ACG | Cybersecurity

ACG CYBERACADEMY

Catalogue de Formations

PRÉSENTATION

Chez ACG Cybersecurity nous comprenons les défis croissants des entreprises dues aux évolutions rapides des menaces numériques. C'est pourquoi, nous avons créé un centre de formation dédié à la sécurité de l'information : « ACG CyberAcademy ».

En tant que pure player de la cybersécurité, nous mettons notre expertise de pointe au service de votre protection numérique, la sécurité de vos systèmes d'information, la gestion des risques ou le développement de votre stratégie cyber. ACG CyberAcademy permettra de faire monter en compétences vos collaborateurs, via des formations certifiantes et des parcours spécifiques.

Grâce à différents partenariats stratégiques, nous offrons une large gamme de formations, allant de la sensibilisation à la gouvernance, en passant par des parcours académiques (Executive MBAs).

Nous sommes certifiés Qualiopi afin de vous offrir des formations et certifications de qualité, et notre CEO a été récompensé cinq années de suite **« Best French Trainer »** par notre partenaire Gold PECB. Nos formateurs, experts dans le domaine, s'engagent à adapter leurs approches à vos besoins et accordent la priorité à votre satisfaction.

ACG CyberAcademy, l'assemblée des experts Cyber.

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE

ACG CYBERSECURITY est certifié ISO 27001 : 2022

Une certification ISO 27001 sur nos principales activités (formation, audit et consulting cybersécurité).

ACG Cybersecurity est partenaire de SWIFT CSP

ACG Cybersecurity est membre de la fédération française de la Cybersécurité

ACG Cybersecurity référencé officiellement comme Prestataire de Terrain par l'ANSSI (Agence nationale de la sécurité des systèmes d'information)

ACG Cybersecurity est membre de :

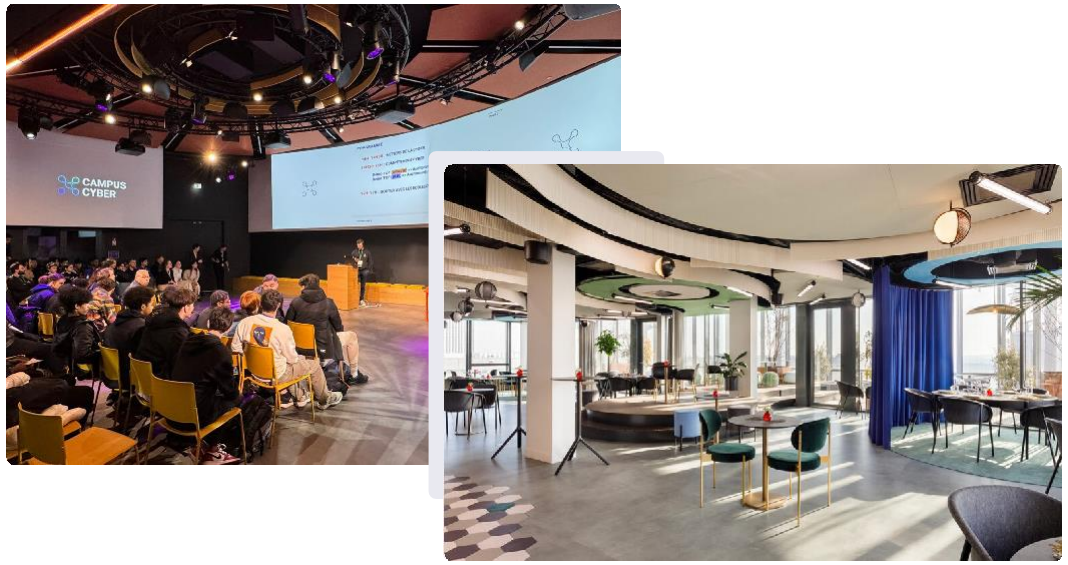
Club EBIOS

ACN Alliance pour la Confiance Numérique

NOTRE CENTRE DE FORMATION

ACG CYBERACADEMY

ACG Cybersecurity est membre associé du Campus Cyber, lieu totem de la cybersécurité en France qui rassemble les principaux acteurs nationaux et internationaux du domaine.



Nos partenaires de certification

PECB ISACA mile2 CompTIA EC-Council

ACG Cybersecurity

ACG Cybersecurity membre associé et résident du Campus Cyber

CAMPUS CYBER RÉSIDENT CAMPUS CYBER ASSOCIÉ CAMPUS CYBER ACTEUR ENGAGÉ

Un engagement pour le développement de nos activités et services dans un éco-système international de la Cybersécurité.

Adresse : Tour Eria, 5-7 rue Bellini, 92800 Puteaux, FRANCE

Sommaire

Management de la sécurité de l'information

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

2 JOURS

1600 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 27001:2022 Transition

PECB

Les Objectifs

- 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.

Le programme

Jour 1

Introduction à la norme ISO/IEC 27001:2022 et comparaison avec la norme ISO/IEC 27001:2013.

Jour 2

Comparaison entre les mesures de l'Annexe A de la norme ISO/IEC 27001:2013 et de la norme ISO/IEC 27001:2022.

Examen de certification.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- 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 plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 27001:2022 Foundation

PECB

Les Objectifs

- Comprendre la mise en œuvre des mesures de sécurité de l'information conformément à la norme ISO/CEI 27002.
- Comprendre la corrélation entre les normes ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes et cadres réglementaires.
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Personnes intéressées par le management de la sécurité l'information et les mesures de sécurité de l'information.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information.
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

Le programme

Jour 1

Introduction à la norme ISO/CEI 27002 et au Système de management de la sécurité de l'information.

Jour 2

Lancement de la phase de reconnaissance.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3380 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27001:2022 Lead Implementer

PECB

Les Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires.
- Maîtrisez les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI.
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique de l'organisation.
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMSI.
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la sécurité de l'information.

Les prérequis de la formation

Pour suivre cette formation ISO 27001 Lead Implementer, une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre sont demandées.

L'audience ciblée

- Responsables ou consultants impliqués dans le management de la sécurité de l'information.
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information.
- Toute personne responsable du maintien de la conformité aux exigences du SMSI.
- Membres d'une équipe du SMSI.

Le programme

Jour 1

Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI.

Jour 2

Planification de la mise en œuvre d'un SMSI.

Jour 3

Mise en œuvre d'un SMSI.

Jour 4

Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3380 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27001:2022 Lead Auditor

PECB

Les Objectifs

- Comprendre le fonctionnement d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001.
- Expliquer la corrélation entre la norme ISO/ CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires.
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011.
- Savoir diriger un audit et une équipe d'audit.
- Savoir interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI.
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Les prérequis de la formation

Pour suivre cette formation ISO 27001 Lead Auditor, une connaissance préalable de la norme ISO 27001 ainsi que des connaissances approfondies sur les principes de l'audit sont nécessaires.

L'audience ciblée

- 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

Le programme

Jour 1

Introduction au Système de management de la sécurité de l'information et à la norme ISO/CEI 27001.

Jour 2

Principes, préparation et déclenchement de l'audit.

Jour 3

Activités d'audit sur site.

Jour 4

Clôture de l'audit.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

2 JOURS

1580 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27002 Foundation

PECB

Les Objectifs

- Comprendre la mise en œuvre des mesures de sécurité de l'information conformément à la norme ISO/CEI 27002.
- Comprendre la corrélation entre les normes ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes et cadres réglementaires.
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre les mesures de sécurité de l'information.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Personnes intéressées par le management de la sécurité l'information et les mesures de sécurité de l'information.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management de la sécurité de l'information et des mesures de sécurité de l'information.
- Personnes souhaitant poursuivre une carrière dans le management de la sécurité de l'information.

Le programme

Jour 1

Introduction à la norme ISO/CEI 27002 et au Système de management de la sécurité de l'information.

Jour 2

Lancement de la phase de reconnaissance.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27002 Lead Manager

PECB

Les Objectifs

- Maîtrisez la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002.
- Maîtrisez les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité de l'information.
- Comprendre la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain.
- Comprendre l'importance de la sécurité de l'information pour la stratégie de l'organisation.
- Maîtrisez la mise en œuvre des processus de la sécurité de l'information.
- Maîtrisez l'expertise pour soutenir une organisation dans la mise en œuvre, la gestion et le maintien des mesures de la sécurité de l'information.
- Maîtrisez la formulation et la mise en œuvre des exigences et des objectifs de la sécurité de l'information.

Les prérequis de la formation

Pour participer à cette formation, il faut avoir une connaissance fondamentale de la norme ISO/IEC 27002 et une connaissance approfondie des mesures de sécurité de l'information.

L'audience ciblée

- Managers ou consultants cherchant à améliorer leurs connaissances concernant la mise en œuvre des mesures de sécurité de l'information dans un SMSI conformément à la norme ISO/IEC 27001
- Personnes responsables de la gestion de la sécurité de l'information, de la conformité, du risque ou de la gouvernance dans une organisation
- Professionnels de l'informatique ou consultants souhaitant améliorer leurs connaissances en matière de sécurité de l'information
- Membres d'une équipe de mise en œuvre d'un SMSI ou de la sécurité de l'information

Le programme

Jour 1

Introduction à la norme ISO/IEC 27002.

Jour 2

Rôles et responsabilités en matière de sécurité de l'information, de mesures relatives aux personnes et de mesures physiques.

Jour 3

Actifs de sécurité de l'information, contrôles d'accès et protection des systèmes et réseaux d'information.

Jour 4

Gestion des incidents de sécurité de l'information et test et surveillance des mesures de sécurité de l'information conformément à la norme ISO/IEC 27002

Jour 5

Examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3700 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 27035 Lead Incident Manager

PECB

Les Objectifs

- Maîtrisez les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/IEC 27035.
- Connaître la corrélation entre la norme ISO/ IEC 27035 et les autres normes et cadres réglementaires.
- Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en œuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information.
- Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information.
- Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents.
- Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux inci- dents.

Les prérequis de la formation

Les fondamentaux du management du risque constitue le prérequis idéal pour suivre ce cours.

L'audience ciblée

- Gestionnaires des incidents de sécurité de l'information.
- Responsables des TIC.
- Auditeurs des technologies de l'information.
- Responsables souhaitant mettre en place une équipe de réponse aux incidents.
- Responsables souhaitant apprendre davantage sur le fonctionnement efficace d'une équipe de réponse aux incidents.
- Responsables des risques liés à la sécurité de l'information.
- Administrateurs professionnels des systèmes informatiques.
- Administrateurs professionnels de réseau informatique.
- Membres de l'équipe de réponse aux incidents.
- Personnes responsables de la sécurité de l'information au sein d'une organisation.

Le programme

Jour 1

Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/IEC 27035.

Jour 2

Conception et préparation d'un plan de gestion des incidents de sécurité de l'information.

Jour 3

Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information.

Jour 4

Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED Chief Information Security Officer

PECB

Les Objectifs

- D'expliquer les principes et concepts fondamentaux de la sécurité de l'information
- De comprendre les rôles et les responsabilités du RSSI, les considérations éthiques qu'ils impliquent et aborder les défis associés à ce rôle
- De concevoir et d'élaborer un programme de sécurité de l'information efficace, adapté aux besoins de l'organisme
- D'adopter les cadres, lois et règlements applicables.
- De communiquer et de mettre en œuvre des politiques efficaces visant à assurer la conformité de la sécurité de l'information
- D'identifier, d'analyser, d'évaluer et de traiter les risques liés à la sécurité de l'information, en utilisant une approche systématique et efficace

Les prérequis de la formation

La principale condition pour participer à cette formation est d'avoir une compréhension fondamentale des principes et des concepts de la sécurité de l'information.

