# La famille des normes
# ISO 27000

PECB
AUTHORIZED
TITANIUM
PARTNER


Oo2 Formations & Consulting

## Formations & Certifications
## Sécurité de l'information

Dans un monde de plus en plus digitalisé et connecté, les data se multiplient. Elles constituent une importante base de renseignements qui joue un rôle fondamental dans la vie des entreprises et des services administratifs. En effet, une mauvaise gestion de ces données peut avoir des conséquences néfastes sur le fonctionnement d'une organisation. Ainsi, il est indispensable de protéger ces données, de les sécuriser en cas de cyberattaque, de bug informatique ou de toute autre forme de défaillance.

Pour donner un cadre de référence complet et efficace, l'Organisation Internationale de Normalisation (ISO) a créé la famille de normes **ISO 27000**. Cette famille de référentiel a pour objectif d'organiser et de structurer les processus liés à la gestion des systèmes d'information peu importe le domaine d'activités. En clair, chaque normes facilitent le **management de la sécurité de vos informations**, notamment vos données financières, vos données clients, vos secrets de fabrications, vos documents soumis à la propriété intellectuelle, les informations relatives au personnel ou encore les données sur vos patients si vous êtes un organisme de santé.

# Sommaire

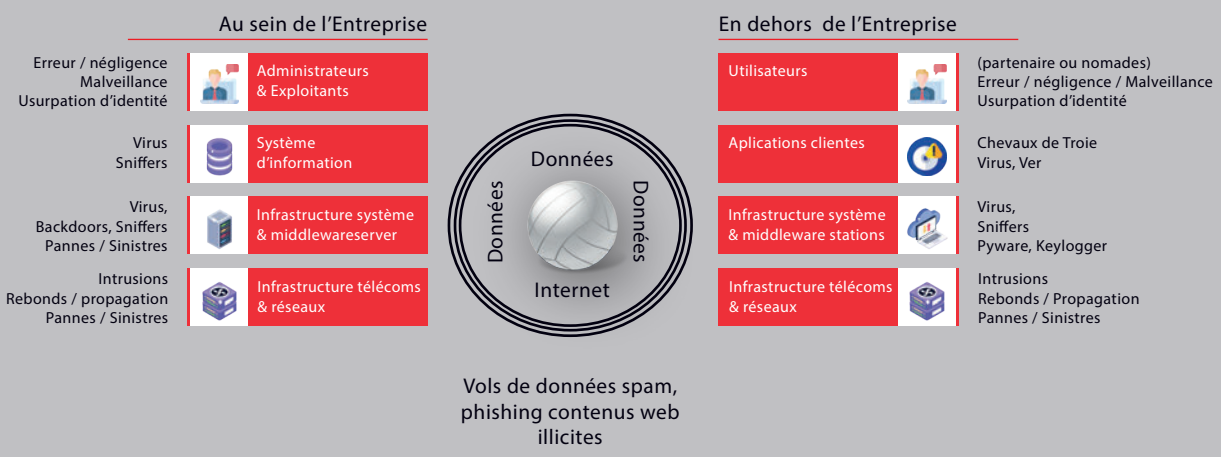
# Qu'est-ce que la **Sécurité de l'information ?**

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir et garantir la sécurité du système d'information.

Le système d'information constitue un patrimoine essentiel des entreprises. Constitué d'un ensemble de ressources matérielle et logicielle, il permet de traiter, stocker et transférer les données des entreprises.

La sécurité a pour objectif de réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations.

**Les menances directes et indirectes sur la pérennité du SI**




Ainsi la sécurité des systèmes d'information vise à une meilleure maîtrise des risques qui pèsent réellement sur l'organisation. Elle a pour objectif de maintenir, à un niveau convenable, les garanties suivantes :

