OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen CISSP

CISSP
Certified Information Systems Security Professional

Certification : CISSP — Certified Information Systems Security Professional (ISC2)

Niveau : Expert / Senior | Public : RSSI / Security architects / Consultants cybersécurité seniors

1. Présentation de la certification

Le **CISSP (Certified Information Systems Security Professional)**, délivré par **ISC2** (anciennement (ISC)²), est **la certification cybersécurité la plus prestigieuse au monde**. Référence absolue pour les RSSI, security architects, consultants seniors, elle valide une **expertise senior** sur l'ensemble des domaines de la sécurité de l'information.

L'examen couvre les **8 domaines** du **CISSP CBK (Common Body of Knowledge)** : Security & Risk Management, Asset Security, Security Architecture & Engineering, Communication & Network Security, IAM, Security Assessment & Testing, Security Operations, Software Development Security. Format **CAT** (Computer Adaptive Test) ou Linear. Prérequis : **5 ans d'expérience** minimum. **OpenCertif est Pearson VUE Authorized Test Center**.

Informations clés

Nom complet	**Certified Information Systems Security Professional**
Acronyme	**CISSP**
Éditeur officiel	**ISC2** (anciennement (ISC)²) — a non-profit
Centre de test	**Pearson VUE** uniquement — OpenCertif est Pearson VUE Authorized Test Center
Modalité	En centre Pearson VUE ou OnVUE (online proctoring)
Format de l'examen	**CAT** (Computer Adaptive Test) en anglais
Format alternatif	**Linear** dans d'autres langues (250 questions, 6h)
Durée CAT	**3 heures** (180 minutes)
Nombre de questions CAT	**100 à 150 questions**
Score requis	**700 / 1000** minimum
Types de questions	QCM + advanced innovative items (drag-and-drop, hotspot)
Tarif	**~749 USD** (tarif standard ISC2)

Langues	**Anglais** (CAT), espagnol, allemand, japonais, chinois (Linear)
Prérequis expérience	**5 ans** minimum dans au moins **2 des 8 domaines** du CBK
Réduction d'expérience	**4 ans** avec diplôme universitaire 4 ans ou cert. équivalente
Option « Associate »	Passer l'examen **sans expérience** — devenir CISSP après 6 ans
Endossement requis	**Endorsement** par un CISSP existant après réussite
Validité de la certification	**3 ans** renouvelables via **CPEs** (40 CPE/an, 120 sur 3 ans)
AMF	Cotisation annuelle ISC2 : **~135 USD** (Annual Maintenance Fee)
Reconnaissance	**DoD 8570**, PCI-DSS, ISO 27001, NIST — gouvernements et corporations
Augmentation salariale	Moyenne +25 % après certification (ISC2 Workforce Study)
Communauté ISC2	**150 000+ CISSP** dans le monde

2. Profil du candidat

En tant que candidat au CISSP, vous développez et validez une expertise senior en cybersécurité couvrant les 8 domaines du CBK. Vous êtes capable de :

- **Concevoir** des programmes de sécurité enterprise.
- **Implémenter** les politiques de sécurité alignées business.
- Gérer la **gouvernance**, le risque et la **compliance (GRC)**.
- Appliquer les frameworks : **ISO 27001**, **NIST CSF**, **COBIT**.
- Classifier et protéger les **actifs** de l'organisation.
- Gérer le **data lifecycle** : creation, retention, destruction.
- Concevoir des **architectures sécurisées** end-to-end.
- Appliquer les **secure design principles** et threat modeling.
- Maitriser la **cryptographie** : symétrique, asymétrique, hashing, PKI.
- Sécuriser les **réseaux** : segmentation, firewalls, VPN, IDS/IPS.
- Maitriser l'**IAM** : authentication, authorization, SSO, MFA, federation.
- Concevoir des **contrôles d'accès** : RBAC, ABAC, MAC, DAC.
- Conduire des **audits** et **vulnerability assessments**.
- Gérer le **pentesting** et red teaming.
- Opérer un **SOC** et répondre aux incidents.
- **Disaster Recovery (DR)** et **Business Continuity (BC)**.
- Intégrer la sécurité dans le **SDLC** (SDLC sécurisé, DevSecOps).
- Maitriser **OWASP Top 10** et secure coding.

