Cours ISO 27001

TD #3

Cadrage SMSI - Correction

Etienne de Séréville, OCS IBM France, Relations Institutionnelles

Agenda

- Cadrage d’un SMSI pour la Société de Robotique – 1h
  - Prise en compte des rubriques d’un SMSI ISO 27001
- Présentation du SMSI par groupe

1. Cadrage d'un SMSI pour la Société de Robotique (SR)

1. Organisation et son contexte
2. Besoins et des attentes des parties intéressées
3. Domaine d'application SMSI – Périmètre de certification
4. Maintenabilité
5. Leadership et engagement
6. Politique de sécurité
7. Rôles, responsabilités et autorités
8. *Appréciation des risques, traitement et options de traitement – Cf. TD#2*
9. *Objectifs de sécurité et plans pour les atteindre – Cf. TD#2*
10. *Ressources – Cf. TD#2*
11. *Compétences – Cf. TD#2*
12. *Sensibilisation – Cf. TD#2*
13. *Communication – Cf. TD#2*
14. Surveillance, mesures, analyse et évaluation
15. Audit interne
16. Revue de direction
17. Non-conformité et actions correctives
18. Amélioration continue du SMSI

1. Concevoir un SMSI: **Organisation et son contexte**

Exemple

- Analyse de l'environnement :
  - Contexte légal et réglementaire français et européen: LPM, RGPD, archives numériques, crypto pour l'export…
  - Marché concurrentiel, client étatiques et privés, exigences techniques pour les robots militaires
  - Implantations internationales sur tous les continents
  - Multisite / redondance potentielle pour la production des 2 usines en France et aux USA
  - Siège en Ile de France, zone à risques naturels limités, risque politique faible, risque géopolitique modéré

- Enjeux externes :
  - Respect des lois et règlements, comme la crypto pour l'exportation
  - Compétition commerciale, innovation et avancées techniques pour les robots, intégrant de nouveaux équipements numériques à sécuriser (capteurs, actionneurs, IA, algorithme de chiffrement…)
  - Obtenir les certifications de qualité et sécurité attendues par le marché pour la production industrielle, les robots et les services associés (pilotage, télémaintenance…)
  - Acquérir des informations sur les menaces cyber et les vulnérabilités récentes sur les technologies utilisées chez SR
  - Attirer les ingénieurs et techniciens aux compétences informatiques, sécurité et cyber au meilleur niveau

- Enjeux internes :
  - Stratégie de SR (extension de l'entreprise, ouverture de nouveaux bureaux…), afin d'anticiper les prochains besoins de sécurité informatique
  - Cartographie informatique à jour, afin d'éviter le shadow IT, améliorer la détection et la réponse à incident
  - Maitrise des risques numériques liés aux robots, au pilotage, à l'ingénierie, à l'informatique interne de SR
  - Avoir connaissance des évolutions technologiques de l'informatique et de la robotique
  - Connaitre les compétences existantes dans le service informatique interne pouvant être mobilisé en cas d'incident
  - Continuum des sécurités physiques et logiques