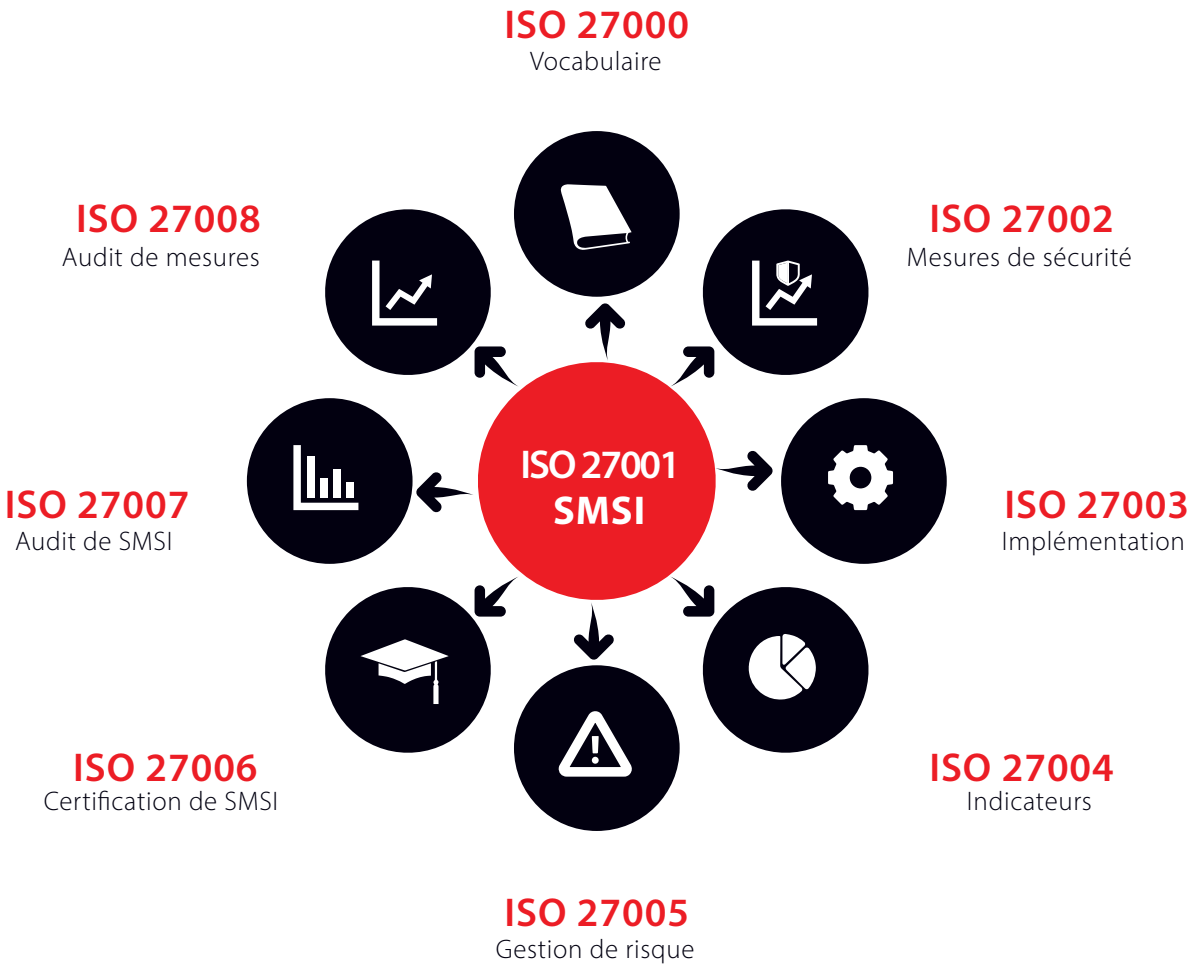
- Disponibilité : garantie que les entités autorisées ont accès à tout moment aux éléments considérés.
- Intégrité : garantie que les ressources sont exactes et complètes (non corrompues).
- Confidentialité : garantie que les ressources sont accessibles au moment voulu par les entités autorisées.
- Traçabilité (preuve): garantie que les accès et tentatives d'accès aux ressources sont tracés et que ces traces sont conservées et exploitables.

Ces quatre principes combinés, («DICT ou DICP»), permettent d'assurer un niveau de sécurité suffisamment élevé pour satisfaire au besoin de sécurité des données de l'entreprise concernée.
Aussi et pour satisfaire aux enjeux de la sécurité de l'information et permettre aux organisations de définir une méthode de management de risques informatiques, ISO a mis en place la famille des normes ISO 27000.

# Panorama
# de la famille ISO 27000

Les normes internationales de la famille ISO 27000 attestent du respect par l'organisme certifié des bonnes pratiques en matière de sécurité de l'information. Parmi les normes les plus utilisées on trouve la norme ISO 27001, qui constitue la norme de référence pour la mise en oeuvre d'un Système de Management de Sécurité de l'Information (SMSI) ainsi que les normes ISO 27002 (Code de bonnes pratiques) et ISO 27005 (Gestion des risques).

Maîtrise **des Normes ISO 27000**
La sécurité par la méthode




**SMSI :** Système de Management de la Sécurité de l'Information

La famille des normes ISO 27000 est vaste. Certaines normes comme la norme ISO 27001 sont des normes d'exigences. D'autres comme la norme ISO 27002 ou 27005 sont des normes de lignes directrices et enfin, on retrouve des normes de lignes directrices propres à un secteur telles que la norme ISO 27034, ISO 27035 ou encore ISO 27799.
Seule la norme ISO 27001 peut déboucher sur une certification de l'entreprise. L'entreprise certifiée prouve qu'elle a mis en place des mesures efficaces et reconnues par la communauté internationale pour protéger son SI et dont les principaux avantages sont :

- identification des menaces et dangers pesant sur le système d'information ;
- mobilisation des équipes autour d'un projet commun ;
- amélioration des pratiques pour sécuriser le système d'information ;
- maitrise des coûts liés à la sécurité et à la cybersécurité (bonnes mesures de sécurité mises en place, suppression des mesures inutiles, etc.) ;
- rendre pérenne l'activité (en protégeant les actifs de votre société) ;
- accroissement de la confiance des clients et de la notoriété de l'entreprise (avantage concurrentiel) ;
- être conforme à la règlementation en matière de gestion des risques et de la sécurité (RGPD en Europe.

