Lisis Conseil

CATALOGUE DES FORMATIONS

Formations sur catalogue ou sur-mesure

Formations inter ou intra entreprises

Promotions pour les adhérents du Clusif

Pour tout programme sur-mesure, nous contacter directement.

Inscriptions aux formations sur: www.lisis-conseil.com

Sécurité des Systèmes d'information

LISIS CONSEIL

8 bis avenue Lily
78170 La Celle Saint Cloud
France

Lisis Conseil

Formations Tous Publics

Sensibilisation à la cybersécurité

1 jour

Participants

Tous les utilisateurs ayant accès au système d'information

Pré-requis

Aucune connaissance particulière.

Objectifs

Présenter les risques pouvant porter atteinte à la sécurité du système d'information. Expliquer et justifier les contraintes de sécurité imposées par la politique de sécurité. Découvrir et comprendre les principales mesures de protection mises en place dans l'entreprise.

Dates des sessions

Nous consulter.

Programme détaillé

La sécurité informatique : les menaces

- Les composantes d'un SI et leurs vulnérabilités
- Menaces

Les mesures de protection

- La protection de l'information
- Les mesures de sécurité demandées aux collaborateurs: postes de travail, accès, données, déplacements, ...
- Les moyens de protection mis en place par la DSI et les autres services contributeurs

La démarche de sécurité du SI pour une entreprise

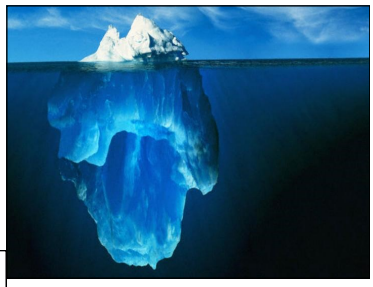
- Analyse des risques, des vulnérabilités et des menaces.
- contraintes légales et réglementaires.
- Pourquoi respecter les exigences de sécurité.
- le rôle du RSSI et du Risk manager.

Droits et devoirs vis-à-vis de la sécurité des SI

- Les aspects sociaux et juridiques. La CNIL, la législation.
- La cyber-surveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.

Lisis Conseil

Formations
Direction des risques



Analyse et gestion des risques
liés à la sécurité des systèmes d'informations

2 jours

Participants
Direction des risques
DSI ou responsable du service informatique.
Responsable sécurité du système d'information (RSSI).
Chef de projet informatique en charge du projet sécurisation.

Pré-requis
Cette formation ne nécessite pas de pré requis.

Objectifs
Apprendre à identifier les risques qui portent sur le système d'information.
Connaitre les principales normes et méthodes d'analyse des risques.
Elaborer et cibler son plan Sécurité des S.I par l'approche risques.

Dates des sessions
Nous consulter.

Programme détaillé

La notion de risque en sécurité des informations:
- Menace, vulnérabilité, potentialité, impact, gravité
- Les types de risques
- la gestion par les risques: principes, avantages

L'identification des biens informationnels
- L'inventaire des biens: organisation, périmètre
- La classification DICT: intérêts, méthode.

L'analyse de risque
- Identification des menaces, des vulnérabilités et des risques.
- Priorisation : la matrice des risques

Les méthodologies utiles
- méthodes françaises: EBIOS, MEHARI
- méthodes internationales
- avantages, inconvénients, choix , personnalisation

Les normes
- La démarche d'analyse de risques dans le cadre 27001, l'approche PDCA
- ISO 27005 : les apports

La gestion des risques
- la palette des actions : prévention, protection, report de risque, externalisation, assurances
- construction du plan de traitement des risques : à partir de la matrice des risques et des autres sources (audits, incidents)

Les chapitres sont illustrés d'exemples concrets et d'une étude de cas complète.

Lisis Conseil

Formations
Responsables Sécurité des S.I

Devenir RSSI

4 jours

Participants
DSI ou responsable du service informatique.
Ingénieur sécurité du système d'information (RSSI).
Chef de projet informatique en charge du projet sécurisation.

Pré-requis
Cette formation ne nécessite pas de prérequis.

Objectifs
Élaborer une démarche pour sécuriser l'information.
Continuer l'activité, gérer les crises.
Comprendre la mission du Responsable Sécurité du Système d'Information.

Dates des sessions
Nous consulter.

Programme détaillé

LES ENJEUX, LA RÉGLEMENTATION, LA POLITIQUE

1 Les enjeux de la sécurité de l'information
Les enjeux de la sécurité de l'information.
La typologie des risques informatiques.
Les aspects juridiques et réglementaires.
Hiérarchisation des risques.

