

Rapport d'analyse de marché

Pertinence de la création d'un groupe de travail
"Sécurité de l'information et protection des données
dans l'administration publique - SIPD"

Rapport d'analyse de marché	1
1. Résumé exécutif / Synthèse	3
1.1 - Objectif du rapport	3
1.2 - Méthode	3
1.3 - Principales conclusions	3
1.4 - Recommandation finale	3
2. Introduction	4
2.1 - Contexte général	4
2.2 - Objectif du rapport	4
2.3 - Méthodologie	4
<i>Tableau: Profil des personnes interrogées</i>	5
3. Constats généraux	6
3.1 - Situation actuelle dans les administrations publiques	6
3.2 - Attentes globales exprimées	7
3.3 - Enjeux identifiés	7
3.4 - Les thématiques identifiées	7
<i>Tableau: Importance des thématiques</i>	8
<i>Tableau: Autres thèmes relevés</i>	8
3.5 - Perception de la coordination existante	8
4. Constats spécifiques aux thématiques	9
4.1 - Maturité et besoins des communes	9
4.2 - Risques liés aux fournisseurs	9
4.3 - Sensibilisation et formation du personnel administratif	10
4.4 - Réponse aux incidents	11
5. Constats spécifiques au GdTS-SIPD	12
5.1 - Attentes envers eCH.ch	12
<i>Tableau : Notoriété d'eCH.ch</i>	12
5.2 - Points de vigilance et freins	13
<i>Tableau : Organisations prêtes à participer</i>	13
5.3 - A quoi ressemble le succès du GdTS-SIPD	14
6. Conclusions et recommandations	15
6.1 - Pertinence globale de la création du groupe	15
6.2 - Périmètre et priorités proposées	15
6.3 - Propositions concrètes	15
7. Annexes	16
<i>Guide d'entretien</i>	16
<i>Liste des personnes interrogées (répondants)</i>	17
<i>Tableau: Idées de normes / initiatives sur lesquelles travailler</i>	18
<i>Tableau: Livrables disponibles</i>	19
<i>Glossaire</i>	20

1. Résumé exécutif / Synthèse

1.1 - Objectif du rapport

Ce rapport présente l'analyse de marché et ses conclusions sur la base des informations recueillies à propos de la pertinence de créer un groupe de travail spécialisé (GdTS) eCH.ch (dans un premier temps, ancré en Suisse romande) sur le thème de la "Sécurité de l'information et la protection des données dans l'administration publique - SIPD".

1.2 - Méthode

Nous avons procédé par des entretiens qualitatifs auprès de 19 personnes représentant 15 organisations différentes. Le panel est constitué de représentants de l'administration publique, de l'économie et du monde académique/recherche. Quatre des six cantons romands ont été consultés.

1.3 - Principales conclusions

- Il y a un vif intérêt sur la thématique, **une volonté marquée de participer activement**. 95% des personnes contactées pour un entretien ont accepté la requête.
- Les quatre domaines étudiés (maturité et besoins, risques fournisseurs, sensibilisation, gestion des incidents) sont les plus pertinents.
- Le GdTS doit être en mesure de fournir des **livrables concrets et réalisables**.
- **Les deux thématiques** "Sécurité de l'information" et "Protection des données" sont indissociables, et **doivent être traités ensemble**.
- Le focus à court terme et la fréquence des séances sont cruciaux dans la capacité et la disponibilité d'implication des membres dans le GdTS
- Il existe de nombreux livrables et meilleures pratiques dans chaque canton qui peuvent être immédiatement partagés (templates, questionnaires, guides de bonnes pratiques)
- Le GdTS ne doit pas être juste "une autre plateforme" qui ajoute de la confusion auprès des acteurs de l'administration publique.

1.4 - Recommandation finale

La pertinence du groupe de travail spécialisé SIPD pour l'administration publique en Suisse romande, **est confirmée**.

Le périmètre (scope), les objectifs, les priorités et la cadence des séances du GdTS doivent être clairement définis. Les premiers livrables doivent être rapidement disponibles, tangibles, applicables et utiles.

Parmi les quatre sous-thèmes explorés, il semble judicieux de se focaliser premièrement sur les aspects liés aux **risques fournisseurs**. C'est à la fois un des thèmes évoqués comme étant le plus important et pour lequel il y a le moins de livrables ou de partage d'expérience, donc où eCH.ch peut avoir le plus d'impact.