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE
La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION.

MON COMPTE FORMATION

# La famille ISO 27000 est pour ceux qui sont impliqués dans la sécurité du système d'information de l'entreprise


Toutes les autres normes de la famille ISO 27000 peuvent conduire à la certification des compétences professionnelles liées à une personne. Cette certfication obtenue après une formation ISO PECB et la réussite de l'examen de certification démontre que vous détenez les compétences nécessaires à l'exercice d'une activité professionnelle en conformité avec ce même référentiel ISO.
Les formations ISO 27000 sont destinées à ceux qui sont impliqués dans la sécurité du système d'information de l'entreprise, dont les responsables de la sécurité et de la conformité de l'information, ainsi que toute son équipe. Elles s'adressent également aux directeurs de projet et aux consultants en sécurité.

Nous vous invitons à présent à découvrir nos offres de formation ISO 27000 et un panorama des compétences à acquérir pour chacune d'entre elles.

éligible en CPF MON COMPTE FORMATION

# ISO 27001

## MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION (SMSI)

**Maîtrisez les connaissances et techniques nécessaires pour la mise en oeuvre et la gestion efficace d'un SMSI**

## Définition

ISO 27001 est la norme centrale de la famille ISO 27000, c'est la norme d'exigences qui définit les lignes directrices pour l'établissement, la mise en oeuvre, la mise à jour et l'amélioration continue d'un système de management de la sécurité de l'information.

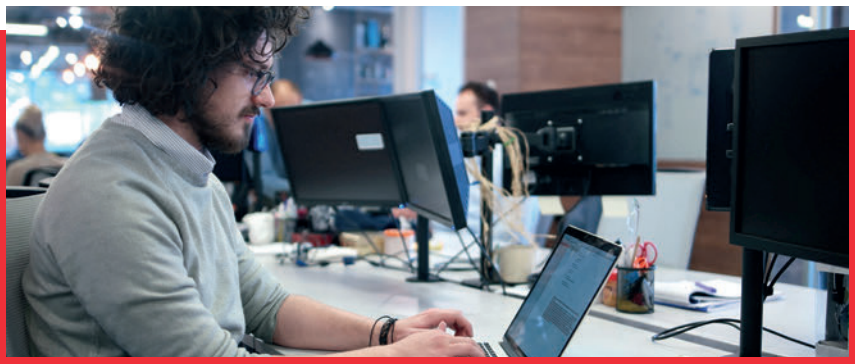
## Pourquoi vous devriez suivre cette formation ?

En suivant cette formation, vous recevez l'expertise nécessaire pour aider les organisations à mettre en oeuvre des politiques et procédures de sécurité de l'information adaptées à leurs besoins et à promouvoir l'amélioration continue de leur système de management.

# Avantages

La certification **ISO/CEI 27001** Management de la sécurité de l'information atteste que vous avez :

- Obtenu l'expertise nécessaire pour aider une organisation à mettre en œuvre un système de management de la sécurité de l'information, conforme à la norme ISO/CEI 27001
- Compris le processus de management des risques, des mesures de sécurité et des obligations de conformité
- Acquis une compréhension du processus de mise en œuvre du système de management de la sécurité de l'information
- Acquis les compétences nécessaires pour gérer une équipe chargée de mettre en œuvre un SMSI
- Acquis les connaissances pour prévenir et évaluer les menaces au sein de votre organisation
- Acquis la capacité à soutenir les organisations dans le processus d'amélioration continue de leur système de management de la sécurité de l'information
- Assimiler les connaissances nécessaires afin d'avoir les meilleures chances d'être engagé dans une carrière en sécurité informatique
- Acquis les compétences nécessaires pour auditer le système de management de la sécurité de l'information de l'organisation



## Les certifications ISO/CEI 27001

**ISO 27001 - Management de la sécurité de l'information - Foundation**
Appréhendez les meilleures pratiques en matière de management de la sécurité de l'information

**ISO 27001 - Management de la sécurité de l'information - Lead Implementer**
Maîtrisez la mise en œuvre et la gestion d'un système de management de la sécurité de l'information conforme à la norme ISO/IEC 27001

**ISO 27001- Management de la sécurité de l'information - Lead Auditor**
Maîtrisez l'audit d'un système de management de la sécurité de l'information conforme à la norme ISO/-CEI 27001

# ISO 27002

## MESURE DE LA SÉCURITÉ DE L'INFORMATION

Code de bonnes pratiques pour le management de la sécurité de l'information

**Démontrez vos aptitudes à mettre en place des mesures de sécurité de l'information au sein d'une organisation**

## Définition

L'ISO/CEI 27002 est une norme internationale qui définit les lignes directrices relatives aux bonnes pratiques de management de la sécurité de l'information. La norme a été élaborée à l'intention des organisations désireuses de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001.

