

Cybersécurité des Systèmes Industriels d'Infrastructure (S2I) :

Livrables du dossier d'homologation

	Nom	Fonction	Date
Rédaction	NIEL Léo	Apprenti Cyber	21/10/2025
Validation	ICD Alexandre SERVOIS	Chef Bureau cybersécurité S2I	05/11/2025

DOCUMENT	STATUT DE LA FOURNITURE	CONDITIONS DE FOURNITURE	CLASSE 1	CLASSE 2	CLASSE 3
DOSSIER DE PRESENTATION					
Rapport d'auto-évaluation (Classification S2I / CYLEX)	Obligatoire		X	X	X
Fiche de présentation du système	Obligatoire		X	X	X
Socle de sécurité	Obligatoire		X	X	X
Stratégie d'homologation (SH)	Obligatoire		X	X	X
<i>Détail : Guide Présentation</i>					
DOSSIER DE SECURITE					
Cartographies	Obligatoire		X	X	X
Procédure d'exploitation de sécurité (PES)	Obligatoire		X	X	X
Notices d'équipements et de procédures	Obligatoire		X	X	X
Plan d'assurance de sécurité (PAS)	Obligatoire	Si cloud externalisé	X	X	X
Tests (Plan de tests, Rapport, Plan d'action)	Optionnel	Si besoin avéré		X	X
Plan de conduite et de reprise (PCA/PRA ; PCI/PRI)	Optionnel	Si besoin avéré		X	X
Analyse de risques (EBIOS RM)	Obligatoire				X
Fiche d'expression rationnelle d'objectifs de sécurité (FEROS)	Obligatoire				X
<i>Détail : Guide Sécurité</i>					
DOSSIER DE CONFORMITE					
Rapport de conformité	Obligatoire		X	X	X
Liste des risques résiduels	Obligatoire		X	X	X
Plan d'amélioration continue de la sécurité (PACS)	Obligatoire		X	X	X
Rapport d'audits	Obligatoire				X
<i>Détail : Guide conformité</i>					
DOSSIER DE COMMISSION					
Support de présentation à la commission	Obligatoire		X	X	X

Synthèse des livrables pour la démarche d'homologation cyber

DOSSIER DE PRESENTATION :

Le dossier de présentation sert à donner une vision complète du système et de l'opération, à évaluer les risques et à préparer la stratégie d'homologation.

Objectif

Constituer la base documentaire pour l'ensemble de la démarche, permettant d'identifier les fonctions, acteurs, risques, et contraintes du système à homologuer.

VERT : Obligatoire pour les classes 1,2 et 3

ORANGE : Obligatoire pour les classes 2 et 3

ROUGE : Obligatoire seulement pour la classe 3

DOCUMENT	STRUCTURE / SECTIONS DETAILLEES	CONTENU ATTENDU
RAPPORT D'AUTO-EVALUATION	Grille d'évaluation CYLEX : analyse sommaire des risques, évaluation de la criticité du système et de son exposition face à la menace cyber. Identification des entités des différents acteurs (AQ, AH, RSSI-P, RSSI-A, CEAH ...) Détection des systèmes techniques : identification des sous-systèmes concernés (chauffage, climatisation, ventilation, énergie, contrôle d'accès, intrusion, vidéosurveillance, SSI, GTB, etc.) et évaluation de leur exposition cyber. Niveau de protection des données et documents manipulés. Besoin en sécurité (Disponibilité, Intégrité, Confidentialité, Traçabilité) Description de l'environnement (Bâtiment, locaux, ...) Evaluation de la menace et des risques	Détermination de la classe d'homologation : - classe 1 - classe 2 - classe 3
FICHE DE PRESENTATION DU SYSTEME	Présentation du système d'information : contexte général, enjeux du SI (périmètre d'emploi, importance, classification, mentions), contexte d'emploi (formation, opération, développement, etc.), acteurs du SI (porteur, autorité, RSSI, intégrateur, opérateur, etc.), contraintes et impératifs (opérationnels et projet). Fonctionnalités / cas d'usage : principales fonctions et cas d'usage du SI, description synthétique.	Décrire de manière synthétique et structurée le périmètre fonctionnel et organisationnel du système d'information dans son contexte d'emploi. Servir de référence unique et à jour tout au long du cycle de vie du projet.

