'un SMSI et un cadre pour sa gestion et son amélioration continues. Les objectifs d'apprentissage sont :

Acquérir une compréhension globale des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un SMSI
Comprendre le fonctionnement d'un SMSI et ses processus
Apprendre à interpréter et à mettre en œuvre les exigences de la norme ISO 27001 dans le contexte spécifique d'un organisme
Acquérir les connaissances nécessaires pour soutenir une organisation dans la planification, la mise en œuvre, la gestion, la surveillance d'un SMSI

Cible ::

Chefs de projet et consultants impliqués et concernés par la mise en œuvre d'un SMSI
Conseillers experts cherchant à maîtriser la mise en œuvre d'un SMSI
Personnes responsables d'assurer la conformité aux exigences de sécurité de l'information au sein d'une organisation.
Membres d'une équipe de mise en œuvre d'un SMSI

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-ILA**	Intitulé de la formation certifiante **: ISO 27001:2022 LA : systèmes de management de la sécurité de l'information**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en management de la sécurité certifié ISO 27001 de JFN

Prerequis :
La principale condition pour participer à cette formation est d'avoir une connaissance générale des concepts du SMSI et d'ISO/IEC 27001
Programme :
Leçon 1 : Introduction à la norme ISO/IEC 27001 et initiation d'un SMSI
Leçon 2 : Planification de la mise en œuvre d'un SMSI
Leçon 3 : Mise en œuvre du SMSI
Leçon 4 : Suivi, amélioration continue et préparation à l'audit de certification du SMSI

L'examen couvre les domaines de compétence suivants :
Domaine 1 : Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)
Domaine 2 : Système de management de la sécurité de l'information (SMSI)
Domaine 3 : Planification de la mise en œuvre d'un SMSI selon ISO/IEC 27001
Domaine 4 : Mise en œuvre d'un SMSI selon ISO/IEC 27001
Domaine 5 : Surveillance et mesure d'un SMSI selon ISO/IEC 27001
Domaine 6 : Amélioration continue d'un SMSI selon ISO/IEC 27001
Domaine 7 : Préparation à un audit de certification du SMSI

Prerequis : Une compréhension de base de la norme ISO/IEC 27001 et une connaissance approfondie des principes d'audit.

ISO/IEC 27001 Lead Auditor

La formation ISO/IEC 27001 Lead Auditor vous permet de développer l'expertise nécessaire à la réalisation d'un audit de système de management de la sécurité de l'information (SMSI) en appliquant des principes, procédures et techniques largement reconnus en audit.
À l'issue de cette formation, les participants seront capables de :
Expliquer les concepts et les principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO 27001
Interpréter les exigences d'ISO 27001 pour un SMSI du point de vue d'un auditeur
Évaluer la conformité du SMSI aux exigences d'ISO 27001, en accord avec les concepts et les principes fondamentaux d'audit
Planifier, réaliser et clôturer un audit de conformité à ISO 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
Gérer un programme d'audit ISO/IEC 27001

Cible :
Auditeurs souhaitant effectuer et diriger des audits de certification du système de management de sécurité de l'information (SMSI)
Managers ou consultants souhaitant maîtriser le processus d'audit d'un système de management de sécurité de l'information
Personnes responsables de maintenir la conformité aux exigences du système de management de sécurité de l'information.
Experts techniques souhaitant se préparer à un audit du système de management de sécurité de l'information.
Conseillers experts en management de sécurité de l'information

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-ILA**	Intitulé de la formation certifiante : **:ISO 27001:2022 LA : systèmes de management de la sécurité de l'information**

Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en management de la sécurité certifié ISO 27001 de JFN

Programme :

Leçon 1 : Introduction au SMSI et à ISO/IEC 27001
Leçon 2 : Principes d'audit, préparation et initiation d'un audit
Leçon 3 : Activités d'audit sur site
Leçon 4 : Clôture de l'audit