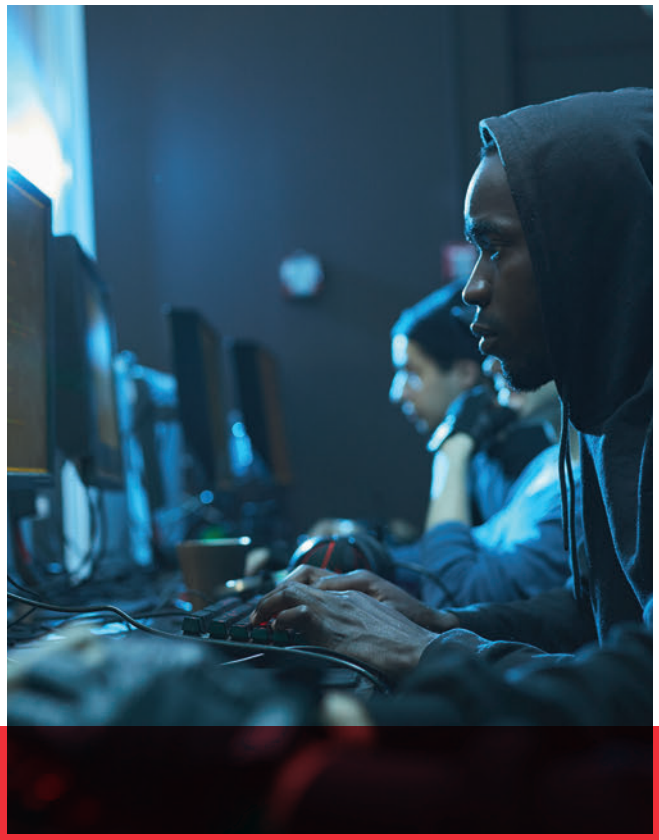
# Pourquoi vous devriez suivre cette formation ?

Cette formation est essentielle car elle s'inscrit en complément de la norme ISO 27001 en vous donnant les lignes directrices fondamentales qui vous aide à initier, mettre en œuvre, maintenir et améliorer le management de la sécurité de l'information au sein d'une organisation. Vous êtes ainsi apte à sélectionner les mesures spécifiques dans un processus de mise en œuvre parmi toutes les mesures de sécurité qui sont énumérées dans la norme.

## Avantages

En devenant un professionnel certifié **ISO/CEI 27002** – vous démontrez que vous avez :

- Compris la mise en œuvre des mesures de sécurité de l'information en conformité avec le cadre et les principes de la norme ISO/CEI 27002
- Compris la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance et la conformité
- Obtenu les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information selon l'ISO/CEI 27002
- Acquis la capacité à effectuer une évaluation périodique des risques dans une organisation
- Obtenu l'expertise nécessaire pour aider les organisations à améliorer leur position en matière de sécurité de l'information



## Les certifications ISO/CEI 27002

**ISO 27002- Mesure de la Sécurité de l'Information – Foundation**
Appréhendez les bonnes pratiques relatives aux mesures de sécurité de l'information, conforme à la norme ISO/CEI 27002.

**ISO 27002- Mesure de la sécurité de l'information – Lead Manager**
Maîtrisez la mise en place et la gestion des mesures de sécurité de l'information conformes à la norme ISO/IEC 27002

éligible en CPF MON COMPTE FORMATION

# ISO 27005

## GESTION DES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION

**La certification ISO 27005, démontre votre expertise dans la gestion des risques liés aux systèmes de l'information**

## Définition

ISO 27001 impose une analyse des risques mais ne propose aucune méthode pour la réaliser. C'est la norme ISO 27005, en complément de la norme ISO 27001, qui propose un recueil de lignes directrices traitant spécifiquement de la gestion des risques dans le contexte de la sécurité des systèmes d'information. Cependant, elle ne fournit aucune méthodologie spécifique à la gestion des risques SSI : **EBIOS, MEHARI** ou encore **OCTAVE** sont les méthodologies les plus utilisées pour répondre au cadre décrit par la norme ISO 27005 pour appliquer les exigences du SMSI.