2. Introduction

2.1 - Contexte général

La sécurité de l'information et la protection des données (SIPD) sont essentielles pour l'administration publique suisse car elles garantissent la souveraineté du pays, protègent les données sensibles des citoyens et maintiennent la confiance du public. Elles permettent aussi de respecter un cadre légal strict et de faire face à des cyber-menaces croissantes. Enfin, elles assurent la continuité des services publics et la protection des infrastructures critiques dans un contexte où la digitalisation des services est en forte progression.

Les standards eCH jouent un rôle central dans la gouvernance numérique suisse en définissant des normes communes pour l'administration. Ils assurent l'interopérabilité à travers tous les niveaux de l'administration, simplifient les échanges de données et soutiennent la mise en œuvre cohérente des services numériques. eCH.ch joue ainsi un rôle structurant dans la transformation numérique du pays.

2.2 - Objectif du rapport

Ce rapport présente l'analyse de marché - la méthodologie, les thèmes, les groupes de personnes interrogées - et les conclusions tirées sur la base des informations recueillies à propos de la pertinence de créer, dans un premier temps en Suisse romande, un GdTS sur le thème de la SIPD.

2.3 - Méthodologie

En septembre et octobre 2025, nous avons procédé à des entretiens qualitatifs qui permettent de mieux recueillir les perceptions, les besoins et les attentes. Le guide de questions est joint en annexe à ce document.

Le panel est constitué de représentants de l'administration publique - communes, cantons, confédération -, de l'économie - prestataires de services - et du monde académique et de la recherche. Quatre des six cantons romands - FR, GE, VD, VS - ont été consultés. **19 personnes qui représentent 15 organisations différentes.**

A noter que certaines personnes interrogées bénéficient d'expériences croisées dans plusieurs secteurs. Un échantillon varié en terme d'expertise spécifique aux technologies de l'information et/ou aux aspects légaux de la protection des données.

95% des personnes contactées pour un entretien ont accepté la requête. Personne n'a refusé, seul quelques personnes n'ont pas répondu à la sollicitation.

Tableau: Profil des personnes interrogées

Admin	Fédéral	Canton	Assoc communes cantonale	Communes	Academie	Corporate	RSSI	DPO
10	1	3	3	3	2	8	4	2

A noter que la somme des profils est supérieure au nombre de personnes interrogées car plusieurs répondants disposaient d'expérience dans plus d'un secteur

Le domaine de SIPD étant très vague, nous avons choisi de le décliner en quatre thèmes:

- La maturité et la capacité des administrations communales à évaluer ses besoins
- La gestion des risques liés aux fournisseurs
- La sensibilisation et formation du personnel administratif
- La gestion des incidents

3. Constats généraux

3.1 - Situation actuelle dans les administrations publiques

Le degré de maturité et la diversité des pratiques varie selon les communes et les cantons.

Dans le canton de **Genève**, le Service intercommunal d'informatique de l'Association des Communes Genevoises (SIACG) identifie, met en œuvre et assure l'exploitation mutualisée des systèmes d'information dont les communes membres ont besoin. Le SIPD fait partie intégrante de la mission du SIACG. Plusieurs formes d'interactions et de coordination existent entre le canton de Genève et le SIACG, essentiellement au niveau compatibilité des systèmes, interfaçage et sécurité des échanges.

Dans le canton de **Fribourg**, l'Association des Communes Fribourgeoises (ACF-FGV) joue un rôle prépondérant dans la sensibilisation, la formation, l'accompagnement dans les procédures d'appels d'offres et d'établissements de contrats fournisseurs. Les services Sécurité de l'information et Protection des données de l'Etat de Fribourg n'interagit pas avec les communes. Les communes sont libres de contracter les prestataires de services appropriés.

Dans le canton de **Vaud**, depuis janvier 2024, en co-financement entre le canton, les communes et les associations intercommunales, un C-SIRT a été créé, vers lequel les communes et associations intercommunales se retournent en cas de cyber-incident. L'Union des Communes Vaudoises (UCV) assure essentiellement des prestations de sensibilisation et de formation des élus et du personnel administratif.

En **Valais**, la Fédération des Communes Valaisannes (FCV-VWG) a peu de visibilité, c'est surtout le pôle Gouvernance Numérique d'Antenne Région Valais Romand qui oeuvre auprès d'une vingtaine de communes du Valais romand, en matière de sensibilisation et agit comme point de contact sur les aspects SIPD. L'Etat du Valais dispose d'un contrat Incident Response Détailler (IRR) dont les communes peuvent également bénéficier.

Au niveau des **communes**, le niveau de maturité SIPD dépend essentiellement des compétences personnelles et/ou professionnelles du Municipal en charge de la thématique. Les communes les plus matures bénéficient d'un(e) municipal(e) expérimenté(e). Les communes les moins matures auront tendance à se reposer sur leur prestataire de services (info-gérance) avec parfois la fausse impression que leur responsabilité, en tant que municipal, est transférée au prestataire de service.