ISO/IEC 27001 Transition

La formation ISO/IEC 27001 Transition permet aux professionnels de bien comprendre les différences entre les normes ISO/IEC 27001:2013 et ISO/IEC 27001:2022 et d'acquérir des connaissances sur les nouveaux concepts introduits par la norme ISO/IEC 27001:2022.
Elle diffère de la certification ISO/IEC 27001:2013, puisque la norme s'intitule désormais Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences.
Elle fournit également des informations détaillées sur les articles révisés, la nouvelle terminologie, et les différences

Objectifs d'apprentissage
les participants seront en mesure de :
Expliquer les différences entre les normes ISO/IEC 27001:2013 et ISO/IEC 27001:2022
Interpréter les nouveaux concepts et les nouvelles exigences de la norme ISO/IEC 27001:2022
Planifier et mettre en œuvre les changements nécessaires à un SMSI existant conformément à la norme ISO/IEC 27001:2022

Cible :

cette formation est destinée aux :

- Personnes souhaitant rester à jour avec les exigences de la norme ISO/IEC 27001 pour un SMSI
- Personnes cherchant à comprendre les différences entre les exigences de la norme ISO/IEC 27001:2013 et celles de la norme ISO/IEC 27001:2022
- Personnes chargées d'assurer la transition d'un SMSI de la norme ISO/IEC 27001:2013 à la norme ISO/IEC 27001:2022
- Responsables, formateurs et consultants impliqués dans le maintien d'un SMSI
- Professionnels souhaitant mettre à jour leur certification à la norme ISO/IEC 27001
-

Les domaines de compétence mis en exergue :
Domaine 1 : Différences entre les principaux articles des normes ISO/IEC 27001:2013 et ISO/IEC 27001:2022
Domaine 2 : Différences entre les mesures de l'Annexe A de la norme ISO/IEC 27001:2013 et celles de la norme ISO/IEC 27001:2022

Prérequis :

Les participants doivent avoir une compréhension fondamentale des concepts de sécurité de l'information et des exigences de la norme ISO/IEC 27001.

Programme :
Leçon1 : Introduction à la norme ISO/IEC 27001:2022 et comparaison avec la norme ISO/IEC 27001:2013
Leçon 2 : Comparaison entre les mesures de l'Annexe A de la [illegible]/IEC 27001:2013 et de la norme ISO/IEC 27001:2022

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-IRM**	Intitulé de la formation certifiante : **: ISO 27005:2022 RM : préconisations pour la gestion des risques liés à la sécurité de l'information**		
Durée : 192 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agréé Pearson VUE)*	**Responsable pédagogique :** Expert en gestion des risques de sécurité certifié ISO 27005 de JFN

Description :

L'ISO / IEC 27005 fournit les lignes directrices pour l'établissement d'une approche systématique de la gestion des risques liés à la sécurité de l'information laquelle est nécessaire pour identifier les besoins organisationnels en matière de sécurité de l'information et pour créer un système efficace de management de la sécurité de l'information. cette norme vient en appui des concepts ISO/IEC 27001 et est conçue pour aider à la mise en œuvre efficace de la sécurité de l'information basée sur une approche de gestion des risques. . Elle prouve que l'apprenant est en mesure d'identifier, d'apprécier, d'analyser, d'évaluer et de traiter les divers risques de sécurité auxquels font face les organisations.

elle aide à aligner correctement le système de management de la sécurité de l'information des organisations avec le processus de gestion des risques liés à la sécurité de l'information.

L'objectif est d'acquérir l'expertise nécessaire à la mise en œuvre d'un système de sécurité de l'information basé sur une approche de gestion des risques.

Le parcours recommandé comporte les différentes parties suivantes :

- ISO/IEC 27005 Introduction
- ISO/IEC 27005 Foundation
- ISO/IEC 27005 Risk Manager
- ISO/IEC 27005 Lead Risk Manager

Prerequis :

Connaître un guide de bonnes pratiques (hygiène ANSSI, ISO 27002 ou équivalent), avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

Programme :

Introduction

Terminologie ISO 27000, définitions de la menace. Vulnérabilité. Risques...

