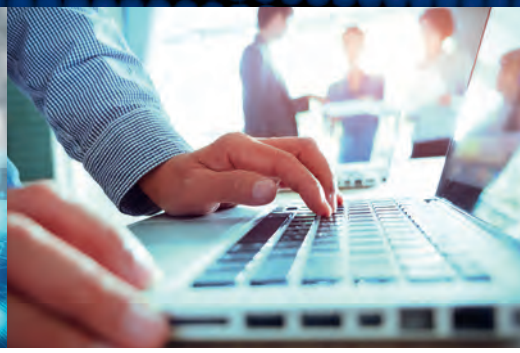
catalogue FORMATIONS

EDITION 2025





Qualiopi processus certifié

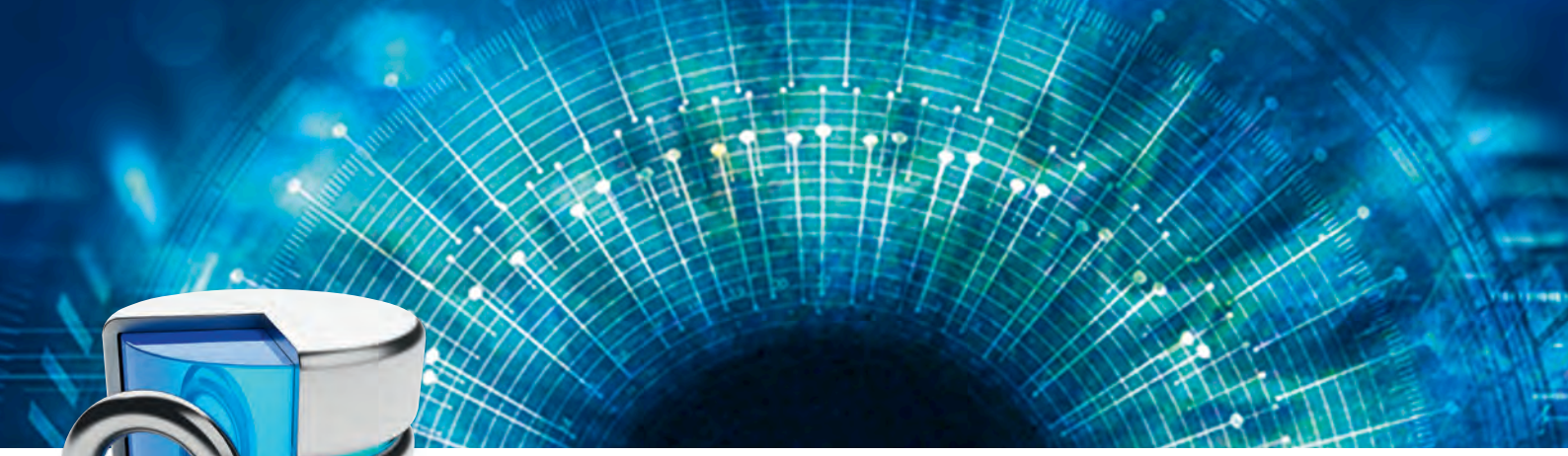
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie "actions de formation"

Organisme de formation déclaré sous le numéro 11755044375

PROSICA

La maîtrise de votre sécurité



PROSICA SAS est une société de conseil et un organisme de formation en cybersécurité.

Chacune de nos formations est une préparation intensive pour acquérir les connaissances et la méthodologie indispensables à la réussite d'un examen et permettre ainsi d'acquérir une certification officielle reconnue par la profession.

NOS ATOUTS

1	Formateurs chevronnés (plus de quinze années d'expérience) et certifiés.
2	Formations très bien notées par nos stagiaires, taux de réussites élevés aux examens démontrant le bon niveau des contenus et la qualité pédagogique des formateurs.
3	Nombreux exemples et cas concrets pour assimiler plus facilement les concepts.
4	Questionnaires d'entrainement pour se préparer aux examens.
5	Plusieurs options complémentaires disponibles en fonction des besoins (inter, intra, formation en anglais ou en français, suivi personnalisé, ouvrages de préparation, accès à un site de préparation…).

PROSICA

La maîtrise de votre sécurité

SOMMAIRE

LE FONDATEUR

Ingénieur Saint-Cyr et ENSEEIHT, Christophe JOLIVET a acquis une solide expérience en cybersécurité et gestion de crise.