Coordination et initiatives existantes

Le fédéralisme suisse est une réalité dans le SIPD aussi. Il existe plusieurs initiatives dans chaque canton qui sont principalement régionales. Nous n'avons pas identifié d'initiatives SIPD supra-cantoniales.

Il existe plusieurs certifications/labels : CyberSafe, ICS square, CyberSeal. Ces certifications/labels donnent parfois une fausse impression de sécurité.

Les partenariats public-privé sont souvent évoqués, mais sont rarement vécus. Il y a une suspicion de la part des communes quant à la pertinence des partenariats à développer avec les acteurs du privé, dû notamment aux impératifs de rentabilité ces derniers.

3.2 - Attentes globales exprimées

Malgré la diversité, parfois la disparité, entre les cantons romands et le rôle des associations intercommunales, il en ressort un très vif intérêt à échanger les meilleures pratiques et partager l'accès aux outils développés.

Besoin de cadre commun, d'échange d'expériences, et de référentiels adaptés aux réalités locales.

3.3 - Enjeux identifiés

Risques et problématiques récurrents

- La délégation par les communes de la gestion SIPD à des info-gérances, avec le sentiment que la responsabilité leur est également déléguée.
- Du côté des prestataires de services, on relève que le marché de l'administration publique est très fragmenté, beaucoup de petites entités. Ce qui pose un problème de rentabilité/profitabilité en raison du manque d'économie d'échelle.
- La surcharge chronique des communes, les ressources et le temps à disposition.

Besoins exprimés par les administrations et partenaires

- Véhiculer les messages auprès des bonnes personnes au sein des communes, s'assurer de la bonne compréhension des messages.
- Des solutions et plateformes sécurisées pour la collaboration entre le législatif et l'exécutif d'une commune, à l'instar de la plateforme La Suite territoriale en France.

État actuel des pratiques, normes, standards utilisés

- Plusieurs certifications et labels sont disponibles. Il apparaît par contre illusoire de les maintenir sur la durée, en raison de manque de ressources (temps et humaines).
- CyberSafe pour les aspects systèmes, collaborateurs et gouvernance des communes.
- CyberSeal pour les aspects organisationnels et techniques des prestataires IT.
- Envisager de déléguer une partie de la certification 27001 à des instances reconnues.

3.4 - Les thématiques identifiées

Pertinence des thèmes

Que ce soit de la part des administrations, comme de celle des prestataires de services, les quatre thèmes:

- évaluation de la situation et des besoins
- gestion des risques liés aux fournisseurs
- sensibilisation et formation du personnel administratif et
- réaction aux incidents,

sont reconnus comme étant les plus importants à l'unanimité des répondants.

Tableau: Importance des thématiques

	Besoins Maturité	Risques Fournisseurs	Sensibilisation Formation	Incident response
ACFR			X	
Antenne Valais romand		X	X	
CIGES		X	X	
Cisco			X	X
Clusis		X	X	
Elca	X		X	
EPFL				X
Etat de Fribourg		X	X	
Etat du Valais		X		X
OFCS + Pomy	X			
Ofisa		X		X
Sigma	X	X		
Villars Sainte Croix		X		X
UCV		X	X	
Yverdon-les-Bains	X		X	

Tableau: Autres thèmes relevés

ACFR	Apprendre à faire le tri dans les sujets, où commence quoi (Sécurité et protection et transparence). Guide pratique, apprendre à naviguer entre les sujets.
Cisco	L'aspect légal pour l'application des normes.
Clusis	Création d'un label suisse souveraineté numérique, gouvernance.
Yverdon-les-Bains	L'aspect gestion des projets de sécurisation / protection des données de la genèse à la mesure d'impact.

3.5 - Perception de la coordination existante

La coordination se situe quasi exclusivement au niveau intercommunal, là où les associations cantonales de communes ont pris un rôle prépondérant. Les échanges entre associations cantonales sont établis. Les organisations métiers (préposés à la protection des données, RSSI, etc) sont rodées.

D'importantes lacunes sont perçues dans la coordination ou la cohérence des approches entre les divers cantons, et avec les divers prestataires.

Les volontés politiques jouent un rôle important dans la cohésion et l'harmonisation des activités.

4. Constats spécifiques aux thématiques

4.1 - Maturité et besoins des communes

Les grandes communes ont les ressources et compétences, les plus petites sont en général moins bien équipées. Elles confient la gestion de leur système d'information en info-gérance à des prestataires de services.

