

Gouvernance cybersécurité et Master Plan SI sur 10 ans

Retour d'expérience
Table ronde du 25.02.2026

Présentation

Commune de Marly :

Marly est une commune accueillante d'environ ~9700 habitants, active et diversifiée tant sur le plan économique que sur celui de la vie sociale. Située au sud de Fribourg, elle propose et gère une multitude de services destinés à la communauté et aux habitants

Qui suis-je :

Je m'appelle Hugo Calhau, Responsable Informatique / RSSI à la Commune de Marly. Depuis juillet 2022, je pilote l'infrastructure SI dans son ensemble et j'assure la fonction de RSSI.

Périmètre & ordres de grandeur du SI :

- 16 bâtiments interconnectés via fibre noire (black fiber) (administration communale, écoles (3 centres scolaires), crèches, AES)
- Deux backbones (dorsales réseau) distincts : Administration et Scolaire
- 3 clusters de pare-feu (dont 2 bastions de sécurité), 60 commutateurs (switches), 200 points d'accès Wi-Fi.
- Environ 200 collaborateurs, ~550 postes clients (PC & Mac), ~50 imprimantes, 30 serveurs et 50 mobiles (téléphones)

Pourquoi ce sujet est politique (avant d'être technique)

- Cybersécurité = continuité des services publics + confiance des citoyens
- Protection des données : obligations (LPD) + responsabilité des autorités
- La gouvernance fixe : qui décide / qui exécute / qui contrôle (auditable)
- **Point clé : sans cadre, les décisions se prennent « en crise »**

La Gouvernance : « Elle décrit l'engagement des autorités communales, tant politiques qu'administratives »

Comment on à démarré : une méthode (pas un catalogue d'outils)

1. État des lieux
 - Cartographier l'existant
 - Identifier dépendances & irritants (coûts, support, sécurité)
2. Cadastre des risques
 - Lister risques majeurs
 - Repérer où l'audit/LPD attend des preuves
3. Gouvernance
 - Rôles, règles, processus
 - Gestion documentaire & validation
4. Priorisation
 - Matrice probabilité × gravité
 - Mesures proportionnées
5. Planification
 - Feuille de route
 - **Master Plan 10 ans (phases, coûts, jalons)**

« État des lieux → Cadastre des risques → Gouvernance → Matrice des risques → Feuille de route → **Master Plan** »

Gouvernance cyber : périmètre & rôles

- Portée
 - Employés, élus, prestataires, partenaires
 - Ensemble des composants et des données du SI (système d'information)
- Rôles clés
 - RSSI : définition des politiques, mise en œuvre des mesures, surveillance et gestion des incidents
 - RSIPD : sécurité de l'information et protection des données

Processus couverts : Incidents, vulnérabilités, actifs, fournisseurs, audits et documentation

But : Sécurité, conformité, protection des données et clarification des responsabilités

« Le Conseil Communal nomme un Responsable de la Sécurité des Systèmes Informatiques (RSSI). »

Gouvernance (processus)



