Rapport de la commission du Conseil communal d'Yverdon-les-Bains chargée de l'examen du préavis PR26.22PR

concernant

une demande de crédit d'investissement de CHF 780'000.- pour la mise en conformité du Service des énergies avec les normes minimales pour les technologies de l'information et de la communication (TIC)

Monsieur le Président,
Mesdames les Conseillères et Messieurs les Conseillers,

La commission a siégé le 15 septembre 2026.

Elle était composée de Mesdames et Messieurs Pascal Beyeler, Viviane Dutu, Pascale Fischer, Salvatore Nielsen, Nadia Rytz, Philippe Pavid, Juan Ramirez, Florian Segginger et du soussigné, désigné président.

La délégation municipale était composée de Mesdames et Messieurs Benoist Guillard, Municipal, André Favre, Chef de service ad intérim, Diego Sanchez Gould, Responsable département systèmes d'information et finances et Leila Wyss, Responsable du système d'information et chargée de transformation. Nous les remercions pour la présentation détaillée du préavis ainsi que pour les réponses apportées aux questions des commissaires.

Présentation de la délégation municipale :

La délégation municipale a présenté le préavis en cinq parties : le contexte des cybermenaces, le cadre réglementaire, les enjeux pour un distributeur et fournisseur d'énergie, l'organisation du projet et sa conclusion.

Contexte : les réseaux d'énergie sont des cibles récurrentes

La délégation a rappelé que les réseaux d'énergie sont des cibles récurrentes de cyberattaques et que la menace progresse : prise de contrôle d'un réseau électrique en Ukraine (2015) et coupure de courant provoquée à Kiev (2016), maliciels détectés dans des centrales nucléaires au Japon, en Allemagne et en Inde, 23 gestionnaires de réseau attaqués simultanément au Danemark (2023), sous-stations attaquées en Pologne avec destruction d'équipements de téléconduite (2025), arrêt d'une centrale de production en Grande-Bretagne (2026). La Suisse n'est pas épargnée : vols de données et rançongiciels ont touché des entreprises (RUAG, Swisscom, Stadler Rail, ABB), des infrastructures (CFF, Swissport) et des collectivités publiques, dont la commune de Rolle (2021), fedpol et des polices cantonales via le prestataire Xplain (2023), et 36 incidents recensés dans les administrations publiques au second semestre 2025. Les attaques par rançongiciel étant précédées de vols de données, la détection est décisive.

Cadre réglementaire

La norme minimale pour les TIC s'inscrit dans la loi du 17 juin 2016 sur l'approvisionnement du pays (LAP ; RS 531). S'il incombe à chaque entreprise ou organisation de se protéger, il est de la responsabilité de l'État de veiller au bon fonctionnement des infrastructures

critiques. La norme, portée par l'Office fédéral de la cybersécurité (OFCS), vise la réduction du risque systémique cyber, l'harmonisation nationale du niveau minimal de cybersécurité, une approche proportionnée et fondée sur le risque, l'auditabilité vis-à-vis des autorités de surveillance sectorielles, ainsi que la confidentialité, l'intégrité, la disponibilité et la traçabilité des systèmes d'information et des systèmes industriels (IT/OT). Sa portée diffère selon le réseau :

Secteur	Situation réglementaire	Conséquence pour le Service des énergies
Électricité	Obligatoire dès le 1er juillet 2026 (art. 5a OApEl)	Démontrer la conformité au niveau de protection applicable
Gaz	Obligatoire depuis le 1er juillet 2025 (art. 39a OSITC, exigences sectorielles)	Démontrer la conformité au niveau de protection applicable
Eau	Référentiel recommandé (SSIGE W1018)	Appliquer une approche cohérente pour les infrastructures essentielles

Pour l'électricité, l'art. 5a OApEl rend les recommandations de la norme minimale TIC (édition de mai 2023) contraignantes selon le niveau de protection applicable, dès le 1er juillet 2026, pour les gestionnaires de réseau de distribution et de transport, les producteurs et exploitants de stockage dès 100 MW pilotables à distance par un seul système, et les prestataires assurant durablement un pilotage à distance. La surveillance est exercée par l'ElCom (Commission fédérale de l'électricité) selon la directive 1/2024 :

Surveillance de l'ElCom (directive 1/2024)	Modalité
Auto-évaluation annuelle	Confirmée par une lettre de la direction concernée
Entrevues sur site	Discussion et présentation des preuves de mise en œuvre
Audits	Sur la base d'indications externes ou d'un échantillon aléatoire

Pour le gaz, l'art. 39a OSITC rend contraignantes, depuis le 1er juillet 2025, les exigences de la norme minimale TIC pour l'approvisionnement en gaz (mai 2024) ; les exploitants doivent prouver à l'autorité de surveillance qu'ils satisfont au niveau de protection prescrit au chapitre 5 de la norme. Pour l'eau, la recommandation SSIGE W1018 (édition 2019) constitue un référentiel sectoriel recommandé, fondé sur une approche par les risques et complété par la norme G1008 pour le gaz et F1001 pour la chaleur et le froid.