Évaluation de la maturité

- Être en capacité de faire la distinction entre la sécurité, la protection des données et la transparence et comment les intégrer dans les processus de la commune. Mise en conformité, remise en conformité. La gouvernance doit être une partie intégrante.
- Le groupe de travail pourrait jouer un rôle dans la reconstruction entre le monde technique et le monde métier.
- Constats sur les outils existants, manques identifiés: il manque un outil qui permette une auto-évaluation. Cependant, l'auto évaluation par des parties qui n'ont pas les connaissances de base pour s'auto évaluer est un problème.
- L'OFCS (Office Fédéral de CyberSécurité) a envoyé un questionnaire à toutes les communes afin de leur permettre de se situer sur l'échelle de la sécurité. Le focus était sur les processus.

Attentes, Besoins et Existant

- Besoin d'un modèle d'évaluation harmonisé.
- Evaluation de la maturité d'une commune par une entité étatique, para-étatique, privée ou not for profit.
- Existe-t-il des solutions qui permettent de travailler de manière sécurisée entre le législatif et l'exécutif d'une commune? Les membres de commissions étudient des dossiers sensibles depuis leur domicile.

Obstacles rencontrés

Les obstacles identifiés sont clairement liés

- à la priorisation politique - la construction d'une place de jeux ou d'un trottoir est plus visible.
- au manque ressources/compétences.

4.2 - Risques liés aux fournisseurs

Dans la gestion des risques liés aux fournisseurs, nous avons couvert les aspects tels que le processus d'appel d'offre, les critères de sélection, les contrats et le monitoring des performances du fournisseur.

- La sélection des fournisseurs et de leurs sous-traitants est une problématique importante et reconnue.
- La certification des plus petits fournisseurs est difficile car ils manquent souvent de moyens pour passer, maintenir et renouveler leurs certifications. Les plus gros fournisseurs ont toutes les certifications nécessaires, ainsi que les procédures en place. Le problème réside auprès des plus petits fournisseurs.
- Le fournisseur doit maîtriser la technologie, la gouvernance et le métier.

- Dépendance potentielle aux mauvais fournisseurs, car les critères d'évaluation des fournisseurs ne sont pas adaptés et/ou peu de fournisseurs répondent aux appels d'offres.
- Il existe un syndrome des "y en a pas des comme nous". On est d'accord qu'il faut harmoniser, mais chaque commune pense avoir des spécificités bien différentes de celles de ses voisins.

Dépendance croissante aux prestataires informatiques

La majorité des communes se tournent vers des prestataires de services tels qu'Ofisa, Ciges, T2i ou Swisscom qui assurent leur info-gérance. Des prestataires de services tels qu'Elca commencent à faire le pas vers l'administration publique, mais les plus petites communes ne sont pas intéressantes en terme de rentabilité. De fait, le choix des communes est restreint. Environ 60% des communes vaudoises traitent avec Ofisa. Ciges est partiellement financé par plusieurs communes valaisannes.

Difficultés dans la gestion contractuelle et l'évaluation des risques

Que ce soit du point de vue des communes ou de celui des prestataires de services, on observe une grande diversité de pratiques. Les communes ont parfois des requêtes non pertinentes (par manque de compréhension ou parce qu'on leur a dit que c'était important). La due diligence de la part des plus petites communes est manquante.

Devant le manque de critères d'évaluation qualitatifs, les communes se basent sur les références d'autres communes et/ou sur le rapport prix/prestation. Il faut une approche qui favorise la prise en compte des choix stratégiques de la commune.

Besoin d'un cadre commun de bonnes pratiques ou de modèles contractuels eCH.

Établir les bons contrats (p.ex avec clauses de reprise des données). Monitorer la qualité des prestations sur plusieurs années. Option de sortie du contrat avant l'échéance. La confiance s'étioule au fil du temps. On peut être très strict sur les équipements, mais on l'est moins sur les personnes qui accompagnent. Quand faire des audits, et qui les fait?

Catalogue de critères / compas qui permettent de mieux choisir le fournisseur.

Des modèles existent auprès d'associations intercommunales et l'OFCS, qui pourraient être relayés par eCH

L'OFCS a publié un catalogue de mesures de protection contre les cyberattaques touchant la chaîne logistique "Cybersécurité tout au long de la chaîne logistique" à l'intention des PME et des communes.