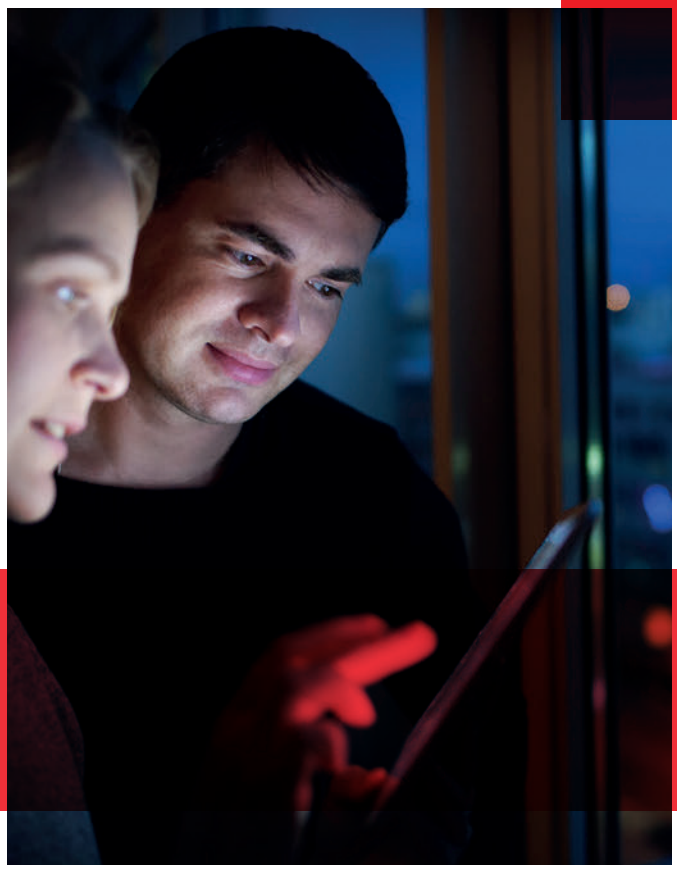
# Pourquoi vous devriez suivre cette formation ?

Parce que cette norme vient en appui de la norme ISO 27001 puisqu'elle a été conçue pour aider à la mise en œuvre efficace de la sécurité de l'information selon une approche de la gestion des risques. En suivant cette formation, vous avez les compétences nécessaires pour lancer le pilotage d'un processus de management des risques liés à la sécurité de l'information : capacité à identifier, hiéarchiser et traiter les divers risques de sécurité de l'information aux quels font face une organisation.

## Avantages

En devenant un professionnel certifié **ISO 27005** : Gestion des risques liés à la sécurité de l'information, vous prouvez que vous êtes capable de :

- Interpréter les exigences de la norme ISO/IEC 27001 dans le cadre d'un programme de management du risque de la sécurité de l'information
- Assurer la gestion des risques en entreprise conformément à la norme ISO/IEC 27005
- Gérer de façon responsable un processus de gestion des risques liés à la sécurité de l'information et assurer la conformité aux exigences légales et réglementaire
- Diriger une équipe de sécurité de l'information et de management du risque



## Les certifications ISO/CEI 27005

**ISO/IEC 27005 Risk Assessment – Foundation**
Maîtrisez les connaissances fondamentales dans la gestion des risques de la sécurité de l'information, dans le cadre de la norme ISO/CEI 27005

**IEC 27005 Risk Manager**
Recevez les compétences nécessaires pour maîtriser les processus de management du risque liés à tous les actifs pertinents pour la sécurité de l'information selon la norme ISO/IEC 27005

# MÉTHODE d'appréciation des Risques MEHARI, EBIOS & OCTAVE


L'appréciation efficace des risques pour les entreprises peut s'avérer très compliquée pour des néophytes. Néanmoins, avec des méthodes d'évaluation des risques, on peut acquérir les connaissances solides, nécessaires pour identifier un risque avec succès et apprécier son niveau dans une organisation. Parmi ces méthodes nous avons **MEHARI, EBIOS** et **OCTAVE.**


- **MEHARI (MEthode Harmonisée d'Analyse de Risque)**

  Développée par le Club de la Sécurité des Systèmes d'Information Français (CLUSIF), MEHARI a pour but la maîtrise parfaite d'une réalisation d'analyse des risques de sécurité de l'information basée sur de la théorie et de la pratique. Cette méthode vous donne les connaissances de base des principes fondamentaux de la sécurité de l'information et de la continuité des activités. La méthode MEHARI vous permet d'identifier les enjeux de la Sécurité des SI.

- **EBIOS (Etude des Besoins et Identification des Objectifs de Sécurité)**

  EBIOS fournit la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son Système d'Information. Elle vous permet d'acquérir les éléments essentiels relatifs à la gestion des risques liés à l'information. Cette méthode possède des caractéristiques uniques qui permettent son usage dans tous les secteurs de la sécurité. EBIOS vous donne les outils nécessaires pour l'identification des risques d'un SI en construction et demeure idéale pour la rédaction de cahiers des charges.

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

  La méthode OCTAVE a pour but de permettre à une entreprise de réaliser par elle-même l'analyse des risques de son Système d'Information. Elle fournit les connaissances et les compétences nécessaires à une exécution optimale de l'évaluation des risques de sécurité ainsi qu'à une gestion opportune des risques en vous familiarisant avec le cycle de vie de ces risques. Cette méthode se base sur des exercices pratiques et des études de cas, permettant de faire une étude complète des risques des organisations.

éligible en CPF MON COMPTE FORMATION

# ISO 27032
## LEAD CYBERSECURITY MANAGER

**Certifiez votre expertise pour planifier, déployer, gérer, contrôler et maintenir un programme de cybersecurity conformément à la norme ISO 27032**

## Définition

La norme ISO/CEI 27032 fait référence à la cybersécurité qui est définie comme la protection de la vie privée, de l'intégrité et de l'accessibilité des données dans le cyberespace. Par conséquent, le cyberespace est reconnu comme une interaction de personnes, de logiciels et de services technologiques mondiaux.