☒

C2-/Interne☒	☒
Réf:- SI_R00.☒	☒
Version:-A0.☒	
Date:-14.10.2024☒	

☒

Index☒

☒

INDEX.....☒	11☒
GOVERNANCE INFORMATIQUE☒	1☒
1 → OBJECTIF☒	1☒
3 → PRINCIPAUX-PROCESSUS, POLITIQUES-ET-NORMES☒	2☒
3.1 → SI.PR01.POLITIQUE-DE-SÉCURITÉ-INFORMATIQUE (PSI)☒	2☒
3.2 → SI.PR02.PROCESSUS-DE-GESTION-DES-ACTIFS-INFORMATIQUES☒	2☒
3.3 → SI.PR03.PROCESSUS-DE-GESTION-DES-MESURES-DE-SÉCURITÉ-TECHNIQUES☒	3☒
3.4 → SI.PR04.PROCESSUS-MESURES-DE-SÉCURITÉ-ORGANISATIONNELLE☒	5☒
3.5 → SI.PR05.PROCESSUS-DE-MONITORAGE-ET-SURVEILLANCE-DES-SYSTÈMES☒	6☒
3.6 → SI.PR06.PROCESSUS-DE-GESTION-DES-VULNÉRABILITÉS☒	7☒
3.7 → SI.PR07.PROCESSUS-CONFIDENTIALITÉ-ET-PROTECTION-DES-DONNÉES☒	8☒
3.8 → SI.PR08.PROCESSUS-DE-GESTION-DU-SUPPORT-&-DES-DEMANDES (ITSM) (EN-COURS)☒	9☒
3.9 → SI.PR09.PROCESSUS-DE-GESTION-DES-INCIDENTS-DE-SÉCURITÉ-INFORMATIQUE☒	9☒
3.10 → SI.PR10.PROCESSUS-DE-GESTION-DES-INTERVENANTS-EXTERNES☒	10☒
3.11 → SI.PR11.PROCESSUS-DE-GESTION-DES-MANQUEMENTS-AUX-DEVOIRS-DE-SERVICE.....☒	11☒
4 → SCHÉMAS☒	11☒
5 → RACI (RESPONSABLE, APPROBATEUR, CONSULTÉ, INFORMÉ)☒☒	11☒
6 → LISTE-DES-ABRÉVIATIONS☒	11☒
7 → ANNEXES☒	12☒

☒

La matrice de risques : un langage commun (politique + technique)

Outil de priorisation : probabilité × gravité = criticité

Exemples de risques « très critiques » : phishing, ransomware, accès non autorisé, etc.

Inclut aussi les risques LPD : non-conformité, obligations de notification, etc.

Ca permet :

- prioriser (quoi d'abord)
- d'expliquer les investissements en termes de réduction de risques
- définir les risques qui sont acceptables

Exemples

Registre des risques			Echelles		Registre des risques					Registre des problèmes		Matrice	Paramétrage		
Ajouter un risque	Supprimer un														
ID	Nature de risque	Description	Gravité	Probabilité	Criticité	Conséquences si avéré 1/5	Conséquences si avéré 2/5	Conséquences si avéré 3/5	Conséquences si avéré 4/5	Conséquences si avéré 5/5	Tendance	Responsable	Actions préventives Mesures de contrôle Recommandées	Actions correctives	Efficacité nécessaire des Mesures de Contrôle
R1	Humain	Attaque par phishing (e-mail)	Catastrophique	Probable		[Vol Perte Diffusion Accès non autorisé] (à)de données	[Répercussions Pertes] financières	Atteinte à la réputation	Indisponnibilité des systèmes et/ou des données	Compromission des systèmes et propagation de malware			-Formation : Formations régulières des employés à la cybersécurité -Procédures : Mise en place de procédures à suivre en cas de réception d'e-mails suspects -Communication interne claire sur les procédures à suivre en cas de réception d'e-mails suspects		Efficace
R2	Technique	Attaque par phishing	Catastrophique	Probable		[Vol Perte Diffusion Accès non autorisé] (à)de données	[Répercussions Pertes] financières	Atteinte à la réputation	Indisponnibilité des systèmes et/ou des données	Compromission des systèmes et propagation de malware			- Mise en place de des filtres anti-phishing - Mise en place de système de sandboxing et filtrage - Mise en place d'un système de déclaration de mails-suspects		Efficace
R3	Technique	Accès non autorisé aux systèmes	Catastrophique	Probable		Indisponnibilité des systèmes et/ou des données	[Vol Perte Diffusion Accès non autorisé] (à)de données	[Répercussions Violations] juridiques et/ou réglementaires	[Répercussions Pertes] financières	Atteinte à la réputation			- Authentification à deux facteurs : Mise en œuvre d'une authentification à deux facteurs. - Politique de gestion et suivi de contrôles d'accès : Limiter l'accès selon POLP - Procédure de révision des droits d'accès : Mise en place procédures d'audit et de révision des droits d'accès		Efficace
R4	Technique	Perte de données sensibles	Catastrophique	Peu probable		Indisponnibilité des systèmes et/ou des données	[Répercussions Pertes] financières	Atteinte à la réputation	n/a	n/a			- Politique de Sauvegardes et de restauration : Disposer de sauvegardes fiables et testez régulièrement leur restauration. - Chiffrement des données : Utiliser un chiffrement robuste pour protéger les données sensibles. - Politique de gestion et suivi de contrôles d'accès : Limiter l'accès aux données sensibles uniquement aux personnes nécessaires - Procédure d'audit et contrôles réguliers : Réaliser des audits de sécurité pour identifier et rectifier les vulnérabilités qui pourraient conduire à une perte de données.		Très efficace
R5	Technique	Virus / Malware	Grave	Probable		Compromission des systèmes et propagation de malware	[Vol Perte Diffusion Accès non autorisé] (à)de données	[Répercussions Violations] juridiques et/ou réglementaires	Indisponnibilité des systèmes et/ou des données	Atteinte à la réputation			- Mise en place de firewalls robustes avec les protection (anti-virus, anti-malware, IDS,IPS, NAC, URL-Filtering, gecontrol) - Mise en place d'anti-virus sur les clients et les serveurs - Mise en place d'un EDR - Mise en place d'appliances de sécurité (IOC, OD, Log, Monitorine)		