Les exigences disponibilité, intégrité et confidentialité.

La prise en compte de la traçabilité/preuve.

Rappel des contraintes réglementaires et normatives (RGPD, LPM/NIS, PCI DSS...).

Le rôle du RSSI versus le Risk Manager.

La norme 31000, de l'intérêt de la norme "chapeau" en référentiel universel.

Le concept "risque SI"

Identification et classification des risques.

Origine des menaces (accidentelle, délibérée, environnementale).

Les conséquences du risque (financier, juridique, humain...).

La gestion du risque (réduction / diminution, évitement de risque, partage).

Le cas particulier du risque numérique en "persistance" (APT).

Comment agir sur le risque (avant, pendant, après l'incident).

Le management de risques selon l'ISO

La méthode de la norme 27001:2022 et son processus de gouvernance par le risque.

L'appréciation initiale en phase plan de la section 6 - Planification.

L'évolution majeure de la norme 27005:2022 : Information Security Risk Management.

Cible :

Chefs de projet, consultants, architectes techniques, responsables de la sécurité des SI, toute personne en charge de la sécurité d'information, de la [illegible] et du risque dans une organisation.

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-IRM**	Intitulé de la formation certifiante : : **ISO 27005:2022 RM : préconisations pour la gestion des risques liés à la sécurité de l'information**		
Durée : 192 *H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en gestion des risques de sécurité certifié ISO 27005 de JFN

La mise en œuvre d'un processus PDCA de management des risques.
Le contexte, l'appréciation, le traitement, l'acceptation et la revue des risques.
Les étapes de l'appréciation des risques (identification, analyse et évaluation).
L'élaboration du plan de traitement sur la base des mesures de la norme ISO 27002.
Le processus de sélection des mesures sur la base de attributs (Préventive, détective ou corrective).
Le choix des mesures de sécurité pour la déclaration d'applicabilité (SoA).

La norme ISO 27005:2022

Introduction à la nouvelle norme ISO 27005:2022, l'influence de EBIOS RM.
Le lien des processus de gestion des risques avec les processus du SMSI.
L'analyse du risque cyber ciblé, comment analyser les APT.
La cyber kill chain, les nouvelles sources de risques et leurs objectifs.
Exemple d'échelle de calcul de vraisemblance/conséquences.
L'approche de la gestion des risques par événement versus par actif.
La description des scénarios stratégiques et opérationnels.
La prise en compte du risque à travers l'écosystème.

Préparation et révision finale

Mise en situation, tests de connaissance de type QCM, études de cas.
Inventaire d'actifs, évaluation des menaces et vulnérabilités.
Élaboration de plans de traitement des risques, etc.
Examen blanc et corrigé interactif.
Les astuces pour éviter les pièges

SO/IEC 27005 Introduction

Description : SO/IEC 27005 Introduction

La formation d'introduction à la norme ISO/IEC 27005 vous permettra d'appréhender les concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence.

Elle permet de comprendre l'importance de la gestion des risques liés à la sécurité de l'information et les avantages que peuvent en tirer les entreprises, la société et le gouvernement. L'objectif est de :

Connaître les concepts, approches, méthodes et techniques permettant de gérer les risques liés à la sécurité de l'information

Comprendre l'importance de la gestion des risques liés à la sécurité de l'information

Cible :

Les personnes intéressées par la gestion des risques liés à la sécurité de l'information

Les personnes souhaitant acquérir des connaissances relatives aux principaux processus de la gestion des risques liés à la sécurité de l'information

les entreprises, organismes gouvernementaux, institutions financières, les fournisseurs de services, et d'autres entités qui traitent des informations sensibles et qui cherchent à protéger ces dernières des risques liés à la sécurité.