L'examen évalue spécifiquement les 8 domaines suivants :

- Security and Risk Management (gouvernance, conformité, risques).
- Asset Security (classification, protection des données).
- Security Architecture and Engineering (cryptographie, secure design).
- Communication and Network Security (protocoles, firewalls, VPN).
- Identity and Access Management (authentification, autorisation, SSO).
- Security Assessment and Testing (audits, pentesting).
- Security Operations (incident response, DRP, BCP, forensics).
- Software Development Security (SDLC, DevSecOps, OWASP).

3. Prérequis et public cible OpenCertif

Le CISSP exige une expérience professionnelle substantielle. ISC2 recommande :

- **5 ans minimum** d'expérience professionnelle rémunérée dans au moins **2 des 8 domaines** du CBK.
- **4 ans** avec diplôme universitaire 4 ans ou certification équivalente (ex : CISA, CISM, OSCP).
- Option **Associate of ISC2** : passer l'examen **sans expérience**, devenir CISSP en accumulant les 5 ans dans les 6 ans suivant.

- Compéhension approfondie des concepts **cybersécurité**.
- Expérience en **architecture de sécurité** et gestion de risques.
- Connaissance des standards : **ISO 27001**, **NIST**, **COBIT**, **ITIL**.
- Maitrise des concepts de **réseau**, OS, applications.
- **Anglais professionnel** obligatoire (examen CAT en anglais uniquement).

Public cible OpenCertif

- **RSSI** (Responsables de la Sécurité des Systèmes d'Information) / **CISO**.
- **Security architects** et **solutions architects** spécialisés.
- **Consultants en cybersécurité seniors** en cabinet ou freelance.
- **Directeurs IT** et **CTO** avec focus sécurité.
- **Auditeurs en sécurité informatique**.
- **Managers d'équipes** de sécurité.
- **Ingénieurs en sécurité** expérimentés.
- **Analystes en gestion de risques** IT.
- **SOC managers** et tech leads SOC.
- **DPO** (Data Protection Officers) en migration vers cyber.
- **Pentesters seniors** souhaitant valider le management side.
- **DevSecOps leaders**.
- Profils **CISA, CISM** souhaitant compléter avec CISSP.
- **Officiers militaires** spécialisés cyber (DoD 8570).
- Candidats aux postes **C-level** en cyber.

4. Domaines de compétences mesurées

L'examen est structuré autour de 8 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version 2026 — aligné sur ISC2 CISSP CBK 2024 / 2026). Les pondérations sont des estimations issues du guide officiel Unity / Certiport.

Domaine	Intitulé	Pondération
1	Security and Risk Management	16 %
2	Asset Security	10 %
3	Security Architecture and Engineering	13 %
4	Communication and Network Security	13 %
5	Identity and Access Management (IAM)	13 %
6	Security Assessment and Testing	12 %
7	Security Operations	13 %
8	Software Development Security	10 %

*Remarque : l'examen UCU Programmer dure environ 50 minutes pour 40 questions, soit environ 1 minute 15 par question. La gestion du temps est essentielle. Le score requis pour valider est de **500 sur 700** (sur une échelle officielle Unity de 200 à 700 points).*

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen CISSP, en s'appuyant sur les Objective Domains publiés par Certiport et Unity Technologies (version 2026 — aligné sur ISC2 CISSP CBK 2024 / 2026).

1 Security and Risk Management — 16 %

1.1 Concepts fondamentaux

- **CIA Triad** : Confidentiality, Integrity, Availability.
- **AAA** : Authentication, Authorization, Accounting.
- **Non-repudiation**, authenticity.
- **Risk** = Threat × Vulnerability × Impact.
- **Defense in depth**.