4.3 - Sensibilisation et formation du personnel administratif

Le fait que certaines communes (Rolle, Montreux) aient communiqué dans la presse sur les cyber-attaques dont elles ont été la cible, est une bonne chose en terme de sensibilisation

Niveau actuel de sensibilisation / formation

Si les communes sont en général sensibilisées aux aspects SIPD, elles pensent souvent qu'elles ne sont pas des cibles potentielles. **Or, il ne faut pas se poser la question de l'intérêt des données, mais du potentiel économique qu'elles représentent.** Les aspects de protection des données sont particulièrement délicats, beaucoup de questions posées aux associations intercommunales. Le niveau de sensibilisation est plus bas que pour l'aspect sécurité de l'information.

Attentes, Besoins et Existant

- Formation de base ICS Square (15h)
- www.elearningcyber.ch développé par la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)
- Initiatives cantonales, outils de l'OFCS, etc.
- Besoin de matériel harmonisé et accessible aux petites communes

4.4 - Réponse aux incidents

Organisation actuelle de la gestion des incidents dans les communes et cantons

Les procédures de signalisation d'incidents varient en fonction des cantons, elles sont en général connues des communes (à minima quel est le point de contact initial). La gestion des incidents et éventuellement des crises est souvent reprise par le canton et/ou les prestataires de services.

La proximité du prestataire (public ou privé) est importante en cas de traitement des incidents.

Ne pas traiter que l'aspect technique, mais également la communication et l'aspect politique. Idée de "Gestion de crise as a Service".

Problèmes rencontrés

La définition d'un incident et l'obligation de signaler un incident ne sont pas toujours claire. A partir de là, il est possible que des incidents réels ne soient pas rapportés.

Diagnostic et audit Cybersécurité pour la mise en place des procédures ad hoc.

Harmonisation des procédures de communication, coordination et reporting.

Attentes, Besoins et Existant

- Guide de bonnes pratiques ou d'un protocole eCH commun.
- Il ne s'agit pas uniquement de l'aspect technologique, mais la communication, la gestion de crise, comment je communique avec les partenaires et fournisseurs.
- C'est la commune qui doit gérer l'incident, doit faire partie de la culture communale.
- L'OFCS publie des instructions qui permettent de réagir en cas de cyberattaques.
- Les cantons le font également, par exemple de canton de Vaud [ici](#)

5. Constats spécifiques au GdTS-SIPD

5.1 - Attentes envers eCH.ch

La notoriété spontanée d'eCH.ch est faible. A la question: "Connaissez-vous eCH.ch ?", la majorité des répondants (73%) ont répondu négativement. Les répondants qui ont répondu positivement utilisent les livrables fournis par eCH.ch, essentiellement les associations de communes et les cantons.

Tableau : Notoriété d'eCH.ch

Répondant	Connait	Ne connait pas
ACFR	Oui engage sur la partie normes	
Antenne Valais romand	Oui normes ech058	
CIGES		Non
Cisco		Pas du tout
Clusis		Non
Elca		Seulement connu de nom
EPFL	Collaboration dans un GdTS	
Etat de Fribourg		Peu connu, c'est l'ACF qui est en contact
Etat du Valais	Oui engage sur la partie normes	
OFCS + Pomy		Pas connu, mais sait que UCV et ACV s'engagent
Ofisa		Connu de nom
Sigma		Pas du tout
UCV	Oui par les normes	
Villars Sainte Croix		Pas du tout
Yverdon-les-Bains		Depuis une semaine

Attentes fonctionnelles

- Les attentes exprimées par les répondants s'articulent en terme de la fourniture de guides pratiques, d'harmonisation et de simplification des procédures, ainsi que de partage d'expériences.

Attentes organisationnelles

- **composition du groupe:** représentativité des divers acteurs de l'administration publique: niveau fédéral, cantonal et communal. Les prestataires de services ne doivent chercher à vendre leurs solutions, mais participer de manière constructive. L'ancrage en Suisse romande est important.
- **rôle:** Identifier et valider la thématique la plus pertinente. Définir les actions et livrables prioritaires. Impliquer les parties judicieuses. Assurer la communication aux divers acteurs publics.

5.2 - Points de vigilance et freins

Risques de redondance

Les répondants soulignent le risque de redondance avec d'autres initiatives, conférences inter-régionales ou groupements. Il faut être attentif à ce que le périmètre du mandat du GdTS-SIPD apporte quelque chose de nouveau, d'utile, de tangible et qui puisse être mis en oeuvre

Groupements, Associations citées

Plusieurs groupements, associations, conférences métiers ont été citées.

- Clusis, ICS square,
- Association des communes suisses, Myni Gmeind, Administration Numérique Suisse Latine,
- Association de secrétaires municipaux, de greffiers, de responsables informatiques, des préposés cantonaux à la protection des données, Cybersécurité Valais, CISO Romandie + TI, l'AVRIC, etc,

Le GdTS-SIPD ne doit avoir que peu ou pas de redondance avec ces organisations.