Après un début de carrière consacré aux systèmes d'information et de communication militaires, il intègre un cabinet de conseil en sécurité de l'information en tant que consultant puis directeur technique. Il coordonne ensuite pendant six ans la sécurité (systèmes d'information, continuité des activités et sûreté) du groupe Eutelsat (opérateur international de télécommunication par satellites). Christophe JOLIVET est titulaire de plusieurs certifications professionnelles : CISSP, CISA, CBCP, ISO 27001 Lead Implementer, CCSP, CCSK, GIAC, PMP, CIPP/E, CPP.

PROSICA EST MEMBRE DES ASSOCIATIONS PROFESSIONNELLES

iapp

ISACA

(ISC)²

PMI Project Management Institute

ASIS INTERNATIONAL Advancing Security Worldwide

Préparation à la certification CISSP®

PROSICA
La maîtrise de votre sécurité

Tél. : 01.73.29.76.01 www.prosica.fr
Contact : formation@prosica.fr

Préparation à la certification CISSP®

5 jours **3000 € HT** (35 heures)

ENJEUX

Le CISSP®[1] est la certification internationale la plus reconnue dans le domaine de la sécurité des systèmes d'information.
Elle apparaît de plus en plus, y compris en France comme un prérequis pour qualifier les compétences des professionnels de sécurité.
L'examen est exigeant et requiert une préparation intensive.

PUBLIC CONCERNÉ

- Professionnels de la sécurité - entreprise et administration : CISO, RSSI, chefs de projets, administrateurs, auditeurs, architectes.
- Prestataires de sécurité : développeurs et chefs de projet des éditeurs, ingénieurs intégrateurs, consultants, ingénieurs avant-ventes

PRÉREQUIS

- 5 ans d'expérience professionnelle en cyber-sécurité.
- Il est possible de passer l'examen en devenant «CISSP associate» avant d'atteindre l'expérience requise.

EXAMEN

- L'examen est indépendant de la formation. Il se déroule sous la responsabilité de l'(ISC)[2] sur ordinateur dans un centre agréé Pearson Vue.
- Il est proposé en anglais et en français.

OBJECTIFS

- Connaitre les concepts fondamentaux du programme officiel, mis jour régulièrement par l'(ISC)[2] : www.isc2.org.
- Adopter une méthodologie de préparation efficace.
- Évaluer le niveau atteint par rapport au niveau attendu pour réussir l'examen.

TARIFS

Formation complète de 5 jours avec :
• supports en français, quizz en anglais et documents annexes **3000 € HT**

LIEU & DATES

Les formations se déroulent en mode "distanciel" en utilisant l'outil TEAMS.

DATES pour 2025

5 jours - 9h30 à 17h30
35 heures

- Lundi 7 au vendredi 11 avril
- Lundi 8 au vendredi 12 décembre

1. *CISSP : Certified Information Systems Security Professional*
2. *(ISC)2 : International Information Systems Security Certification Consortium : https://www.isc2.org/*

Préparation à la certification CISSP®

PROGRAMME DÉTAILLÉ

DOMAINE 1: Sécurité et gestion des risques

- Principaux concepts
- Gouvernance
- Conformité
- Aspects légaux et réglementaires
- Éthique et déontologie
- Politiques, standards, procédures
- Continuité des activités
- Sécurité des personnes
- Gestion des risques
- Modélisation des menaces
- Intégration de la sécurité dans les projets
- Sensibilisation et formation

COSO, COBIT, officiers de sécurité, auditeurs, due care, due diligence, documentation, CLOUD, infogérance, séries ISO 2700, STRIDE, CRAMM, IRAM2, OCTAVE, EBIOS, impact, vraisemblance, acceptation, transfert, évitement, contre-mesures, recrutement, formation, sensibilisation, tableaux de bord, budget, sites de secours, plans de continuité, communication de crise, RTO, MTD, RPO, pénal, civil, common law, tort law, cybercriminalité, propriété intellectuelle, droits des marques, données à caractère personnel, surveillance, code de déontologie professionnel.

DOMAINE 2: Protection des actifs

- Classification
- Propriétaire de l'information
- Données à caractère personnel
- Conservation des données
- Sécurité des données
- Exigences de traitement

Quality control, quality assurance, cycle de vie de l'information, classification, data remanence, anonymisation, chiffrement des supports amovibles, chiffrement de bout en bout.