1.2 Gouvernance sécurité

- **Security policies**, standards, procedures, guidelines.
- **RACI matrix** : Responsible, Accountable, Consulted, Informed.
- Alignement business-sécurité.
- **Frameworks** : ISO 27001/27002, NIST CSF, COBIT 5, ITIL.
- Comité de pilotage sécurité.

1.3 Conformité et réglementations

- **RGPD** / GDPR (Europe).
- **HIPAA** (santé US).
- **PCI-DSS** (cartes bancaires).
- **SOX** (Sarbanes-Oxley).
- **NIS2** et DORA (Europe).
- **FISMA**, FedRAMP (US gov).

1.4 Risk Management

- **Risk assessment** : qualitative vs quantitative.
- **ALE = SLE × ARO** (Annual Loss Expectancy).
- **Risk treatment** : Accept, Avoid, Transfer, Mitigate.
- **Risk register** et monitoring.
- Threat modeling : **STRIDE**, **PASTA**, DREAD.

1.5 Business Continuity

- **BCP** (Business Continuity Plan).
- **BIA** (Business Impact Analysis).
- **RTO** et **RPO**.
- **MTBF**, MTTR.

1.6 Personnel security

- **Background checks**.
- **Security awareness training**.
- **Separation of duties**.
- **Least privilege**.
- **Mandatory vacation**, job rotation.
- **Termination procedures**.

1.7 Ethics professionals

- **ISC2 Code of Ethics**.
- Reporting violations.
- Conflict of interest.

2 Asset Security — 10 %

2.1 Classification des données

- **Public**, **Internal**, **Confidential**, **Restricted**.
- **Government** : Top Secret, Secret, Confidential, Unclassified.
- Labels et marquage.
- **Data owners**, custodians, users.

2.2 Data lifecycle

- **Create**, **Store**, **Use**, **Share**, **Archive**, **Destroy**.
- **Data retention** policies.
- **Data destruction** : wiping, degaussing, crushing.
- **NIST 800-88**.

2.3 Data protection

- **Data at rest** : disk encryption.
- **Data in transit** : TLS, IPSec.
- **Data in use** : memory encryption.
- **DLP** (Data Loss Prevention).

2.4 Privacy

- **PII**, **PHI**, **SPI**.
- Data subject rights (GDPR).
- **Privacy by design**.
- **Pseudonymization** et anonymization.

3 Security Architecture and Engineering — 13 %

3.1 Secure design principles

- **Zero Trust**.
- **Least privilege**.
- **Defense in depth**.
- **Fail secure** vs fail safe.
- **Trust but verify**.

3.2 Security models

- **Bell-LaPadula** (confidentiality).
- **Biba** (integrity).
- **Clark-Wilson** (integrity).
- **Brewer-Nash** (chinese wall).
- **Common Criteria** et EAL.

3.3 Cryptographie

- **Symmetric** : AES, 3DES, ChaCha20.
- **Asymmetric** : RSA, ECC, ECDSA.
- **Hashing** : SHA-256, SHA-3, BLAKE2.
- **HMAC**, digital signatures.
- **PKI** : CA, RA, certificates X.509.
- **Quantum cryptography** et post-quantum.

3.4 Cloud security

- **Shared responsibility model**.
- **SaaS**, **PaaS**, **IaaS**.
- **CASB** (Cloud Access Security Broker).
- **SASE**, **SSE**.
- Container security : K8s, Docker.

3.5 Physical security

- **CPTED** (Crime Prevention Through Environmental Design).
- Fire suppression : FM200, dry pipe.
- Access controls : **mantraps**, badges, biométrie.
- Environmental : HVAC, power, UPS.

4 Communication and Network Security — 13 %

4.1 OSI et TCP/IP

- **7 layers OSI**.
- **4 layers TCP/IP**.
- Protocols par layer.