2 La réglementation
Les textes de normalisation : ISO et Sarbanes-Oxley.
Les aspects légaux.
La sécurité des données.
La surveillance et le droit des salariés.
Les assurances et leurs garanties en cas de sinistre, Les conditions d'exclusion.

3 Élaborer sa politique de sécurité
Rechercher les solutions soit curatives soit préventives.
Planifier leur mise en œuvre.
Budgéter le plan de sécurisation.
Les indicateurs de performance du plan de sécurisation.

4 Prévenir les risques via des actions auprès des utilisateurs
Des règles simples peuvent éviter de gros tracas.
Enrichir la connaissance collective par les incidents.
Gérer les départs, la malveillance.
Communiquer sur la sécurité.
Former les nouveaux arrivants.

LA CONTINUITÉ, LE PILOTAGE, LA MISSION DU "RSSI"

1 Assurer la continuité d'activité
Les principales situations d'urgence.
Établir un plan SOS informatique, agir par priorité.
Identifier les limites de l'exercice.
Gérer les situations d'urgence.
La continuité pour satisfaire les clients.
Les risques majeurs :
incendie, inondation...

2 Gérer les situations de crise
Organiser la gestion d'une crise et assurer la logistique :
qui fait quoi, où, comment et quand ?

Formaliser les processus de décision.
Adopter la communication associée.

3 Le tableau de bord de pilotage
Quels indicateurs suivre ?
Démarche de pilotage en utilisant les résultats du tableau de bord sécurité.

4 La mission du "RSSI" en synthèse
Rôle et responsabilités.
Niveaux d'autorité.

Lisis Conseil

Formations
Responsables Sécurité des S.I

Indicateurs et tableaux de bord de la sécurité

1 jour

Participants

Responsable sécurité du système d'information (RSSI).
Risk manager.
DSI ou responsable du service informatique.

Pré-requis

Bonnes connaissances des fonctions de responsable sécurité des SI.

Objectifs

Apprendre à choisir les indicateurs de sécurité adaptés.
Mettre en place le circuit de collecte des indicateurs.
Apprendre à construire son tableau de bord Sécurité desSI.

Dates des sessions

Nous consulter.

Programme détaillé

Piloter la sécurité

- Les 4 outils du RSSI pour piloter sa fonction
- L'évolution du niveau de sécurité: l'approche PDCA de la norme ISO 27001.
- Définir la stratégie de métriques.
- indicateurs simples, indicateurs complexes, tableaux de bord

Le choix des indicateurs

- Rappels de sécurité : plan d'action et thèmes ISO 27002.
- Indicateurs opérationnels, fonctionnels et stratégiques
- Les apports de la norme ISO 27004 dans le projet de définition.
- Les phases d'un projet de définition d'indicateurs sécurité.
- Combien d'indicateurs mettre en place, et lesquels.
- Pour qui élaborer des indicateurs: notion d'audience, définition de la communication.

La mise en place de la collecte

- Rappels d'organisation
- Intégration de la collecte dans l'organisation en place: enjeux, pérennité, coûts
- Fiches de définition des indicateurs simples et complexes
- Mise en place du circuit et phase d'adaptation

Tableaux de bord

- Fréquence d'élaboration, usage
- Le reporting au management, au Comité Sécurité, aux Directions métiers.
- L'affinage des plans sécurité grâce aux tableaux de bord

Les chapitres sont illustrés d'exemples concrets et d'exercices.

Lisis Conseil

Formations
Responsables Sécurité des S.I

Audits et contrôles de sécurité
Comment les réaliser

1 jour

Participants
RSSI.
Risk Manager.
Responsables du contrôle interne,
Auditeurs internes ou externes,

Pré-requis
Avoir des connaissances de base sur la sécurité des systèmes d'information

Objectifs
Apprendre à préparer et à effectuer un audit sur la sécurité des systèmes d'information, dans le respect de la norme ISO 19011 (audit des systèmes de management). Cette étape d'audit s'inscrit dans la démarche ISO 27001 (phase CHECK).

Dates des sessions
Nous contacter.

Programme détaillé

Le pilotage de la sécurité des SI
- jeu d'introduction
- rappels ISO 27001
- surveiller et réévaluer
- contraintes règlementaires et normatives
- définitions et Histoire

Le métier de l'auditeur sécurité
- les normes qui régissent le métier de l'auditeur
- critères de succès
- principes d'un audit
- Contexte de la mission, facteur déclenchant
- Audit interne / audits externes

Les 6 phases d'un audit
- Déclenchement: nomination, objectifs, champ, référentiel, faisabilité, équipe, premier contact.
- Revue documentaire.
- Préparation de l'audit sur site: plan d'audit, classification des écarts, critères de risques, préparation des interviews et des tests, questionnaires.
- Audit sur site: réunion d'ouverture, communication, interviews, recueil des preuves, rédaction des constats et des conclusions, réunion de pré-restitution et réunion de clôture.
- Rapport d'audit: rapport provisoire, retour d'informations et rapport final.
- Clôture et suivi
- Quelques chiffres sur les entreprises en France

Étude de cas

Les chapitres sont illustrés d'exemples concrets.

