POLITIQUE INTERNE / INTERNAL POLICY

POLITIQUE GENERALE DE SECURITE DE L'INFORMATION

Gestion documentaire

Projet : Certification TISAX
Objet : ISMS documentation
Classification : Restricted
Version : B
Date : 11 novembre 2024

Auteurs : Stéphane LAVERDURE – DSI

Version du document :

Version	Date	Auteur	Commentaires
A	02/11/2022	Alain Ennaji / Nuno Leitao	Version initiale
B	14/01/2025	Stéphane Laverdure	Version modifiée

Table des matières

Table des matières 2
1. Contexte de l'organisation 3
1.1. Engagement de la direction 3
1.2. Définition des enjeux 3
1.2.1. Enjeux internes 3
1.2.2. Enjeux externes 3
1.3. Définition des objectifs 3
1.4. Parties intéressées 3
2. Organisation du Système de Management de la Sécurité de l'Information (SMSI) 4
2.1. Domaine d'application : Définition et champ d'application du SMSI 4
2.2. Déclaration d'applicabilité 4
2.3. Politique de sécurité 5
2.4. Rôles et responsabilités du SMSI 5
3. Gestion du Système de Management de la Sécurité de l'Information (SMSI) 7
3.1. Comitologie 7
3.3. Evaluation de la performance 8
3.3.1. KPI 8
3.3.2. Audits internes et externes 8
3.3.3. Contrôles et révisions 9
3.4. Communication 9
3.5. Amélioration continue 9
3.5.1. Gestion des non-conformités et actions correctives 9
3.5.2. Plan d'action d'amélioration 9
4. Identification et gestion des risques 9
4.1. Identification et appréciation 10
4.2. Plan de traitement des risques 10
4.3. Revue de l'analyse de risque 10
5. Dérogations 11
6. Glossaire 11

1. CONTEXTE DE L'ORGANISATION

1.1. Engagement de la direction

L'engagement de la direction figure dans la lettre de direction :
E_M1_F11_A_Strategy_Letter_GMD_EUROCAST_TISAX_01.pdf

1.2. Définition des enjeux

1.2.1. Enjeux internes

- Créer et diffuser une culture de la sécurité de l'information.
- Assurer la continuité du système d'information
- Protéger le savoir-faire de GMD EUROCAST contre toute perte de confidentialité et d'intégrité.
- Maîtriser les risques stratégiques et opérationnels.

1.2.2. Enjeux externes

- Respecter les exigences des clients en termes de conformité.
- Protéger la confidentialité des informations des clients.
- Assurer la continuité du service aux clients.
- Promouvoir l'approche sécurité afin d'accéder à de nouveaux marchés.

1.3. Définition des objectifs

En définissant son Système de Management de la Sécurité de l'Information (SMSI), GMD EUROCAST s'est fixé les objectifs de sécurité :

- **OBJ.01** Assurer le bon fonctionnement et l'évolution des outils envers les collaborateurs de l'entreprise.
- **OBJ.02** Accroître la maturité de la sécurité de l'information sur les sites industriels de Delle et Reyrieux en obtenant la labellisation TISAX en juin 2025.
- **OBJ.03** Réorganiser le SMSI pour permettre le pilotage de la sécurité des sites industriels depuis le pôle Reyrieux, et préparer le déploiement du SMSI sur l'ensemble des sites, en obtenant le label TISAX en SGA dès juin 2025 et en préparant la labellisation des sites industriels pour juin 2026.
- **OBJ.04** Assurer la disponibilité des services envers les clients de GMD Eurocast.
- **OBJ.05** Protéger la confidentialité et l'intégrité des données confiées par les clients et garantir la sécurité des données confiées aux parties prenantes.

1.4. Parties intéressées

La mise en œuvre du SMSI doit viser à assurer aux parties intéressées le respect des attentes suivantes :

Source	Titre	Exigences
Externe	Tous les clients	• Respecter les exigences des clients en termes de conformité

7/1

		• Protéger la confidentialité et intégrité des informations relatives aux clients
Externe	Autorités règlementaires de chaque pays dans lesquels GMD EUROCAST est présent	• Respect des lois et règlements en vigueur
Interne	Tous les employés	• Confiance et respect internes pour un climat de travail de qualité
Interne	Direction	• Protection des investissements • Maintenir et développer la performance de l'entreprise • Protection de l'image de GMD Eurocast

1.5. Exigences réglementaires applicables

Les exigences règlementaires applicables, par pays, sont recensées dans le système de veille règlementaire RedOnline. La prise en compte des exigences légales doit être validée au sein de cet outil. Des objectifs de conformité et un indicateur de suivi de la conformité y est évalué.