Format, légitimité, gouvernance

- Le GdTS doit représenter les trois niveaux de l'administration publique (fédéral, cantonal et communal), les différents cantons romands dans un premier temps, les diverses parties prenantes (administration et plusieurs prestataires. Le milieu académique/recherche est moins crucial dans une première phase).
- Deux prestataires de services relèvent l'importance du point de la non disqualification de leur société aux appels d'offres dans le cas où ils prendraient part au GdTS-SIPD.
- La neutralité des prestataires de services est cruciale. Charte à mettre en place

Mobiliser les acteurs

- Si la thématique SIPD est unanimement reconnue comme étant de la plus haute importance, la disponibilité des répondants est très souvent citée comme une barrière à une participation active.
- Certains prestataires de services pointent le nombre et la longueur des procédures d'appels d'offres publics comme étant un frein à leur engagement sur le marché de l'administration publique.

Tableau : Organisations prêtes à participer

ACFR	Oui
Antenne Valais Romand	Oui intérêt tant que ça sert
CIGES	Oui
Cisco	Oui, à voir en fonction de la pertinence des thèmes et du temps
Clusis	Oui
Elca	Oui, besoin de retour du marché
EPFL	Si eCH.ch devenait membre de C4DT oui, sinon pas dans le core focus de C4DT
Etat de Fribourg	Oui avec deux personnes

Etat du Valais	À voir, il y a beaucoup de choses en Valais
OFCS	pas au niveau municipal, par contre intéressant pour partager ce qui a été fait au niveau OFCS
Ofisa	Oui, dépendaient de la charge de travail
Sigma data	Intéressé mais pas le temps
UCV	Oui
Villars Sainte Croix	Pourquoi pas, si ça peut aider
Yverdon-les-Bains	Fort intérêt de la part d'Yverdon-les-Bains. Echange avec les autres communes

5.3 - A quoi ressemble le succès du GdTS-SIPD

La mission, le focus, les objectifs et les livrables sont clairement définis.

Par exemple:

- **Mission:** Le groupe de travail a pour mission de **développer, maintenir et promouvoir** des **standards, recommandations et bonnes pratiques** visant à garantir un niveau élevé de **sécurité de l'information et de protection des données** dans les processus et systèmes liés à la transformation numérique de l'administration public suisse.
- **Focus:** Le groupe de travail se **focalise prioritairement** sur les communes romandes et sur l'aspect de **gestion des risques liés aux fournisseurs**. Les thèmes de la maturité, de la sensibilisation et de la réponse aux incidents restent toutefois importants et seront traités de manière appropriée.
- **Objectifs:** Livrer un guide de meilleures pratiques pour la sélection et le suivi de performance de fournisseurs. Bibliothèque de templates de contrats-types.

Attentes exprimées par les répondants

A la question: quels sont les éléments qui vous feront dire que le GdTS-SIPD est un succès", les réponses sont:

- **Livrables**
 - Des livrables clairement définis (cité 6 fois)
- **Synergie / Notoriété**
 - Notoriété auprès des acteurs du marché, ils se tournent naturellement vers eCH lorsque des projets SIPD sont étudiés.
 - Mise en place de plateforme pour synergie, co-crédation de plateforme, marketplace.
 - Neutralité des représentants de l'économie privée, adoption d'une charte.
 - Relais locaux pour la propagation des pratiques.
 - Assouplissement du cadre légal de manière à faire avancer les choses.

6. Conclusions et recommandations

6.1 - Pertinence globale de la création du groupe

A l'unanimité, les répondants à l'étude de marché sont très favorables à la création d'un Groupe de Travail Spécialisé pour la Sécurité de l'Information et la Protection des Données

Conditions de succès : représentativité, mandat clair, livrables tangibles

6.2 - Périmètre et priorités proposées

Toutes les thématiques abordées sont importantes aux yeux des répondants, toutefois il est impératif de se focaliser afin d'optimiser les chances de succès du GdTS. La thématique prioritaire est la **gestion des risques liés aux fournisseurs**. Les entretiens échangés laissent apparaître une grande disparité entre cantons et entre communes. C'est à la fois un des thèmes évoqués comme étant le plus important et pour lequel il y a le moins de livrables ou de partage d'expérience, donc où eCH.ch peut avoir le plus d'impact.

Possibilités de sous-groupes: Suivant le cycle d'un partenariat avec un fournisseur. De la qualification des besoins, aux critères de sélection, au suivi de la performance, aux aspects de gouvernance. Sans oublier les documents, guides, modèles.