Lisis Conseil

Formations Direction

Définir sa politique de Sécurité (PSSI)

1 jour

Participants

Responsable sécurité du système d'information (RSSI).
Risk manager, Compliance manager.
DSI ou responsable du service informatique.
Directeur général.

Pré-requis

Aucun.

Objectifs

Apprendre à élaborer la politique de sécurité la plus adaptée à ses enjeux.
Apprendre à l'utiliser comme outil de communication, d'action, de reporting et d'audit.

Dates des sessions

Nous consulter.

Programme détaillé

Manager la sécurité

- La notion de SMSI: système de management de la sécurité des informations (norme ISO 27001)
- Les étapes de mise en place d'un SMSI
- Les outils nécessaires: politique et charte, plan d'actions sécurité, contrôles.
- La politique de sécurité (PSSI): contenu, structure, intérêts, inconvénients.

Elaborer sa PSSI

- Le rôle du responsable sécurité (RSSI) et des autres Directions dans l'élaboration de la PSSI
- Quels référentiels utiliser comme base
- Définir les usages futurs et l'audience de la PSSI
- Choisir le périmètre couvert
- Circuit d'élaboration, de relecture et de validation

Rédiger la PSSI

- Structure-type, quel niveau de détails
- Applicabilité: lois et règlementations à respecter ou faire respecter par la PSSI
- Cas des entreprises internationales
- Validité de la PSSI: quelle fréquence de mise à jour ?

Les multiples usages de la PSSI

- La PSSI outil de construction du plan Sécurité
- La PSSI outil de communication et de formation
- La PSSI outil de base pour les revues internes et les audits/ norme ISO 27002
- La PSSI outil de construction des indicateurs
- La PSSI comme passeport vers la certification.

Les chapitres sont illustrés d'exemples concrets et d'études de cas.

Lisis Conseil

Formations
Direction

Plans de continuité des activités
Se préparer et faire face aux sinistres

2 jours

Participants
Responsable Continuité,
Risk Manager ou RSSI.
Directeurs ou responsables informatiques,
Correspondants Sécurité,
chefs de projets MOA et MOE,
Auditeurs internes ou externes,

Pré-requis
Aucun.

Objectifs
Apprendre à mener à bien un projet de continuité d'activité en accord avec les normes et standards du domaine (27001, ISO 22301, BS 25999, ITIL V3...).
De l'analyse des risques et de la conception des plans jusqu'aux tests, au maintien en conditions opérationnelles et à la cellule de crise.

Dates des sessions
Nous contacter.

Programme détaillé

Pourquoi gérer la continuité ?
- L'importance stratégique de l'information.
- Les enjeux pour l'entreprise
- lois et réglementations, normes et standards.

Définitions et concepts
- Définir la stratégie de continuité.
- Glossaire: PCA, PRA, BCP, DRP, plan de reprise, etc...
- les critères DICP

Le projet Continuité
- Les phases d'un projet plan de continuité et ses particularités

Analyse des risques
- Les composantes du risque.
- Les principes des différentes méthodes et standards (COBIT,ISO...).
- La matrice des risques et son apport pour le plan de continuité.

L'identification du périmètre
- l'étude des activités critiques (BIA) d'une entreprise.
- La notion de Service Delivery Objectives, DMIA, PDMA

Le choix des moyens de continuité
- Élaborer les scénarios.
- Les différents sites de repli (hot, warm, cold sites, reciprocal agreement...) et les critères de décision.

La rédaction des Plans de continuité
- La composition des Plans et procédures.
- Les équipes de secours : constitution, rôle

Procédures d'escalade et gestion de crise
- La gestion de l'escalade en phase avec le RTO.
- La constitution de la cellule de crise.
- Les principes de déclenchement du plan de secours.

Tester les plans de continuité
- Tests et entrainement des équipes
- Les différents types de tests
- Le suivi des recommandations.

La continuité d'activité en tant que processus ITIL et le maintien en condition opérationnelle du plan.

Les chapitres sont illustrés d'exemples concrets.

Lisis Conseil

Formations Sur Mesure

Thèmes

Pour toute autre formation sur des thèmes de sécurité des informations, nous contacter sur www.lisis-conseil.com

Notre équipe est à votre écoute pour vous aider dans la création de vos formations sur mesure.