DOMAINE 3: Ingénierie de la sécurité

- Principes de conception
- Modèles de sécurité
- Évaluation et mesures
- Capacité de sécurité des systèmes
- Architectures
- Environnements WEB
- Mobilité
- Systèmes embarqués
- Cryptographie
- Sécurité physique

Quantique, algorithmes, fonctions à sens unique, signature électronique, PKI, collision, vecteur d'initialisation, transposition, permutation, chiffrement par flot, par bloc, symétrique, asymétrique, longueur de clé, DES, 3DES, AES, CCMP, Rijndael, Blowfish, RC5, RC4, Diffie-Hellman, RSA, El Gamal, ECC, MAC, HMAC, MD5, SHA-3, HAVAL, paradoxe des anniversaires, distribution des clés, révocation, recouvrement, brute-force, cryptanalyse, rainbow table, X509, watermarking, processeurs, mémoires, systèmes d'exploitation, SABSA, TOGAF, ITIL, Bell-LaPadula, Biba, Clarck-Wilson, Muraille de Chine, Graham-Denning, critères communs, ITSEC, PCI-DSS, isolation des processus, virtualisation, canaux cachés, mainframes, XML, SAML, systèmes distribués, grid computing, analyse de vulnérabilités, vitrage, menaces naturelles, alimentation électrique, portes, clôtures, détection d'intrusion, vidéoprotection, éclairage, contrôle des accès, capteurs infrarouges, serrures, coffres, salles informatiques, UPS, HVAC, protections incendie.

DOMAINE 4: Réseaux et télécommunications

- Principes
- Composants réseaux
- Canaux sécurisés
- Attaques réseaux
- Systèmes embarqués
- Cryptographie
- Sécurité physique

Modèle OSI, TCP/IP, OSPF, BGP, IPv6, DHCP, ICMP, RPC, DNS, NIS, SMB, SMTP, FTP, HTTP, Proxy, SCADA, PLC, Modbus, routeurs, DMZ, commutateurs, câblage, GSM, UMTS, CDMA, 5G, WI-FI, Bluetooth, ARP, NAC, firewall, NAT, VPN, VLAN, PABX, VoIP, Peer-to-peer, IRC, Jabber, RADIUS, SNMP, MPLS, WAN, ATM, FR, SDN, S/MIME, scans, fragmentation IP, Spoofing.

DOMAINE 5: Gestion des identités

- Contrôles d'accès logiques et physiques
- Identification et authentification
- Identité as a service
- Intégration des tierces-parties
- Mécanismes
- Attaques liées au contrôle d'accès
- Gestion des accès

Défense en profondeur, séparation des rôles, domaines de confiance, classification de l'information, habilitations, DAC, MAC, ACL, matrice des droits, RBAC, carte à puce, token, annuaires, LDAP, SSO, Kerberos, SAML, Open ID, DDOS, rémanence, rejeu, ingénierie sociale, craquage de mots de passe, usurpation, écoute, émanation électromagnétique, TEMPEST, SLE, ALE, EF, ARO.

Préparation à la certification CISSP®

PROGRAMME DÉTAILLÉ

DOMAINE 6 : Évaluation et test de la sécurité

- Stratégies
- Tests de sécurité
- Contrôle des processus
- Analyse des rapports
- Audits internes et externes

Vulnérabilités, audits, tests d'intrusion, IDS-IPS, SIEM, SEM, SIM, Syslog, RUM, Synthetic Performance, SAST, DASP, RASP Fuzzing, Red Team, Double Blind, CVE, SCAP, CVSS, ISCM, ISAE 3402.

DOMAINE 7 : Sécurité de l'exploitation

- Investigations numériques
- Exigences légales
- Supervision de la sécurité
- Sécurité des ressources (Cloud, virtualisation…)
- Concepts de sécurité liés à l'exploitation
- Gestion des supports
- Gestion des incidents de sécurité
- Gestion des mesures préventives
- Gestion des correctifs
- Gestion des changements
- Stratégies de reprise informatique
- Plan de secours informatiques
- Test des plans de secours
- Participation aux exercices de continuité
- Gestion de la sécurité physique
- Sécurité des personnes

Besoin d'en connaitre, moindre privilège, comptes privilégiés, séparation des tâches, archivage, gestion des supports amovibles, licences, gestion des incidents, ISO 27035, gestion des problèmes, audits, gestion des configurations, systèmes redondés, vulnérabilités, RAID, investigation numérique, éléments de preuve, analyse logicielle, File Slack, clauses de sécurité contractuelles, DLP.