Etat (2023)



Date de création	28.11.2022
Date de la version	21.09.2023
Numéro de version	V2.3

[Matrice de criticité des risques](#) |
 [Guide d'utilisation](#) |
 [Echelles](#) |
 [Registre des risques](#) |
 [Registre des problèmes](#) |
 [Matrice](#) |
 [Paramétrage](#)

Nom / Code projet	SIPD Commune de Marly
Référence	SI_R10.A0

Service / Secteur	Administration générale / Inform
Responsable	Hugo Calhau, Nicolas Gex

LÉGENDE »

- R1 Attaque par phishing (e-mail)
- R2 Attaque par phishing
- R3 Accès non autorisé aux systèmes
- R4 Perte de données sensibles
- R5 Virus / Malware
- R6 Divulgence d'informations confidentielles
- R7 Hameçonnage via un site web public
- R8 Accès physique non autorisé
- R9 Vol de matériel informatique
- R10 Intrusion dans le réseau par un employé malveillant (menace interne)
- R11 Fraude interne
- R12 Perte de matériel contenant des données sensibles
- R13 Attaque par force brute sur les systèmes d'authentification
- R14 Compromission de fournisseurs tiers ou de partenaires
- R15 Incident de sécurité impliquant des appareils personnels (BYOD)
- R16 Manque de sensibilisation à la sécurité parmi les employés
- R17 Utilisation non sécurisée de l'Internet public
- R18 Attaques par ransomware
- R19 Vol d'identité en ligne
- R20 Logiciels non autorisés sur les systèmes de l'entreprise
- R21 Fuite d'information via les médias sociaux
- R22 Erreurs humaines menant à des fuites de données
- R23 Cyber-espionnage
- R24 Insuffisance des politiques de sécurité
- R25 Intrusion par l'intermédiaire de fournisseurs tiers non sécurisés

	Improbable	Peu probable	Probable R1 R2 R3	Très probable
Catastrophique		R4 R6 R23 R39 R49 R57 R60 R69	R25 R26 R29 R30 R33 R35 R41 R45 R52 R54 R55 R56 R14 R15	R18 R31 R32 R55
Grave	R42	R8 R10 R11 R12 R21 R34 R38 R40 R47 R48 R51 R56 R58 R63 R64	R16 R17 R19 R24 R27 R28 R36 R37 R46 R53 R61 R65	R7 R22 R43 R44 R50
Majeur			R9 R20	
Mineur				

Leviers pour convaincre : audits (SIPD) & contrôles

- Audit = référentiel externe : écarts, priorités, preuve de progression, suivre les actions
- Thèmes couverts (extraits)
 - Personnel (confidentialité, formation)
 - Actifs (inventaire, cycle de vie)
 - Droits d'accès (rôles, need-to-know)
 - Fournisseurs/externalisation
 - Gestion incident (voies d'info, fall-back)

Bénéfice politique : décisions basées sur des faits + rend la progression démontrable (rapports).