La Municipalité a retenu un référentiel unique appliqué aux trois réseaux : obligation légale démontrable pour l'électricité et le gaz, même démarche par cohérence pour l'eau. La conformité doit être démontrée à l'autorité, documents et preuves à l'appui ; il s'agit d'être capable de prouver que les mesures sont effectivement mises en œuvre, évaluées et améliorées dans le temps.

Enjeux pour le Service des énergies

La cyberattaque est identifiée dans la matrice des risques du Service des énergies comme un risque à probabilité élevée et à impact majeur. Quatre scénarios sont en jeu pour la sécurité des réseaux, chacun associé à un objectif de protection :

Interruption d'exploitation Perturbation de la distribution d'électricité, de gaz ou d'eau **Objectif : continuité d'approvisionnement**	**Accès non autorisé** Intrusion dans les systèmes de gestion (IT) et de conduite (OT) **Objectif : détecter les incidents et réagir**
Atteinte à l'intégrité Altération des données, des mesures et des commandes à distance **Objectif : protection des IT/OT**	**Rétablissement difficile** Absence de capacité éprouvée de détection et de reprise rapide **Objectif : assurer la récupération et la résilience**

Organisation du projet et feuille de route

Les travaux préparatoires ont été réalisés de 2024 à 2026 dans le cadre de la phase 5 du projet Gouvernance SI, financé par le préavis PR22.15PR, avec l'accompagnement de Kudelski Security. Ils comprennent les audits TIC des trois réseaux, les analyses de risques, la feuille de route, les offres, l'analyse des exigences légales, la politique et les directives SI, la matrice RACI ainsi que les bases du rapport et du préavis. Les écarts relevés par les audits ont été transformés en livrables : la demande porte sur la mise en œuvre de mesures déjà identifiées et non sur de nouvelles études.

La mise en œuvre se déroule d'octobre 2026 à novembre 2027 en trois phases, chacune close par un jalon de validation du comité de pilotage. Le phasage traite en premier les éléments dont la conformité exige une revue sur plus d'une année. La clôture, dès novembre 2027, comprend la validation de l'ensemble des livrables et leur transfert au projet Gouvernance SI pour la pérennisation.

Projet Gouvernance SI – phase 5 (PR22.15)	Phase 1	Phase 2	Phase 3	Clôture
2024 – 2026	**Oct. 2026 – fév. 2027**	**Fév. – juin 2027**	**Juin – nov. 2027**	**Dès nov. 2027**
• Audits TIC électricité, gaz et eau • Analyses des risques par réseau • Feuille de route • Offres • Analyse des exigences légales • Politique SI • Directives SI • Matrice RACI • Bases du rapport et du préavis	• Gestion des risques • Gestion des accès • Sensibilisation • Environnement des activités	• Sécurité des données • Sécurité de l'exploitation • Risques liés aux tiers	• Surveillance et sécurité • Réponse aux incidents • Récupération	• Validation de tous les livrables • Transfert au projet Gouvernance SI pour la pérennisation
Coûts externes	**CHF 88'650**	**CHF 182'250**	**CHF 172'500**	**Total CHF 443'400**

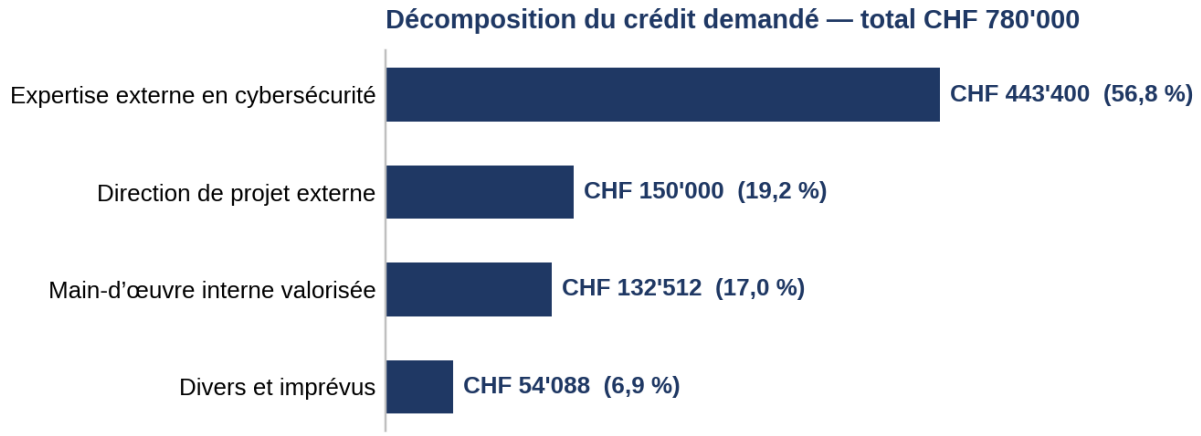
L'organisation du projet repose sur des rôles et des instances définis :