2. Concevoir un SMSI: **Besoins et des attentes des parties intéressées**

Exemple

- Besoins et des attentes des parties intéressées
  - Parties intéressées externes :
    - Les régulateurs et législateurs : respect des lois et règlements liés aux SSI de SR: LPM pour les SIIV, RGPD pour les données personnelles des salariés de SR, archives comptables de SR fiables
    - Les actionnaires : maîtrise des risques numériques de SR, en particulier la conformité RGPD pour éviter des amendes, éviter des impacts de réputation suite à divulgation publiques de données des clients de SR
    - Les fournisseurs : sécurité dans les échanges numériques avec SR pour éviter la propagation des malwares et autres attaques cyber, sécurité des passerelles avec les clouds externes (DB externes…), consignes de sécurité pour le prestataire informatique qui assure la maintenance informatique
    - Les concurrents : limitation des informations publiables pour éviter l'espionnage industriel
    - Les clients: sécurité des informations échangées avec SR, comme les cahiers des charges des robots, les rapports de fonctionnement des robots, les flux de pilotage des robots
    - Les groupes d'activistes: limiter les informations publiables pour éviter les actions malveillantes des hacktivistes
  - Parties intéressées internes:
    - Les décideurs: allocation des budgets pour l'achat de logiciels de sécurité, budget de formation à la cybersécurité des ingénieurs de conception des robots etc.
    - Les propriétaires de processus, propriétaires de systèmes et propriétaires d'information: accompagnement pour réaliser les évaluations des risques stratégiques de sécurité des processus métier et information essentielles
    - Les fonctions de support telles que l'informatique ou les ressources humaines: accompagnement pour réaliser les évaluations des risques opérationnels de sécurité des robots, de l'informatique interne, des SI métiers (SI RH, ERP…), sécurisation des SI de conception et de pilotage des robots
    - Les employés et utilisateurs: sensibilisation et formation à la sécurité informatique
    - Les spécialistes de la sécurité interne: niveau de sécurité des centres de données, des locaux techniques informatiques, des alimentations électriques, de la climatisation des salles informatiques, etc.

3. Concevoir un SMSI: Domaine d'application SMSI – Périmètre de certification

Exemple

- Le siège, le bureau d'étude, le centre de télé opérations, les usines de robot, les 10 bureaux à l'étranger, les locaux techniques pour les serveurs et les équipements réseau de proximité
- Le personnel utilisateur de l'informatique: managers, commerciaux, ingénieurs, techniciens en robotique, personnel administratif, informaticiens de l'entreprise
- Les applications informatiques pour la conception des robots: C&DAO, MAO…
- Les machines spéciales et automates programmables des 2 usines
- Les logiciels pour la gestion administrative de l'entreprise: ERP, CRM…
- Les logiciels d'infrastructures (annuaires…)
- Les serveurs d'applications et d'infrastructure
- Les matériels utilisateurs: portable, tablette, smartphone, imprimante…
- Les logiciels en Saas

4. Concevoir un SMSI: **Maintenabilité**

Exemple

- Etablir le SMSI: plan projet de déploiement du SMSI au sein de SR, ses 2 usines et des filiales commerciales à l'étranger
- Mise en œuvre du SMSI: suivi du projet SMSI par le comité projet Sécurité régulier au siège de SR
- Mise à jour du contexte de SR: légal et réglementaire, implantation géographique, périmètre de SR, innovations technologiques à prendre en compte, développement commercial…
- Mise à jour des besoins et des attentes des parties intéressées: nouveaux clients pour les robots, nouveaux fournisseurs de logiciel en Saas, nouvelles attentes des décideurs (utiliser des logiciels qualifiés par l'ANSSI)…
- Mise à jour du périmètre informatique à prendre en compte pour le SMSI: nouveaux bureaux, nouveaux services aux clients (expl: maintenance des robots…), nouveaux logiciels de conception des robots à sécuriser…
- Mise à jour de l'infrastructure informatique du SMSI: intégration des correctifs, revue des comptes d'accès…

5. Concevoir un SMSI: **Leadership et engagement**

Exemple

- Note d'engagement de la direction pour l'obtention d'une certification ISO 27001
- Objectifs SSI: protection des données de conception (savoir-faire) des robots, besoin de disponibilité du pilotage des robots, protection des données personnelles des employés et des clients, la sécurisation des flux entre les usines et les bureaux de conception….
- Exigences intégrées aux processus métiers: confidentialité des données personnelles des salariés SB, intégrité des données de conception des robots, disponibilité des flux de pilotage, confidentialité des flux de données en Saas…
- Formation et sensibilisation de la direction et des managers de SR à la SSI
- Processus achat de SR pour la prise en compte de la sécurité numérique dans les cahiers des charges pour les fournisseurs informatiques
- Processus de recrutement des ingénieurs et techniciens comprenant une dimension sécurité numérique dans les descriptifs de poste, en particulier pour les ingénieurs de conception des robots qui doivent répondre à des exigences de sécurité
- Comités de sécurité niveau direction, intégrant les services de SR concernés par la SSI: service en charge de la sécurité physique, achats, RH…
- Communication régulière de la direction sur le sujet SSI