But : Il légitime la gouvernance (processus, documentation, responsabilités, etc.)

Leviers pour convaincre : Pentest (test d'intrusion) : mesurer, corriger, re-tester (preuves)

- Tester la résistance réelle, produire un rapport et un plan de remédiation
- Un contre-audit valide l'efficacité des corrections
- Utile politiquement : investissement mesurable (avant/après)

Internaliser et réduire les prestataires : contrôle + économies

Spécificité (Commune de Marly)

- Stratégie : reprendre la maîtrise des briques critiques (serveurs, sauvegardes, sécurité)
- Résultat attendu : réduire la dépendance aux prestataires, renforcer la gouvernance et mieux maîtriser les coûts
- Argument politique : générer des économies à long terme afin de financer la trajectoire définie dans le **Master Plan**

Passerelle vers le politique : Commission des Systèmes d'Information (CoSI)

Pourquoi

- Comprendre, analyser et « traduire » les sujets informatiques avant toute décision

Mission

- Analyser les aspects techniques, financiers et les risques.
- Transmettre aux groupes politiques et au Conseil général une synthèse claire et accessible (avantages, coûts, risques, impacts)

Composition

- Conseillers communaux (Administration générale / Finances) et représentants de l'administration.
- Conseillers généraux (représentants des partis) et experts externes, selon les domaines

Circuit de décision (pratique recommandée)

- Le service informatique prépare et documente les propositions
- La CoSI les challenge, les priorise et facilite la compréhension.
- Le Conseil communal arbitre.
- Le Conseil général statue (message d'investissement)

Master Plan 10 ans : vision, phasage, cohérence

Le Master Plan transforme une liste de projets en une trajectoire cohérente

Briques stratégiques

- Sécurité
- Cycle de vie
- Formation
- Logiciels
- Cloud
- ERP
- Informatique communale

Apports

- Vision (où on va)
- Phasage (quand)
- Coûts/ROI (combien/pourquoi)
- Cohérence (interconnexions)

Exemple de notre Master Plan 10 ans

1 → Table des matières

- 1 → Introduction 5
- 1.1 → L'informatique dans l'Administration Communale 5
- 1.2 → Objectifs du Master Plan 5
- 2 → État actuel de l'infrastructure informatique et des solutions logicielles 7
- 2.1 → L'environnement actuel de l'infrastructure (état fin 2023) et bref historique 7
- 2.1.1 → Historique 7
- 2.1.2 → État de l'infrastructure informatique (fin 2023) 7
- 2.2 → Solutions logicielles actuelles 12
- 2.2.1 → Bureautique 12
- 2.2.2 → ERP 12
- 2.2.3 → GED 12
- 2.2.4 → Gestion du Service Social 13
- 2.2.5 → Gestion des amendes et des autorisations de parcage 13
- 2.2.6 → Geoconcept 13
- 2.2.7 → Aquametro 13
- 3 → Analyse des besoins 14
- 3.1 → Besoins actuels et futurs en termes de logiciels, hardware et sécurité 14
- 3.1.1 → Sécurité 14
- 3.1.2 → Hardware 17
- 3.1.3 → Logiciels 17
- 3.2 → Résultats des audits de sécurité et mesures correctives nécessaires 19
- 3.3 → Exigences pour le remplacement périodique du matériel 20
- 3.4 → Analyse pour le remplacement actuel du ERP (système de gestion de la commune) 21
- 3.5 → Évaluation de l'introduction de serveurs hébergés au lieu de serveurs en SMaaS 22
- 4 → Plan d'action Stratégique 24
- 4.1 → Mise en œuvre de mesures de renforcement de sécurité pour les serveurs et les clients 24
- 4.2 → Processus de remplacement du matériel 24
- 4.3 → Mise en place de solutions cloud avec Microsoft 365 E5 et Azure AD 24
- 4.4 → Introduction d'un nouveau ERP 26
- 4.5 → Remplacement des serveurs SMaaS par des serveurs hébergés 27
- 5 → Plan de formation des Utilisateurs 29

