SECURITE DES SYSTEMES D'INFORMATION

Code **SECU10-1**	**Objectifs** • Maîtriser le processus de gouvernance de la sécurité • Utiliser les référentiels métiers et les normes associées de la série ISO 27K • Connaître le cadre juridique français et européen (LPM, NIS, RGPD, …) • Planifier un plan d'actions pour atteindre les objectifs de la politique de sécurité • Elaborer une riposte adéquate et proportionnée pour réduire les risques cyber
	Public Ingénieurs prenant les fonctions de RSSI, directeurs ou responsables informatiques. Ingénieurs ou correspondants Sécurité, chefs de projets intégrant des contraintes de sécurité.
Durée 3 jours	**Prérequis** Aucune connaissance particulière.

INTRODUCTION

- La définition des actifs processus/information et actifs en support (informatique).
- La classification DICT/P : Disponibilité, Intégrité, Confidentialité et Traçabilité/Preuve.
- La définition du risque SSI et ses propriétés spécifiques (vulnérabilités, menaces).
- Les différents types de risques : accident, erreur, malveillance.
- L'émergence du cyber risque, les APT, se préparer à une cyber crise.
- Les sources d'information externes incontournables (ANSSI, CLUSIF, ENISA, etc.).

LA TASK FORCE SSI : DE MULTIPLES PROFILS METIERS

- Le rôle et les responsabilités du RSSI / CISO, la relation avec la DSI.
- Vers une organisation structurée et décrite de la sécurité, identifier les compétences.
- Le rôle des "Assets Owners" et l'implication nécessaire de la direction.
- Les profils d'architectes, intégrateur, auditeurs, pen-testeurs, superviseurs, risk manager, etc.
- Constituer une équipe compétente, formée et réactive aux évolutions du cyber espace.

LES CADRES NORMATIFS ET REGLEMENTAIRES

- Intégrer les exigences métiers, légales et contractuelles. L'approche par la conformité.
- Un exemple de réglementation métier : PCI DSS pour protéger ses données sensibles.
- Les mesures de sécurité pour atteindre un objectif de confidentialité, intégrité des données.
- Un exemple de réglementation juridique : directive NIS/ Loi Programmation Militaire.
- Les 4 axes de la sécurité vue par l'Europe et l'ANSSI : Gouvernance, Protection, Défense et Résilience.
- Les mesures de sécurité pour atteindre un objectif de disponibilité, intégrité des processus.
- La norme ISO 27001 dans une démarche système de management (roue de Deming/PDCA).
- Les bonnes pratiques universelles de la norme ISO 27002, la connaissance minimale indispensable.
- Les domaines de la sécurité : de la politique à la conformité en passant par la sécurité informatique.
- Elaborer un Plan d'Assurance Sécurité dans sa relation client/fournisseur.

L'ANALYSE DE RISQUE

- Intégration de l'Analyse des risques au processus de gouvernance de la sécurité.
- Identification et classification des risques, risques accidentels et cyber risques.

- Les normes ISO 31000 et 27005 et la relation du processus risque au SMSI ISO 27001.
- De l'appréciation des risques au plan de traitement des risques : les bonnes activités du processus.
- Connaitre des méthodes pré définies : approche FR/EBIOS RM, approche US/NIST, etc.

LES AUDITS DE SECURITE ET LA SENSILISATION DES UTILISATEURS

- Les catégories d'audits, de l'audit organisationnel au test d'intrusion.
- Les bonnes pratiques de la norme 19011 appliquées à la sécurité.
- Comment qualifier ses auditeurs ? – exemple avec les PASSI en France.
- Sensibilisation à la sécurité : Qui ? Quoi ? Comment ?
- De la nécessité d'une sensibilisation programmée et budgétisée.
- Les différents formats de sensibilisation, présentiel ou virtuelle ?
- La charte de sécurité, son existence légale, son contenu, les sanctions.
- Les quiz et serious game , exemple avec le MOOC de l'ANSSI.

LE COUT DE LA SECURITE ET LES PLANS DE SECOURS

- Les budgets sécurité, les statistiques disponibles.
- La définition du Return On Security Investment (ROSI).
- Les techniques d'évaluation des coûts, les différentes méthodes de calcul, le calcul du TCO.
- La couverture des risques et la stratégie de continuité.
- Plans de secours, de continuité, de reprise et de gestion de crise, PCA/PRA, PSI, RTO/RPO.
- Développer un plan de continuité, l'insérer dans une démarche sécurité.

CONCEVOIR DES SOLUTIONS OPTIMALES

- Structurer sa protection logique et physique. Savoir élaborer une défense en profondeur.
- Les trois grands axes de la sécurité informatique (réseaux, données, logiciels).
- Cloisonner ses réseaux sensibles, les technologies firewall réseaux et applicatif.
- Rendre ses données illisibles pendant le stockage et le transport, les techniques cryptographiques.
- Sécuriser ses logiciels par le durcissement et une conception secure.
- Gestion des vulnérabilités logicielles, savoir utiliser CVE/CVSS.

SUPERVISION DE LA SECURITE

- Indicateurs opérationnels de gouvernance et de sécurité.
- Le pilotage cyber : tableau de bord ISO compliant.
- Préparer sa défense (IDS, détection incidents, etc.).
- Traitement des alertes et cyber forensics, le rôle des CERT

LES ATTEINTES JURIDIQUES AU STAD

- Rappel, définition du Système de Traitement Automatique des Données (STAD).
- Types d'atteintes, contexte européen, la loi LCEN. Le règlement RGPD.
- Quels risques juridiques pour l'entreprise, ses dirigeants, le RSSI ?

RECOMMANDATIONS POUR UNE SECURISATION " LEGALE " DU SI

- La protection des données à caractère personnel, sanctions prévues en cas de non-respect.
- De l'usage de la biométrie en France.
- La cybersurveillance des salariés : limites et contraintes légales.
- Le droit des salariés et les sanctions encourues par l'employeur.