L'audience ciblée

- Professionnels activement impliqués dans la gestion de la sécurité de l'information
- Responsables informatiques chargés de superviser les programmes de sécurité de l'information
- Professionnels de la sécurité qui aspirent à accéder à des postes de direction, tels que les architectes de la sécurité, les analystes de la sécurité et les auditeurs de la sécurité
- Professionnels responsables de la gestion des risques et de la conformité en matière de sécurité de l'information au sein des organismes

RSSI expérimentés désireux d'améliorer leurs connaissances, de rester à jour sur les dernières tendances et d'affiner leurs compétences en matière de leadership

- Cadres, y compris les DSI, les PDG et les directeurs de l'exploitation, qui jouent un rôle crucial dans les processus de prise de décision liés à la sécurité de l'information
- Professionnels souhaitant accéder à des postes de direction dans le domaine de la sécurité de l'information

Le programme

Jour 1

Fondamentaux de la sécurité de l'information et rôle d'un RSSI

Jour 2

Programme de conformité en matière de sécurité de l'information, gestion des risques, architecture et conception de la sécurité

Jour 3

Mesures de sécurité, gestion des incidents et gestion des changements

Jour 4

Sensibilisation à la sécurité de l'information, surveillance et mesurage, amélioration continue

Jour 5

Examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

4 JOURS

2833 € HT

FORMATION
CERTIFIANTE

NIVEAU
AVANCÉ

KIT DE FORMATION
OFFICIELLE

ACCESSIBLE AU PMR

ISACA CERTIFIED Information Security Manager

Les Objectifs

- Apprendre les processus et les meilleures pratiques pour gérer et évaluer les risques liés à la sécurité de l'information.
- Développez les compétences nécessaires pour concevoir et mettre en œuvre un programme de sécurité de l'information qui s'aligne sur les objectifs et les stratégies d'une organisation.

Les prérequis de la formation

Pour être éligible à passer l'examen CISM, vous devez avoir cinq ans ou plus d'expérience professionnelle dans la sécurité de l'information. Au moins trois de ces années doivent être réparties dans un minimum de trois domaines de pratique professionnelle, avec une année ou plus dans chacun. Ces domaines comprennent la gestion de la sécurité de l'information.

L'audience ciblée

CISM s'adresse aux professionnels de la sécurité de l'information ayant au moins cinq années d'expérience professionnelle pertinente, dont au moins trois années dans le rôle de respon- sable de la sécurité de l'information. Les titres de poste incluent :

- CISO (Chief Information Security Officer).
- CSO (Chief Security Officer).
- Directeur/Gestionnaire/Consultant en Sécurité.
- Directeur/Gestionnaire/Consultant en Technologies de l'Information (TI).
- Directeur et Gestionnaire en Conformité / Risques / Vie privée.

Le programme

Domaine 1

Gouvernance de la sécurité de l'information.

Domaine 2

Gestion des risques liés à la sécurité de l'information.

Domaine 3

Programme de sécurité de l'information.

Domaine 4

Gestion des incidents.

Les plus

- Cours animé par un formateur certifié ISACA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3167 € HT

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

ISACA CERTIFIED Information Systems Auditor

ISACA

Les Objectifs

- Développer et mettre en œuvre une stratégie d'audit informatique basée sur les normes d'audit informatique.
- Planifier des audits spécifiques pour déterminer si les systèmes d'information sont protégés, contrôlés et apportent de la valeur à l'organisation.
- Mener des audits conformément aux normes d'audit informatique pour atteindre les objectifs d'audit planifiés.
- Rapporter les conclusions de l'audit et formuler des recommandations aux parties prenantes clés pour communiquer les résultats et apporter des changements lorsque nécessaire.
- Effectuer des suivis ou préparer des rapports d'état pour s'assurer que des mesures appropriées ont été prises par la direction en temps opportun.

Les prérequis de la formation

Un an d'expérience en tant qu'auditeur de systèmes d'information. Vous pouvez également soumettre un an d'expérience en audit non informatique. Un diplôme de deux ou quatre ans peut être substitué à l'exigence d'expérience, à condition que votre diplôme ait été obtenu au cours des 10 dernières années.

L'audience ciblée

Professionnels en début de carrière à mi-carrière cherchant à obtenir une reconnaissance et une crédibilité accrues dans leurs interactions avec les parties prenantes internes et externes, les régulateurs et les clients. Les rôles professionnels incluent :

- Directeurs/Responsables/Consultants en audit informatique.
- Auditeurs informatiques et internes.
- Directeurs de la conformité, des risques et de la confidentialité.
- Directeurs / Responsables / Consultants en informatique.

Le programme

Domaine 1

Processus d'audit du système d'information.

Domaine 2

Gouvernance et gestion des technologies de l'information.

Domaine 3

Acquisition, développement et mise en œuvre de systèmes d'information.

Domaine 4

Exploitation des systèmes d'information et résilience de l'entreprise.

Domaine 5

Protection des actifs informationnels.

Les plus

- Cours animé par un formateur certifié ISACA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CISA

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION

5 JOURS

3499 € HT

FORMATION CERTIFIANTE

LEVEL 300

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

MILE2 CERTIFIED Information System Security Officer

Les Objectifs

Upon completion, Certified Information Systems Security Officer students be able to establish industry acceptable Cyber Security and Information Systems management standards with current best practices.

Les prérequis de la formation

- Mile2's C)SP
- Mile2's C)ISSM
- 12 months of Information Systems Management Experience

L'audience ciblée

- IS Security Officers
- IS Managers
- Risk Managers
- Auditors
- Info Systems Owners
- IS Control Assessors
- System Managers
- Government Employees

Le programme

Module 1
Risk Management

Module 2
Security Management

Module 3
Identification and Authentication

Module 4
Access Control

Module 5
Security Models and Evaluation Criteria

Module 6
Operations Security

Module 7
Vulnerability Assessments

Module 8
Symmetric Cryptography and Hashing

Module 9
Network Connections

Module 10
Network Protocols and Devices

Module 11
Telephony, VPNs, and Wireless

Module 12
Security Architecture and Attacks

Module 13
Software Development Security

Module 14
Database Security

Module 15
Malware and Attacks XVI

Module 16
Business Continuity

Module 17
Incident Management, Law and Ethics

Module 18
Physical Security

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Cybersécurité

PECB Cybersecurity Foundation

PECB

2 JOURS

1333 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Expliquer les concepts et principes fondamentaux de la cybersécurité
- Identifier les principales normes et les principaux cadres de cybersécurité, tels que l'ISO/IEC 27032 et le cadre de cybersécurité du NIST
- Expliquer les approches, les méthodes et les techniques permettant d'assurer la la cybersécurité

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Managers et consultants souhaitant approfondir leurs connaissances en matière de connaissances en matière de cybersécurité
- Les professionnels souhaitant se familiariser avec les meilleures pratiques en matière de gestion de la cybersécurité
- Les personnes chargées de mener des activités de cybersécurité au sein de leur organisation
- Personnes souhaitant faire carrière dans la cybersécurité

Le programme

Jour 1

Introduction aux concepts fondamentaux de la cybersécurité

Jour 2

Approches du programme de cybersécurité et examen du certificat

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED Lead Pen Test Professional

PECB

5 JOURS

4050 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Savoir interpréter et illustrer les principaux concepts et principes relatifs au test d'intrusion.
- Comprendre les connaissances techniques de base nécessaires pour organiser et mener à bien un ensemble efficace de tests d'intrusion.
- Apprendre comment planifier efficacement un test d'intrusion et identifier un domaine d'application approprié et adapté en fonction du risque.
- Acquérir les connaissances et les compétences pratiques sur les outils et les techniques utilisés pour effectuer efficacement un test d'in- trusion.
- Gérer efficacement le temps et les ressources nécessaires à l'échelle d'un test d'intrusion spécifique.

Les prérequis de la formation

Une compréhension fondamentale des tests d'intrusion et une connaissance approfondie de la cybersécurité.

L'audience ciblée

- Professionnels informatiques souhaitant améliorer leurs connaissances et leurs compétences techniques.
- Auditeurs souhaitant comprendre les processus du test d'intrusion.
- Responsables des technologies de l'information et de gestion de risques souhaitant acquérir une compréhension plus détaillée de l'utilisation appropriée et bénéfique des tests d'intrusion.
- Gestionnaires d'incidents et professionnels de la continuité des activités cherchant à utiliser les tests dans le cadre de leurs régimes de test.
- Testeurs d'intrusion.
- Pirates respectant le code déontologique.
- Professionnels de la cybersécurité.

Le programme

Jour 1

Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application.

Jour 2

Connaissances techniques fondamentales et techniques (avec des exercices pratiques dans tous les domaines).

Jour 3

Sous-composants du PRS, sites de reprise et activation du plan de reprise après sinistre.

Jour 4

Analyse des résultats des tests, rapports et suivi.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED Lead Cybersecurity Manager

PECB

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en œuvre et gérer un programme de cybersécurité.
- Expliquer la corrélation entre la norme ISO/ IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents.
- Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes.
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité.

Les prérequis de la formation

Pour bénéficier pleinement de cette formation, les participants doivent avoir une compréhension fondamentale des concepts et de la gestion de la cybersécurité.

L'audience ciblée

- Aux responsables et dirigeants impliqués dans la gestion de la cybersécurité.
- Aux personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité.
- Aux professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité.
- Aux professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes.
- Aux cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité.

Le programme

Jour 1

Introduction à la cybersécurité et initiation à la mise en œuvre d'un programme de cybersécurité.

Jour 2

Rôles et responsabilités en matière de cybersécurité, gestion des risques et mécanismes d'attaque.

Jour 3

Mesures de sécurité, communication, sensibilisation et formation en matière de cybersécurité.

Jour 4

Management des incidents de cybersécurité, surveillance et amélioration continue.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED Lead Ethical Hacker

PECB

5 JOURS

3700 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Maîtrisez les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion.
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes.
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique.

Les prérequis de la formation

La principale condition pour participer à cette formation est d'avoir une connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation. Il est recommandé aux participants d'avoir une connaissance des réseaux informatiques et des concepts de programmation.

L'audience ciblée

- Personnes souhaitant acquérir des connaissances sur les principales techniques utilisées pour réaliser des tests d'intrusion.
- Personnes impliquées dans la sécurité de l'information qui cherchent à maîtriser les techniques de piratage éthique et de tests d'intrusion.
- Personnes responsables des systèmes de la sécurité d'information, telles que les responsables de la sécurité de l'information et les professionnels de la cybersécurité.
- Membres de l'équipe de sécurité de l'information voulant améliorer leurs connaissances de la sécurité de l'information.
- Managers ou conseillers experts souhaitant apprendre à gérer des activités de piratage éthique.
- Experts techniques souhaitant apprendre comment planifier et réaliser un test d'intrusion.

Le programme

Jour 1

Introduction au piratage éthique.

Jour 2

Lancement de la phase de reconnaissance.

Jour 3

Lancement de la phase d'exploitation.

Jour 4

Post-exploitation et rapports.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED Lead Cloud Security Manager

PECB

5 JOURS

2700 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un programme de sécurité du cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes et cadres réglementaires.
- Apprendre à interpréter les lignes directrices des normes ISO/IEC 27017 et ISO/IEC 27018 dans le contexte spécifique d'un organisme.
- Développer les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud.
- Acquérir les connaissances pratiques pour conseiller un organisme dans la gestion d'un programme de sécurité du cloud en suivant les bonnes pratiques.

Les prérequis de la formation

La principale exigence participer à cette formation est d'avoir une compourpréhension fondamentale des normes ISO/IEC 27017 et ISO/ IEC 27018 et une connaissance générale des concepts du cloud computing.

L'audience ciblée

- Professionnels de la sécurité du cloud et de la sécurité de l'information cherchant à gérer un programme de sécurité du cloud.
- Managers ou consultants cherchant à maîtriser les bonnes pratiques de sécurité du cloud.
- Personnes chargées de maintenir et de gérer un programme de sécurité du cloud.
- Experts techniques cherchant à améliorer leurs connaissances en matière de Conseillers experts en sécurité du cloud.

Le programme

Jour 1

Introduction aux normes ISO/IEC 27017 et ISO/ IEC 27018 et à l'initiation d'un programme de sécurité du cloud.

Jour 2

Gestion des risques de sécurité du cloud com-puting et mesures spécifiques au cloud.

Jour 3

Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud.