DOMAINE 8 : Sécurité des développements

- Intégration de la sécurité dans le cycle de développement
- Environnement de développement sécurisé
- Évaluation de la sécurité des développements internes
- Acquisition des logiciels et sécurité

Exigences fonctionnelles et techniques, tests, CMMI, gestion du changement, correctifs, MPM, RAD, JAD, CASE, extreme programming, bases de données, programmation objet, entrepôts de données, metadata, OLAP, data mining, TOC/TOU, OWASP, Open Source, full disclosure, langages, sécurité java, erreurs de programmation, virus, vers, sécurité des systèmes d'exploitation, bac à sable, AGILE, SCRUM, DEVSECOPS.

APPROCHE PÉDAGOGIQUE

- Acquisition des connaissances issues du programme officiel avec des supports en français et de nombreux exemples pour illustrer les concepts.
- La révision des définitions essentielles par des « flashcards ».
- La résolution de quizz pour chaque domaine reflétant le style de l'examen.
- Des conseils méthodologiques et la remise de documents annexes pour approfondir.
- Un examen blanc d'entrainement et sa correction.

Sécurité du Cloud Computing

Préparation à la certification CCSK
(Certificate of Cloud Security Knowledge)

Préparation à la certification CCSP
(Certified Cloud Security Professional)

PROSICA
La maîtrise de votre sécurité

Tél. : 01.73.29.76.01 www.prosica.fr
Contact : formation@prosica.fr

Préparation à la certification CCSK

1 900€ HT
2 jours (14 heures)

ENJEUX

Dans le cadre de leur migration Cloud, les organisations publiques et privées ont besoin de professionnels en cybersécurité qui maitrisent les concepts et les risques liés au Cloud.

La certification CCSK (Certificate of Cloud Security Knowledge) de la Cloud Security Alliance est largement reconnue pour fournir les fondamentaux indispensables dans ce domaine.

PROSICA propose une formation de deux jours pour acquérir les connaissances et la méthodologie indispensables à la réussite de l'examen CCSK.

PUBLIC CONCERNÉ

- Toute personne (1 an d'expérience en cybersécurité requis) souhaitant maitriser les basiques de la sécurité du Cloud en vue d'obtenir la certification CCSK :
  - Responsable Sécurité des Systèmes d'Information.
  - Consultant en sécurité des systèmes d'information.
  - Auditeurs IT.
  - Chef de projet Cloud.
  - Architecte et intégrateur CLOUD.
  - Ingénieurs avant-ventes des fournisseurs et brokers de Cloud.

PRÉREQUIS

- 1 an d'expérience en cybersécurité requis

EXAMEN

- L'examen, indépendant de la formation est en anglais. Il est réalisé en ligne à une date choisie par chaque candidat sur le site de la Cloud Security Alliance.
- L'examen comprend 60 questions pour une durée de 90 min. Le résultat est donné connu dès la fin de l'examen. L'organisation de l'examen est sous la responsabilité de la Cloud Security Alliance (https://cloudsecurityalliance.org).

OBJECTIFS

- Maîtriser les concepts au programme de l'examen du CCSK.
- Évaluer ses connaissances afin de déterminer le travail de révision restant à produire.
- S'entrainer à répondre à des questions dans un temps imparti.

TARIFS

TARIFS	Formation de 2 jours avec : • supports en français et documents annexes • pauses café et viennoiseries, déjeuners	**1 900 € HT**
OPTIONS	• Inscription à l'examen du CCSK	**500 € HT**
	• Livre de préparation numérique ou papier	**60 € HT**
	• Suivi individualisé de 6 mois par le formateur (réponse aux questions sous 48h ouvrées)	**150 € HT**

LIEU & DATES

Les formations se tiennent en mode "distanciel" en utilisant l'outil TEAMS.

DATES pour 2025

2 jours - 9h30 à 17h30

- Jeudi 30 au vendredi 31 janvier
- Jeudi 27 au vendredi 28 mars
- Jeudi 9 au vendredi 10 octobre

Préparation à la certification CCSK

PROGRAMME DÉTAILLÉ

JOUR 1

- **Introduction et présentation de la certification CCSK.**

Architectures et exigences de sécurité des services CLOUD	• Caractéristiques, services, rôles, déploiements, responsabilités. • Architectures. • Risques (référentiels, méthodes, guide ENISA). • Security-as-a-Service.
Sécurité des données dans le Cloud	• Cycle de vie des données. • Services de stockage Cloud. • Données à caractère personnel. • Data Loss Prevention. • Chiffrement et autres techniques.
Sécurité des opérations :	• Durcissement systèmes et réseaux. • Administration et exploitation. • Réaction aux incidents de sécurité.
Quizz et correction.	

