

Professional Evaluation and Certification Board

recognizes that

Business and Information Technology - BIT

is officially approved as

Authorized Platinum Partner

Certificate number: ATP250053
Performance period: 2025-01-01 to 2025-12-31
Valid until: December 31, 2026

Tim Rama
CEO

ISO27001 Lead Implementer Certification

Du 14 au 17 Décembre 2026

Introduction

La formation certifiante *ISO27001 lead implementer* permet aux participants de maîtriser la mise en œuvre et la gestion d'un système de management de la sécurité de l'information (SMSI), conforme à la norme ISO/IEC 27001 :2022

Résumé de la Formation

La formation certifiante ISO27001 Lead Implementer permet aux participants de développer l'expertise nécessaire pour assister une organisation dans la mise en œuvre et la gestion d'un Système de Management de la Sécurité de l'Information (SMSI) tel que spécifié dans l'ISO/CEI 27001:2022. Les participants pourront aussi acquérir des bases solides concernant les bonnes pratiques utilisées pour la mise en œuvre des mesures de la sécurité de l´information à partir des domaines de l'ISO 27002:2022. Cette formation est pleinement compatible avec les normes ISO27003 (Lignes directrices pour l'implémentation d'un SMSI), ISO 27004 (Mesure de la sécurité de l'information) et ISO27005 (Gestion des risques liés à la sécurité de l'information).

Objectifs de la Formation

- Comprendre la mise en œuvre d'un Système de Management de la Sécurité de l'Information conforme à l'ISO 27001 :2022
- Acquérir une compréhension globale des concepts, démarches, normes, méthodes et techniques nécessaires pour gérer efficacement un Système de Management de la Sécurité de l'Information
- Acquérir l'expertise nécessaire pour assister une organisation dans la mise en œuvre, la gestion et le maintien d'un SMSI, tel que spécifié dans l'ISO 27001
- Acquérir l'expertise nécessaire pour gérer une équipe de mise en œuvre d'ISO 27001

Public visé

La formation s'adresse aux :

- Responsables de la Sécurité du Système de l'Information (RSSI)
- Gestionnaires de projets de conformité
- Gestionnaires des Risques
- Conseillers experts en technologies de l'information
- Auditeurs ISO 27001 internes et externes
- Membres d'une équipe de sécurité de l'information

Informations Générales sur la Formation et l'examen

- ✓ Cette formation permet aux participants d'avoir la certification ISO 27001 Lead Implementer
- ✓ La formation est donnée en français et un support (cours, exercices, corrigés) en français sera remis à chaque participant.
- ✓ Chaque session est limitée à un maximum de **15 personnes**
- ✓ L'examen est en français

Organisme de certification des personnes

PECB - «Professional Evaluation and Certification Board (PECB) », est un organisme de certification de personnes accrédité selon la norme ISO/IEC 17024 − Exigences générales pour les organismes procédant à la certification des personnes.

Principaux organismes d'accréditation de PECB (ISO/IEC 17024)

- **IAS** (International Accreditation Service) – réf. IAS-PCB-111
- **UKAS** (United Kingdom Accreditation Service) – réf. UKAS-No. 21923
- **COFRAC** (Comité français d'accréditation) – réf. COFRAC N° 4-0637 [1]

Travaux pratiques :

Par des exercices réalisés en séance et des discussions, les participants seront capables de comprendre comment mettre en place un système de management de la sécurité de l'information selon la norme ISO 27001

Formatrice

Sonia Kallel, certifiée ISO 27001 LI et LA et certifiée PECB Formatrice, est consultante experte et auditrice tierce partie en sécurité des systèmes d'informations et détient plusieurs références dans la mise en place et l'audit de la sécurité de l'information et l'analyse des risques en Tunisie et à l'étranger.

Programme détaillé de la Formation

Jour 1: Introduction au concept de Système de Management de la Sécurité de l'Information (SMSI) tel que défini par l'ISO 27001; Initialisation d'un SMSI

▸ Introduction aux systèmes de management et à l'approche processus

▸ Présentation de la suite des normes ISO 27000 ainsi que du cadre normatif, légal et réglementaire

▸ Principes fondamentaux de la sécurité de l'information

▸ Analyse préliminaire et détermination du niveau de maturité d'un système de management de sécurité de l'information existant

▸ Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI

Exercices

Jour 2: Planifier la mise en œuvre d'un SMSI basé sur l'ISO 27001

▸ Définition du périmètre (domaine d'application) du SMSI

▸ Développement de la politique et des objectifs du SMSI

▸ Sélection de l'approche et de la méthode d'évaluation des risques

▸ Gestion des risques: identification, analyse et traitement du risque (d'après les dispositions de l'ISO 27005)

▸ Rédaction de la Déclaration d'Applicabilité

Exercices

Jour 3: Mettre en place un SMSI basé sur l'ISO 27001

- Mise en place d'une structure de gestion de la documentation
- Conception et implémentation des mesures de sécurité
- Développement d'un programme de formation et de sensibilisation, et communication à propos de la sécurité de l'information
- Gestion des incidents (d'après les dispositions de l'ISO 27035)
- Gestion des opérations d'un SMSI

Exercices

Jour 4 : Contrôler, surveiller, mesurer et améliorer un SMSI conformément à la norme ISO 27001

- Contrôler les mesures de sécurité du SMSI
- Développement de mesures, d'indicateurs de performance et de tableaux de bord conformes à l'ISO 27004
- Audit interne ISO 27001
- Revue du SMSI par les gestionnaires
- Mise en œuvre d'un programme d'amélioration continue
- Préparation à l'audit de certification ISO 27001

Exercices

Jour 5 : Examen de certification