



## Formation

Cette formation a pour but de préparer les candidats à l'examen du CISA (Certified Information Systems Auditor), la certification internationale délivrée par l'ISACA, examen qui se déroule chaque année en juin et décembre.

**Attention :** Elle n'est en aucun cas une formation à l'audit du système d'information, L'inscription à cette formation est totalement indépendante de celle à l'examen qui doit se faire sur le site de l'**ISACA** (<http://www.isaca.org>).

Titre	<b>CISA ( Certified Information Systems Auditor)</b>
Durée	5 jours soit 35 heures et 8 heures de travail individuel à réaliser le soir après les cours.
Langue	Français
Coût	230 000 da HT demi pension <ul style="list-style-type: none"> <li><input type="checkbox"/> Les frais d'examen ne sont pas compris dans le prix de cette session,</li> <li><input type="checkbox"/> Le Support de formation et le Manuel Officiel de préparation au CISA sont fournis au démarrage de la session de formation,</li> </ul>
Objectifs	<ul style="list-style-type: none"> <li><input type="checkbox"/> Analyser les différents domaines du programme sur lequel porte l'examen,</li> <li><input type="checkbox"/> Assimiler le vocabulaire et les idées directrices de l'examen,</li> <li><input type="checkbox"/> S'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire.</li> </ul>
Public concerné	<ul style="list-style-type: none"> <li><input type="checkbox"/> Auditeurs confirmés ou informaticiens (DSI, Ingénieurs, Experts Consultants) qui souhaitent obtenir la certification CISA (Certified Information Systems Auditor) délivrée par l'ISACA, et préparer l'examen. Celui-ci dure 4 heures et utilise un questionnaire constitué de 200 questions portant sur l'ensemble des domaines relevant de l'audit du système d'information. Réussite à l'examen avec au moins un score de 450 points sur 800 (*).</li> </ul>
Contenu	<p style="text-align: center;"><b>Programme</b></p> <p>Le programme du séminaire suit les 6 domaines définis pour l'examen :</p> <p><b>JOUR 1 :</b></p> <p><b>Domaine 1 :</b> Processus d'audit des SI</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Les standards d'audit,</li> <li><input type="checkbox"/> L'analyse de risque et le contrôle interne,</li> <li><input type="checkbox"/> La pratique d'un audit SI.</li> </ul> <p><b>Domaine 2 :</b> Gouvernance des SI</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Stratégie de la gouvernance du SI,</li> <li><input type="checkbox"/> Procédures et Risk management,</li> <li><input type="checkbox"/> La pratique de la gouvernance des SI,</li> <li><input type="checkbox"/> L'audit d'une structure de gouvernance.</li> </ul> <p><b>JOUR 2</b></p> <p><b>Domaine 3 :</b> Gestion du cycle de vie des systèmes et de l'infrastructure</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Gestion de projet : pratique et audit,</li> <li><input type="checkbox"/> Les pratiques de développement,</li> <li><input type="checkbox"/> L'audit de la maintenance applicative et des systèmes,</li> <li><input type="checkbox"/> Les contrôles applicatifs.</li> </ul>



Contenu du programme (suite)	<p><b>JOUR 3</b></p> <p><b>Domaine 4</b> : Fourniture et support des services</p> <ul style="list-style-type: none"> <li>☒ Audit de l'exploitation des SI,</li> <li>☒ Audit des aspects matériels du SI,</li> <li>☒ Audit des architectures SI et réseaux.</li> </ul> <p><b>JOUR 4</b></p> <p><b>Domaine 5</b> : Protection des avoirs informatiques</p> <ul style="list-style-type: none"> <li>☒ Gestion de la sécurité : politique et gouvernance,</li> <li>☒ Audit et sécurité logique et physique,</li> <li>☒ Audit de la sécurité des réseaux,</li> <li>☒ Audit des dispositifs nomades.</li> </ul> <p><b>JOUR 5</b></p> <p><b>Domaine 6</b> : Plan de continuité et plan de secours informatique</p> <ul style="list-style-type: none"> <li>☒ Les pratiques des plans de continuité et des plans de secours,</li> <li>☒ Audit des systèmes de continuité et de secours.</li> </ul> <p>Dans chaque exposé, l'accent sera mis sur les éléments organisationnels et technologiques fondamentaux et leurs impacts sur la stratégie d'audit en termes de validité et d'exhaustivité des éléments audités conformément à l'approche ISACA.</p>
Méthode	<ul style="list-style-type: none"> <li>☒ Un <b>questionnaire d'auto-évaluation</b> sur les différents domaines vous est proposé avant votre inscription à l'examen pour vous permettre d'évaluer éventuellement vos lacunes et y remédier en suivant une formation sur la sécurité, la sécurité des réseaux et Internet que vous propose <b>SecuCERT</b>,</li> <li>☒ Ensemble d'exposés couvrant chaque domaine du programme de l'examen.</li> <li>☒ A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISA (ou d'examens comparables).</li> <li>☒ Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.</li> </ul>
Lieu de l'examen	Voir sur le site <a href="http://www.isaca.org">http://www.isaca.org</a>
Bénéfice attendus de la formation	<ul style="list-style-type: none"> <li>☒ Reconnaissance Internationale des compétences en audit des systèmes d'information,</li> <li>☒ Savoir dialoguer avec le management pour la mise en oeuvre des mesures de sécurité pertinentes à l'atteinte des objectifs Business,</li> <li>☒ Appréhender le rôle de l'Auditeur des SI dans l'organisation.</li> </ul>
Intervenant	Les sessions sont animées par des Experts Seniors certifiés CISA, CISM, CBCP, CISSP®, Lead Auditor : ISO/CEI 27001 et Risk Manager : ISO/CEI 27005.
Mode	Formation inter – entreprises
Pré-requis	<ul style="list-style-type: none"> <li>☒ Il est vivement recommandé aux auditeurs peu habitués à la problématique des réseaux et de la sécurité de suivre au préalable le séminaire.</li> <li>☒ La compréhension de l'anglais est nécessaire car la documentation fournie aux participants est en anglais.</li> </ul>

Nb Consulting Siège Social : N°8 Lotissement El-Fadjre, Batna , ALGERIE

Site Web : [www.nb-consulting-dz.com](http://www.nb-consulting-dz.com) /E-mail : nb.consulting.informatique@gmail.com

[contact@nb-consulting-dz.com](mailto:contact@nb-consulting-dz.com)

Tel : +213 (0)558 13 18 88/ Fax : +213(0)33 85 43 85

N°Immatriculation Au RC 1159892/11 رقم التسجيل