MOTS CLÉS : IaaS, PaaS, SaaS, Cloud privé et public, ISO 17789, NIST 500-292, Orchestration, responsabilités clients / fournisseurs, TOGAF, SABSA, CSA, Jéricho, CAIQ, CCM, ISO 27001, ISO 27017, ISO 27018, COBIT, STAR, ISO 31000, NIST 800-37, durcissement, SIEM, correctifs, SecCM, SCAP, pseudo anonymisation, algorithmes de dispersion, IRM, DRM, KMIP, KMS, HSM.

JOUR 2

Sécurité des plateformes Cloud et des infrastructures	• Réseaux et communications (flux, administration). • Virtualisation. • Continuité des activités.
Sécurité des applications et IAM	• Principes de déploiement. • Audits et tests. • Failles applicatives. • Gestion des identités et des accès.
Aspects juridiques et conformité	• Panorama des aspects légaux et réglementaires. • Référentiels et bonnes pratiques de sécurité. • Certifications et homologation. • Gestion des contrats. • Audits
Quizz et correction.	

MOTS CLÉS : NIS Directive, Due diligence, ISAE, SOC, STAR, ISO15408, SecNumCloud, eDiscovery, Forensic, ESI, VLAN, VxLAN, SDN, SDP, bastion, containers, serverless, CIS hardening guidelines, segmentation, stockage objet et volume, CI/CD, DevSecOps, SDLC, STRIDE, DREAD, ISO 27034, OWASP, SOAP, API, REST, OCCI, CSA Top Threats, API, CVSS, SAML, OAUTH, OpenID, CASB

APPROCHE PÉDAGOGIQUE

Les formateurs PROSICA sont des experts reconnus et expérimentés qui interviennent régulièrement en conseil d'entreprises publiques et privées ainsi que d'administrations dans le domaine de la sécurité du Cloud.

L'approche pédagogique alterne :

- L'acquisition des connaissances en vidéo-projection.
- L'illustration des concepts par des exemples actualisés.
- Le contrôle des connaissances au travers de quizz interactifs.
- La résolution de questionnaires en anglais de préparation à la certification CCSK.

Chaque stagiaire reçoit un support de formation en français reprenant les points à maîtriser.

- Les tests pratiques sont similaires à l'examen de certification.

PROSICA
La maîtrise de votre sécurité

Tél. : 01.73.29.76.01 www.prosica.fr
Contact : formation@prosica.fr

Sécurité du Cloud Computing
préparation à la certification CCSP

3 900€ HT
5 jours (35 heures)

ENJEUX

Les services de Cloud Computing publics sont de plus en plus prisés par les entreprises de toute taille. Réactivité, automatisation, service à la demande, connectivité, disponibilité, souplesse, mobilité sont des bénéfices auxquels adhèrent les décideurs et les utilisateurs. Les aspects sécurité doivent être intégrés à différentes étapes : rédaction des cahiers des charges, choix des solutions, conception des architectures, examen des clauses contractuelles, conformité légale, mise en œuvre et exploitation du service, interface entre les équipes informatiques internes, gestion des incidents…

PROSICA propose une formation intensive de cinq jours pour acquérir les connaissances et la méthodologie indispensables à tout professionnel des systèmes d'information souhaitant comprendre les enjeux de sécurité et tenir un rôle actif dans les projets de Cloud Computing.

Cette formation intensive permet de préparer la certification CCSP.

PUBLIC CONCERNÉ

- Professionnels des systèmes d'information : CISO, RSSI, architectes, chefs de projet hébergeurs, auditeurs

PRÉREQUIS

- 5 ans d'expérience professionnelle en systèmes d'information, dont 3 ans en sécurité.
- Il est possible de passer l'examen avec moins d'expérience et d'être "CCSP associate" jusqu'à obtenir l'expérience requise pour être certifié.

EXAMEN

- L'examen CCSP est indépendant de la formation. Il se déroule sous la responsabilité de l'(ISC)2[1] sur ordinateur dans un centre agréé Pearson Vue.
- Il est disponible en langue anglaise.