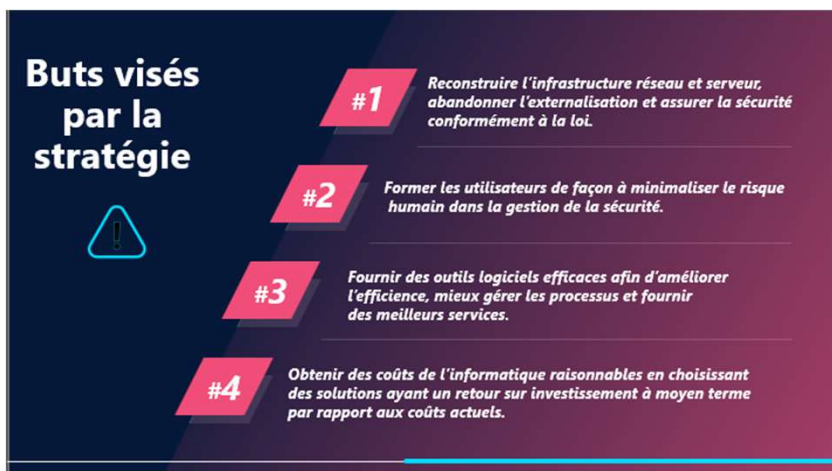


Master Plan des Systèmes d'Information 2024 - 2034

<i>C4 - Confidentiel</i>
Réf.: SI_R20
Version: A0
Date: 13.10.2023

- 5.1 → Plan de formation sur les nouvelles solutions logicielles 29
- 5.2 → Formation sur l'utilisation du nouveau ERP 29
- 5.3 → Sensibilisation à la sécurité et aux meilleures pratiques 29
- 6 → Estimation des coûts 30
- 6.1 → Détail des dépenses 31
- 6.2 → Détail des économies réalisées 33
- 6.3 → Calcul du retour sur investissement 34
- 7 → Plan de mise en œuvre 35
- 7.1 → Renforcement de la sécurisation des serveurs et des clients 35
- 7.2 → Remplacement de matériel selon leur cycle de vie 35
- 7.3 → Cycle de formation des utilisateurs, audits de sécurité et remédiation des failles 35
- 7.4 → Nouvelles solutions logicielles 36
- 7.5 → Solutions cloud avec Microsoft 365 E5 et Azure 36
- 7.6 → Remplacement du ERP actuel et re-engineering des processus administratifs 37
- 7.7 → Remplacement des serveurs en SMaaS par un système hébergé 37
- 8 → Conclusion 38
- 9 → Lexique des abréviations 39

Exemple : Présentation Master Plan 10 ans CG



Solutions vs Risques

- On part des risques prioritaires → on définit les capacités (prévenir / détecter / répondre)
 - Exemples de capacités
 - ✓ Protection (prévention)
 - ✓ Détection & surveillance
 - ✓ Réponse & continuité
 - ✓ Gestion fournisseurs
- On retient ensuite des solutions proportionnées, compatibles entre elles et évolutives.

Repères pour réussir (démarche duplicable)

- 1) Gouvernance écrite : périmètre, rôles, processus, documentation
- 2) Pilotage politique : arbitrer le risque résiduel, suivre les jalons
- 3) Leviers : audits (SIPD), pentests (test d'intrusion), rapports réguliers
- 4) Trajectoire 5-10 ans : investissements + coûts récurrents + ROI (retour sur investissement)
- 5) Internalisation ciblée : maîtriser les briques critiques

Questions ?