Instance	Composition et rôle
Mandant	Municipalité · Service des énergies
Comité de pilotage	Direction du Service des énergies · Office de l'informatique
Direction de projet	Direction de projet externe · qualité et suivi de projet
Équipe de réalisation	Responsables d'actifs informationnels · responsables réseaux · informatique · partenaire spécialisé en cybersécurité

La délégation y voit trois garanties de maîtrise : des décisions rapides au comité de pilotage, une expertise spécialisée mobilisée au bon niveau et une appropriation durable par les équipes internes. Le projet est suivi à la revue mensuelle des projets stratégiques du SEY, de manière à ce que la direction ait une vision claire de l'avancement de sa mise en œuvre.

Coûts

Le crédit demandé de CHF 780'000.- se décompose comme suit :



Risques du projet

Le projet dispose d'un registre des risques, de mesures de réduction identifiées et d'un suivi régulier en comité de pilotage. Trois risques principaux ont été présentés :

Risque	Mesure de maîtrise
Disponibilité des ressources internes et informatiques	Ateliers ciblés, validation des ressources et arbitrage par le comité de pilotage
Délais liés à l'acquisition des prestations externes	Analyse du cadre des marchés publics et anticipation de la procédure
Retard de mise en conformité	Audits, analyse des risques et feuille de route déjà réalisés ; avancement formalisé et suivi

Conclusions :

Au terme de ses travaux, la commission retient les éléments suivants.

Les obligations de cybersécurité applicables aux réseaux d'électricité et de gaz sont contraignantes, respectivement depuis le 1er juillet 2026 et le 1er juillet 2025, et exigent une conformité démontrable vis-à-vis des autorités de surveillance, documents et preuves à l'appui. La cyberattaque figure dans la matrice des risques du Service des énergies comme un risque à probabilité élevée et à impact majeur, et les incidents survenus ces dernières années à l'étranger comme en Suisse confirment que les réseaux d'énergie et les collectivités publiques sont des cibles.

La commission constate que les travaux préparatoires sont achevés : les audits TIC des trois réseaux, les analyses de risques et la feuille de route ont été réalisés dans le cadre du projet Gouvernance SI (PR22.15PR), avec l'appui d'un partenaire spécialisé. Le calendrier, les livrables et l'organisation du projet sont définis, chaque phase faisant l'objet d'un jalon de validation par le comité de pilotage. La demande porte ainsi sur la mise en œuvre de mesures déjà identifiées par les audits, et non sur de nouvelles études.

La commission relève que le crédit de CHF 780'000.- permet d'engager la mise en œuvre d'octobre 2026 à novembre 2027, qu'il se compose pour l'essentiel de prestations externes spécialisées (56,8 %) et d'une direction de projet externe (19,2 %), et que la main d'œuvre interne y est valorisée à hauteur de CHF 132'512.-. Elle prend acte de l'importante charge de travail que le projet représente pour le Service des énergies, charge qui doit être absorbée pour répondre à l'évolution du cadre légal, ainsi que de la constitution d'une équipe de projet inter-départements et inter-services regroupant les spécialistes de chaque secteur.

La commission prend acte enfin que le projet dispose d'un registre des risques suivi en comité de pilotage, qu'il est inscrit à la revue mensuelle des projets stratégiques du SEY, et qu'à sa clôture les livrables seront transférés au projet Gouvernance SI afin d'en assurer la pérennisation.

C'est donc à la majorité de ses membres, que la commission vous recommande, Monsieur le Président, Mesdames les Conseillères et Messieurs les Conseillers, d'accepter les conclusions de ce préavis.

Yverdon-les-Bains, le 22.09.2026

Kevin Delay