Programme :

Introduction aux fondamentaux de la gestion des risques liés à la sécurité de l'information en utilisant la norme ISO/IEC 27005

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-IRM**	Intitulé de la formation certifiante **: : ISO 27005:2022 RM : préconisations pour la gestion des risques liés à la sécurité de l'information**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en gestion des risques de sécurité certifié ISO 27005 de JFN

ISO/IEC 27005 Foundation

Description : elle couvre les domaines de compétences suivants :

Domaine 1 : Concepts fondamentaux de la gestion des risques liés à la sécurité de l'information

Domaine 2 : Approches et processus de gestion des risques liés à la sécurité de l'information

Cible : La formation ISO/IEC 27005 Foundation est destinée aux :

Professionnels de la gestion des risques

Professionnels souhaitant se familiariser avec les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information

Personnel chargé de la gestion des risques liés à la sécurité de l'information dans son domaine de responsabilité

Personnes intéressées par une carrière dans la gestion des risques liés à la sécurité de l'information

Programme :

Leçon 1 : Introduction à la norme ISO/IEC 27005 et aux concepts fondamentaux de la gestion des risques liés à la sécurité de l'information

leçon 2 : Gestion des risques liés à la sécurité de l'information et

Examen

Débouchés :

Au terme de cette formation, les participants seront en mesure de :

- Décrire les principaux concepts, principes et définitions de la
- gestion des risques
- Interpréter les lignes directrices de la norme ISO/IEC 27005 pour la gestion des risques liés à la sécurité de l'information
- Identifier les approches, les méthodes et les techniques utilisées pour la mise en
- œuvre et la gestion d'un programme de gestion des risques liés à la sécurité

ISO/IEC 27005 Risk Manager

Cette formation vous permettra de développer les compétences nécessaires pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. elle présentera également d'autres méthodes d'appréciation des risques telles que OCTAVE, EBIOS, MEHARI et la méthodologie harmonisée EMR.

Cible :

La formation s'adresse aux :

- Responsables de la sécurité d'information
- Membres d'une équipe de sécurité de l'information
- Tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation
- Tout individu mettant en œuvre ISO/IEC 27001, désirant se conformer à la norme ISO/IEC 27001 ou impliqué dans un
- programme de gestion des risques
- Consultants des TI
- Professionnels des TI
- Agents de la sécurité de l'information
- Agents de la protection des données personnelle

SECURITE INFORMATIQUE ET CYBERSECURITE : ISO 27000

Référence **SI-IRM**	Intitulé de la formation certifiante : : **ISO 27005:2022 RM : préconisations pour la gestion des risques liés à la sécurité de l'information**		
Durée : 192*H*	**Période :** *nous consulter*	**Lieu :** *JFN (centre agrée Pearson VUE)*	**Responsable pédagogique :** Expert en gestion des risques de sécurité certifié ISO 27005 de JFN

Leçon 1 Introduction au programme de gestion des risques conforme à ISO/IEC 27005