6.3 - Propositions concrètes

Mandat et périmètre du groupe

Identifier et valider les sujets "Fournisseurs" les plus pertinents. Définir les actions et livrables prioritaires. Impliquer les parties adéquates. Assurer la communication aux divers acteurs publics et privés.

Représentation souhaitée

- Les trois niveaux de l'administration publique (fédéral, cantonal et communal).
- Représentants des associations intercommunales.
- Représentants des prestataires de services.
- Représentants des associations métiers et groupements SIPD
- Représentants académiques / Recherche (facultatif)

Étapes suivantes

Validation de la recommandation par eCH.ch

Création et lancement du core team du GdTS

Définition et validation du mandat et des objectifs

Recrutement de membres additionnels

Organisation opérationnelle

7. Annexes

Guide d'entretien

Objectif de l'étude	
<p>L'analyse de potentiel a pour objectif de valider la pertinence, les besoins et les success factors d'un groupe spécialisé dédié à la "Sécurité de l'information et protection des données (SPID)", et quels sont les domaines potentiels qui devraient être adressés en priorité. (cybersécurité, gouvernance SSI, conformité au réglementations, protection des données, ...)</p>	
<p>Nous avons identifié 4 thèmes principaux:</p> <ul style="list-style-type: none"> - Evaluation de la situation et des besoins des collectivités publiques (readiness / maturité assessment) - Gestion des risques liés aux fournisseurs: exigences lors d'appel d'offres, contenu du contrat, contrôle du fournisseur, monitoring de la performance - Formation/Sensibilisation du personnel - Réaction aux incidents 	
Thèmes	Questions prestataires
Quelles sont les parties qui ont un intérêt à s'engager pour créer un nouveau groupe spécialisé sur le sujet.	Connaissez-vous eCH.ch ? Qu'est-ce que ça évoque pour vous?
	Que pensez-vous de la pertinence d'un tel groupe de travail spécialisé SIPD?
	Voyez-vous d'autres thèmes que les quatre évoqués ?
	Faites vous partie d'un groupe de travail sur l'un ou l'autre de ces sujets ?
	Quels échanges entretenez vous avec les acteurs du secteur public (administration / prestataires de services / académique)
Valider les thèmes / le contenu et les acteurs engagés de l'éventuel groupe spécialisé	Quels domaines / sujets devraient être traités en priorité ? Cybersécurité / Protection des données / Gouvernance SSI / Conformité aux réglementations / Maturity assessment / Risques fournisseurs / Formation du personnel / incident response / autre
	Quels sont les pain points à votre niveau ?
	Quels sont les success factors?
	Seriez-vous prêt à participer activement?
	Quelles compétences pouvez-vous amener à ce groupe de travail?
Créer une esquisse d'un ou de plusieurs premiers standards ou bonnes pratiques concrets	Y a-t-il des normes ou standard ou bonne pratique en particulier ou en priorité qui devraient faire l'objet de ce groupe de travail spécialisé ?

Prestation et process potentiels	
Evaluation de la situation et des besoins (readiness / maturité assessment)	Comment évaluez-vous la maturité des acteurs de l'administration publique face à l'évaluation de leur propre situation et de leurs besoins (note et exemples)
	Qu'est-ce qui fonctionne bien? Qu'est-ce qui doit être amélioré?
Gestion des risques liés aux fournisseurs: exigences lors d'appel d'offres, contenu du contrat, contrôle du fournisseur, monitoring de la performance	Comment évaluez-vous la maturité des acteurs de l'administration publique face aux risques liés au choix des fournisseurs (note et exemples)
	Qu'est-ce qui fonctionne bien? Qu'est-ce qui doit être amélioré?
Formation/Sensibilisation du personnel	Comment évaluez-vous la maturité des acteurs de l'administration publique face à la formation et la sensibilisation du personnel (note et exemples)
	Qu'est-ce qui fonctionne bien? Qu'est-ce qui doit être amélioré?
Réaction aux incidents	Comment évaluez-vous la maturité des acteurs de l'administration publique en cas de réaction aux incidents (note et exemples)
	Qu'est-ce qui fonctionne bien? Qu'est-ce qui doit être amélioré?
En général	Quel potentiel d'optimisation voyez-vous (low hanging fruit)
Objets de la validation	
	Y a-t-il un réel besoin de coordination et/ou d'échange sur cette thématique, et qui n'est pas déjà couvert par un autre groupe / dans un autre cadre
	- Y a-t-il une réelle volonté de la part des acteurs de participer activement à ce groupe spécialisé et quel pourrait être un premier résultat concret

Liste des personnes interrogées (répondants)

