LSI Learny Society International

IA / CYBER / TECH

PROGRAMME DE FORMATION

Gouvernance & conformité cyber

Relier cyber-risque, gouvernance et obligations.

DURÉE	PUBLIC	FORMAT
28 h	**Professionnels et apprenants concernés par le parcours ; adaptation au secteur possible.**	**Présentiel · Distanciel · Hybride**

Ce que vous allez savoir faire

- Relier cyber-risque, gouvernance et obligations
- Comprendre RGPD, ISO 27001 et NIS2
- Construire un plan de conformité proportionné

Votre formation, en un coup d’œil

Durée	28 h	**Public**	Professionnels et apprenants concernés par le parcours ; adaptation au secteur possible.
Prérequis	Positionnement / expérience professionnelle selon le niveau.	**Modalités**	Présentiel, classe virtuelle ou hybride selon la proposition.
Tarif	Sur devis - prix et modalités communiqués avant engagement.	**Délai d’accès**	Réponse initiale sous 48 à 72 h ouvrées ; démarrage selon calendrier et financement.

Objectifs pédagogiques

- Relier cyber-risque, gouvernance et obligations
- Comprendre RGPD, ISO 27001 et NIS2
- Construire un plan de conformité proportionné

Résultats attendus

À l’issue du parcours, le bénéficiaire doit pouvoir mobiliser les compétences décrites ci-dessus et les appliquer dans les exercices, simulations ou productions prévus. Les critères de réussite sont observables dans le scénario pédagogique.

Statut / certification

Action de formation professionnelle donnant lieu à une attestation de fin de formation / réalisation et à un bilan des acquis. Aucune certification RNCP/RS ni grade académique n’est inclus par défaut, sauf mention explicite dans la proposition contractuelle.

Le parcours LSI

01 Diagnostic
Niveau, besoin, contraintes.

02 Proposition
Programme, formateur, calendrier.

03 Déploiement
Présentiel, distanciel ou hybride.

04 Évaluation
Acquis, attestation et bilan.

Programme détaillé

Chaque séquence est conçue pour produire un apprentissage observable. Les cas, exemples et outils peuvent être contextualisés au secteur du client sans réduire les objectifs ni la durée contractualisée.

Cours 1 · 7 h · Gouvernance SSI

Objectif du cours : Analyser et traiter « Gouvernance SSI » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Gouvernance SSI Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - SMSI Comprendre SMSI, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - risk treatment / Statement of Applicability Comparer risk treatment et Statement of Applicability dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - NIS2 art. 21 Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Réponse - incident reporting Construire une mesure technique/opérationnelle autour de incident reporting et définir son owner.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	Exercice table-top - preuves d'audit Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H7	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Référentiel / vigilance : Références : ISO/IEC 27001:2022, NIST CSF 2.0, NIS2. NIS2 impose notamment gouvernance, gestion des risques, incident, continuité, supply chain, vulnérabilités, cyber-hygiène, cryptographie, RH/accès et MFA selon le périmètre.

Cours 2 · 7 h · Gestion des risques et registres de contrôles

Objectif du cours : Analyser et traiter « Gestion des risques et registres de contrôles » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - Gestion des risques et registres de contrôles Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - SMSI Comprendre SMSI, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - risk treatment / Statement of Applicability Comparer risk treatment et Statement of Applicability dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - NIS2 art. 21 Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Réponse - incident reporting Construire une mesure technique/opérationnelle autour de incident reporting et définir son owner.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	Exercice table-top - preuves d'audit Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H7	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Référentiel / vigilance : Références : ISO/IEC 27001:2022, NIST CSF 2.0, NIS2. NIS2 impose notamment gouvernance, gestion des risques, incident, continuité, supply chain, vulnérabilités, cyber-hygiène, cryptographie, RH/accès et MFA selon le périmètre.

Cours 3 · 7 h · RGPD

Objectif du cours : Analyser et traiter « RGPD » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - RGPD Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - SMSI Comprendre SMSI, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - risk treatment / Statement of Applicability Comparer risk treatment et Statement of Applicability dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - NIS2 art. 21 Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Réponse - incident reporting Construire une mesure technique/opérationnelle autour de incident reporting et définir son owner.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	Exercice table-top - preuves d'audit Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H7	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Référentiel / vigilance : Références : ISO/IEC 27001:2022, NIST CSF 2.0, NIS2. NIS2 impose notamment gouvernance, gestion des risques, incident, continuité, supply chain, vulnérabilités, cyber-hygiène, cryptographie, RH/accès et MFA selon le périmètre.

Cours 4 · 7 h · ISO 27001

Objectif du cours : Analyser et traiter « ISO 27001 » avec une approche risque, des contrôles proportionnés et des preuves de mise en œuvre.

SÉQ.	SOUS-SECTION / CONTENU	PREUVE / CRITÈRE
H1	Scénario de menace - ISO 27001 Identifier actifs, dépendances, menace, vulnérabilité, impact et niveau de risque.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H2	Contrôle - SMSI Comprendre SMSI, conditions d'efficacité, limites et preuve de mise en œuvre.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H3	Contrôle - risk treatment / Statement of Applicability Comparer risk treatment et Statement of Applicability dans une défense en profondeur.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H4	Lab / logs - NIS2 art. 21 Analyser une configuration, un journal ou une chronologie d'incident et identifier anomalies/écarts.	Production/score LMS + justification. Réussite : critères de la tâche atteints sur au moins 3/4 dimensions.
H5	Réponse - incident reporting Construire une mesure technique/opérationnelle autour de incident reporting et définir son owner.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H6	Exercice table-top - preuves d'audit Prendre des décisions sous contrainte de temps, disponibilité et communication.	Lab ou analyse documentée. Réussite : mécanisme/risque correctement expliqué et choix défendu par au moins 2 critères.
H7	After-action review Produire constats, causes, actions prioritaires, responsables, échéances et éléments de preuve.	Grille finale + livrable/performance + action de transfert. Réussite : ≥3/4 critères majeurs au niveau attendu.