SOCLE DE SECURITE	Exigences de sécurisation : identification et description des exigences obligatoires et optionnelles applicables au système, issues des référentiels réglementaires, normatifs et internes (DIR 39, IGI 1300, guides ANSSI, etc.). Dérogations : présentation des exigences non conformes, partiellement appliquées ou différées, avec justification et niveau d'acceptabilité associé. Options non retenues et mesures sans objet : recensement des exigences non pertinentes au regard du périmètre, accompagnées d'une justification (architecture, contexte, contraintes techniques). Annexes : suivi de la conformité, références réglementaires et normatives, grille d'évaluation, traçabilité des exigences.	Définir les règles de cybersécurité applicables au système d'information, préciser les exigences imposées et les éventuelles dérogations. Servir de référence centrale pour la Procédure d'Exploitation de Sécurité (PES) et les vérifications de conformité tout au long du cycle de vie du SI.
---------------------------------	--	--

STRATEGIE D'HOMOLOGATION

Cible d'homologation : niveau de classification du SI (Secret Défense, Confidentiel Défense, Diffusion Restreinte...), mentions de protection, objectifs complémentaires (intégrité, disponibilité, traçabilité), version et date de la fiche de présentation du périmètre, observation éventuelle.

Organisation de la démarche d'homologation : méthode retenue (référence, déploiement, autre), modalités spécifiques en cas d'homologation de déploiement, procédure de vérification et de contrôle (audits de sécurité, tests), entités responsables.

Commission d'homologation : Identification des entités des différents acteurs (AQ, AH, RSSI-P, RSSI-A, CEAH ...)

Description des livrables : ensemble des pièces constitutives (décision précédente, fiche de périmètre, stratégie d'homologation, PES, PAS, certificat de conformité générique, etc.), avec responsable, approbateur et date.

Planification : calendrier de la démarche — période de déploiement, dates prévisionnelles de mise en service, remise du dossier, fiche de synthèse et décision d'homologation.

Schéma fonctionnel : Présentation schématique (VAUBAN) des différentes fonctions du système à homologuer

Définir la **démarche complète d'homologation** du système : son périmètre, sa méthode, son organisation, ses contrôles et sa planification. Permettre à l'autorité d'homologation d'avoir une **vision claire de la stratégie, des responsabilités et du suivi** tout au long du cycle de vie du SI.

Cette stratégie est à faire valider officiellement par l'AH (NeMO)

[Retour au TABLEAU](#)

DOSSIER DE SECURITE :

Le dossier de sécurité contient les informations nécessaires à l'exploitation du système en toute sécurité.

Objectif

Fournir une description détaillée du périmètre technique, applicatif et des règles d'exploitation.

VERT : Obligatoire pour les classes 1,2 et 3

ORANGE : Obligatoire pour les classes 2 et 3

ROUGE : Obligatoire seulement pour la classe 3

DOCUMENT	STRUCTURE / SECTIONS DETAILLEES	CONTENU ATTENDU
CARTOGRAPHIES	Cartographie physique : schémas des infrastructures matérielles et équipements. Cartographie logique : réseaux, flux, segmentations, interconnexions et plan d'adressage IP. Cartographie des applications : services, applications et dépendances. Cartographie administration et supervision : revue des comptes et profils, outils de gestion, supervision et contrôle.	Représentation visuelle des systèmes et réseaux, améliore la compréhension globale.

PROCEDURES D'EXPLOITATION DE SECURITE (PES)

Responsabilités : chaînes fonctionnelles SSI, habilitations nécessaires, sensibilisation et formation du personnel.

Protection des données et accès : confidentialité des données métiers et personnelles, mesures techniques et organisationnelles, gestion des utilisateurs, administrateurs, droits d'accès et authentifications.

Sécurité des systèmes et applications : description des différents systèmes (applications, réseau, administration, équipements actifs, filtrage, cloisonnement, hébergement et interconnexions).

Sécurité physique et environnementale : description de l'environnement, des locaux techniques, serveurs et sécurité des équipements (blocage physique des ports, fermeture à clef, code, etc. ...).

Procédure de maintenance : description du MCO / MCS (fréquence et traçabilité), plan de sauvegarde et restauration des systèmes et données, journalisation, modalité d'intervention (responsabilités des différents personnels), mise à jour des documents de référence (cartographies, liste des équipements, etc...).

Protection des communications et menaces : sécurisation des liaisons, cryptographie et protection contre les codes malveillants (antivirus).

Gestion des incidents : détection, signalement, analyse des journaux et traçabilité.

Décrire de manière **synthétique et structurée** l'ensemble des **procédures opérationnelles de sécurité**, préciser les mesures **organisationnelles et techniques** à mettre en œuvre, identifier les **responsabilités** des acteurs, fournir une référence unique pour l'exploitation sécurisée et le suivi de la conformité du SI.