En complément, les exigences réglementaires applicables liées à la sécurité de l'information doivent être recensées pour chaque pays dans le fichier géré par la DSI de GMD_Eurocast : E_M3_F14_Registre_de_veille_règlementaire_SSI.xlsx.

Pour chaque exigence légale identifiée relative à la sécurité de l'information, doit être suivi :

- L'applicabilité de l'exigence à GMD Eurocast,
- L'état de la conformité,
- Les éventuelles actions à mener.

2. Organisation du Système de Management de la Sécurité de l'Information (SMSI)

2.1. Domaine d'application : Définition et champ d'application du SMSI

Le périmètre d'évaluation TISAX définit le périmètre de l'évaluation. Cette évaluation porte sur l'ensemble des processus, procédures et ressources placés sous la responsabilité de l'organisation évaluée qui sont pertinents pour la sécurité des objets de protection et leurs objectifs de protection tels qu'ils sont définis dans les objectifs d'évaluation listés dans les sites listés.

L'évaluation est réalisée en appliquant à minima le niveau d'évaluation le plus élevé listé dans l'un des objectifs d'évaluation listés. L'évaluation porte sur l'ensemble des critères d'évaluation listés dans les objectifs d'évaluation listés.

La gouvernance de la SSI s'applique à l'entité Pôle Fonderie GMD EUROCAST, aux sites industriels de Reyrieux et de Delle, et aux personnes qui y sont contractuellement rattachées. L'objectif d'évaluation TISAX du SMSI est « Information with High Protection Needs », poursuivi en Simplified Group Assessment :

- Site Central : Pôle Fonderie GMD Eurocast.

- Sites industriels : Reyrieux et Delle.

Ce périmètre et le site concerné sont définis dans le document *TISAX Scope Excerpt propres à chaque site.*

2.2. Déclaration d'applicabilité

Pour protéger les actifs informationnels et gérer les installations de traitement de l'information, la déclaration d'applicabilité indique quelles exigences du standard TISAX sont appliquées par l'organisation. Elle fait partie intégrante de la documentation obligatoire qui doit être présentée à un auditeur externe lorsque le SMSI est soumis à un audit indépendant.

Toutes les questions de contrôle « Information Security » du *VDA_ISA_6.0.3* sont applicables.

2.3. Politique de sécurité

La politique de sécurité de l'information est un ensemble de règles d'exigences appliquées au SMSI, résultant de l'analyse des risques et des mesures de couverture des risques associées.

Les détails des exigences sont formalisés dans le document :
E_S5_I9_B_Politique_de_sécurité_des_systèmes_d_information_FR.docx.

2.4. Rôles et responsabilités du SMSI

Le sponsor

La direction générale de GMD EUROCAST est impliquée, en tant que sponsor, dans le SMSI pour le maintenir à jour et l'améliorer. Le sponsor de GMD EUROCAST est responsable du SMSI, il doit :

- Présider la Revue De Direction (RDD),
- Approuver la présente Politique générale de sécurité des systèmes d'information (PGSSI), ainsi que la Politique de Sécurité des Systèmes d'Information (PSSI),
- Assurer que les objectifs de la sécurité de l'information sont établis et sont compatibles avec la stratégie de GMD EUROCAST,
- Assurer la vérification de l'intégration du SMSI,
- Donner ses orientations sur ses choix et ses priorités par rapport au Système d'Information,
- Valider le Système d'Information et toutes les décisions relatives à la sécurité avec le Responsable SMSI/RSSI.