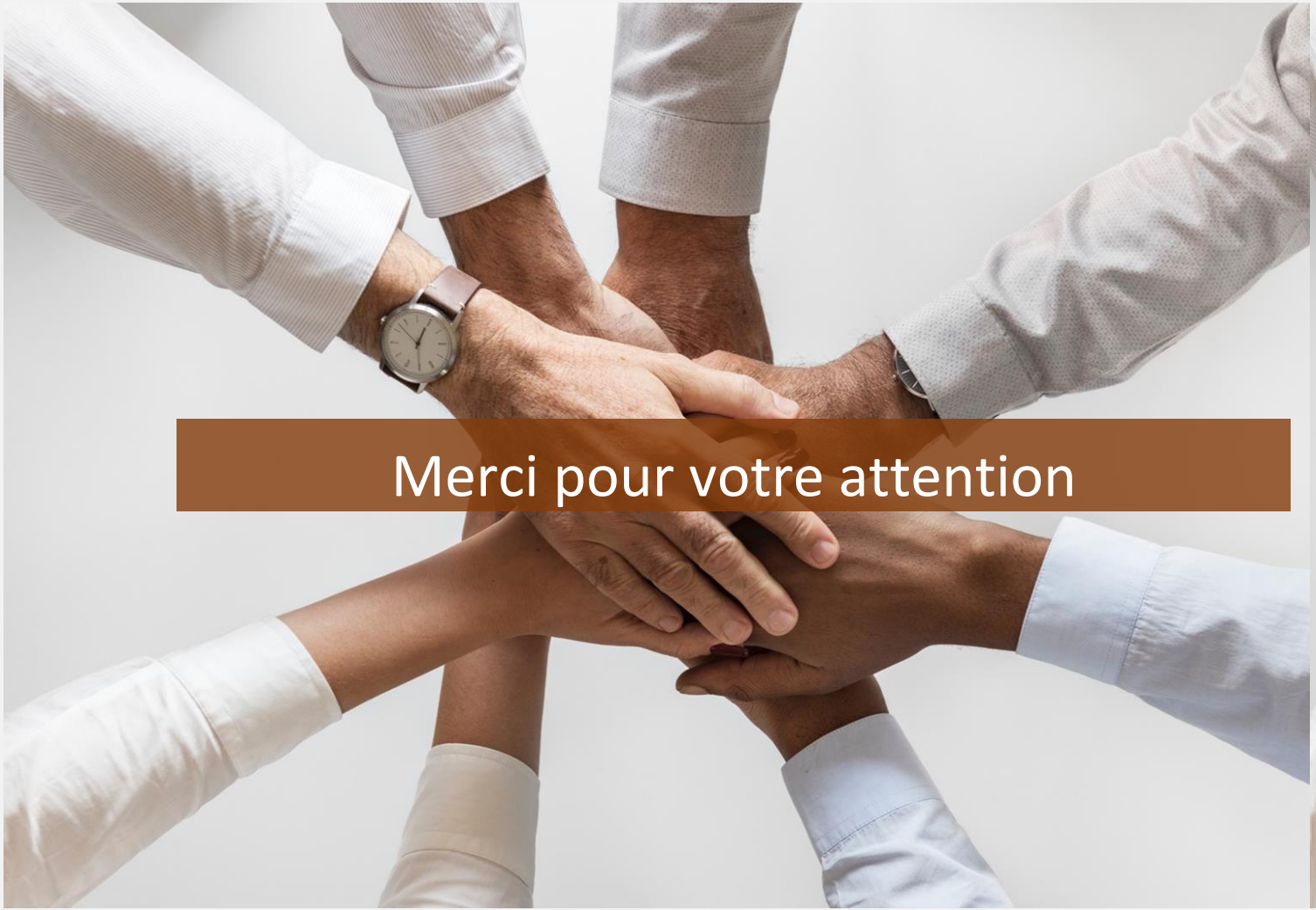
Objectifs et structure de la formation
Cadres normatifs et règlementaires
Concepts et définitions du risque
Programme de gestion des risques
Établissement du contexte

Leçon 2 Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005

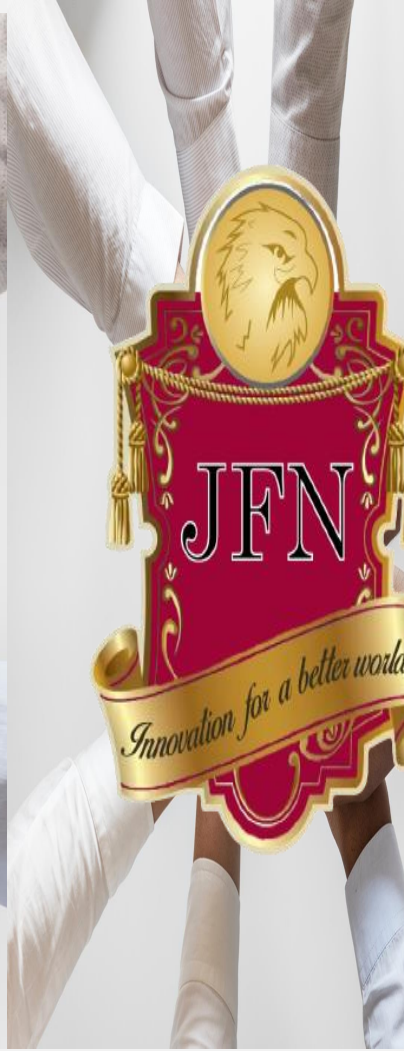
Identification des risques
Analyse et évaluation des risques
Appréciation du risque avec une méthode quantitative
Traitement des risques
Acceptation des risques et gestion des risques résiduels
Communication relative aux risques
Surveillance et réexamen des risques