OBJECTIFS

- Connaitre les concepts fondamentaux du programme officiel des certifications, mis jour régulièrement par l'(ISC)2[1] et la Cloud Security Alliance.
- Adopter une méthodologie de préparation efficace.
- Évaluer le niveau atteint par rapport au niveau attendu pour réussir les examens.

TARIFS & OPTIONS

TARIFS	Formation complète de 5 jours avec : • supports en français et documents annexes	**3 900 € HT**
OPTIONS	• Livre de préparation en anglais	**60 € HT**
	• Suivi individualisé de 6 mois par le formateur (réponse aux questions sous 48h ouvrées)	**150 € HT**

LIEU & DATES

Les formations sont organisées en mode "distanciel" en utilisant l'outil TEAMS.

DATES pour 2025

5 jours - 9h30 à 17h30

- Lundi 12 au vendredi 16 mai
- Lundi 17 au vendredi 21 novembre

1. (ISC)2 : International Information Systems Security Certification Consortium : https://www.isc2.org/

Sécurité du Cloud Computing
préparation à la certification CCSP

PROGRAMME DÉTAILLÉ

- Introduction et présentation de la certification CCSP.
- Architectures et exigences de sécurité des services CLOUD :
  - Caractéristiques, services, rôles, déploiements, responsabilités.
  - Architectures (TOGAF, SABSA, CSA, Jéricho).
  - Risques (référentiels, méthodes, guide ENISA).
- Sécurité des données dans le Cloud (1ère partie) :
  - Cycle de vie des données.
  - Services de stockage Cloud.
  - Données à caractère personnel.

→ **Cas concrets :**
- Modèles associés à des exemples de solutions Cloud.
- Analyses et traitement des risques d'une migration Microsoft 365.

- Quizz et correction.
- Sécurité des plateformes Cloud et des infrastructures (1ère partie) :
  - Réseaux et communications (flux, administration).
  - Virtualisation.
  - Continuité des activités.
- Aspects juridiques et conformité (1ère partie) :
  - Panorama des aspects légaux et réglementaires.
  - Règlement Européen sur la Protection des Données Personnelles et Services Cloud.
  - Référentiels et bonnes pratiques de sécurité.

→ **Cas concrets :**
- Comparaisons de clauses de certification STAR de fournisseurs Cloud.
- Sécurité des réseaux d'administration.

- Quizz et correction.
- Sécurité des données (2ème partie) :
  - Data Loss Prevention.
  - Chiffrement et autres techniques (FHE, pseudo anonymisation, algorithmes de dispersion, Information Right Management).
- Sécurité des plateformes Cloud et des infrastructures (2ème partie) :
  - Software Defined Networking.
  - Segmentation des réseaux Cloud et VXLAN.
- Sécurité des applications :
  - Principes de déploiement (SDLC, STRIDE, DREAD, ISO 27034).
  - Audits et tests.
  - Failles applicatives (OWASP, CSA Top Threats, API, CVSS)
  - Gestion des identités et des accès (SAML, OAUTH, OpenID).

→ **Cas concrets :**
- Risques Microsoft 365.
- Évaluation CAIQ Saleforce et Microsoft

- Quizz et correction.
- Sécurité des opérations :
  - Conception et sécurité du Datacenter.
  - Durcissement systèmes et réseaux (exemple hardening AWS, gestion des logs, gestion des correctifs, IDPS, SecCM, protocole SCAP).
  - Administration et exploitation.
  - Réaction aux incidents de sécurité (exemples, processus, investigations numériques).
- Aspects juridiques et conformité (2ème partie) :
  - Certifications et homologation (SOC, STAR, ISO 15408, SecNumCloud).
  - Gestion des contrats.

→ **Cas concrets :**
- Réaction à un DDoS.
- Cloud et conformité légale
- Évaluation d'un niveau de sécurité en utilisant le référentiel Cloud Control Matrix.

- Examen blanc de simulation d'examen CCSP et correction.

APPROCHE PÉDAGOGIQUE

- Acquisition des connaissances issues du programme officiel avec des supports en français et de nombreux exemples pour illustrer les concepts.
- La résolution de cas concrets liés à la sécurité en environnement Cloud.
- La révision des définitions essentielles par des « flashcards ».
- La résolution de quizz pour chaque domaine reflétant le style de l'examen.
- Des conseils méthodologiques et la remise de documents annexes pour approfondir.
- Un examen blanc d'entrainement et sa correction.