Jour 4

Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED Lead SCADA Security Manager

PECB

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre et expliquer l'objectif et les risques des systèmes SCADA, des systèmes de contrôle distribués et des automates programmables logiques programmables.
- Comprendre les risques auxquels sont confrontés ces environnements et les approches appropriées pour gérer ces risques.
- Développer l'expertise nécessaire pour soutenir un programme de sécurité SCADA proactif, y compris les politiques et la gestion des vulnérabilités.
- Définir et concevoir une architecture de réseau intégrant des contrôles de sécurité avancés pour SCADA.
- Expliquer la relation entre les contrôles de gestion, opérationnels et techniques dans un programme de sécurité SCADA.
- Améliorer la capacité à concevoir des systèmes SCADA résilients et à haute disponibilité.
- Apprendre à gérer un programme d'activités de tests de sécurité efficaces.

Les prérequis de la formation

Une compréhension fondamentale de la sécurité SCADA.

L'audience ciblée

- Les professionnels de la sécurité souhaitant acquérir des compétences professionnelles en matière de sécurité SCADA.
- Les professionnels de l'informatique qui souhaitent améliorer leurs compétences et leurs connaissances techniques.
- Les responsables des technologies de l'information et de la gestion des risques qui cherchent à mieux comprendre les systèmes ICS et SCADA.
- Les développeurs de systèmes SCADA.
- Ingénieurs et opérateurs SCADA.
- Les professionnels de l'informatique SCADA.

Le programme

Jour 1

Introduction à SCADA et ICS.

Jour 2

Conception d'un programme de sécurité et d'une architecture de sécurité du réseau.

Jour 3

Mise en œuvre des contrôles de sécurité ICS, de la gestion des incidents et de la continuité des activités.

Jour 4

Tests de sécurité des systèmes SCADA.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

SUR DEMANDE

SUR DEMANDE

FORMATION CERTIFIANTE

DÉBUT DE CARRIÈRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

CompTIA PenTest+ PTO-001

CompTIA

Les Objectifs

- CompTIA certifications align with the skillsets needed to support and manage cybersecurity.

Successful candidates will also have the intermediate skills and best practices required to customise assessment frameworks to effectively collaborate on and report findings and communicate recommended strategies to improve the overall state of IT security.

"PenTest+ demonstrates knowledge beyond entry-level and that the individual is competent to add value within a pentester team immediately; this person can hit the ground running."

Gavin Dennis
Senior IT Security Consultant

Les prérequis de la formation

- Network+, Security+ or equivalent knowledge.
- Minimum of 3-4 years of hands-on information security or related experience.
- While there is no required prerequisite, PenTest+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

L'audience ciblée

- Penetration/Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations

Le programme

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

CompTIA PenTest+ meets the ISO 17024 standard. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Over 1.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

- Exam Lenght : 1 exam, 90 questions, 165 minutes
- Performance-based Questions : Yes
- Penetration testing and vulnerability assessment

« CompTIA PenTest+ exam is different because it is not only technical, but also demonstrates that a candidate has the ability to understand and deliver results. A manager could hire a PenTest+ certified individual and fully trust that he or she would alleviate day to day operations."

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CompTIA PenTest+

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CompTIA PenTest+ PTO-002

5 JOURS

3950 € HT

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

CompTIA certifications align with the skillsets needed to support and manage cybersecurity.

Les prérequis de la formation

- Network+
- Security+ or equivalent knowledge.
- Minimum of 3-4 years of hands-on experience working in a security consultant or penetration tester job role.

L'audience ciblée

- Penetration Tester
- Security Consultant
- Cloud Penetration Tester
- Web App Penetration Tester
- Cloud Security Specialist
- Network & Security Specialist
- Information Security Engineer
- Security Analyst

Le programme

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to:

- Plan and scope a penetration testing engagement.
- Understand legal and compliance requirements.
- Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results.
- Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations.
- Exam Lenght : 1 exam, 90 questions, 165 minutes
- Performance-based Questions
- Penetration testing and vulnerability assessment

CompTIA PenTest+ exam is different because it is not only technical, but also demonstrates that a candidate has the ability to understand and deliver results. A manager could hire a PenTest+ certified individual and fully trust that he or she would alleviate day to day operations."

Josh Skorich
Managing Principal

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

SUR DEMANDE

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

CompTIA CASP+

Les Objectifs

Information security threats are on the rise globally. Organizations are increasingly concerned over the lack of adequately trained senior IT security staff's ability to effectively lead and manage the overall cybersecurity resiliency against the next attack. Updates to CASP+ qualify advanced skills required of security architects and senior security engineers to effectively design, implement, and manage cybersecurity solutions on complex enterprise networks.

- Security Architecture – Expanded coverage to analyze security requirements in hybrid networks to work toward an enterprise-wide, zero trust security architecture with advanced secure cloud and virtualization solutions.
- Security Operations – Expanded emphasis on newer techniques addressing advanced threat management, vulnerability management, risk mitigation, incident response tactics, and digital forensics analysis.
- Security Engineering and Cryptography – Expanded to focus on advanced cybersecurity configurations for endpoint security controls, enterprise mobility, cloud/hybrid environments, and enterprise-wide PKI and cryptographic solutions.
- Governance, Risk, and Compliance – Expanded to support advanced techniques to prove an organization's overall cybersecurity resiliency metric and compliance to regulations, such as CMMC, PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Les prérequis de la formation

- Recommend 10 years of IT administration,
- Including 5 years hands-on, technical security experience.

L'audience ciblée

- Security Architect
- Senior Security Engineer
- SOC Manager
- Security Analyst
- IT Cybersecurity Specialist/INFOSEC Specialist
- Cyber Risk Analyst

Le programme

CASP+ is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. Successful candidates will have the knowledge required to :

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise
- Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment
- Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques
- Consider the impact of governance, risk, and compliance requirements throughout the enterprise.

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CompTIA CySA+

5 JOURS

4400 € HT

FORMATION CERTIFIANTE

NIVEAU INTERMÉDIARE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

Proactively Monitor and Detect. Demonstrate your skills in detecting and analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management (SIEM), endpoint detection and response (EDR) and extended detection and response (XDR).

- Respond to Threats, Attacks and Vulnerabilities. Prove your knowledge of incident response and vulnerability management processes and highlight the communication skills critical to security analysis and compliance.
- Demonstrate Competency of Current Trends. Valuable team members can show knowledge of current trends that affect the daily work of security analysts, such as cloud and hybrid environments.

Les prérequis de la formation

The great majority of candidates with IT certifications are more confident in their abilities (92%). Furthermore, most have more confidence to explore new job opportunities (81%).

- PearsonVUE

2023 Value of IT Certification Candidate Report; 2021 Value of IT Certification Employer Report.

Nearly all IT managers (97%) recognize the value certified professionals bring to the organization such as boosting productivity, helping to meet client requirements and closing organizational gaps.

- Skillsoft IT Skills & Salary Report 2022.

L'audience ciblée

- Security Analyst
- Security Operations Center (SOC) Analyst
- Incident Response Analyst
- Vulnerability Management Analyst
- Security Engineer

Le programme

CySA+ is a global, vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork.

The CompTIA CySA+ CS0-003 certification exam ensures the candidate has the knowledge and skills required to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence conceptsUse appropriate tools and prioritize and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities.

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MILE2 CERTIFIED Penetration Testing Engineer

5 JOURS

3499 € HT

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

Upon completion, the Certified Penetration Testing Engineer, C)PTE, candidate will have solid knowledge of testing and reporting procedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTE exam.

Les prérequis de la formation

- Mile2 C)PEH or equivalent knowledge
- 12 months of Networking Experience
- Sound Knowledge of TCP/IP
- Basic Knowledge of Linux
- Microsoft Security experience

L'audience ciblée

- Pen Testers
- Security Officers
- Ethical Hackers
- Network Auditors
- Vulnerability assessors
- System Owners and Managers
- Cyber Security Engineers

Le programme

Module 1

Business & Technical Logistics of Pen Testing

Module 02

Information Gathering

Module 03

Detecting Live Systems

Module 04

Banner Grabbing and Enumeration

Module 05

Automated Vulnerability Assessment

Module 06

Hacking an OS

Module 07

Advanced Assessment and Exploitation Techniques

Module 08

Evasion Techniques

Module 09

Hacking with PowerShell

Module 10

Networks and Sniffing

Module 11

Hacking Web Tech

Module 12

Mobile and IoT Hacking

Module 13

Report Writing Basics

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CYBERSÉCURITÉ

MILE2 CERTIFIED Penetration Testing Consultant

5 JOURS

3499 € HT

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

Upon completion, the Certified Penetration Testing Consultant, C)PTC, candidate will have solid knowledge of testing and reporting proceedures which will prepare them for upper management roles within a cybersecurity system. They will be able to competently take the C)PTC exam.

Les prérequis de la formation

- Mile2 C)PEH and C)PTE or equivalent knowledge
- 2 years of experience in Networking Technologies
- Sound Knowledge of TCP/IP
- Computer Hardware Knowledge

L'audience ciblée

- IS Security Officers
- Cybersecurity Managers / Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Le programme

Module 1

Penetration Testing 6 Team Formation

Module 2

NMAP Automation

Module 3

Exploitation Process

Module 4

Fuzzing with Spike

Module 5

Simple Buffer - Overflow

Module 6

Stack Based Windows - Buffer Overflow

Module 7

Web Application - Security and Exploitation

Module 8

Linux Stack Smashing & Scanning

Module 9

Linux Address Space - Layout Randomization

Module 10

Windows Exploit - Protection

Module 11

Getting Around SHE - ASLR

Module 12

Penetration Testing - Report Writing

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MILE2 CERTIFIED Cybersecurity Systems Manager

4 JOURS

2999 € HT

FORMATION CERTIFIANTE

LEVEL 350

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

Upon completion, Certified Cybersecurity Systems Manager students will have a strong foundation in Cyber Security & IS management standards with current best practices and will be prepared to competently take the C)CSSM exam.

Les prérequis de la formation

- Mile2's C)SP
- 12 months of Information Systems Experience

L'audience ciblée

- Penetration Testers
- Microsoft Administrators
- Security Administrators
- Active Directory Admins

Le programme

Module 1

Introduction

Module 02

Architectural Frameworks and Compliance

Module 03

Risk Management and Controls

Module 04

Evaluating Systems and Management Strategies

Module 05

Incident Management, Law, and Ethics

Module 06

Business Continuity and Disaster Recovery Processes

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

MILE2 CERTIFIED Cybersecurity Systems Auditor

4 JOURS

2999 € HT

FORMATION CERTIFIANTE

LEVEL 400

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

Upon completion, Certified Cybersecurity Systems Auditor students will be able to establish industry acceptable Cyber Security & IS management standards with current best practices and be prepared to competently take the C)CSSA exam.

Les prérequis de la formation

- Mile2's C)SP
- 12 months of Information Systems Experience

L'audience ciblée

- IS Security Officers
- Privacy Officers
- Health IS Managers
- Risk Mangers
- Info Security managers
- Government employees

Le programme

Module 1

The Process of Auditing Information Systems

Module 02

Risk-Based Auditing

Module 03

Audit Planning and Performance

Module 04

IS Systems Reports

Module 05

IT Governance and Management

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Continuité et Reprise d'Activité PCA et PRA

CONTINUITÉ, RÉSILIENCE ET REPRISE

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 22301 Foundation

PECB

Les Objectifs

- Comprendre les éléments et le fonctionne- ment d'un Système de management de la continuité d'activité et ses principaux processus.
- Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres régle- mentaires.
- Connaître les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management de la continuité d'activité.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Toute personne impliquée dans le management de la continuité d'activité.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus d'un Système de management de la continuité d'activité.
- Personnes souhaitant poursuivre une carrière dans le management de la continuité d'activité.

Le programme

Jour 1

Introduction aux concepts du Système de management de la continuité d'activité, tels que définis par l'ISO 22301.

Jour 2

Exigences relatives au Système de management de la continuité d'activité et examen de certification.

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED ISO 22301 Lead Implementer

PECB

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires.
- Maîtrisez les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMCA.
- Savoir interpréter les exigences de la norme ISO 22301 dans un contexte spécifique de l'organisation.
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMCA.
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la continuité d'activité.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies des principes de sa mise en œuvre.