# Pourquoi vous devriez suivre cette formation ?

Cette formation vous permet d'acquérir les connaissances et les compétences nécessaires à la mise en œuvre et la gestion d'un programme de cybersécurité basé sur la norme ISO/IEC 27032 : vous êtes en mesure de protéger les données et la confidentialité d'une organisation contre les cyberattaques et lui permettez de réagir et de récupérer plus rapidement en cas d'incident.

## Avantages

En devenant un professionnel certifié **ISO/IEC 27032** – Lead Cybersecurity Manager, vous êtes apte à :

- Connaître les composants et les opérations d'un programme de cybersécurité en conformité avec la norme ISO 27032
- Maîtriser les concepts, méthodes, normes et techniques pour gérer un programme de cybersécurité
- Expliquer l'objectif, le contenu et la corrélation entre l'ISO 27032 et d'autres normes et référentiels
- Piloter un programme de cybersécurité tel que spécifié dans la norme ISO 27032


**ISO 27032 Lead Cyber Security Manager**

Maîtrisez la mise en œuvre et la gestion d'un programme de cybersécurité conforme à la norme ISO/IEC 27032.

éligible en CPF MON COMPTE FORMATION

# ISO 27034
## SÉCURITÉ DES APPLICATIONS

**La certification ISO 27034 prouve votre expertise à assurer la sécurité des applications au sein d'un organisme**

## Définition

La norme ISO/CEI 27034 fournit une approche systématique qui guide les organisations dans la mise en œuvre des concepts, des principes et des processus de sécurité dans la structure de sécurité des applications. La sécurité des applications est un concept international qui soutient le cadre de sécurité de l'information et guide une organisation vers la réalisation d'une solide structure de sécurité de l'information au sein de ses opérations.

## Pourquoi vous devriez suivre cette formation ?

Cette formation vous dote de la maîtrise des meilleures pratiques en matière de techniques de sécurité des applications et vous aide à développer vos aptitudes à identifier et éviter les vulnérabilités courantes des applications.

# Avantages

En devenant un professionnel certifié **ISO/CEI 27034** – Sécurité des Applications ; vous êtes apte à :

- Comprendre les principes fondamentaux de la sécurité des applications et leurs relations avec les autres normes de sécurité de l'information
- Comprendre le rôle et les exigences de chacune des parties prenantes de l'organisation
- Apprendre les bonnes pratiques, les concepts et techniques pour appliquer les directives de sécurité dans une organisation
- Acquérir des compétences professionnelles pour gérer un projet de mise en œuvre de la sécurité des applications
- Développer les connaissances nécessaires pour fournir les meilleures pratiques de sécurité d'application au sein d'une organisation

## Les certifications ISO/CEI 27034

**ISO 27034 Sécurité des applications – Foundation**
Maîtrisez les fondamentaux de la sécurité des applications et les différents processus impliqués dans la mise en place de la norme ISO/CEI 27034

**ISO 27034 Sécurité des applications – Lead Implementer**
Maîtrisez la mise en œuvre, la gestion et le maintien de la sécurité des applications en conformité avec la norme ISO/CEI 27034

**ISO 27034 Sécurité des applications – Lead Auditor**
Maîtrisez la conduite d'un audit de sécurité des applications conforme à la norme ISO/CEI 27034

éligible en CPF MON COMPTE FORMATION

# ISO 27035

## GESTION DES INCIDENTS DE SÉCURITÉ DE L'INFORMATION

**Maitrisez les techniques nécessaires pour évaluer et améliorer votre réponse aux incidents de sécurité avec la certification ISO 27035**

# Définition

En cybersécurité, la détection des évènements suspects et la mise en œuvre de réactions adaptées est une tâche fondamentale mais difficile. La norme ISO/IEC 27035, système de gestion des incidents de sécurité informatique, aide l'entreprise à améliorer sa capacité de réaction face aux incidents en la dotant d'outils sur la manière de détecter, signaler et évaluer d'éventuels incidents de sécurité et vulnérabilités.

# Pourquoi vous devriez suivre cette formation ?

ISO/IEC 27035 est une norme internationale qui s'applique à tous les professionnels intéressés par la sécurité des technologies de l'information et désireux d'acquérir les compétences et les connaissances les plus élevées pour protéger leur organisation contre les incidents de sécurité et réduire les répercussions financières de tels incidents sur l'entreprise.