NOTICES D'EQUIPEMENTS ET DE PROCEDURES	Description des équipements Caractéristiques techniques (marque, modèle, version, firmware), fonctions principales, configuration et rôle dans le système industriel. Procédures d'exploitation Modes opératoires pour le démarrage, l'arrêt, la mise à jour, la maintenance et les interventions spécifiques sur les équipements. Responsabilités et habilitations Répartition des rôles entre exploitants, mainteneurs, administrateurs et RSSI, niveau d'habilitation requis et traçabilité des actions. Sécurité et conformité Intégration des exigences du socle de sécurité et du Plan Assurance Sécurité (PAS), application des règles organisationnelles et techniques. Mise à jour et évolution Procédures de révision des notices, validation par le RSSI ou autorité compétente, intégration des changements matériels, logiciels ou organisationnels. Annexes et suivi documentaire Historique des versions, liste des documents applicables et de référence, correspondance avec les PES et le PAS.	Fournir une description structurée et détaillée des équipements (marque, type, firmware, etc. ..) et procédures d'exploitation (démarrage, arrêt, mise à jour, actions etc. ..)
--	--	---

PLAN D'ASSURANCE DE SECURITE (PAS)

Responsabilités : chaînes de responsabilités interne au prestataire, habilitations nécessaires, sensibilisation et formation du personnel.

Protection des données et accès : confidentialité des données métiers et personnelles, mesures organisationnelles et techniques, gestion des utilisateurs et administrateurs, droits d'accès et authentifications, contrôle des flux d'information.

Sécurité des systèmes et applications : description des différents systèmes (applications, réseaux, serveurs, équipements), filtrage, cloisonnement, hébergement et interconnexions, mesures de protection contre les vulnérabilités et incidents techniques.

Sécurité physique et environnementale : description de l'environnement, des locaux techniques et serveurs, protection physique des équipements (blocage physique des ports, fermeture à clef, badges, vidéosurveillance), mesures environnementales (incendie, température, inondation), contrôle et suivi des interventions sur site.

Protection des communications et menaces : sécurisation des liaisons entre client et prestataire, cryptographie des flux critiques et échanges sensibles, protection contre les codes malveillants (antivirus), surveillance et alertes en temps réel.

Uniquement dans le cas d'une externalisation

Décrire de manière synthétique et structurée l'ensemble des mesures d'assurance sécurité pour une **prestation externe**, préciser les obligations contractuelles et réglementaires, identifier les responsabilités des acteurs, fournir une référence unique pour le suivi de la sécurité et de la conformité du service.

PLAN DE CONDUITE ET DE REPRISE (PCA/PRA & PCI/PRI)	Objet : définir les mesures permettant d’assurer la continuité des activités, la reprise après incident et la résilience du système ou du SI en cas de sinistre ou panne. Périmètre : Identifier les processus métiers vitaux, les services essentiels et les composants techniques critiques (systèmes, réseaux, applications, données) nécessitant une protection prioritaire et une remise en service rapide en cas d’interruption. Organisation et responsabilités : rôles et responsabilités des acteurs internes et externes, circuits de décision et points de contact. Procédures : actions immédiates pour limiter l’impact, basculement vers les moyens de secours, restauration des services, intégrité des données et retour à un état normal d’exploitation. Mesures préventives et résilience : Mettre en place des dispositifs techniques et organisationnels visant à limiter les impacts d’une panne ou d’un sinistre : redondance des ressources, sauvegardes régulières et testées, protection physique et environnementale des infrastructures critiques. Tests et exercices : Planifier des exercices de simulation (panne, sinistre, cyberattaque) pour valider l’efficacité du plan, évaluer la réactivité des équipes et identifier les axes d’amélioration. Intégrer systématiquement les retours d’expérience dans la mise à jour du plan et des procédures associées.	Garantir la continuité et la résilience du SI et des infrastructures, assurer la clarté des rôles et responsabilités, et constituer la référence unique pour le maintien, le test et l’évolution des dispositifs de continuité et de reprise d’activité.
--	--	---

ANALYSE DE RISQUE (EBIOS RM)

Objet : identifier, évaluer et hiérarchiser les **risques** pesant sur le **système d'information**, déterminer les **menaces** et **vulnérabilités** associées, et définir les **mesures de sécurité prioritaires** à mettre en œuvre.