6. Concevoir un SMSI: **Politique de sécurité**

Exemple

- PSSI générale pour SR et politiques thématiques, en particulier concernant:
  - La cryptographie pour les flux de pilotage
  - La confidentialité des données pour les bases de conception (secrets de fabrication, ordre de fabrication)
  - La continuité /reprise du service de pilotage des robots
  - Le contrôle des accès pour les données personnelles, de direction…
- PSSI décrivant l'organisation SSI interne sous la responsabilité du RSSI
- PSSI décrivant la comitologie: comité stratégique annuel au siège, comité opérationnel mensuel avec usine et bureaux, comité projets mensuel avec DSI et métiers
- Documents techniques d'architecture SSI des robots, du centre de pilotage, du réseau international pour l'informatique interne SR, des serveurs et de l'infrastructure (à diffusion restreint au service informatique de SR)
- Guide de paramétrage et de configuration des équipements (à diffusion restreint au service informatique de SR)
- Communication de la PSSI en interne suivant le besoin d'en connaitre
- Mise à la disposition des parties intéressées: synthèse de la PSSI mise à disposition pour les commerciaux de SR à destination des clients à leur demande

7. Concevoir un SMSI: **Rôles, responsabilités et autorités**

Exemple

- RSSI responsable du SMSI de SR reportant directement à la direction, assisté d'un chef de projet SMSI
- Correspondants sécurité dans chaque services de SR en charge de l'application du SMSI dans son service
- Correspondant sécurité dans chaque bureau commercial de SR en charge de l'application du SMSI dans son bureau, et vigilent à la conformité légale et réglementaire locale du pays
- Equipe SSI sous la responsabilité du RSSI ayant les compétences sur les technologies de l'informatique interne et des technologies robotiques utilisées, sur les méthodes d'évaluation des risques de l'informatique de gestion, industrielle et embarquée, sur les audits organisationnels et techniques
- Communication sur le suivi de la conformité du SMSI, et compte rendu à la direction des performances de SSI
- Activités attribuées:
  - Coordonner l'établissement, la mise en œuvre, la maintenance, le suivi de la performance et de l'amélioration du SMSI: chef de projet SMSI
  - Donner des conseils sur l'évaluation et le traitement des risques de sécurité: risque manager de SR
  - Concevoir des processus et des systèmes de sécurité de l'information: RSSI
  - Etablir des normes concernant la détermination, la configuration et le fonctionnement des mesures de sécurité: équipe SSI
  - Gérer les incidents de sécurité de l'information: RSSI
  - Auditer et améliorer le SMSI: équipe SSI
- Désignation des propriétaires des informations/actifs/biens et des processus: dirigeants/managers, utilisateurs/administrateurs, chef de projet
- Autorités de référence externes: Ministère de l'Industrie, ANSSI

14. Concevoir un SMSI: **Surveillance, mesures, analyse et évaluation**

Exemple

- Surveillance
  - Processus SSI (classification des actifs, sauvegardes, gestion des accès, gestion des règles des firewall…)
  - Activités sur les actifs avec SIEM+SOC et règles de détection pour les risques résiduels
  - Des configurations en continu des serveurs frontaux Internet, les routeurs backbone, les automates d'usines…
  - Niveau de menace extérieur: malwares les plus actifs, indices de compromission à utiliser, TTP les plus utilisés
- Mesures
  - Indicateurs processus: complétudes des procédures SSI, comptes orphelins, effacement support d'information…
  - Indicateurs Incidents: nombre, type, fréquence, cible, impacts…
  - Indicateurs Menaces: type, détection
  - Audits organisationnels et physique, architecturaux, de revue de code, de configurations et d'intrusion
- Analyse
  - Dysfonctionnement des processus SSI: sauvegardes incomplètes, comptes des démissionnaires non supprimés…
  - Incidents SSI issus du SOC, du Support Utilisateur, de la production informatique et des réseaux
  - Etudes des audits et forensique, recherche des causes structurelles (limites organisationnelles et technologiques, capacités et moyens restreints…)
- Evaluation
  - Appréciation des impacts des dysfonctionnement et incidents pour SR pour recommandations d'amélioration
  - Revue des indicateurs et du pilotage associé