4.2 Protocols

- **HTTPS**, TLS 1.3, mTLS.
- **SSH**, SFTP, SCP.
- **IPSec**, GRE, MPLS.
- **DNS Sec**, DoH, DoT.
- **802.1X**, RADIUS, TACACS+.

4.3 Network segmentation

- **VLANs**, **microsegmentation**.
- **DMZ**, internal zones.
- **Zero Trust Network Access (ZTNA)**.
- **SDN** et NFV.

4.4 Firewalls et IDS/IPS

- **Stateful** vs **stateless** firewalls.
- **NGFW** (Next Gen Firewall).
- **WAF** (Web Application Firewall).
- **IDS**, **IPS**, **NIDS**, **HIDS**.
- **SIEM** integration.

4.5 VPN et remote access

- **Site-to-site VPN** : IPSec.
- **Remote access VPN** : SSL VPN.
- **Always-on VPN**.
- **SASE** et SSE.

4.6 Wireless security

- **WPA3**, WPA2.
- **802.11i**.
- **Bluetooth** security.
- **NFC**, RFID.
- Rogue APs, evil twin.

5 Identity and Access Management (IAM) — 13 %

5.1 Identification et Authentication

- **Something you know** : password.
- **Something you have** : token, smart card.
- **Something you are** : biométrie.
- **Somewhere you are** : location.
- **Something you do** : behavior.
- **MFA** (Multi-Factor Authentication).

5.2 Authorization models

- **RBAC** (Role-Based Access Control).
- **ABAC** (Attribute-Based).
- **MAC** (Mandatory Access Control).
- **DAC** (Discretionary).
- **Rule-based**.

5.3 Federation et SSO

- **SAML 2.0**.
- **OAuth 2.0**, **OIDC**.
- **JWT** tokens.
- **Kerberos**.
- **LDAP**, Active Directory.

5.4 PAM (Privileged Access Management)

- **Vaulting** de credentials privilégiés.
- **Just-in-time** access.
- **Session recording**.
- **Break glass** procedures.

5.5 Identity lifecycle

- **Provisioning** et deprovisioning.
- **Joiner / Mover / Leaver**.
- **Access reviews**.
- **SoD** (Separation of Duties).

6 Security Assessment and Testing — 12 %

6.1 Vulnerability assessment

- **Scanning** : Nessus, Qualys, OpenVAS.
- **CVE** et **CVSS** scoring.
- Prioritization.
- **Patch management**.

6.2 Penetration testing

- **Black box**, **white box**, **grey box**.
- **Reconnaissance**, scanning, exploitation, post-exploitation.
- **PTES** methodology.
- **OWASP Testing Guide**.
- **Red team** vs **blue team** vs **purple team**.

6.3 Audits

- **Internal** vs **external** audits.
- **SOC 2** Type I et II.
- **ISO 27001** certification.
- **PCI-DSS** assessment (QSA).

6.4 Continuous monitoring

- **SIEM** : Splunk, QRadar, Sentinel, Chronicle.
- **SOAR** : automatisation.
- **UEBA** (User and Entity Behavior Analytics).
- **Threat hunting**.

7 Security Operations — 13 %

7.1 SOC operations

- **SOC tiers** : 1, 2, 3.
- **Playbooks** et runbooks.
- **Threat intelligence**.
- **MITRE ATT&CK;** framework.

7.2 Incident Response

- **NIST SP 800-61** phases : Preparation, Detection, Containment, Eradication, Recovery, Lessons Learned.
- **IRP** (Incident Response Plan).
- **CERT** / CSIRT.
- **Tabletop exercises**.
- Communication interne et externe.

7.3 Forensics

- **Chain of custody**.
- **Digital forensics** tools : Autopsy, FTK, EnCase.
- Memory forensics : Volatility.
- Network forensics : Wireshark, Zeek.
- **Evidence preservation**.