La liste des personnes interrogées est fournie en pièce jointe à ce document

Tableau: Idées de normes / initiatives sur lesquelles travailler

Besoins	Self assessment tool / Maturity assessment
Besoins	Diagnostic CyberSafe
Besoins	Registre de traitement des données pour l'ensemble des communes
Fournisseurs	Sélection de fournisseurs: check list, modèle d'évaluation
Fournisseurs	Modèle pour appels d'offre qui laisse une marge de manoeuvre pour les choix stratégiques.
Fournisseurs	Modèles de contrats tels que ceux promus par l'OFCS
Fournisseurs	Catalogues de questions
Fournisseurs	Solutions & plateformes sécurisées pour la collaboration entre législatif et exécutif (voir exemple français La suite territoriale)
Formation	Incentive / subvention aux communes qui se certifient (idem énergie renouvelable)
Formation	Définir des package de formation, pack 1, 2 et 3 qui soient définis pour les public cibles (municipal, personnel, etc).
Formation	Vulgarisation et partage de bonnes pratiques
Formation	Formation régulière et ponctuelle sur les nouvelles menaces, tendances
Formation	www.Elearningcyber.ch
Formation	Créer les documents de base pour l'hygiène du personnel administratif
Incidents	Définir un service de base, un niveau minimum de sécurité (idem ceinture de sécurité)
Incidents	Définir un minimum vital (MFA, backup, etc)
Incidents	Chatbot, AI pour le tri des faux-positifs (exemple si une imprimante clignote en orange .. est-ce un incident?)
Incidents	Définir la mise en place d'une cellule de crise, qui fait quoi, quelles priorités. Compte en bitcoin (plan Covid pour les cyberattaques). La communication est clé: définir les intervenants, juridique, protection des données, communications.

Tableau: Livrables disponibles

Maturité	OFCS questionnaire envoyé à toutes les communes pour se situer sur l'échelle de sécurité, focus processus. Etat de Vaud a envoyé un benchmark aux communes
Maturité	CyberSafe (poussé par l'UCV)
Maturité	Registre des activités de traitement a été renforcé par l'Antenne région Valais
Maturité	LLM assistant AI pour répondre aux questions des communes (VS)
Maturité	Les normes, e-gov portal intercantonal (NE, JU, et VS), comment intégrer les communes, qui pilote quoi.
Fournisseurs	Des templates existent auprès d'associations intercommunales et OFCS, qui pourraient être relayés par eCH
Fournisseurs	Label CyberSeal pour les prestataires IT
Fournisseurs	Catalogue de mesures de protection contre les cyberattaques touchant la chaîne logistique " <u>Cybersécurité tout au long de la chaîne logistique</u> " de l'OFCS
Formation	<u>Cours de base ICS Square</u> 15h
Formation	www.Elearningcyber.ch
Formation	DFJP a crée cybersecurityforyou.ch
Formation	Etat du Valais a développé une plateforme d'awareness (exemple campagne de fishing)
Formation	Campagne de sensibilisation / fishing par Ansam / Ofisa
Formation	https://www.kyos.ch/securite/security-awareness/
Formation	UCV Ma Commune en un click https://www.ucv.ch/guichet-numerique
Formation	Formation mise en place avec HES-SO (MAS SIPD)
Incident	L'OFCS publie des instructions qui permettent de réagir en cas de <u>cyberattaques</u> . Les cantons le font également, par exemple de canton de Vaud ici
Incident	Accompagnement gestion de crise, marché suivre, liste d'actions
Incident	Prévention: subvention 3k CHF de matériel IPS/IDS
Incident	Délégation d'un expert forensic

Glossaire

Abréviation	Dénomination
ACF-FGV	Association des Communes Fribourgeoises
ANS	Administration Numérique Suisse
AVRIC	Association Vaudoise des Responsables Informatiques communaux
C-SIRT	Computer Security Incident Response Team - Centre de veille, d'alerte et de réponse aux attaques informatiques
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
DPO	Data Protection Officer - Délégué à la protection des données
FCV-VWG	Fédération des Communes Valaisannes
GdTS	Groupe de Travail Spécialisé
NCSC	National Cyber Security Center (BACS en allemand, OFCS en français)
OFCS	Office Fédéral de CyberSécurité (BACS en allemand, NCSC en anglais)
OFIT	Office fédéral de l'informatique et de la télécommunication
PPP	Partenariat Public-Privé
RSSI	Responsable de la Sécurité des Systèmes d'Information
SIACG	Service intercommunal d'informatique de l'Association des Communes Genevoises
SIPD	Sécurité de l'Information et Protection des données
UCV	Union des Communes Vaudoises