15. Concevoir un SMSI: **Audit interne**

Exemple

- Type d'audit interne :
  - De conformité réglementaire RGPD
  - De sécurité : application de la PSSI dans les 2 usines et les bureaux commerciaux internationaux
  - De comparaison avec les standards: ANSSI, ISO27002/4/5/35, NIST
- Planifier par périmètre organisationnel et technique: géographie, usines/bureaux, systèmes/réseaux…
  - Audits statistiques organisationnels et physique annuels, architecturaux semestriels, de revue de code trimestriels, de configurations et d'intrusion mensuels
  - Audits complets sur les robots avant livraison, complet pour le pilotage robot
  - Recommandations d'amélioration intégrées dans le plan d'actions SSI
- Critères d'audit ou « ensemble d'exigences utilisé comme référence vis-à-vis de laquelle les preuves objectives sont comparées », définition ISO19011 *Lignes directrices pour l'audit des systèmes de management*
  - Exigences de la PSSI et des documents SSI internes
  - Exigences des guides de l'ANSSI, des normes ISO2700x, des Guidelines du NIST

16. Concevoir un SMSI: **Revue de direction**

Exemple

- Présentation de l'état de la menace cyber, de la vulnérabilité de SR (audits et incidents), des risques, des évolutions de l'informatique des usines, des bureaux, des réseaux, des fournisseurs…
- Suivi des actions SSI: état des lieux de la sécurité, plan d'actions pluriannuels intégrant les résultats des audits, résultats des actions réalisées et en cours
- Performance: pour la réduction des risques SSI de SR du fait de la réalisation des actions, évolution de la cartographie des risques SSI
- Informations émanant de la direction: nouvelle orientation de SR conduisant à une priorisation nouvelle des actions SSI, précision et périmètre des indicateurs SSI…
- Format: tableaux de bord SSI et scorecards Sécurité informatique, actualisés avec les audits, les évolutions de l'informatique interne

17. Concevoir un SMSI: **Non-conformité et actions correctives**

Exemple

- Non-conformité identifiée par les audits et les revues suivant le planning prévu
- Analyse des non-conformités et enseignements (problèmes ITIL)
- Formalisation du plan d'actions correctives à intégrer au plan d'actions SSI
- Suivi du plan par le comité projet SSI, et mise à jour de la PSSI et autres documents SSI de SR pour intégrer la concrétisation des actions
- Vérification de réalisation des actions du plan:
  - Si une action se conclue par la mise en œuvre d'un processus: écriture de la procédure et indicateurs de réalisation de ladite procédure : exemple: procédure de destruction des disque durs des robots en cas de changement, indicateur de suivi de la destruction effective des disques retirés
  - Si une action se conclue par l'utilisation d'un logiciel: écriture de la documentation d'utilisation du logiciel et indicateur de rapport d'utilisation

18. Concevoir un SMSI: **Amélioration continue du SMSI**

Exemple

- Pilotage en continu des étapes (PDCA) chez SR, et évidences de mise en œuvre : note de direction, PSSI, évaluation des risques, PTR, audits, CR de comités etc.
- Adéquation du SMSI et de la certification ISO27001 avec les attentes du marché de la robotique militaire et civile, remontée client
- Efficacité du SMSI: réduction des risques SSI de SR, visible avec la cartographie des risques
- Pertinence du SMSI: mesure de l'effort consacré au SMSI (temps de l'équipe SMSI et des partenaires impliqués, procédures de pilotage du SMSI, licences logiciel et maintenance) vs réduction des risques