L'audience ciblée

- Responsables ou consultants impliqués dans le management de la continuité d'activité.
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la continuité d'activité.
- Toute personne responsable du maintien de la conformité aux exigences du SMCA.
- Membres d'une équipe du SMCA.

Le programme

Jour 1

Introduction à la norme ISO 22301 et initialisation d'un SMCA.

Jour 2

Planification de la mise en œuvre d'un SMCA.

Jour 3

Mise en œuvre d'un SMCA.

Jour 4

Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMCA.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CONTINUITÉ, RÉSILIENCE ET REPRISE

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 22301 Lead Auditor

PECB

Les Objectifs

- Comprendre le fonctionnement d'un Système de management de la continuité d'activité (SMCA), conforme à la norme ISO 22301
- Expliquer la corrélation entre la norme ISO 22301 et les autres normes et cadres réglementaires.
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011.
- Savoir diriger un audit et une équipe d'audit.
- Savoir interpréter les exigences d'ISO 22301 dans le contexte d'un audit du SMCA.
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 22301 et des connaissances approfondies sur les principes de l'audit.

L'audience ciblée

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management de la continuité d'activité.
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management de la continuité d'activité.
- Toute personne responsable du maintien de la conformité aux exigences du SMCA.
- Experts techniques désirant préparer un audit du Système de management de la continuité d'activité.
- Conseillers spécialisés en management de la continuité d'activité.

Le programme

Jour 1

Introduction au Système de management de la continuité d'activité et à la norme ISO 22301.

Jour 2

Principes, préparation et déclenchement de l'audit.

Jour 3

Activités d'audit sur site.

Jour 4

Clôture de l'audit.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

3 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED Disaster Recovery Manager

PECB

Les Objectifs

- Connaître la corrélation entre la reprise d'activité après et d'autres normes, cadres réglementaires et domaines des TI.
- Comprendre les concepts, les approches, les méthodes et les techniques utilisées pour la mise en œuvre et la gestion efficace d'un plan de reprise d'activité après sinistre.
- Savoir interpréter les stratégies de reprise d'activité après sinistre des TIC dans le contexte spécifique d'une organisation.
- Développer l'expertise pour soutenir une organisation afin de planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement les services de reprise après sinistre en conformité avec les meilleures pratiques.

Les prérequis de la formation

Une compréhension fondamentale des services de reprise d'activité après sinistre et une connaissance approfondie des principes de gestion.

L'audience ciblée

- Professionnels de reprise d'activité après sinistre souhaitant acquérir une connaissance approfondie des meilleures pratiques en matière de reprise d'activité après sinistre.
- Personnes responsables de la mise en œuvre et la gestion continue d'un plan de reprise d'activité après sinistre dans une organisation.
- Membres de l'équipe chargée de la reprise d'activité après sinistre.

Le programme

Jour 1

Introduction à la reprise d'activité après sinistre et lancement d'un plan de reprise d'activité après sinistre.

Jour 2

Stratégies d'atténuation des risques et planification de la reprise d'activité après sinistre

Jour 3

Services sous-traités de reprise d'activité après sinistre, réponse et activation, formation et test.

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED Lead Disaster Recovery Manager

PECB

Les Objectifs

- Expliquer les concepts fondamentaux de la reprise après sinistre et de ses différents aspects.
- Lancer le projet de planification de la reprise après sinistre selon les meilleures pratiques.
- Effectuer une évaluation des risques et une analyse d'impact sur l'activité et concevoir des stratégies d'atténuation.
- Élaborer un plan de reprise après sinistre et analyser le plan de réponse aux incidents, le plan d'urgence et le plan de gestion de crise.
- Effectuer des tests de reprise après sinistre et prendre des mesures de performance nécessaires.

Les prérequis de la formation

La principale condition pour participer à cette formation est d'avoir une connaissance générale des concepts et stratégies de reprise après sinistre.

L'audience ciblée

- Professionnels ou consultants souhaitant apprendre à mettre en œuvre des projets de planification de la reprise après sinistre, à réaliser des évaluations des risques et des AIA, ainsi qu'à effectuer des tests de reprise après sinistre et à prendre des mesures de performance nécessaires.
- Responsables de l'établissement d'un plan de reprise après sinistre dans une organisation.
- Personnes chargées de maintenir l'infrastructure informatique d'une organisation.
- Membres d'une équipe de reprise après sinistre.

Le programme

Jour 1

Introduction à la planification de la reprise après sinistre et à l'évaluation des risques.

Jour 2

Analyse d'impact sur l'activité et élaboration du plan de reprise après sinistre (PRS).

Jour 3

Sous-composants du PRS, sites de reprise et activation du plan de reprise après sinistre.

Jour 4

Test de reprise après sinistre, mesure des performances et amélioration continue.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED DORA Lead Manager

PECB

5 JOURS

3900 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre le paysage règlementaire et les exigences en matière de conformité du règlement DORA, se basant sur cinq piliers fondamentaux, parmi lesquels la gestion des risques liés aux TIC, la gestion et la notification des incidents liés aux TIC, les tests de résilience opérationnelle numérique et la gestion des risques liés aux prestataires tiers.
- Mettre en œuvre des stratégies et mesures pour améliorer la résilience opérationnelle et atténuer les risques liés aux TIC dans les institutions financières, en se conformant aux exigences de DORA et aux meilleures pratiques du secteur.
- Identifier, analyser, évaluer et gérer les risques liés aux TIC qui concernent les entités financières .
- Développer et maintenir des cadres robustes de gestion des risques liés aux TIC, des plans de réponse en cas d'incident et des plans de continuité opérationnelle et de reprise après sinistre.
- Favoriser la collaboration et la communication avec les principales parties prenantes pour réussir la mise en œuvre et le respect permanent de DORA.
- Utiliser des outils et des méthodologies du secteur pour suivre, évaluer et gérer les risques et les vulnérabilités liés aux TIC, améliorant la posture de sécurité globale des institutions financières.

Les prérequis de la formation

La principale exigence pour participer à cette formation est d'avoir une compréhension fondamentale des concepts de la sécurité de l'information et de la cybersécurité et de se familiariser avec les principes de gestion des risques liés aux TIC.

L'audience ciblée

- Cadres supérieurs et décideurs des institutions financières
- Responsables de la conformité et gestionnaires de risques
- Professionnels des TI
- Personnel des affaires juridiques et réglementaires
- Consultants et conseillers spécialisés dans la règlementation financière et la cybersécurité

Le programme

Jour 1
Introduction des concepts et exigences de DORA

Jour 2
Gestion des risques et incidents liés aux TIC

Jour 3
Gestion des risques liés aux prestataires tiers et partage des informations

Jour 4
Réévaluation et amélioration continuelle

Jour 5
Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CONTINUITÉ, RÉSILIENCE ET REPRISE

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED Lead Crisis Manager

PECB

Les Objectifs

- Personnes responsables de la mise en place d'une capacité de gestion des crises au sein d'une organisation
- Personnes responsables de la mise en œuvre d'un plan et d'une structure de gestion des crises au sein de l'organisation
- Le(s) responsable(s) de crise

Les membres des équipes de gestion de crise

- Personnes cherchant à comprendre en profondeur la gestion de crise
- Les personnes souhaitant démarrer ou faire progresser leur carrière dans le domaine de la gestion de crise
- Consultants, conseillers et professionnels souhaitant acquérir une connaissance approfondie des lignes directrices de l'ISO 22361 sur la gestion de crise

Les prérequis de la formation

Les participants qui souhaitent suivre cette formation doivent avoir une compréhension fondamentale des concepts, du cadre et du processus de gestion de crise.

L'audience ciblée

- Expliquer les concepts fondamentaux et les principes de la gestion des crises sur la base de la norme ISO 22361
- Établir, maintenir et améliorer en permanence un cadre de gestion des crises comprenant le leadership, la structure, la culture et les compétences.
- Anticiper, évaluer, prévenir et préparer les crises
- Réagir aux crises, s'en remettre et en tirer des enseignements afin d'améliorer la capacité de gestion des crises de l'organisation.

Le programme

Jour 1

Introduction à l'ISO 22361 et à la gestion de crise

Jour 2

Framework de gestion de crises

Jour 3

Prévention et préparation aux crises

Jour 4

Réponse aux crises et rétablissement

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CONTINUITÉ, RÉSILIENCE ET REPRISE

5 JOURS

3499 € HT

FORMATION CERTIFIANTE

LEVEL 200

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

MILE2 CERTIFIED Security Principles

Les Objectifs

Upon completion, the Certified Security Principles candidate will not only be able to competently take the C)SP exam but will also understand the principle security knowledge to keep companies' IP and IT infrastructure safe.

Les prérequis de la formation

- 12 Months of experience with server administration
- Mile2 C)SA1, C)SA2, C)HT,C)OST and C)NP
- Equivalent Knowledge

L'audience ciblée

- IT Professionals
- Server Administrators
- Virtualization and Cloud Administrators

Le programme

Module 1

Intro to IT Security

Module 2

Risk Management

Module 3

Understanding of Cryptography

Module 4

Understanding Identity and Access Management

Module 5

Managing Data Security

Module 6

Managing Network Security

Module 7

Managing Server/Host Security

Module 8

Application Security for Non Developers

Module 9

Understanding Mobile Device Security

Module 10

Managing Day to Day Security

Module 11

Understanding Compliance and Auditing

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Gouvernance, risque et conformité

GOUVERNANCE, RISQUE ET CONFORMITÉ

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 37001 Foundation

PECB

Les Objectifs

- Décrire les concepts, principes et définitions du management anticorruption.
- Expliquer les principales exigences d'ISO 37001 pour un système de management anticorruption.
- Identifier les actions et approches potentielles que les organisations peuvent utiliser pour atteindre la conformité à ISO 37001.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques.
- Personnel participant aux activités d'appréciation des risques selon la méthode EBIOS.
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS.
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode EBIOS.

Le programme

Jour 1

Introduction au système de management anti-corruption (SMAC) et aux articles 4-6 d'ISO 37001.

Jour 2

Articles 7-10 d'ISO 37001 et examen du certificat

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

GOUVERNANCE, RISQUE ET CONFORMITÉ

2 JOURS

1333 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 38500 Foundation

PECB

Les Objectifs

- Comprendre les éléments fondamentaux de la gouvernance des technologies de l'information pour l'entreprise.
- Comprendre les principes de bonne gouvernance des TI.
- Connaître les approches, les méthodes et les techniques permettant de gouverner efficacement l'utilisation des TI.

Le programme

Jour 1

Introduction aux pratiques de gouvernance des TI selon la norme ISO/IEC 38500.

Jour 2

Principes de la gouvernance des TI et examen de certification.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Toute personne impliquée dans la gouvernance des technologies de l'information pour l'entreprise.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus de la gouvernance des technologies de l'information.
- Personnes souhaitant poursuivre une carrière dans la gouvernance des technologies de l'information pour l'entreprise.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED ISO/IEC 38500 IT Governance Manager

3 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre les principes fondamentaux de l'ISO/IEC 38500 et apprendre à les interpréter.
- Connaître le modèle ISO/IEC 38500 Évaluer – Diriger - Surveiller.
- Acquérir les connaissances nécessaires pour évaluer, diriger et surveiller l'utilisation des technologies de l'information dans une organisation.
- Comprendre COBIT 5 et CGEIT

Les prérequis de la formation

Suivre la formation ISO/IEC 38500 IT Corporate Governance Manager ne nécessite aucun prérequis.

L'audience ciblée

- Toute personne impliquée dans la gouvernance des technologies de l'information pour l'entreprise.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus de la gouvernance des technologies de l'information.
- Personnes souhaitant poursuivre une carrière dans la gouvernance des technologies de l'information pour l'entreprise.

Le programme

Jour 1

Introduction aux pratiques de gouvernance des TI selon la norme ISO/IEC 38500.