Référentiel / vigilance : Références : ISO/IEC 27001:2022, NIST CSF 2.0, NIS2. NIS2 impose notamment gouvernance, gestion des risques, incident, continuité, supply chain, vulnérabilités, cyber-hygiène, cryptographie, RH/accès et MFA selon le périmètre.

Modalités pédagogiques et qualité

Méthodes mobilisées

- Positionnement initial et contextualisation aux situations de travail du bénéficiaire.
- Apports ciblés, démonstrations, exercices guidés et entraînement progressif.
- Mises en situation, études de cas, simulations ou productions concrètes selon le domaine.
- Feedback du formateur, correction par critères observables et plan de progression.
- Ressources numériques / LMS lorsque prévues dans le scénario pédagogique.

Moyens pédagogiques et techniques

- Supports formateur, fiches de travail, études de cas et ressources décrites dans le scénario pédagogique.
- En distanciel : visioconférence et espace numérique / LMS ; ordinateur, connexion internet, micro et audio requis côté bénéficiaire.
- Assistance technique et pédagogique appropriée pendant les séquences à distance ; les activités et leurs durées sont indiquées dans le parcours.
- En présentiel : salle adaptée, accès aux supports, outils de projection et connexion lorsque les exercices le nécessitent.

Suivi de l’exécution

- Feuilles d’émargement ou traces de connexion selon la modalité.
- Productions, quiz, exercices, simulations et/ou dépôts LMS servant de preuves d’activité.
- Suivi des absences et échanges avec le bénéficiaire / commanditaire lorsque nécessaire.

Évaluation des acquis

mise en situation ou livrable final évalué avec grille de critères et plan de progression.

- Positionnement ou diagnostic initial lorsque le niveau de départ conditionne le parcours.
- Évaluations formatives pendant les cours et feedback correctif.
- Évaluation finale par test, étude de cas, simulation, production ou examen blanc selon la formation.
- Bilan des acquis communiqué au bénéficiaire ; attestation de fin de formation / réalisation.

Indicateurs de résultats

Indicateurs spécifiques à cette référence : données historiques non consolidées dans le référentiel au 05/09/2026. LSI suit a minima l’assiduité, la satisfaction, l’atteinte des objectifs et, lorsqu’un examen externe est préparé, le résultat communiqué par les candidats. Les indicateurs sont publiés dès qu’un volume de cohortes permet une lecture pertinente.

Accès, organisation et accessibilité

Modalités d’accès	Prise de contact -> diagnostic / positionnement -> proposition pédagogique et financière -> validation administrative -> planification.
Délai d’accès	Réponse initiale sous 48 à 72 h ouvrées annoncée par LSI. Le délai réel jusqu’au démarrage dépend des disponibilités, du financement et du calendrier convenu.
Horaires / calendrier	Dates, horaires et rythme détaillés communiqués dans la proposition, la convention ou la convocation avant inscription définitive.
Formateur(s)	Sélectionnés selon expertise métier / linguistique et expérience pédagogique. Identité et éléments utiles communiqués avant inscription définitive.
Accessibilité handicap	Besoins d’aménagement recueillis dès le diagnostic. Adaptations pédagogiques, techniques ou organisationnelles étudiées ; orientation vers un partenaire compétent si nécessaire.
Contact	Marcus Détrez - Fondateur LSI Education - marcus@lsi-education.com - lsi-society.com/contact
Tarif / règlement	Sur devis. Modalités de règlement dans le devis ou la convention. Les conditions financières applicables aux personnes physiques finançant elles-mêmes leur formation sont remises avant engagement.
Règlement intérieur	Le règlement intérieur applicable à la formation est mis à disposition avant inscription définitive.
Référent commanditaire	Pour les formations commandées par une organisation, les coordonnées de la personne chargée des relations avec les stagiaires côté commanditaire figurent dans les documents de session.

À FINALISER AVANT USAGE CONTRACTUEL	Identité juridique complète, SIRET, NDA, référent handicap nominatif si distinct, calendrier de session, formateurs affectés et tarifs chiffrés. Ces données ne sont pas inventées dans la plaquette.

Cadre de référence

- Code du travail, art. L6353-8 : informations mises à disposition avant inscription définitive.
- Code du travail, art. D6353-1 : mentions applicables aux conventions de formation.
- Code du travail, art. D6313-3-1 : exigences spécifiques aux actions réalisées en tout ou partie à distance.
- Référentiel national qualité - Guide de lecture Qualiopi, critère 1 / indicateur 1.
- Cette plaquette ne remplace pas le devis, la convention/contrat, la convocation ni le règlement intérieur.

POUR ALLER PLUS LOIN

Catalogue LSI
Programmes, parcours et demande de devis :
lsi-society.com/formations