## Avantages

En devenant un professionnel certifié **ISO/CEI 27035** – Information Security Incident Management, vous êtes apte à :

- Comprendre les concepts, les approches et les outils pour une gestion efficace des incidents de sécurité de l'information
- Éliminer toute interruption possible et les impacts négatifs sur les opérations commerciales
- Apprendre les techniques les plus avancées pour réagir correctement et efficacement face aux incidents de sécurité de l'information
- Améliorer vos compétences en gestion de la sécurité de l'information et votre analyse des processus d'incidents
- Acquérir les connaissances nécessaires pour mettre en place et piloter une équipe de gestion des incidents de sécurité de l'information
- Obtenir des connaissances sur les bonnes pratiques de gestion de la sécurité de l'information

## Les certifications ISO/CEI 27035

**ISO/CEI 27035 Gestion des incidents de sécurité – Lead Incident Manager**
Maîtrisez la gestion des incidents de sécurité de l'information selon la norme ISO/CEI 27035


# ISO 27701

## MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE

**Démontrez votre expertise dans la mise en place d'un système de management de la protection de la vie privée au sein d'un organisme**

## Définition

Promulguée en 2019, ISO/IEC 27701 vient compléter et étendre les normes ISO 27001 et ISO 27002 relativement à la protection des données personnelles. La norme aide ainsi les organismes à établir, à tenir à jour et à améliorer continuellement un système de management en matière de protection de la vie privée (SMVP) sur la base du SMSI existant et conformément aux exigences de la norme ISO/IEC 27001 et aux orientations de la norme ISO/IEC 27002.

## Pourquoi vous devriez suivre cette formation ?

Dans un monde ultra connecté, la protection de la vie privée devient une préoccupation majeure pour les entreprises pour limiter les coûts induits par une violation de leurs données mais aussi pour se conformer aux obligations légales de plus en plus contraignantes (ex : la RGPD en Europe). ISO/IEC 27701 est la première norme internationale qui permet aux organisations de toute taille, les administrations comme les entreprises de protéger et contrôler efficacement les données personnelles qu'elles doivent traiter.

# Avantages

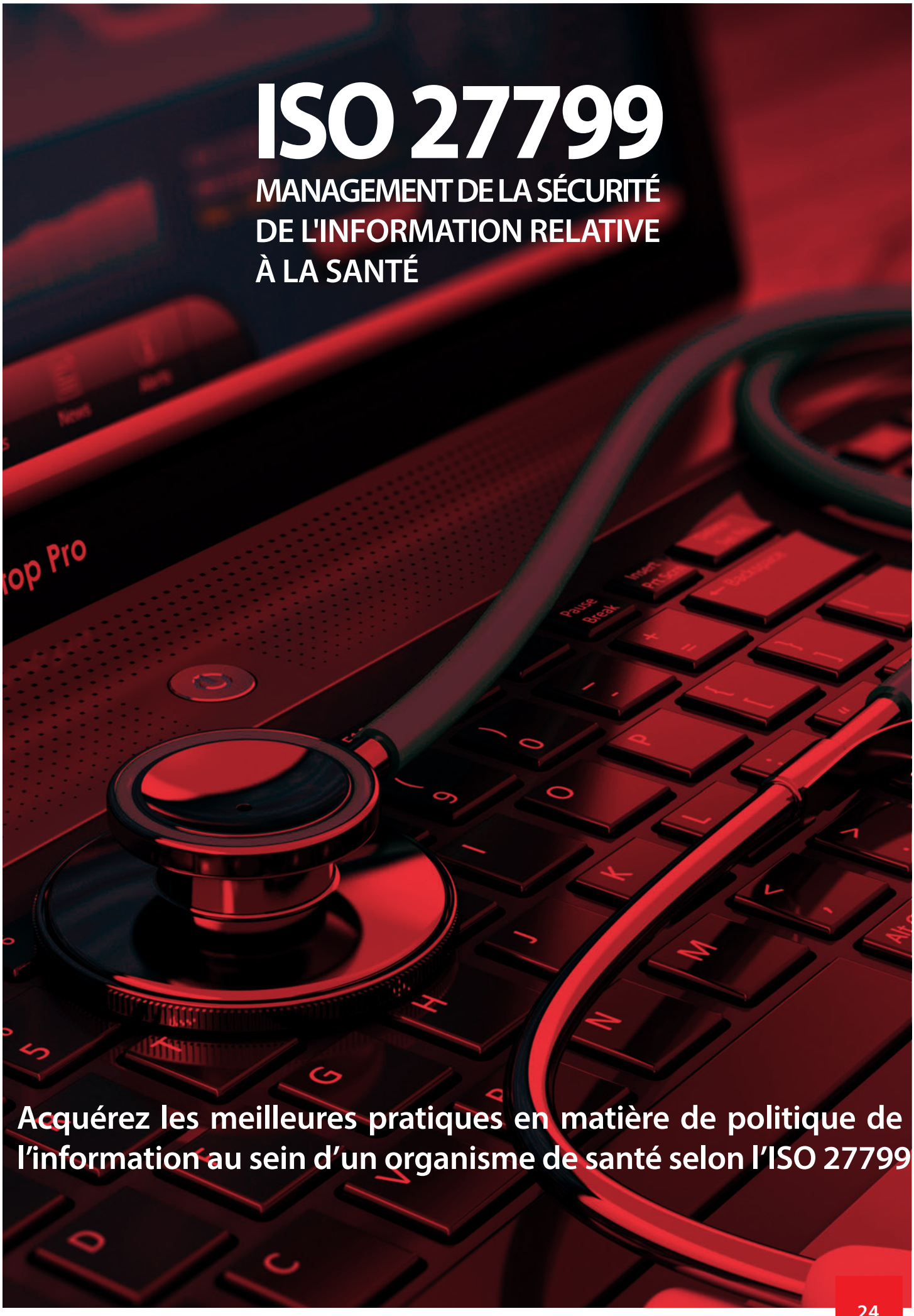
En devenant certifié I**SO/IEC 27701** – Management de la protection de la vie privée, vous démontrez votre aptitude à :