Jour 2

Principes de la gouvernance des TI et examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

GOUVERNANCE, RISQUE ET CONFORMITÉ

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 38500 Lead IT Governance Manager

PECB

Les Objectifs

- Maîtriser les principes fondamentaux de l'ISO/IEC 38500, leurs avantages ainsi que leur application dans une organisation.
- Comprendre le modèle ISO/IEC 38500 Évaluer - Diriger - Surveiller et apprendre à l'intégrer au sein d'une organisation.
- Comprendre COBIT 5 et CGEIT et comment ils complètent l'ISO/IEC 38500.
- Savoir appliquer, gérer et surveiller efficacement la gouvernance des TI au sein de l'organisation
- Acquérir l'expertise pour conseiller une organisation sur les meilleures pratiques de la Gouvernance TI en conformité avec l'ISO/IEC 38500, COBIT 5 et CGEIT afin d'assurer une bonne gouvernance des technologies de l'information

Les prérequis de la formation

Une compréhension fondamentale de l'ISO/IEC 38500 et une connaissance approfondie de la gouvernance des TI.

L'audience ciblée

- Gestionnaires ou consultants chargés d'assurer une bonne gouvernance des TI au sein d'une organisation et une gestion efficace de ses risques
- Conseillers spécialisés souhaitant acquérir une connaissance approfondie des principaux concepts et principes de la gouvernance des TI.
- Experts techniques désirant formaliser, modifier et / ou étendre les objectifs liés à la technologie de l'information d'une organisation
- Membres de groupes de surveillance des ressources au sein d'une organisation.
- Membres de l'équipe de gouvernance des technologies de l'information et / ou de la sécurité de l'information.

Le programme

Jour 1

Introduction à la gouvernance des TI et à la norme ISO/IEC 38500.

Jour 2

Stratégie des technologies de l'information et acquisition

Jour 3

Performance et gestion des risques

Jour 4

Gestion des ressources, conformité et comportement humain

Jour 4

Examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

GOUVERNANCE, RISQUE ET CONFORMITÉ

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED NIS 2 Directive Lead Implementer

PECB

Les Objectifs

- Expliquer les concepts fondamentaux de la transformation numérique et des technologies de transformation numérique, y compris l'intelligence artificielle, l'informatique en nuage, le big data, l'apprentissage automatique, l'Internet des objets (IoT) et la blockchain.
- Adopter les approches et méthodologies utilisées pour la mise en œuvre des stratégies de transformation numérique au sein d'une organisation.
- Soutenir une organisation dans la conception, la mise en œuvre, la surveillance et l'amélioration efficaces d'une stratégie de transformation numérique.
- Surveiller et mesurer les résultats de la stratégie de transformation numérique.
- Expliquer et appliquer les approches et techniques utilisées pour établir une culture numérique et communiquer la stratégie de transformation numérique.

Les prérequis de la formation

Les principales exigences pour participer à cette formation sont d'avoir une compréhension fondamentale de la cybersécurité.

L'audience ciblée

- Professionnel de la cybersécurité souhaitant acquérir une compréhension approfondie des exigences de la directive NIS 2 et apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes, des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes
- Responsables et professionnels de l'informatique souhaitant acquérir des connaissances sur la mise en œuvre de systèmes sécurisés et améliorer la résilience des systèmes critiques.
- Les responsables gouvernementaux et réglementaires chargés de l'application de la directive NIS 2.

Le programme

Jour 1

Introduction à la directive NIS 2 et lancement de la mise en œuvre de la directive NIS 2.

Jour 2

Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques.

Jour 3

Contrôles de cybersécurité, gestion des incidents et gestion de crise.

Jour 4

Communication, tests, contrôle et amélioration continue de la cybersécurité.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

ISACA CERTIFIED in the Governance of Enterprise IT

ISACA

Les Objectifs

- Apprendre à définir, établir et administrer un cadre de gouvernance de l'informatique d'entreprise.
- Apprendre à vous assurer que les investis- sements activés par l'informatique sont administrés pour fournir des avantages commerciaux optimisés.
- Apprendre à soutenir et à permettre la réalisation des objectifs de l'entreprise.

Les prérequis de la formation

Vous devez avoir au moins cinq ans d'expérience dans la gestion, le rôle consultatif ou de supervision, et/ou le soutien de la gouvernance des contributions liées à l'informatique au sein d'une entreprise.

L'audience ciblée

Professionnels ayant 5 ans d'expérience ou plus dans l'établissement et la gestion d'un cadre de gouvernance de l'informatique et de la technologie (I&T), ainsi que dans des rôles consultatifs ou de supervision, et/ou soutenant d'une autre manière la gouvernance des contri- butions liées à l'informatique. Cela inclut :

- SVP, VP, Directeurs.
- Professionnels informatiques soutenant la haute direction : Consultants, Cadres supérieurs, Gestionnaires, Ingénieurs seniors.
- La gouvernance relève en fin de compte de la responsabilité de la haute direction et du conseil d'administration. Par conséquent, une compréhension de haut niveau de la gouvernance de l'I&T est essentielle à ce niveau pour qu'ils puissent habiliter les praticiens de la gou- vernance et parrainer les bonnes initiatives.

Le programme

Domaine 1

Gouvernance de l'informatique d'entreprise.

Domaine 2

Ressources informatiques.

Domaine 3

Réalisation des avantages.

Domaine 4

Optimisation des risques.

Les plus

- Cours animé par un formateur certifié ISACA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CGEIT

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Risk Management

RISK MANAGEMENT

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 31000 Foundation

PECB

Les Objectifs

- Résumer les principaux concepts et principes du management du risque tels qu'ils sont définis dans la norme ISO 31000.
- Expliquer les lignes directrices d'ISO 31000 pour l'établissement du cadre de management du risque.
- Décrire l'application du processus de management du risque conformément aux lignes directrices d'ISO 31000.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Professionnels du management du risque.
- Les personnes souhaitant acquérir des connaissances sur les lignes directrices ISO 31000 relatives aux principes, au cadre et au processus de management du risque.
- Personnes responsables de la création et de la protection de la valeur au sein d'une organisation.
- Personnel chargé du management du risque et des opportunités dans son domaine de responsabilité.
- Les personnes intéressées par une carrière de manager du risque.

Le programme

Jour 1

Introduction à la gestion des risques, aux composantes de la norme ISO 31000 et initiation au processus de gestion des risques.

Jour 2

L'évaluation des risques, le traitement du risque, enregistrement et élaboration de rapports, suivi et revue, communication et consultation selon la norme ISO 31000.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED ISO 31000 Risk Manager

PECB

3 JOURS

2100 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre les concepts et les processus fondamentaux relatifs au management du risque.
- Connaître la corrélation entre la norme ISO 31000 et la norme CEI/ISO 31010, ainsi qu'avec d'autres normes et cadres réglementaires.
- Comprendre les approches, les méthodes et techniques utilisées pour gérer le risque dans un organisme.
- Savoir interpréter les principes et les lignes directrices de la norme ISO 31000.

Les prérequis de la formation

Des connaissances fondamentales de la norme ISO 31000 et des connaissances approfondies sur le management du risque.

L'audience ciblée

- Professionnels du management du risque.
- Les personnes souhaitant acquérir des connaissances sur les lignes directrices ISO 31000 relatives aux principes, au cadre et au processus de management du risque.
- Personnes responsables de la création et de la protection de la valeur au sein d'une organisation.
- Personnel chargé du management du risque et des opportunités dans son domaine de responsabilité.
- Les personnes intéressées par une carrière de manager du risque.

Le programme

Jour 1

Introduction aux principes et au cadre organisationnel de l'ISO 31000.

Jour 2

Processus de management du risque conforme à la norme ISO 31000.

Jour 3

Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010 et examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

5 JOURS

3800 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 31000 Lead Risk Manager

PECB

Les Objectifs

- Démontrer leur compréhension des principes de management du risque, tels que formulés dans ISO 31000.
- Établir, maintenir et améliorer continuellement un cadre de management du risque, conformément aux lignes directrices d'ISO 31000.
- Appliquer le processus de management du risque, conformément aux lignes directrices d'ISO 31000.
- Planifier les processus d'enregistrement et d'élaboration des rapports sur les risques, ainsi que les activités de communication sur les risques.
- Surveiller, passer en revue et améliorer le cadre et le processus de management du risque en fonction des résultats des activités de management du risque.

Les prérequis de la formation

Avoir une bonne compréhension de la norme ISO 31000:2018 et de disposer de compétences avancées dans la gestion du risque.

L'audience ciblée

- Responsables ou consultants désirant maîtriser les compétences pour accompagner un organisme pendant la mise en œuvre d'un cadre organisationnel et d'un processus de management du risque conforme à la norme ISO 31000.
- Professionnels responsables de la création et de la préservation de la valeur dans les organismes grâce au management efficace des risques.
- Conseillers spécialisés désirant acquérir des connaissances approfondies liées aux principaux concepts, processus et stratégies de management du risque.
- Membres d'une équipe chargée du management du risque.

Le programme

Jour 1

Introduction à la norme ISO 31000 et aux processus de management du risque.

Jour 2

Établissement du contexte, appréciation et traitement du risque selon la norme ISO 31000.

Jour 3

Acceptation, communication et concertation, enregistrement et rapports, surveillance et revue du risque selon la norme ISO 31000.

Jour 4

Techniques d'appréciation du risque conformes à la norme CEI/ISO 31010.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

3 JOURS

2150 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED EBIOS Risk Manager

PECB

Les Objectifs

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS.
- Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail.
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés.
- Acquérir les compétences nécessaires afin de mener une étude EBIOS.
- Acquérir les compétences nécessaires pour gérer les risques de sécurité des systèmes d'information appartenant à un organisme.
- Développer les compétences nécessaires pour analyser et communiquer les résultats d'une étude EBIOS.

Les prérequis de la formation

Une connaissance en gestion du risque est recommandée.

L'audience ciblée

- Personnes souhaitant apprendre les concepts fondamentaux du management des risques.
- Personnel participant aux activités d'appréciation des risques selon la méthode EBIOS.
- Responsables désirant comprendre les techniques d'appréciation des risques basées sur la méthode EBIOS.
- Responsables souhaitant maîtriser les techniques d'analyse et de communication des résultats d'appréciation des risques selon la méthode EBIOS.
-

Le programme

Jour 1

Introduction à la méthode d'appréciation des risques EBIOS.

Jour 2

Introduction à la méthode d'appréciation des risques EBIOS.

Jour 3

Introduction à la méthode d'appréciation des risques EBIOS et examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 27005 Foundation

PECB

Les Objectifs

- 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 de l'information.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- 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

Le programme

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

Jour 2
Gestion des risques liés à la sécurité de l'information et examen

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

3 JOURS

2150 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27005 Risk Manager

PECB

Les Objectifs

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité.
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005.
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information.
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information.

Les prérequis de la formation

La formation Les fondamentaux du management du risque constitue le prérequis idéal pour suivre ce cours.

L'audience ciblée

- 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/CEI 27001, désirant se conformer à la norme ISO/ CEI 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 personnelles.

Le programme

Jour 1

Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005.

Jour 2

Mise en œuvre d'un processus de gestion des risques conforme à la norme ISO/CEI 27005.

Jour 3

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

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

5 JOURS

2950 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/CEI 27005 Lead Risk Manager

PECB

Les Objectifs

- Expliquer les concepts et principes de gestion des risques définis par les normes ISO/IEC 27005 et ISO 31000.
- Mettre en place, maintenir et améliorer un cadre de gestion des risques liés à la sécurité de l'information conformément aux lignes directrices de la norme/IEC 27005.
- Appliquer les processus de gestion des risques liés à la sécurité de l'information conformément aux lignes directrices de la norme/IEC 27005.
- Planifier et mettre en place des activités de communication et de consultation sur les risques
- Surveiller, réviser et améliorer le cadre et le processus de gestion des risques liés à la sécurité de l'information en fonction des résultats des activités de gestion de ces risques

Les prérequis de la formation

La participation à cette formation requiert une compréhension fondamentale de la norme/IEC 27005 et des connaissances approfondies de la gestion des risques et de la sécurité de l'information.

L'audience ciblée

- Responsables ou consultants impliqués ou responsables de la sécurité de l'information dans une organisation.
- Personnes responsables de la gestion des risques liés à la sécurité de l'information.
- Membres des équipes de sécurité de l'information, professionnels de l'informatique et responsables de la protection de la vie privée.
- Personnes responsables du maintien de la conformité aux exigences de sécurité de l'information de la norme/IEC 27001 au sein d'une organisation.
- Gestionnaire de projet, consultants ou conseillers experts cherchant à maîtriser la gestion des risques liés à la sécurité de l'information.