Directeur des Systèmes d'Information (DSI) :

Le DSI de GMD Eurocast doit :

- Identifier les plans d'actions annuels et pluriannuels appropriés,
- Proposer, pour arbitrage et validation, les orientations du SI au sponsor de GMD EUROCAST lors de la revue de direction,
- Elaborer et mettre en œuvre le plan de reprise d'activité en cas de sinistre majeur,
- Définir les objectifs de contrôle de la sécurité opérationnelle pour mesurer l'application et l'efficacité des exigences de sécurité.
- Organiser et animer la RDD, le COSSI et les CPSSI.

Le Responsable de la Sécurité du Système d'Information (RSSI)

Le RSSI de GMD EUROCAST définit la stratégie globale de sécurité des systèmes d'information en :

- Suivant les indicateurs de performance et l'avancement du plan d'action du SMSI,
- Construisant et tenant à jour l'analyse des risques,
- Définissant les exigences de sécurité à appliquer pour couvrir les risques majeurs identifiés,
- Prend en charge la mise en œuvre des actions de traitement des risques et tâches d'amélioration du Système de Sécurité de l'Information,
- Collectant les indicateurs de performance et maintenant à jour le plan d'action,
- Supervisant et participant à la mise en œuvre des mesures de sécurité du SI,

- Supervisant les processus de gestion des incidents de sécurité et les actions correctives et préventives associées,
- Rendant compte au sponsor :
    - Du niveau de couverture des risques de sécurité du SI identifiés par GMD EUROCAST,
    - Des nouveaux risques identifiés,
- Assurant des révisions périodiques des documents techniques, conformément à la politique de gestion documentaire.
- Organiser et animer les COPIL SMSI locaux.

Il propose, pour arbitrage et validation au sponsor, les changements à apporter au plan d'action en cours d'année.

Il pilote opérationnellement le plan d'action et coordonne les différents contributeurs de la SSI au quotidien.

En cas de détection d'une anomalie ou d'un incident de sécurité de l'information, il supervise le traitement et, le cas échéant, alerte les services ou partenaires concernés et/ou les personnes compétentes.

Le Responsable SMSI (RSMSI) :

Le Responsable SMSI de GMD Eurocast doit :

- Rendre compte de l'efficacité du SMSI,
- Lors des comités opérationnels (COSSI), assure que les documents supports sont disponibles, proposant les ordres du jour et rédigeant les comptes rendus de réunion sous forme de relevés d'informations, actions et décisions,
- S'assurer que la PGSSI et la PSSI sont bien communiquées à tous les collaborateurs de l'organisation,
- Superviser le processus de révision et de validation des documents.

Le Responsable SMSI doit également assurer le suivi de la mise en conformité des sites aux politiques de sécurité de l'information.

Les Correspondants Locaux de la Sécurité de l'Information (CL-SI) :

Les Correspondants Locaux de la Sécurité de l'Information de GMD Eurocast doivent :

- Assurer la communication et le déploiement des politiques de sécurité de l'information.
- Mettre en œuvre le plan de contrôles et revues *E_S5_F5_B_Control_Review_and_Audit_Planning _FR_EN.xlsx* local, et informer le RSMSI de la réalisation des contrôles et des écarts éventuels.
- Suivre les plans d'actions et de traitement des risques locaux.
- Assurer la remontée d'incidents locaux au RSSI.
- Assurer la collecte des indicateurs spécifiques au site.
- Tenir à jour le self-assessment local et participer aux audits du SMSI.
- Participer au COPIL SMSI Local.
- Participer à la RDD du site pour remonter les KPI et informations relatives à la Sécurité de l'Information.

Collaborateurs

Tous les collaborateurs se trouvant dans le périmètre du SMSI doivent :

- Respecter l'intégralité de la PSSI,
- Être sensibilisés à la sécurité,
- Signaler les incidents au RSSI ou au responsable du SMSI,
- Participer à la construction de l'analyse des risques et du plan de couverture des risques.

Le Data Protection Officer (DPO)

Le DPO doit :

- S'assurer de la conformité des données personnelles de GMD EUROCAST avec le règlement général sur la protection des données (RGPD),
- S'assurer que le registre des traitements est tenu à jour,
- Informer la direction générale des non-conformités potentielles au RGDP.