Périmètre : délimiter le **champ de l'analyse** (systèmes, processus métiers, données, interconnexions, acteurs) en tenant compte du **contexte opérationnel, organisationnel et réglementaire**.

Méthodologie : appliquer l'approche EBIOS Risk Manager fondée sur l'**expression** des besoins et objectifs de sécurité, la **construction** des scénarios de menace, l'**évaluation** des impacts et des **probabilités**, et la **détermination** des risques résiduels.

Résultats attendus : production d'une **cartographie des risques**, identification du **niveau de criticité** et priorisation des **mesures de sécurité** ; élaboration de **recommandations** pour le **socle de sécurité**, les **plans d'assurance** et les **procédures d'exploitation**.

Responsabilités : préciser les **acteurs impliqués** dans la conduite et la **validation de l'analyse** (RSSI, responsables métiers, RCP/PO, direction de projet, autorités compétentes).

Annexes et références : fiches de périmètre, critères et échelles de sécurité, référentiels réglementaires et normatifs, documentation technique, comptes rendus d'ateliers et hypothèses de travail.

Servir de **base objective** à la **démarche d'homologation de sécurité**, orienter le **plan de traitement des risques** et assurer la **traçabilité des risques résiduels** identifiés sur le **système d'information**.

FICHE D'EXPRESSION RATIONNELLE D'OBJECTIFS DE SECURITE (FEROS)	Présentation : la FEROS permet de déterminer les besoins de sécurité, les exigences de sécurité constituant le socle de sécurité, et les objectifs de sécurité définis à partir d'une analyse de risques complète. Elle reflète les résultats de l'analyse de risques mise en œuvre et finalise l'étude itérative de cette analyse. La FEROS ne reproduit pas l'analyse de risques mais peut y adjoindre le rapport d'analyse si nécessaire, sous format numérique. La description du SI est fournie dans la fiche de présentation du périmètre d'homologation. Cadrage de l'analyse de risques : méthode et outil, périmètre, valeurs métiers et biens essentiels, critères de sécurité, hypothèses. Socle de sécurité : réglementation et textes applicables, normes et standards, modèle d'héritage, exigences de sécurité non conformes. Présentation des risques : identification et synthèse des risques, distinction entre risques intentionnels et involontaires, cartographie et évaluation. Objectifs de sécurité : définition des objectifs de sécurité, mesures associées, acteurs et responsabilités. Matrice des risques : correspondance entre risques et objectifs, priorisation des mesures. Risques résiduels : risques restant après mise en œuvre des mesures et justification. Annexes : fiche de présentation du périmètre d'homologation, critères de sécurité et échelle des grandeurs utilisées, rapport de l'analyse de risques si besoin, liste des exigences de sécurité si absente du rapport.	Couvre la formalisation des besoins de sécurité, la synthèse des risques identifiés, l'établissement du socle de sécurité, la correspondance entre risques et objectifs de sécurité, ainsi que la justification des risques résiduels.
--	---	---

[Retour au TABLEAU](#)

DOSSIER DE CONFORMITE :

Le dossier de conformité évalue le respect des exigences de sécurité et l'état global de conformité du système.

Objectif

Attester que le système respecte les exigences définies et fournir une synthèse de l'état de sécurité pour la commission d'homologation.

VERT : Obligatoire pour les classes 1,2 et 3

ORANGE : Obligatoire pour les classes 2 et 3

ROUGE : Obligatoire seulement pour la classe 3

DOCUMENT	STRUCTURE / SECTIONS DETAILLEES	CONTENU ATTENDU
RAPPORT DE CONFORMITE	Présentation : le Rapport de Conformité évalue l'application des règles définies dans le socle de sécurité du système d'information. Il permet de vérifier si les exigences de sécurité sont respectées et d'identifier les écarts éventuels, en s'appuyant sur les résultats des audits, des contrôles et du suivi des mesures de sécurité. Ce document fournit une vue globale du niveau de conformité du SI et sert de base à la prise de décisions correctives et préventives. Objectifs : mesurer le niveau de conformité du SI par rapport au socle de sécurité, détecter les non-conformités, prioriser les actions correctives, renforcer la résilience du SI, améliorer les pratiques organisationnelles et techniques, et soutenir la mise à jour du socle de sécurité et des PES. Méthodologie : contrôle systématique des exigences du socle de sécurité, réalisation de tableaux de conformité pour chaque règle, analyse des écarts identifiés, suivi des recommandations issues des audits et inspections, et reporting synthétique sur l'état de conformité. Résultats et suivi : synthèse des critères évalués avec mention de leur conformité (conforme, partiellement conforme, non conforme), observations associées, priorisation des actions correctives et préventives, indicateurs de mesures pour évaluer de manière exhaustive le niveau de maturité cyber du SI. Annexes : tableaux de conformité détaillés, rapports d'audits et d'inspections associés, indicateurs de performance, références au socle de sécurité et aux PES, et plan d'action correctif recommandé.	Assurer un niveau de conformité mesurable et maintenu du SI, anticiper et réduire les risques, renforcer la sécurité organisationnelle et technique, et garantir la pérennité des mesures de sécurité mises en œuvre.