Le programme

Jour 1
Introduction à la norme ISO/IEC 27005 et à la gestion des risques

Jour 2
Identification, évaluation et traitement des risques conformément à la norme ISO/IEC 27005

Jour 3
Acceptation, communication, consultation, surveillance et révision des risques liés à la sécurité de l'information

Jour 4
Méthodes d'évaluation des risques

Jour 5
Examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

RISK MANAGEMENT

3 JOURS

2750 € HT

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

ISACA CERTIFIED in Risk and Information System Control

ISACA

Les Objectifs

La désignation CRISC ne certifiera pas seulement les professionnels possédant des connaissances et une expérience dans l'identification et l'évaluation des risques spécifiques à une entité, mais elle les aidera également à assister les entreprises dans l'accomplissement de leurs objectifs commerciaux en concevant, mettant en œuvre, surveillant et maintenant des contrôles de sécurité de l'information efficaces et efficients, basés sur les risques.

Les prérequis de la formation

Pour obtenir la certification CRISC, un minimum de trois ans d'expérience professionnelle cumu- lative est requis, au cours desquelles vous avez effectué les tâches d'un professionnel CRISC dans au moins deux des quatre domaines CRISC. Parmi ces deux domaines requis, l'un doit être soit le Domaine 1, soit le Domaine 2.

L'audience ciblée

Professionnels ayant 5 ans d'expérience ou plus Professionnels de la gestion des risques informatiques ayant au moins 3 ans d'expérience professionnelle pertinente en matière de risques informatiques et de contrôle des systèmes d'information, y compris :

- Responsables informatiques.
- Analystes de risques informatiques.
- Consultants en informatique.
- Responsables consultatifs en risques /sécurité informatique.
- Responsables de la conformité informatique.
- Spécialistes de l'évaluation des risques informatiques.

Le programme

Domaine 1

Gouvernance.

Domaine 2

Évaluation des risques.

Domaine 3

Réponse et Rapport sur les Risques.

Domaine 4

Technologies de l'information et Sécurité.

Les plus

- Cours animé par un formateur certifié ISACA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CRISC

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Protection de la vie privée et des données

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

5 JOURS

3700 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 27701 Lead Implementer

PECB

Les Objectifs

- Maîtrisez les concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un PIMS.
- En savoir plus sur la corrélation entre ISO/ IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et d'autres normes et cadres réglementaires.
- Comprendre le fonctionnement d'un PIMS selon ISO/IEC 27701 et ses principaux proces- sus.
- Apprendre à interpréter les exigences d'ISO/ IEC 27701 dans le contexte spécifique d'une organisation.
- Développer l'expertise nécessaire pour aider une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et le maintien efficaces d'un PIMS.

Les prérequis de la formation

Une compréhension fondamentale en matière de management de la protection de la vie privée et une connaissance approfondie des principes de mise en œuvre du PIMS.

L'audience ciblée

- Directeurs et consultants impliqués dans la confidentialité et la gestion des données.
- Experts-conseils cherchant à maîtriser la mise en œuvre d'un système de management de la protection de la vie privée.
- Responsables des informations personnellement identifiables (IPI) au sein des organisa- tions.
- Responsables de la conformité aux exigences des lois sur la protection des données.
- Membres de l'équipe PIMS.

Le programme

Jour 1

Introduction à l'ISO/IEC 27701 et initiation au PIMS.

Jour 2

Planification de la mise en œuvre d'un PIMS.

Jour 3

Mise en œuvre d'un PIMS.

Jour 4

Surveillance du PIMS, amélioration continue et préparation d'un audit de certification.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures
- Formation éligible au CPF

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

5 JOURS

2950 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO/IEC 27701 Lead Auditor

PECB

Les Objectifs

- Comprendre un système de management de la protection de la vie privée (PIMS) et ses processus basés sur ISO/IEC 27701.
- Identifier la relation entre ISO/IEC 27701, ISO/ IEC 27001, ISO/IEC 27002 et les autres normes et cadres réglementaires.
- Comprendre le rôle de l'auditeur dans la planification, la direction et le suivi d'un audit de système de management selon ISO 19011.
- Apprendre à interpréter les exigences de la norme ISO/IEC 27701 dans le contexte d'un audit du PIMS.

Les prérequis de la formation

Une compréhension fondamentale de la sécurité de l'information et de la protection de la vie privée, ainsi qu'une connaissance approfondie des principes d'audit.

L'audience ciblée

- Auditeurs cherchant à réaliser et à diriger des audits de certification du système de management de la protection de la vie privée (PIMS).
- Gestionnaires ou consultants souhaitant maîtriser un processus d'audit du PIMS.
- Personnes responsables du maintien de la conformité aux exigences du PIMS.
- Experts techniques souhaitant se préparer à un audit du PIMS.
- Experts-conseils en matière de protection des informations d'identification personnelle (IIP).
- Délégués à la protection des données (DPO).

Le programme

Jour 1

Introduction au système de management de la protection de la vie privée (PIMS) et à la norme ISO/IEC 27701.

Jour 2

Principes d'audit, préparation et ouverture d'un audit.

Jour 3

Activités d'audit sur site.

Jour 4

Clôture de l'audit.

Jour 5

Examen de certificataion

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

5 JOURS

3900 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB GDPR CERTIFIED Data Protection Officer

PECB

Les Objectifs

- Acquérir une compréhension approfondie des concepts fondamentaux et des éléments du Règlement sur la protection des données.
- Comprendre l'objectif, le contenu et la corrélation entre le Règlement général sur la protection des données et les autres cadres réglementaires.
- Acquérir une compréhension approfondie des concepts, des approches, des méthodes et des techniques permettant une protection efficace des données à caractère personnel.
- Savoir interpréter les exigences relatives à la protection des données dans le contexte particulier d'un organisme.
- Acquérir l'expertise nécessaire pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir un cadre de conformité en ce qui concerne le RGPD.

Les prérequis de la formation

Les participants à cette formation doivent avoir une compréhension fondamentale du RGPD et une connaissance approfondie des exigences en matière de protection des données.

L'audience ciblée

- À des responsables de projets et consultants qui désirent préparer et aider un organisme à mettre en œuvre les nouvelles procédures et à adopter les nouvelles exigences présentées dans le RGPD.
- Aux délégués à la protection des données et membres de la direction générale responsables de la protection des données à caractère personnel d'une entreprise et de la gestion de ses risques.
- Aux membres d'équipes de sécurité de l'information, de gestion des incidents et de continuité des activités.
- Aux conseillers spécialisés en sécurité des données à caractère personnel.
- Aux spécialistes des questions techniques et de conformité qui désirent se préparer à occuper un poste de délégué à la protection des données.
- Délégués à la protection des données (DPO).

Le programme

Jour 1

Introduction au RGPD et mise en œuvre de la conformité au RGPD.

Jour 2

Planification de la mise œuvre du RGPD.

Jour 3

Déploiement du RGPD.

Jour 4

Surveillance et amélioration continue de la conformité au RGPD.

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PROTECTION DE LA VIE PRIVÉE ET DES DONNÉES

4 JOURS

SUR DEMANDE

FORMATION CERTIFIANTE

NIVEAU AVANCÉ

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

ISACA CERTIFIED Data Privacy Solutions Engineer

ISACA

Les Objectifs

Dans ce cours d'ingénieur en solutions de protection des données personnelles, les participants apprendront comment créer des solutions protégeant la vie privée et seront responsables des stratégies de protection des renseignements personnels de leur entreprise pour soutenir sa croissance sans entrave.

Les participants acquerront l'ensemble des compétences techniques requises de conceptions avancées en matière de protection de la vie privée afin de développer une compréhension commune des meilleures pratiques dans toute votre organisation. Les participants apprendront également à mettre en œuvre l'évaluation de l'impact sur la vie privée (PIA), les stratégies contre les menaces, les attaques et les vulnérabilités liées à la confidentialité - y compris le cryptage, le hachage et la désidentification, l'inventaire des données et la classification (par exemple, marquage, suivi, SOR).

Les prérequis de la formation

Vous devez avoir un minimum de 3 années d'expérience cumulée à accomplir les tâches d'un professionnel CDPSE. L'expérience professionnelle pour la certification CDPSE doit être acquise dans les 10 années précédant la date de demande de certification. Les candi- dats ont 5 ans à compter de la date de réussite pour faire leur demande.

L'audience ciblée

Professionnels de l'informatique qui mettent en œuvre la première ligne de défense contre les violations de données et fournissent des solutions techniques de protection de la vie privée, notamment :

- Ingénieur logiciel principal - Protection des données et des systèmes.
- Architecte de domaine (Conformité aux soins juridiques, confidentialité).
- Ingénieur en sécurité et confidentialité.
- Architecte de solutions de confidentialité.
- Chef de projet informatique.
- Data scientist spécialisé en confidentialité.
- Analyste de confidentialité.
- Responsable de la confidentialité principal.

Le programme

Domaine 1

Gouvernance de la vie privée.

Domaine 2

Architecture de la vie privée.

Domaine 3

Cycle de vie des données.

Les plus

- Cours animé par un formateur certifié ISACA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CDPSE

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Qualité management

QUALITÉ MANAGEMENT

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 9001 Foundation

PECB

Les Objectifs

- Décrire les concepts, principes et définitions du management qualité.
- Expliquer les principales exigences de la norme ISO 9001 relatives à un système de management de la qualité.
- Identifier les éventuelles actions et approches que les organisations peuvent utiliser pour se conformer à la norme ISO 9001.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Responsables et consultants souhaitant acquérir des connaissances sur les concepts fondamentaux du management de la qualité.
- Professionnels souhaitant se familiariser avec les exigences de la norme ISO 9001 relatives à un SMQ.
- Personnel responsable du maintien et de l'amélioration de la qualité des produits et services de son organisation.
- Personnes souhaitant faire carrière dans le management de la qualité.

Le programme

Jour 1

Introduction aux concepts de qualité, au SMQ et aux articles 4 à 6 de la norme ISO 9001

Jour 2

Articles 7 à 10 de la norme ISO 9001 et examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

QUALITÉ MANAGEMENT

5 JOURS

2950 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 9001 Lead Implementer

PECB

Les Objectifs

- Comprendre la corrélation entre la norme ISO 9001 et les autres normes et cadres réglementaires.
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMQ .
- Savoir interpréter les exigences de la norme ISO 9001 dans un contexte spécifique de l'organisation
- Savoir accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMQ .
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au Système de management de la qualité.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre.

L'audience ciblée

- Responsables ou consultants impliqués dans le management de la qualité.
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la qualité.
- Toute personne responsable du maintien de la conformité aux exigences du SMQ.
- Membres d'une équipe du SMQ.

Le programme

Jour 1

Introduction à la norme ISO 9001 et initialisation d'un SMQ

Jour 2

Planification de la mise en œuvre d'un SMQ

Jour 3

Mise en œuvre d'un SMQ

Jour 4

Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMQ

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

QUALITÉ MANAGEMENT

5 JOURS

2950 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 9001 Lead Auditor

PECB

Les Objectifs

- Comprendre le fonctionnement d'un Système de management environnemental (SME) conforme à la norme ISO 14001.
- Expliquer la corrélation entre la norme ISO 14001 et la norme ISO 14040, ainsi qu'avec d'autres normes et cadres réglementaires.
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011.
- Savoir diriger un audit et une équipe d'audit.
- Savoir interpréter les exigences d'ISO 14001 dans le contexte d'un audit du SME.
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de l'audit.

L'audience ciblée

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management environnemental.
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management environnemental.
- Toute personne responsable du maintien de la conformité aux exigences du SME.
- Experts techniques désirant préparer un audit du Système de management environnemental.
- Conseillers spécialisés en management environnemental.