Réponse aux incidents de sécurité – ISO 27035

PROSICA
La maîtrise de votre sécurité
Tél. : 01.73.29.76.01 www.prosica.fr
Contact : formation@prosica.fr

Réponse aux incidents de sécurité – ISO 27035

1 900€ HT
2 jours (14 heures)

ENJEUX

Les entreprises et les administrations ont mis en œuvre de nombreuses mesures de prévention en matière de cybersécurité mais les mécanismes de détection et surtout de réaction sont souvent moins avancés.
Les vulnérabilités exploitables sont nombreuses et nul n'est à l'abri d'un incident majeur impactant la sécurité des systèmes d'information de son entité.
PROSICA propose une formation pour acquérir les connaissances et mettre en place les outils indispensables pour élaborer un processus solide de détection et de réaction aux incidents de sécurité.
La formation est destinée à toute personne amenée à mettre en place ou à intervenir dans la gestion des incidents de sécurité.

PUBLIC CONCERNÉ

- DSI, CIO, RSSI, CISO, responsables Security Operation Center, responsables production, consultants

PRÉREQUIS

- 3 ans d'expérience professionnelle en sécurité des systèmes d'information.

OBJECTIFS

- Savoir catégoriser un événement et un incident de sécurité.
- Connaitre la méthode (aspects organisationnels, techniques et juridiques) pour mettre en place un processus de gestion des incidents de sécurité adapté à une entité.
- Maitriser les concepts fondamentaux de gestion d'une cybercrise.

TARIFS

TARIF	Formation de 2 jours avec : • supports en français	1 900 € HT

LIEU & DATES

Les formations se tiennent en mode "distanciel" en utilisant l'outil TEAMS.

DATES pour 2025

2 jours - 9h30 à 17h30

- Jeudi 13 au vendredi 14 mars
- Jeudi 26 au vendredi 27 juin

Réponse aux incidents de sécurité – ISO 27035

PROGRAMME DÉTAILLÉ

JOUR 1

- **Catégorisation des événements et des incidents de sécurité :**
  - Cartographie de cas réels
  - Revue des normes et documentations disponibles
- **Environnement extérieur :**
  - Les services de gendarmerie et de police
  - L'agence nationale de sécurité des systèmes d'information
  - Les CERT (computer and emergency response team)
- **Étude et résolution de cas concrets :**
  - DDoS
  - Attaque ciblée
- **Élaboration d'un processus de gestion des incidents de sécurité :**
  - Veille, détection, qualification et réaction, outils disponibles, reporting
  - Interactions avec la politique de sécurité
  - Rôle du SOC (Security Operation Center)
  - Communications interne et externe
  - Composition et fonctionnement de la cellule de réaction aux incidents
  - Tableau de bord des incidents
  - Liens avec les processus ITIL
  - Présentation des outils CTI (Cyber Threat Intelligence)
  - Les outils du SOC (SOAR, SIEM)

JOUR 2

- **Aspects légaux et réglementaires :**
  - Cadre légal français
  - Fraudes informatiques
  - Dépôt de plainte
  - Investigations, « forensics »
- **Gestion des crises :**
  - Incidents et crises
  - Capacité à gérer une crise :
    - Se préparer - Évaluer une situation
    - Prendre des décisions - Maîtriser la communication
- **Étude et résolution de cas concrets :**
  - Défiguration de site WEB
  - Divulgation d'un document stratégique

APPROCHE PÉDAGOGIQUE

- Acquisition des connaissances issues des normes et des bonnes pratiques avec des supports en français et de nombreux exemples pour illustrer les concepts.
- La résolution de cas concrets.
- Des conseils méthodologiques et la remise de documents annexes pour approfondir.

Data Protection Officer

Délégué à la Protection des Données

Certification CIPP/E

(Certified Information Privacy Professional/Europe)

PROSICA
La maîtrise de votre sécurité

Tél. :01.73.29.76.01 www.prosica.fr
Contact : formation@prosica.fr

Data Protection Officer • Délégué à la Protection des Données • Certification CIPP/E

1 900€ HT
2 jours (14 heures)

ENJEUX

Le Règlement Général sur la Protection des Données (General Data Protection Regulation) qui doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique et qui remplace la Directive 95/46/CE comprend un champ d'application très large.

La désignation d'un délégué est obligatoire pour les organismes publics et les entreprises privées qui réalisent un suivi des personnes à grande échelle ou traitent des données sensibles.