- Comprendre le processus de mise en œuvre du système de management de la protection de la vie privée
- Aider une organisation à mettre en œuvre un système de management de la protection de la vie privée conforme à la norme ISO/IEC 27701
- Soutenir le processus d'amélioration continue du système de management de la protection de la vie privée dans les organisations
- Protéger la réputation de l'organisation
- Construire la confiance du client
- Augmenter la satisfaction de la clientèle
- Augmenter la transparence des processus et procédures de l'organisation
- Maintenir l'intégrité des informations des clients et des autres parties intéressée

## Les certifications ISO/CEI 27701

**ISO 27701 Management de la protection de la vie privée – Lead Implementer**
Maîtrisez la mise en œuvre et la gestion d'un système de management de la protection de la vie privée conforme à la norme ISO/IEC 27701

**SO 27701 Management de la protection de la vie privée – Lead Auditor**
Maîtrisez l'audit d'un système de management de la protection de la vie privée conforme à la norme ISO/CEI 27701




# ISO 27799

## MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION RELATIVE À LA SANTÉ

**Acquérez les meilleures pratiques en matière de politique de l'information au sein d'un organisme de santé selon l'ISO 27799**

# Définition

Cette norme définit une série de mesures de sécurité adaptées à la protection des informations de santé et précise les bonnes pratiques en matière de sécurité des informations de santé. Cette norme n'a pas été conçue pour se substituer aux normes ISO 27001 et ISO 27002, mais pour préciser les mesures de sécurité adaptées aux systèmes d'information de santé.

# Pourquoi vous devriez suivre cette formation ?

Si vous travaillez pour un organisme de santé dont les systèmes d'information sont souvent vulnérables, cette formation vous procure les lignes directrices pour aider votre établissement à gérer de manière sécurisée les informations personnelles qu'il traite. Vous pouvez suivre cette formation quel que soit la taille ou le type de votre organisme de santé.

## Avantages

En devenant un professionnel certifié **ISO 27799** – Management de la sécurité de l'information relative à la santé, démontrez votre capacité à :

- Comprendre la mise en œuvre des mesures de sécurité de l'information dans les organismes de santé conforme au cadre et aux principes de l'ISO 27799
- Comprendre la relation entre les différents éléments de mesure de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain
- Soutenir un organisme de santé dans la mise en œuvre et la gestion des mesures de sécurité de l'information en conformité à l'ISO 27799
- Réaliser, de manière périodique, une appréciation des risques dans un organisme de santé
- Aider les organismes de santé à jouer un rôle actif et important dans la protection des données personnelles de leurs patients
- Améliorer la sécurité de l'information au sein des organismes de santé

## Les certifications ISO/CEI 27799

**ISO 27799 Management de la sécurité de l'information dans le secteur de la santé – Foundation**
Appréhendez les meilleures pratiques en matière de management de la sécurité de l'information dans le domaine de la santé

**ISO 27799 Management de la sécurité de l'information dans le secteur de la santé – Lead Manager**
Maîtrisez les principes du management de la sécurité de l'information dans le secteur de la santé selon la norme ISO 27799

# La famille des normes
# ISO 27000

Oo2 Formations & Consulting

PECB AUTHORIZED TITANIUM PARTNER



## France

128 rue de la Boétie
75008 Paris

Tel : +33(0) 188 24 70 33
+33(0) 188 24 70 34
Email : contact@oo2.fr

## Sénégal

4313 Allées Seydou Nourou Tall
Point E, Immeuble 713, 2 ème étage
BP 45617 Dakar

Tel : +221 33 825 45 54
+221 33 825 72 34
Email : contact@oo2.sn

## Côte d'Ivoire

Bd VGE - Marcory
Immeuble Le Massaï
1163 Abidjan 27

Tel : +225 27 225 03 445
+225 27 215 92 870
Email : contact@oo2.ci

## Burkina Faso

Avenue du Dr Kwamé
N'Krumah Ouagadougou 01
BP 513

Tel : +226 55 77 87 11
+226 55 79 11 42
Email : contact@oo2.fr

## Bénin

Quartier Fidjrossè Fiyégnon 2
Cotonou, Bénin

Tel : +229 69 25 89 89
Email : contact@oo2.bj


www.oo2.fr