Le programme

Jour 1

Introduction au Système de management de la qualité et à la norme ISO 9001

Jour 2

Principes, préparation et déclenchement de l'audit

Jour 3

Activités d'audits sur site

Jour 4

Clôture de l'audit

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Durabilité

PECB CERTIFIED ISO 14001 Foundation

PECB

2 JOURS

1400 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre les éléments et le fonctionnement d'un Système de management environnemental et ses principaux processus.
- Connaître la corrélation entre la norme ISO 14001 et les autres normes et cadres règlementaires.
- Comprendre les approches, les méthodes et les techniques permettant de mettre en œuvre et de gérer un Système de management environnemental.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Toute personne impliquée dans le management environnemental.
- Personnes souhaitant acquérir des connaissances relatives aux principaux processus du Système de management environnemental.
- Personnes souhaitant poursuivre une carrière dans le management environnemental.

Le programme

Jour 1

Introduction aux concepts du Système de management environnemental, tels que définis par l'ISO 14001

Jour 2

Exigences relatives au Système de management environnemental et examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

DURABILITÉ

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 14001 Lead Implementer

PECB

Les Objectifs

- Comprendre la corrélation entre la norme ISO 14001 et la norme ISO 14040, ainsi qu'avec d'autres normes et cadres réglementaires.
- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SME
- Savoir interpréter les exigences de la norme ISO 14001 dans un contexte spécifique de l'organisme
- Savoir soutenir un organisme dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SME
- Acquérir l'expertise nécessaire pour conseiller un organisme sur la mise en œuvre des meilleures pratiques relatives au Système de management environnemental.

.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre.

L'audience ciblée

- Responsables ou consultants impliqués dans le management environnemental
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management environnemental
- Toute personne responsable du maintien de la conformité aux exigences du SME
- Membres d'une équipe du SME

Le programme

Jour 1

Introduction à la norme ISO 14001 et initialisation d'un SME

Jour 2

Planification de la mise en œuvre d'un SME

Jour 3

Acceptation, communication, consultation, surveillance et révision des risques liés à la sécurité de l'information

Jour 4

Méthodes d'évaluation des risques

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

DURABILITÉ

5 JOURS

3450 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 14001 Lead Auditor

PECB

Les Objectifs

- Comprendre le fonctionnement d'un Système de management environnemental (SME) conforme à la norme ISO 14001.
- Expliquer la corrélation entre la norme ISO 14001 et la norme ISO 14040, ainsi qu'avec d'autres normes et cadres réglementaires.
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011.
- Savoir diriger un audit et une équipe d'audit
- Savoir interpréter les exigences d'ISO 14001 dans le contexte d'un audit du SME.
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de l'audit.

L'audience ciblée

- Auditeurs souhaitant réaliser et diriger des audits de certification du Système de management environnemental.
- Responsables ou consultants désirant maîtriser le processus d'audit du Système de management environnemental.
- Toute personne responsable du maintien de la conformité aux exigences du SME.
- Experts techniques désirant préparer un audit du Système de management environnemental
- Conseillers spécialisés en management environnemental.

Le programme

Jour 1

Introduction au Système de management environnemental et à la norme ISO 14001

Jour 2

Principes, préparation et déclenchement de l'audit

Jour 3

Activités d'audit sur site

Jour 4

Clôture de l'audit

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Santé et sécurité

PECB CERTIFIED ISO 45001 Foundation

2 JOURS

1500 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Comprendre les concepts, définitions et approches de base en matière de santé et de sécurité au travail.
- Se familiariser avec les exigences de la norme ISO 45001 relatives à un système de management de la santé et de la sécurité au travail.
- Développer une compréhension générale de la façon dont les exigences de la norme ISO 45001 pourraient être appliquées dans un organisme.

Les prérequis de la formation

Aucun prérequis n'est nécessaire pour participer à cette formation.

L'audience ciblée

- Managers/consultants cherchant à se familiariser avec les concepts de base de la santé et de la sécurité au travail.
- Personnes souhaitant créer des lieux de travail plus sûrs et plus sains au sein de leur organisation.
- Personnes souhaitant se familiariser avec les principales exigences de la norme ISO 45001 pour un système de management de la santé et de la sécurité au travail.
- Personnes souhaitant poursuivre une carrière en santé et sécurité au travail.

Le programme

Jour 1

Introduction au management de la santé et de la sécurité au travail, au SMSST et aux articles 4 à 6 d'ISO 45001

Jour 2

Articles 7 à 10 de la norme ISO 45001 et examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED ISO 45001 Lead Implementer

5 JOURS

2250 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de la santé et de la sécurité au travail (SMSST) conformément à la norme ISO 45001.
- Interpréter les exigences de la norme ISO 45001 pour un SMSST du point de vue d'un auditeur.
- Initier et planifier la mise en œuvre d'un SMSST conformément à la norme ISO 45001, en utilisant la méthodologie IMS2 de PECB et d'autres meilleures pratiques.
- Accompagner une organisation dans le fonctionnement, le maintien et l'amélioration continue d'un SMSST conformément à la norme ISO 45001.
- Préparer une organisation à se soumettre à un audit de certification par un tiers.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de sa mise en œuvre.

L'audience ciblée

- Personnes chargées du maintien et de l'amélioration de la sécurité sur le lieu de travail.
- Agents, consultants et conseillers en matière de santé et de sécurité au travail.
- Professionnels souhaitant se familiariser avec la méthodologie IMS2 de PECB pour la mise en œuvre d'un SMSST.
- Personnes chargées de maintenir la conformité du SMSST aux exigences de la norme ISO 45001.
- Membres des équipes de santé et sécurité au travail
- Personnes aspirant faire carrière en tant que responsables de la mise en œuvre d'un SMSST, consultants ou agents.

Le programme

Jour 1

Introduction à la norme ISO 45001 et lancement de la mise en œuvre d'un SMSST

Jour 2

Plan de mise en œuvre d'un SMSST

Jour 3

Mise en œuvre d'un SMSST

Jour 4

Évaluation des performances du SMSST, amélioration continue et préparation à l'audit de certification

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

PECB CERTIFIED ISO 45001 Lead Auditor

5 JOURS

2250 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

Les Objectifs

- Expliquer les concepts et les principes fondamentaux d'un système de management de la santé et de la sécurité au travail (SMSST) conformément à la norme ISO 45001.
- Interpréter les exigences de la norme ISO 45001 pour un SMSST du point de vue d'un auditeur.
- Évaluer la conformité du SMSST aux exigences de la norme ISO 45001, en accord avec les concepts et les principes fondamentaux d'audit.
- Planifier, réaliser et clôturer un audit de conformité à la norme ISO 45001, conformément aux exigences de la norme ISO/ IEC 17021-1, aux lignes directrices de la norme ISO 19011 et aux autres meilleures pratiques d'audit.
- Gérer un programme d'audit conformément à la norme ISO 45001.

Les prérequis de la formation

Une bonne connaissance de la norme ISO 14001 et des connaissances approfondies des principes de l'audit.

L'audience ciblée

- Auditeurs intéressés par la réalisation et la direction d'audits de certification de SMSST.
- Responsables ou consultants désireux d'approfondir leurs connaissances du processus d'audit de SMSST.
- Auditeurs internes et personnes responsables du maintien de la conformité aux exigences de la norme ISO 45001.
- Experts techniques souhaitant se préparer à un audit de SMSST.
- Conseillers experts en management de la santé et de la sécurité au travail.

Le programme

Jour 1

Introduction au SMSST et à la norme ISO 45001

Jour 2

Principes d'audit, préparation et lancement d'un audit

Jour 3

Activités d'audit sur site

Jour 4

Clôture de l'audit

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Transformation Numérique

TRANSFORMATION NUMÉRIQUE

5 JOURS

3350 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED Digital Transformation Officer

PECB

Les Objectifs

- Expliquer les concepts fondamentaux de la transformation numérique et des technologies de transformation numérique, y compris l'intelligence artificielle. l'intelligence artificielle, l'informatique en nuage, le big data, l'apprentissage automatique, l'IdO et la blockchain
- Adopter les approches et les méthodologies utilisées pour la mise en œuvre des stratégies de transformation numérique dans une organisation.
- Soutenir une organisation dans la conception, la mise en œuvre, le suivi et l'amélioration efficaces d'une stratégie de transformation numérique.
- Contrôler et mesurer les résultats de la stratégie de transformation numérique.
- Expliquer et appliquer les approches et les techniques utilisées pour établir une culture numérique et communiquer la stratégie de transformation numérique.

Les prérequis de la formation

Les principales exigences pour participer à cette formation sont d'avoir une compréhension fondamentale des concepts des technologies de l'information et une connaissance générale de la transformation numérique

L'audience ciblée

- Les managers et les dirigeants qui cherchent à prospérer dans l'économie numérique
- Les personnes chargées de transformer les opérations de l'organisation grâce aux technologies numériques
- Les professionnels de l'informatique ou les consultants qui cherchent à améliorer leurs connaissances en matière de conception et de stratégie numériques afin de soutenir les initiatives de transformation numérique de l'organisation les initiatives de transformation numérique de l'organisation
- Les cadres supérieurs des secteurs du numérique, de l'information, du marketing et de l'informatique qui cherchent à comprendre comment les technologies numériques peuvent être utilisées pour transformer les processus des entreprises.

Le programme

Jour 1

Introduction à la transformation numérique

Jour 2

Technologies, approches et méthodologies de la transformation numérique et planification de la stratégie de transformation numérique

Jour 3

Gestion des risques liés à la transformation numérique et mise en œuvre de la stratégie de transformation numérique

Jour 4

Communication et suivi de la stratégie de transformation numérique

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

TRANSFORMATION NUMÉRIQUE

2 JOURS

1333 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 42001 Foundation

PECB

Les Objectifs

- Expliquer les concepts et principes de la gestion de l'intelligence artificielle.
- Décrire les principales exigences de la norme ISO/IEC 42001 pour un système de management de l'intelligence artificielle (SMIA).
- Identifier des approches, méthodes et techniques utilisées pour mettre en oeuvre, gérer et améliorer un SMIA.

Les prérequis de la formation

Il n'y a pas de prérequis pour s'inscrire à cette formation.

L'audience ciblée

- Professionnels désireux d'avoir une compréhension fondamentale des exigences de la norme ISO/IEC 42001
- Managers et consultants désireux d'en savoir plus sur la gestion de l'intelligence artificielle
- Personnes impliquées dans la gestion ou la mise en œuvre de systèmes d'IA
- Personnes chargées de la supervision des projets liés à l'IA .

Le programme

Jour 1

Introduction au système de management de l'intelligence artificielle (SMIA) et à ISO/IEC 42001

Jour 2

Système de management de l'intelligence artificielle (SMIA) et examen de certification

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

TRANSFORMATION NUMÉRIQUE

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 42001 Lead Implementer

PECB

Les Objectifs

- Expliquer les concepts et principes fondamentaux d'un SMIA conformément à la norme ISO/IEC 42001.
- Interpréter les exigences de la norme ISO/IEC 42001 applicables à un SMIA du point de vue d'un Implementer (responsable de la mise en œuvre).
- Lancer et planifier la mise en œuvre d'un SMIA conformément à la norme ISO/IEC 42001 en utilisant la méthodologie IMS2 de PECB et d'autres meilleures pratiques.
- Soutenir une organisation dans l'exploitation, la maintenance et l'amélioration continue d'un SMIA conformément à la norme ISO/IEC 42001.
- Préparer une organisation à faire l'objet d'un audit de certification effectué par une tierce partie.

Les prérequis de la formation

Avoir des connaissances de base sur la norme ISO 42001 et sur le fonctionnement d'un système de management de l'IA (SMIA).

L'audience ciblée

- Professionnels chargés de superviser et de gérer les projets d'IA.
- Consultants des stratégies de mise en œuvre de l'IA.
- Conseillers experts et spécialistes désirant maîtriser la mise en œuvre pratique d'un SMIA conformément à la norme ISO/IEC 42001.
- Personnes chargées de veiller à ce que les projets d'IA soient conformes aux exigences en la matière au sein d'une organisation.
- Membres des équipes de mise en œuvre d'un SMIA participant à la mise en œuvre des systèmes d'IA.
- Cadres et dirigeants souhaitant prendre des décisions éclairées concernant la mise en œuvre de l'IA et sa conformité à la norme ISO/IEC 42001.