Au-delà des cas obligatoires, la désignation d'un DPO est fortement encouragée car elle permet de confier à un expert la coordination des actions en matière de protection des données personnelles. PROSICA propose une formation de deux jours alternant théorie et cas pratiques permettant d'acquérir les connaissances principales en matière de droit européen et de maitriser les fondamentaux de la fonction de DPO. Cette formation est aussi une solide préparation à la certification individuelle CIPP/E[1] (International Association of Privacy Professionals) proposée par l'IAPP (iapp.org).

PUBLIC CONCERNÉ

- Toute personne amenée à travailler dans le cadre de la conformité des traitements de données personnelles.

PRÉREQUIS

- Aucun prérequis particulier n'est nécessaire pour suivre la formation.

EXAMEN

- L'examen CIPP/E est indépendant de la formation. Il se déroule sous la responsabilité de l'IAPP sur ordinateur dans un centre agréé.
- Il est disponible en langue anglaise et française.

OBJECTIFS

- Connaitre les concepts fondamentaux du programme officiel de la certification CIPP/E.
- Savoir mettre en place un programme de conformité au RGPD.
- Illustrer les concepts par la résolution de cas concrets.

TARIFS

TARIFS	Formation de 2 jours avec : • supports en français et documents annexes • pauses café et viennoiseries, déjeuners	1 900 € HT
OPTIONS	• Livre de préparation en anglais	90 € HT
	• Suivi individualisé de 6 mois par le formateur (réponse aux questions sous 48h ouvrées)	150 € HT

LIEU & DATES

Les formations se tiennent en mode "distanciel" en utilisant l'outil TEAMS.

DATES pour 2025

2 jours - 9h30 à 17h30

- Jeudi 16 au vendredi 17 janvier
- Jeudi 25 au vendredi 26 septembre

1. *CIPP/E : Certified Information Privacy Professional / Europe*

Data Protection Officer

▪ Délégué à la Protection des Données ▪ Certification CIPP/E

PROGRAMME DÉTAILLÉ

JOUR 1

Introduction

- Origine de la protection des données personnelles.
- Évolution du cadre juridique européen et français.
- Institutions européennes et françaises.

RGPD[1] Concepts clés

- Données à caractère personnel et traitement.
- Catégories sensibles.
- Responsable de traitement, sous-traitance, droits de la personne.
- Champ territorial.
- Cas d'exclusion.

➔ **Cas concret n°1 :** Résolution d'un quizz « vrai / faux » sur les principes clés du RGPD.

RGPD Sécurité des données

- Panorama des menaces.
- Analyse des risques.
- Incidents de sécurité.
- Mesures de protection.
- Sécurité et sous-traitance.
- Cas du Cloud Computing.

➔ **Cas concret n°2 :** Étude de cas – faire trouver les faiblesses potentielles d'une solution de gestion de ressources humaines en mode Software-as-a-service.

RGPD Transfert et sanctions

- Autorités de régulation.
- Sanctions.
- Notification en cas de divulgation.

JOUR 2

RGPD Le DPO

- Rôle et missions.
- CIL et DPO.
- Lignes directrices du WP29.
- Les outils du DPO.

➔ **Cas concret n°3 :** Définir un plan de travail du DPO.

RGPD Cas de mises en conformité

- Traitement de données médicales.
- Traitement de données employeurs.
- Activités de surveillance.
- Direct marketing.

➔ **Cas concret n°4 :** Jeux de rôles, mises en situation et corrections.

> Réunion DPO / responsable sécurité : mise en place d'un système de vidéo-protection.

> Réunion DPO / responsable marketing : mise en place d'un nouveau site WEB.

> Réunion DPO / responsable clients : mise en place d'un système de gestion des plaintes clients.

> Réunion DPO / directeur informatique : mise en place d'un centre d'appels.

> Réunion DPO : responsable RH : mise en place d'un outil de gestion de carrière suivant le modèle Software-as-a-Service.

> Administration et exploitation.

> Réaction aux incidents de sécurité (exemples, processus, investigations numériques).

APPROCHE PÉDAGOGIQUE

- Acquisition des connaissances issues du programme officiel et du règlement européen avec des supports en français et de nombreux exemples pour illustrer les concepts.
- La résolution de cas concrets.
- La résolution de quizz reflétant le style de l'examen.
- Des conseils méthodologiques et la remise de documents annexes pour approfondir.

1. (Règlement général sur la protection des données - règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016