Les propriétaires d'actifs

L'objectif des règles suivantes est de mettre en place et de maintenir une protection appropriée des actifs de GMD EUROCAST et de ses clients :

- Lors de l'analyse des risques, chaque responsable de service réalise et tient à jour un inventaire de tous les actifs informationnels indispensables à son bon fonctionnement. Cet inventaire comprend notamment les données techniques internes, les clients ainsi que les données financières et commerciales,
- Les actifs support sont également identifiés : équipements d'infrastructure de systèmes et de réseaux, applications, base de données, etc.,
- Chaque actif a un propriétaire désigné.

Le propriétaire d'un actif :

- Est responsable de la maintenance de cet actif, de son contrôle, de sa classification en termes de confidentialité et de sa protection,
- Définit les règles permettant l'utilisation de cet actif dans de bonnes conditions de sécurité. Ces règles sont documentées dans le SMSI (politiques, procédures, instructions, chartes et normes de sécurité),
- Faire appliquer ces règles et contrôler leur mise en œuvre.

Les propriétaires de risques :

Chaque propriétaire de risque est responsable du choix des méthodes de traitement des risques, de la validation des plans d'actions destinés à traiter ces risques et de l'allocation des ressources nécessaires à la réalisation de ces plans.

3. Gestion du Système de Management de la Sécurité de l'Information (SMSI)

3.1. Comitologie

Les instances de pilotage de la sécurité de l'information SMSI au site central sont :

- La RDD (Revue De Direction), réalisée de manière annuelle, en présence du sponsor. C'est l'organe de décision du sponsor de suivi des risques et de suivi de la maturité du SMSI,
- Le COSSI (Comité Opérationnelle de Sécurité des Systèmes d'Information), de manière trimestrielle, intégrant les responsables de service. Il représente le suivi technique des plans d'actions, des solutions de sécurité et des aspects opérationnels de l'analyse de risque, ainsi que des indicateurs de sécurité,
- Le CPSSI (Comité de Pilotage de la Sécurité des Systèmes d'Information) traite des incidents de sécurité, de la gestion des changements, etc.

Nom	Fréquence	Participants	Points abordés	Livrable
CPSSI	Mensuelle	DSI RSMSI RSSI Parties prenantes intéressées	• Gestion des incidents de sécurité • Gestion des changements • Suivi des revues et contrôles	CR de CPSSI
COSSI	Trimestrielle	CPSSI Responsables de service	• Suivi des indicateurs du SMSI • Suivi de l'avancement des plans d'action • Suivi du plan de traitement des risques	CR de COSSI

RDD	Annuelle	COSSI Sponsor	• Bilan de la performance du SMSI sur l'année écoulée • Revue des objectifs sécurité et des plans d'action pour l'année à venir	CR de RDD

De plus, chaque site doit également organiser les instances de pilotage suivantes :

Nom	Fréquence	Participants	Points abordés	Livrable
COPIL SMSI Local	Semestriel	CL-SI Responsables de service RSSI	• Suivi des indicateurs du SMSI • Suivi de l'avancement des plans d'action • Suivi du plan de traitement des risques	CR de COPIL
RDD site (Intégrée à la RDD existante)	Annuelle	CL-SI Sponsor	• Bilan de la performance du SMSI sur l'année écoulée. • Revue des objectifs sécurité et des plans d'action pour l'année à venir.	CR de RDD site

3.2. Gestion documentaire de la politique de sécurité

La gestion documentaire respecte un formalisme pour les documents du SI qui sont :

- Les politiques,
- Les processus,
- Les procédures,
- Les instructions techniques (modes opératoires),
- Les enregistrements.

Pour chacun de ces documents, il est nécessaire de mettre en place :

- Une identification unique,
- Un cycle de création, modification, approbation et validation,
- Une classification en termes de confidentialité, suivant quatre niveaux : public, restricted, sensitive, confidential,
- Leur durée de vie et leur temps de conservation.

La documentation du SMSI doit être revue sur une base régulière, annuelle. L'ensemble de ces règles et usages est défini au sein de la procédure de gestion documentaire : *E_M2_P1_Maîtrise_des_documents.xlsm*.

3.3. Evaluation de la performance

3.3.1. KPI

Les KPI sont des indicateurs qui permettent de mesurer les objectifs. Ils sont construits par l'ensemble des acteurs du périmètre SMSI, consolidés par le RSMSI et présentés lors des COSSI et de la RDD. L'ensemble des KPIs est centralisé dans le document : E_*S5_F4_Report_A3_IT_Indicators_Incident_FR_EN.xslx*.