Le programme

Jour 1

Introduction à l'ISO/IEC 42001 et au lancement de la mise en œuvre d'un SMIA

Jour 2

Plan de mise en œuvre d'un SMIA

Jour 3

Mise en œuvre d'un SMIA

Jour 4

Suivi, amélioration continue et préparation à l'audit de certification du SMIA

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

TRANSFORMATION NUMÉRIQUE

5 JOURS

2917 € HT

FORMATION CERTIFIANTE

NIVEAU FONDAMENTAL

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

PECB CERTIFIED ISO 42001 Lead Auditor

PECB

Les Objectifs

- Expliquer les concepts et principes fondamentaux d'un système de management de l'IA conformément à la norme ISO/IEC 42001.
- Interpréter les exigences de la norme ISO/IEC 42001 relatives à un système de management de l'IA du point de vue d'un auditeur.
- Évaluer la conformité d'un système de management de l'IA aux exigences de la norme ISO/IEC 42001, dans le respect des concepts et principes fondamentaux de l'audit.
- Planifier, mener et clôturer un audit de conformité à la norme ISO/IEC 42001, dans le respect des exigences de la norme ISO/IEC 17021-1, des lignes directrices de la norme ISO 19011 et d'autres meilleures pratiques en matière d'audit h Gérer un programme d'audit ISO/IEC 42001.

Les prérequis de la formation

Avoir des connaissances de base sur la norme ISO 42001 et sur le fonctionnement de l'intelligence artificielle.

Savoir lire et comprendre l'anglais pour pouvoir consulter le support de cours et passer l'examen de certification.

L'audience ciblée

- Personnes ayant une expérience en matière d'audit, interne ou externe, désirant se spécialiser dans l'audit des systèmes de management de l'IA.
- Gestionnaires ou consultants souhaitant maîtriser le processus d'audit des systèmes de management de l'IA.
- Personnes responsables du maintien de la conformité aux exigences du système de management de l'IA au sein d'une organisation h Conseillers experts en management de l'IA.
- Professionnels chargés d'analyser et de comprendre les besoins des entreprises pour la mise en œuvre de l'IA.
- Personnes impliquées dans le développement et la mise en œuvre de solutions d'IA et dans la conception de l'architecture .

Le programme

Jour 1

Introduction au système de management de l'intelligence artificielle et à la norme ISO/IEC 42001

Jour 2

Principes d'audit, préparation et lancement d'un audit

Jour 3

Activités d'audit sur place

Jour 4

Clôture de l'audit

Jour 5

Examen de certification.

Les plus

- Cours animé par un formateur certifié PECB
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

Core

CORE

5 JOURS

3350 € HT

FORMATION CERTIFIANTE

DÉBUT DE CARRIÈRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

CompTIA Security+

Les Objectifs

Launch a Successful Cybersecurity Career. Develop a core foundation of essential skills, paving the way for a fulfilling career. More job roles use Security+ for baseline cybersecurity skills than any other certification in the industry.

- Assess On-the-Job Skills. Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam. These practical questions assess your ability to effectively problem solve in real-life situations and demonstrate your expertise to potential employers immediately.
- Embrace the Latest Trends. Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools. By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT, you will be well-equipped to excel in the ever-evolving cybersecurity landscape.

Les prérequis de la formation

The Nearly all IT managers (97%) recognize the value certified professionals bring to the organization such as boosting productivity, helping to meet client requirements and closing organizational gaps.

- Skillsoft IT Skills & Salary Report 2022

L'audience ciblée

- Security Specialist
- Security Administrator
- Systems Administrator
- Help Desk Analyst
- Security Analyst
- Security Engineer

Le programme

CompTIA Security+ is the first early career cybersecurity certification a candidate should earn.

- It equips cybersecurity professionals with the foundational security skills necessary to safeguard networks, detect threats, and secure data through performance-based questions—helping them open the door to a cybersecurity career and become a trusted defender of digital environments.

The CompTIA Security+ 701 exam verifies the candidate has the knowledge and skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CORE

5 JOURS

2950 € HT

FORMATION CERTIFIANTE

DÉBUT DE CARRIÈRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

CompTIA Network+

CompTIA

Les Objectifs

CompTIA Network+ represents the latest advancements in networking, covering the most in-demand skills related to network deployment, performance, security, troubleshooting and more. The CompTIA Network+ certification will certify that the successful candidate has the knowledge and skills required to:

- Establish network connectivity by deploying wired and wireless devices.
- Explain the purpose of documentation and maintain network documentation.
- Configure common network services.
- Explain basic data-center, cloud, and virtual-networking concepts.
- Monitor network activity and troubleshoot performance and availability issues.
- Implement network security hardening techniques.
- Manage, configure, and troubleshoot network infrastructure.

Les prérequis de la formation

- 9-12 months in the IT networking field recommended
- With over 3 million certifications granted in key tech domains, CompTIA's credentials reliably indicate professional competence.

L'audience ciblée

- Junior Network Administrator
- NOC Technician
- Systems Administrator
- Datacenter Support Technician
- Telecommunications Technician
- IT Support Manager
- Tier II Support Technician

Le programme

Network+ is a global IT certification validating candidates have the core skills necessary to establish, maintain, troubleshoot and secure networks regardless of technology or platform.

- The only certification on the market aligned to job roles for early-career networking professionals.

– Network+ is a crucial stepping-stone for early career professionals seeking a high-growth career in networking and cybersecurity, validating a wide range of practical skills needed to harden networks, deploy wired and wireless solutions, and ensure critical network availability.

- Network+ exclusively validates vendor-neutral network management knowledge.

– Network+ is the premier vendor-neutral IT infrastructure certification, validating the fundamental skills required for early-career networking job roles and preparing candidates to effectively manage and maintain modern network environments, including cloud, virtualization, and IoT.

- The industry standard for establishing hands-on networking expertise across any environment. – Network+ aligns with global IT standards and best practices and proves early-career networking professionals have the hands-on and technical skills required to manage network connectivity in any environment, preparing them for the diverse challenges they can expect to face in their IT careers.

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

CompTIA Network+

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CORE

5 JOURS

3150 € HT

FORMATION CERTIFIANTE

DÉBUT DE CARRIÈRE

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

CompTIA A+ Core Series

Les Objectifs

Les professionnels qui obtiennent la certification CompTIA A+ sont reconnus comme des experts en résolution des problèmes. Ils assurent l'assistance des principales technologies actuelles, de la sécurité à la mise en réseau en passant par la virtualisation et bien plus. CompTIA A+ constitue la norme du secteur pour débuter une carrière informatique dans le monde numérique actuel.

Les prérequis de la formation

La nouvelle version de CompTIA A+ met l'accent sur les technologies et les compétences dont les professionnels de l'informatique ont besoin pour accompagner des effectifs hybrides.

- CompTIA A+ tient compte du recours accru aux applications SaaS (software as a service) pour le travail à distance.
- La nouvelle version de CompTIA A+ cible davantage le dépannage et les méthodes de diagnostic et de correction à distance des problèmes logiciels, matériels ou de connectivité courante.
- CompTIA A+ cible l'évolution des technologies principales, de l'infrastructure Cloud à la gestion des données et l'écriture de scripts en passant par la sécurité des appareils IoT.
- Les techniciens font régulièrement face à différents systèmes d'exploitation, et A+ aborde dorénavant les principaux systèmes, leurs cas d'usage et les méthodes pour assurer leur bon fonctionnement.
- CompTIA A+ tient compte de la nature évolutive du poste, lorsque de nombreuses tâches sont envoyées à des fournisseurs spécialisés. Le personnel certifié est en mesure d'évaluer s'il est préférable de réparer un élément sur site ou s'il est plus intéressant en termes de temps et d'argent d'envoyer les technologies propriétaires directement aux fournisseurs.

L'audience ciblée

- Spécialiste du support informatique
- Technicien de centre d'assistance
- Technicien sur site
- Spécialiste du support de niveau I
- Spécialiste du support bureautique
- Ingénieur réseau adjoint
- Technicien de support systèmes
- Administrateur systèmes junior

Le programme

CompTIA A+ valide les compétences requises pour installer et configurer les appareils et logiciels de l'utilisateur final, connecter des appareils aux réseaux, effectuer des tâches élémentaires pour renforcer la cybersécurité, résoudre des problèmes courants (diagnostic et résolution des problèmes) et faire preuve de connaissances élémentaires en matière de scripts, de Cloud et de virtualisation.

Les plus

- Cours animé par un formateur certifié CompTIA
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

CORE

4 JOURS

2999 € HT

FORMATION CERTIFIANTE

LEVEL 100

KIT DE FORMATION OFFICIELLE

ACCESSIBLE AU PMR

MILE2 CERTIFIED Network Principles

Les Objectifs

Upon completion, the Certified Network Principles candidate will be able to competently take the C)NP exams well as the Comp TIA Network+ exam. You will have the knowledge to keep a companies' IP network infrastructure secure.

Les prérequis de la formation

(Any of the following Mile2 Courses)

- C)HT/C)OST or equivalent knowledge

L'audience ciblée

- Everyone
- End Users
- Employees
- Managers

Le programme

Module 1

Intro to Network Fundamentals

Module 2

The Physical Networking Fundamentals

Module 3

TCP/IP Primer

Module 4

Connecting Networks with Switches and Routers

Module 5

Wireless Networking

Module 6

Security Principles

Module 7

Defending the Network

Module 8

Network Technology Boom

Module 9

Day to Day Networking

Module 10

Network Planning

Les plus

- Cours animé par un formateur certifié Mile2
- Consultez le programme, l'agenda de prochaines sessions et téléchargez les brochures

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

EXECUTIVE MBAs

12 - 36 MOIS

48 CRÉDITS

COURS EN LIGNE, SYNCHRONES ET ASYNCHRONES

ANGLAIS & FRANÇAIS

Cybersecurity

Audience

Designed for candidates seeking managerial or executive positions in Information Security.

Download the presentation brochure

Business Continuity Management

Audience

Designed for candidates seeking managerial or executive positions in Business Continuity.

Download the presentation brochure

Governance, Risk and Compliance

Audience

Designed for candidates seeking managerial or executive positions in Risk Management.

Download the presentation brochure

Work Experience

A minimum of 2 years of relevant working experience. Although you are not required to have previous experience in business administration, you are expected to have a background on the field in which you are pursuing the Executive MBA program.

ACG Cybersecurity

ACADEMIC PARTNER

PECB UNIVERSITY
EXISTIMATIO PER VERITATEM

Campus Cyber, Tour Eria, 5 – 7 Rue Bellini, 92800 Puteaux https://acgcyberacademy.fr formation@acgcybersecurity.fr +33 1 89 62 34 30

NOS VALEURS

COMPÉTENCE

ACG Cybersecurity s'engage à ne pas revendiquer une compétence qu'elle ne possède pas.

CONFIDENTIALITÉ

L'entreprise agit en toute confidentialité et respecte ses accords. Elle s'engage à protéger les données fournies lors de ses missions.

RESPONSABILITÉ

ACG Cybersecurity vérifie que le mandataire ou le signataire du client a bien responsabilité ; et autorité vis-à-vis des systèmes.

ENGAGEMENT

ACG Cybersecurity certifie que tous les employés de la société ont accepté les principes et règles du code d'éthique et de déontologie.

ASSURANCE

ACG Cybersecurity dispose d'assurances en responsabilité civile professionnelle couvrant toutes ses prestations.

TRANSPARENCE

ACG Cybersecurity fournit à ses clients les informations relatives à son identité, ses actionnaires, son personnel, ses sous-traitants, ses méthodologies et pratiques.

COORDONNÉES

Campus Cyber

Tour Eria, 5-7 Rue Bellini,
92800 Puteaux, France

E-mail

contact@acgcybersecurity.fr

formation@acgcybersecurity.fr

Téléphone

+33 1 89 62 34 30

Nos sites web

acgcyberacademy.fr

acgcybersecurity.fr

BIENVENUE CHEZ ACG CYBERSECURITY

L'expertise pour la réussite de vos projets en Cybersécurité.

ACG | Cybersecurity