7.4 Disaster Recovery

- **DRP** (Disaster Recovery Plan).
- **RTO/RPO** targets.
- Hot site, warm site, cold site.
- **Backup strategies** : 3-2-1 rule.
- DR testing : tabletop, walkthrough, simulation, parallel, full interruption.

7.5 Logging et monitoring

- **Log aggregation**.
- **Log retention** per compliance.
- **Time synchronization (NTP)**.
- **Centralized logging**.

8 Software Development Security — 10 %

8.1 SDLC sécurisé

- **Secure SDLC** : security à chaque étape.
- **Waterfall**, **Agile**, **DevOps**.
- **DevSecOps** et shift-left security.
- **Threat modeling** en design.

8.2 Secure coding

- **OWASP Top 10** : Injection, Broken Auth, XSS, CSRF, etc.
- **Input validation** et output encoding.
- **Authentication** et session management.
- **Cryptographic storage**.
- **Error handling** approprié.

8.3 Application testing

- **SAST** (Static Application Security Testing).
- **DAST** (Dynamic).
- **IAST** (Interactive).
- **SCA** (Software Composition Analysis).
- **Fuzz testing**.
- Code reviews.

8.4 API security

- **OWASP API Top 10**.
- **OAuth** et OIDC pour APIs.
- Rate limiting et throttling.
- API gateways.

8.5 Container et CI/CD security

- Image scanning : **Trivy**, Clair, Snyk.
- **Kubernetes** security.
- **Secrets management** : Vault.
- **Supply chain security**.
- **SBOM** (Software Bill of Materials).

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au CISSP à travers un parcours blended-learning complet, combinant ressources e-learning interactives, projets pratiques en GRC, IAM, cryptographie, architecture sécurité, network security, IR/DR, DevSecOps et 8 domaines CBK et accompagnement tutoré.

Format de la formation

Durée recommandée	**200 à 400 heures de préparation** recommandées (6 à 12 mois selon expérience). OpenCertif structure ce parcours sur 100 à 150 heures de formation tutorée expert complétées par 100 à 250 heures d'auto-formation et examens blancs
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Unity Certified User Courseware officiel (GMetrix) + ressources OpenCertif (modules Rise 360, scénarios immersifs)
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert Unity certifié + classes virtuelles bimensuelles
Pratique requise	Au moins 150 heures de pratique Unity (recommandation officielle Unity Technologies)
Évaluations	Quiz formatifs par module, 3 projets pratiques Unity, examens blancs CertPREP
Certification finale	Passage de l'examen CISSP en centre OpenCertif (CATC Certiport)

Parcours d'apprentissage proposé

- **Module 1 :** CIA Triad, AAA, defense in depth.
- **Module 2 :** Frameworks : ISO 27001, NIST CSF, COBIT.
- **Module 3 :** RGPD, HIPAA, PCI-DSS, NIS2.
- **Module 4 :** Risk management quantitatif et qualitatif.
- **Module 5 :** Business Continuity et BIA.
- **Module 6 :** Personnel security et awareness.
- **Module 7 :** ISC2 Code of Ethics.
- **Module 8 :** Data classification et lifecycle.