LISTE DES RISQUES RESIDUELS

Présentation : le document recense les **risques résiduels** identifiés après mise en œuvre des mesures de sécurité prévues. Il constitue un élément clé pour la **prise de décision de l'autorité d'homologation** et le suivi de la sécurité du système.

Identification des risques résiduels : description synthétique de chaque risque restant, nature (intentionnel ou involontaire), probabilité et impact résiduel, niveau de criticité.

Mesures déjà mises en œuvre : rappel des mesures appliquées pour réduire les risques et justification de leur efficacité partielle ou limitée.

Justification des risques acceptés : explication de la raison pour laquelle certains risques ne peuvent être éliminés ou réduits, incluant contraintes techniques, organisationnelles ou réglementaires.

Responsabilités et suivi : identification des acteurs responsables du suivi des risques résiduels et des actions correctives éventuelles à prévoir.

Annexes : tableaux synthétiques des risques résiduels, liens vers les documents d'analyse de risques et le socle de sécurité.

Fournir une vision claire et structurée **des risques restant** après mise en œuvre des mesures, justifier leur acceptation et permettre un suivi continu pour l'homologation et la gestion de la sécurité.

**PLAN D'AMÉLIORATION
CONTINUE DE LA
SÉCURITÉ (PACS)**

Présentation :

Le PACS définit les actions à réaliser régulièrement pour maintenir et améliorer la sécurité du système d'information. Il s'appuie sur les audits, les incidents et le suivi des mesures existantes, et constitue un outil stratégique pour assurer la résilience, la conformité et la mise à jour du SI.

Méthodologie :

Les actions sont identifiées pour chaque domaine critique et planifiées selon leur fréquence. Leur réalisation est suivie via un tableau centralisé, mis à jour régulièrement et revu par le RSSI. Les ajustements sont faits en fonction des incidents, des retours d'expérience et de l'évolution du contexte opérationnel ou réglementaire.

Actions planifiées :

Chaque action inclut la description, le responsable, la fréquence de réalisation, les indicateurs de suivi et les preuves de mise en œuvre telles que rapports, journaux ou captures d'écran.

Suivi et pilotage :

Le tableau de suivi centralisé permet de mesurer l'avancement, d'identifier les écarts et de mettre à jour les priorités. Le PACS est ajusté en continu pour refléter les changements dans le SI ou les nouvelles exigences.

Le PACS permet d'assurer une amélioration continue, mesurable et documentée de la sécurité du SI, en combinant planification, périodicité, suivi opérationnel et traçabilité des actions.

RAPPORT D'AUDITS

Présentation : le rapport d'audits synthétise les **contrôles effectués** sur le système d'information et évalue la **conformité aux exigences de sécurité** définies dans le socle de sécurité et la PES. Il constitue un support essentiel pour la validation de l'homologation et le suivi de la sécurité.

Objectifs des audits : vérifier la conformité aux exigences réglementaires, normatives et internes, détecter les non-conformités ou anomalies, et identifier les axes d'amélioration pour réduire les risques résiduels.

Méthodologie : description des techniques utilisées (audit documentaire, contrôle technique, tests de sécurité, évaluation organisationnelle), périmètre couvert, échantillons et critères d'évaluation.

Résultats des audits : synthèse des constats, liste des non-conformités, anomalies détectées, niveaux de criticité et recommandations associées.

Actions correctives : mesures préconisées pour traiter les non-conformités, responsables identifiés, planning de mise en œuvre et suivi.

Annexes : tableaux détaillés des constats, preuves des vérifications, rapports complémentaires, suivi des actions correctives et liens vers la PES et le socle de sécurité.

Fournir une vision claire et structurée **des résultats des audits**, permettre **la prise de décisions** pour la sécurité, justifier l'état du système et préparer les actions correctives ou l'évolution du plan de sécurité.

[Retour au TABLEAU](#)