Le RSSI de GMD Eurocast est également responsable du suivi des indicateurs de la Sécurité de l'Information des sites inclus dans le périmètre du SMSI. Ces indicateurs sont suivis au sein du même document.

3.3.2. Audits internes et externes

Les règles ci-après ont pour objectif de s'assurer de la conformité des systèmes d'information avec les politiques de sécurité de GMD EUROCAST :

- Des audits de sécurité sur les projets peuvent être réalisés par le CPSSI, afin de vérifier que les activités réalisées sont conformes aux politiques et règles de sécurité du Groupe,
- La conformité du SMSI par rapport aux exigences TISAX est vérifiée tous les ans,

- Les activités d'audit de sécurité et de test de la sécurité des systèmes d'information sont planifiées, afin de réduire autant que possible le risque de perturbation des processus métiers.

3.3.3. Contrôles et révisions

En cours d'années, des contrôles et revues sont décidés auprès des collaborateurs lors des réunions hebdomadaires de l'équipe IT. La méthodologie choisie est la suivante :

- Désignation d'une personne au sein d'une équipe,
- La personne désignée doit s'approprier le périmètre cible avant d'effectuer le contrôle d'un sujet du SMSI,
- Elle réalise le compte-rendu du contrôle avant de le communiquer au RSMSI,
- Le collaborateur présente les résultats obtenus au cours de la réunion suivante,
- Le RSMSI prend en compte les résultats et complète le cas échéant le plan d'amélioration sécurité.

De plus, l'ensemble des contrôles et revues opérationnelles (revue des droits systèmes, applicatifs, réseaux, test du PCA, tests des sauvegardes, ...) est centralisé dans le fichier : *E_S5_F5_Control_Review_and_Audit_Planning_FR_EN.xlsx*.

3.4. Communication

La communication sur les enjeux internes et externes du SMSI est définie vers les parties intéressées.

La PGSSI est communiquée aux parties intéressées qui en font la demande ou lorsqu'un changement majeur est déployé.

En interne, la communication est réalisée au travers de :

- Emails réguliers de sensibilisation,
- L'équipe RH,
- Informations lors des différents comités de pilotage.

La communication vers les parties intéressées pertinentes (ANSSI, CNIL, Autorités) est également intégrée dans le processus de gestion de crise.

3.5. Amélioration continue

3.5.1. Gestion des non-conformités et actions correctives

Les non-conformités sont identifiées lors des audits internes et externes, et en continu par les collaborateurs. Chaque non-conformité doit donner lieu à un traitement :

- Analyse de la cause racine,
- Formalisation de la correction,
- Définition, présentation et validation du plan d'action correctif auprès du CPSSI.

La synthèse des non-conformités est présentée au sponsor lors de la RDD.

3.5.2. Plan d'action d'amélioration

Un plan d'action global centralise les différents chantiers sécurité, décidés à partir de différentes sources : analyse de risques, comités de pilotage, résultats des audits, incidents de sécurité, failles de vulnérabilité... Il s'agit du document *Plan_d_Action_Eurocast*.

4. Identification et gestion des risques

Une analyse des risques est effectuée annuellement par le RSSI. Elle s'appuie sur les principes de la méthodologie EBIOS.

Elle a pour objet d'identifier et d'apprécier les risques bruts, puis de vérifier la réduction effective des risques traités, d'accepter le niveau de risque résiduel, de prendre en compte les nouveaux risques, d'analyser les dérogations et d'ajuster le plan d'action si besoin.

Une revue intermédiaire peut être déclenchée à la demande du comité de pilotage en dehors de la planification annuelle, en cas d'occurrence d'un événement susceptible d'impacter significativement la sécurité de l'information : changement majeur (déménagement, évolution règlementaire, changement organisationnel), incident de sécurité critique, etc.

4.1. Identification et appréciation

L'analyse de risque chez GMD Eurocast se base sur l'identification de(s) :

- Actifs essentiels et leur classification,
- L'inventaire des bien supports,
- L'analyse des scénarios d'attaques sur les biens supports composés de la vulnérabilité et de la menace
- La caractérisation des risques qui sont la composition de la vraisemblance du scénario d'attaque avec l'impact sur l'actif essentiel.