- **Module 9 :** Data protection : at rest, in transit, in use.
- **Module 10 :** Privacy : PII, PHI, GDPR.
- **Module 11 :** Secure design principles et Zero Trust.
- **Module 12 :** Security models : Bell-LaPadula, Biba, Clark-Wilson.
- **Module 13 :** Cryptography : symétrique, asymétrique, hashing, PKI.
- **Module 14 :** Cloud security et shared responsibility.
- **Module 15 :** Physical security et CPTED.
- **Module 16 :** OSI / TCP/IP et protocols.
- **Module 17 :** Network segmentation et microsegmentation.
- **Module 18 :** Firewalls, IDS/IPS, WAF.
- **Module 19 :** VPN et SASE.
- **Module 20 :** Wireless security : WPA3, 802.11i.
- **Module 21 :** IAM : MFA, federation, SSO.
- **Module 22 :** Authorization models : RBAC, ABAC, MAC, DAC.
- **Module 23 :** SAML, OAuth, OIDC, Kerberos.
- **Module 24 :** PAM et privileged access.
- **Module 25 :** Vulnerability assessment et CVSS.
- **Module 26 :** Pentesting : black, white, grey box.
- **Module 27 :** Audits SOC 2, ISO 27001, PCI-DSS.
- **Module 28 :** SIEM, SOAR, UEBA.
- **Module 29 :** SOC operations et MITRE ATT&CK.;
- **Module 30 :** Incident Response NIST SP 800-61.
- **Module 31 :** Digital forensics et chain of custody.
- **Module 32 :** Disaster Recovery : hot/warm/cold sites.
- **Module 33 :** SDLC sécurisé et DevSecOps.
- **Module 34 :** OWASP Top 10 et secure coding.
- **Module 35 :** SAST, DAST, IAST, SCA.
- **Module 36 :** API et container security.
- **Module 37 :** Tests blancs CISSP Boson + Sybex.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources officielles Unity Technologies et Certiport suivantes sont fortement recommandées :

- Site officiel ISC2 : **isc2.org**.
- **CISSP CBK Official Study Guide** (Sybex) — référence absolue.
- **CISSP Official Practice Tests** (Sybex).
- **(ISC)² CISSP Study App** (officielle).
- **Eleventh Hour CISSP** (Eric Conrad) — révisions express.
- **Boson CISSP Practice Exams** — examens blancs réputés.
- **Adam Gordon CISSP Mind Maps** — révisions visuelles.
- **Pete Zerger CISSP YouTube** (gratuit, excellent).
- **Destination Certification** Rob Witcher CISSP MasterClass.
- **CISSP Reddit** : r/cissp (communauté active).
- **Certification Station** (Discord et forums).
- **Cybrary** et **Pluralsight** CISSP courses.
- Réservation Pearson VUE : **home.pearsonvue.com**.
- Endorsement assistance : ISC2 community.
- **CPE submissions** : isc2.org / Members.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement auprès d’un centre Certiport
Centre d’examen	OpenCertif — Centre Certiport Authorized Testing Center (CATC) / Pearson VUE
Mode de passage	En centre uniquement (Unity n’autorise pas l’examen OnVUE à distance pour les certifications UCU — présence sur site requise)
Pièce d’identité	1 pièce d’identité avec photo obligatoire le jour de l’examen (pour les mineurs : autorisation parentale et CNI / passeport)
Aménagements	Demande possible auprès de Certiport (temps additionnel, assistance technique)
Résultat	Score communiqué immédiatement à la fin de l’examen (échelle 200-700, seuil de réussite 500)

Validité de la certification	3 ans à partir de la date de réussite — attribuée une seule fois (stackable, pas de renouvellement payant requis)
Politique de reprise	Délai d’attente de 24 heures avant la 1re reprise. Voucher retake à utiliser sous 60 jours après l’échec.
Badge numérique	Badge officiel délivré via Credly et intégrable à LinkedIn, CV, portfolio, sites de recrutement

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au CISSP, l'équipe OpenCertif reste à votre disposition. OpenCertif est un Centre Certiport Authorized Testing Center (CATC) habilité à délivrer les certifications Unity Certified User.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base des Objective Domains officiels publiés par Certiport pour la certification CISSP, dans sa version applicable (version 2026 — aligné sur ISC2 CISSP CBK 2024 / 2026). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Unity Technologies via Certiport.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle Certiport : certiport.pearsonvue.com/Certifications/Unity/Certified-User/Certify
Source officielle Unity : unity.com/products/unity-certifications/user-programmer

Page OpenCertif : opencertif.fr/unity-user-programmer