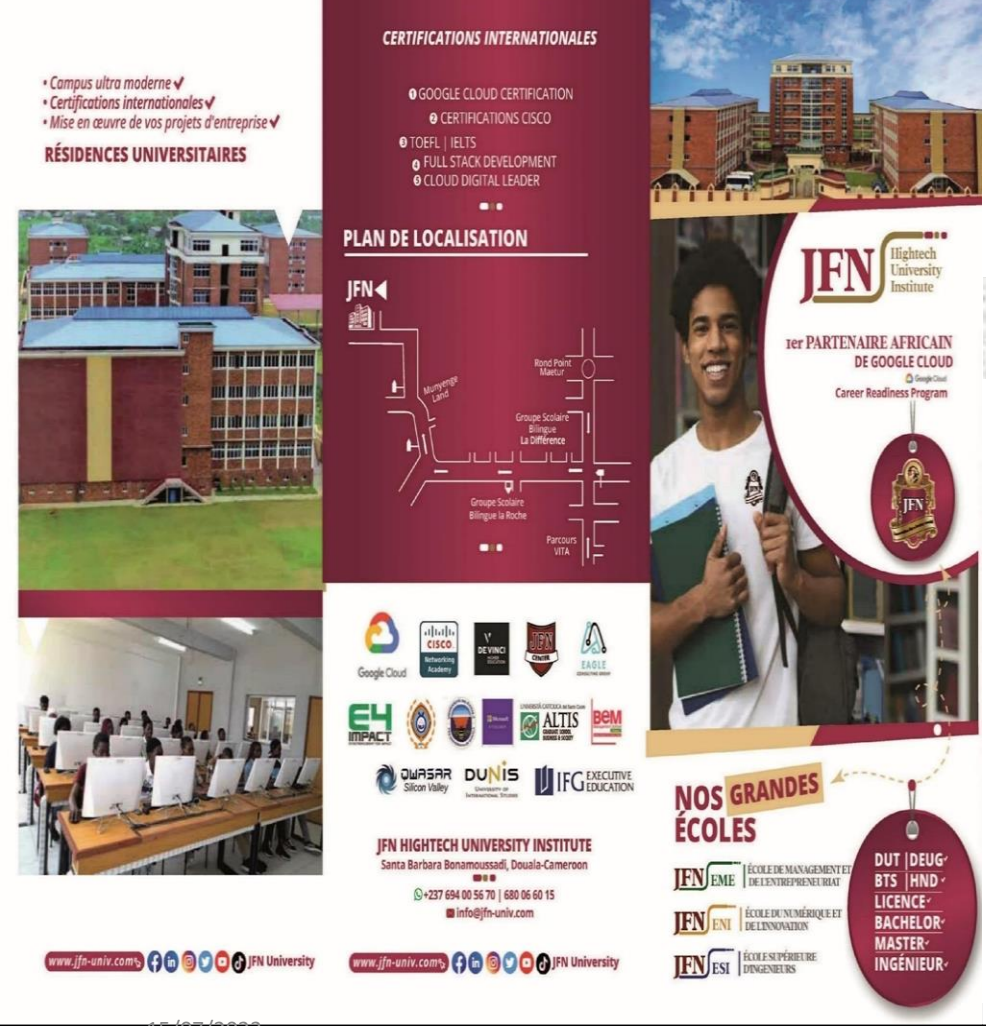
Leçon 3 Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

Méthode OCTAVE
Méthode MEHARI
Méthode EBIOS
Méthodologie harmonisée d'EMR



Merci pour votre attention





- ☑ Innovation,
- ☑ Entrepreneuriat,
- ☑ Formation Professionnelle et Continue