Les critères d'acceptation sont déterminés dans les échelles définies dans le document d'analyse de risques.

Les propriétaires de risques sont définis et précisés dans l'analyse de risque. Le résultat d'analyse de risque est formalisé dans le document : *E_S5_F7_Analyse_de_risque_SSI_FR.xlsm*.

Les risques à superviser par les sites industriels sont identifiés centralement et recensés au sein du même document, dans une feuille à part. L'état de couverture des risques propres aux sites industriels doit être évalué individuellement sur chaque site, et suivi centralement par le RSSI.

4.2. Plan de traitement des risques

Une fois les risques appréciés, l'organisme doit proposer un ensemble de plans d'actions afin de réduire ces risques. Ces plans d'actions sont pris en référence aux exigences du standard TISAX.

L'ensemble de ces points doit être régulièrement accepté par le sponsor au cours des COSSI et revue de direction successifs.

Les sites industriels doivent également identifier les actions nécessaires à la couverture des risques qui leur sont spécifiques.

Le plan de traitement des risques et le plan d'action qui en découle sont définis dans le document : *E_S5_F7_Analyse_de_risque_SSI_FR.xlsm*.

4.3. Revue de l'analyse de risque

Critères de réalisation :

L'analyse de risque doit être revue régulièrement, ainsi qu'à l'issue de tout événement pouvant toucher les facteurs d'impact ou de vraisemblance d'un quelconque risque. Le changement de l'analyse de risque est effectué sur :

- Changement majeur,
- Incident critique,
- Veille et information relatives aux vulnérabilités,
- Revues périodiques planifiées,
- Résultats des audits et contrôles.

Les évènements suivants doivent être pris en considération lors des revues :

- Les nouveaux contrôles de sécurité mis en œuvre depuis la dernière évaluation des risques,

- Les incidents survenus depuis la dernière évaluation des risques au sein du périmètre de l'analyse.

5. Dérogations

L'ensemble des règles énoncées dans la PGSSI constitue des exigences de sécurité à respecter. Toutefois, à titre exceptionnel, des dérogations peuvent être établies dans un cadre spécifique :

- Demande exprimée par un employé et approbation formelle du RSSI ou du sponsor du SMSI sous la forme d'une fiche de dérogation,
- Tenue d'un registre des dérogations par le RSSI,
- Chaque dérogation est limitée dans le temps et sa pertinence doit faire l'objet d'un suivi régulier. Ce suivi est intégré dans le plan de contrôle, d'audit et de révision.

6. Glossaire

Abréviation	Définition
RSSI	Responsable de la Sécurité des Systèmes d'Information
PGSSI	Politique Générale de la Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
PSSI	Politique de Sécurité des Systèmes d'Information

Rédacteur	Vérificateur	Approbateur
Directeur Système d'Information Stéphane LAVERDURE	Le Sponsor Alain GIL	Directeur Général, Yves MAYET

- Les incidents survenus depuis la dernière évaluation des risques au sein du périmètre de l'analyse.

5. Dérogations

L'ensemble des règles énoncées dans la PGSSI constitue des exigences de sécurité à respecter. Toutefois, à titre exceptionnel, des dérogations peuvent être établies dans un cadre spécifique :

- Demande exprimée par un employé et approbation formelle du RSSI ou du sponsor du SMSI sous la forme d'une fiche de dérogation,
- Tenue d'un registre des dérogations par le RSSI,
- Chaque dérogation est limitée dans le temps et sa pertinence doit faire l'objet d'un suivi régulier. Ce suivi est intégré dans le plan de contrôle, d'audit et de révision.

6. Glossaire

Abréviation	Définition
RSSI	Responsable de la Sécurité des Systèmes d'Information
PGSSI	Politique Générale de la Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information
PSSI	Politique de Sécurité des Systèmes d'Information

Rédacteur	Vérificateur	Approbateur
Directeur Système d'Information Stéphane LAVERDURE le 10/03/2025	Le Sponsor Alain GIL 10/03/2025	Directeur Général, Yves MAYET