MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

EXAMEN PROFESSIONNEL D'INGENIEUR PRINCIPAL DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2024 -

Lundi 26 juin 2023

Etude de cas à partir de deux dossiers techniques de trente pages maximum, soumis au choix du candidat le jour de l'épreuve écrite, permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

Durée : 4 heures

Sujet n° 2

Le dossier documentaire comporte 27 pages. (hors les 2 pages de l'énoncé du sujet).

Il vous est rappelé que votre identité ne doit figurer que dans l'en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettez en fin d'épreuve entrainera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A …, B…, Y…, Z…).

IMPORTANT

1. LES COPIES SERONT RENDUES EN L'ÉTAT AU SERVICE ORGANISATEUR.
   A L'ISSUE DE L'ÉPREUVE, CELUI-CI PROCÉDERA À L'ANONYMISATION DE LA COPIE.
2. NE PAS UTILISER DE CORRECTEUR OU D'EFFACEUR SUR LES COPIES.
3. ECRIRE EXCLUSIVEMENT EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.
4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE SUR LA COPIE.

Sujet n°2

Audit et plan d'amélioration du service numérique d'un SGCD

Vous êtes chef du service numérique dans un secrétariat général commun départemental (SGCD).

Le nouveau préfet de département, qui a pris ses fonctions récemment, a demandé à la mission audit, qualité, évaluation (MAQE) de la direction du numérique (DNUM) du ministère de l'intérieur et des outre-mer de réaliser un diagnostic 360° sur le fonctionnement de votre service depuis la création du SGCD le 1er janvier 2021.

Cet audit a fait apparaître les principaux constats suivants :

- organisation du service numérique mal définie (absence de feuille de route, manque de communication sur les services offerts, organisation du télétravail mal défini, niveau de compétences des agents du service numérique hétérogène) ;
- accompagnement numérique perfectible des agents (dématérialisation, gestion électronique des documents (GED), outils collaboratifs et de visioconférence) ;
- méconnaissance des marchés spécifiques au domaine informatique ;
- absence de processus de gestion des incidents et des demandes et d'outil de ticketing ;
- niveau de satisfaction du support numérique de proximité jugé bon par les utilisateurs de la préfecture et moyen par les agents des directions départementales interministérielles (DDI) gérées par le service numérique du SGCD ;
- absence d'interopérabilité entre les infrastructures téléphoniques de la préfecture, des sous-préfectures et des DDI, rendant impossible l'utilisation d'un annuaire téléphonique commun ;
- absence de doctrine sur la sûreté bâtimentaire des DDI, contrairement à la préfecture et aux sous-préfectures qui sont raccordées sur un même système d'information gérant le contrôle d'accès, la vidéoprotection et la détection anti-intrusion ;
- sécurité des systèmes d'information peu maîtrisée (pas de plan de résilience ou de plan de continuité d'activité, stratégie de sauvegarde des données mal définie).

Fort de cet audit, le préfet vous demande de lui proposer un plan d'amélioration rédigé sous forme de note à son attention sur les aspects organisationnels et techniques, tout en mettant l'accent sur l'utilisateur au centre.

Vous présenterez une démarche méthodologique d'actions priorisées permettant la mise en œuvre de ce plan.

Dossier documentaire :

Document 1	Extrait Diagnostic flash 360° DNUM/MAQE (pages 2 à 5) Documentation interne MIOM/SG/DNUM	Pages 1 à 4
Document 2	Extrait ANSSI : les 10 règles d'or pour la conception et la mise en œuvre de services numériques https://www.ssi.gouv.fr/10-regles-dor-pour-la-conception-et-la-mise-en-oeuvre-de-services-numeriques/	Page 5
Document 3	Extraits du guide d'audit des systèmes d'information (Comité d'harmonisation de l'audit interne de l'État) : https://www.economie.gouv.fr/files/files/directions_services/chaie/guide-audit-si.pdf?v=1631609349 - Audit du support utilisateurs et de la gestion du parc - Audit des marchés spécifiques au domaine informatique	Pages 6 à 10
Document 4	Extrait du tableau de suivi de la feuille de route sur la convergence ATE : les 12 chantiers numériques sur la convergence du socle informatique de l'administration de l'État Source : Documentation interne MIOM/SG/DMATES	Pages 11 et 12
Document 5	Article du 8/8/2019 gazette des communes création des SGC et des DDI	Page 13
Document 6	Produits de l'Intérieur / Le catalogue de services numériques du Ministère de l'Intérieur et des Outre-mer / Sauvegarde et récupération de données. https://pi.interieur.rie.gouv.fr/home-dnum/infrastructure-et-dev/securite-et-surete/sauvegarde-et-recuperation-de-donnees/	Pages 14 et 15
Document 7	Document ITIL 2011 : Processus d'amélioration continue des services 09-Q7-ITIL_2011_Overview-diagram-French_1111071.pdf	Page 16
Document 8	Extraits du guide du Secrétariat Général à la Défense et à la Sécurité Nationale pour réaliser un plan de continuité d'activité : https://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf#%5B%7B%22num%22%3A189%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22Fit%22%7D%5D - Pourquoi élaborer un plan de continuité et d'activité ? - Fiche 1 : comment lancer une démarche de continuité d'activité ? - Fiche guide synthétique pour l'auto-évaluation des bonnes pratiques - Fiche modèle de RETEX	Pages 17 à 23
Document 9	Extraits du guide ANSSI pour les recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection. https://www.ssi.gouv.fr/uploads/2020/03/anssi-guide-recommandations_securisation_systemes_controle_acces_physique_et_videoprotection-v2.0.pdf - Étapes préliminaires à la mise en place d'un système de contrôle d'accès ou de vidéoprotection. (pages 19 à 21) - Exemple d'architecture générale d'un système de contrôle physique et de vidéoprotection. (Figure 2.1 page 17)	Pages 24 à 27

GÉNÉRALITÉS

1

Comme tout diagnostic dans le cadre d'une mission d'évaluation, les points forts et les points à améliorer sont mis en exergue. Cela permet à l'entité SIC d'avoir une vision précise d'une situation existante au regard des bonnes pratiques appliquées dans la gestion des services informatiques. Ce diagnostic explore l'ensemble des axes contributeurs à la fourniture d'un service conforme aux attentes des clients internes. Il s'agit d'identifier les écarts par rapport à une cible « idéale » et aux bonnes pratiques et de mesurer un niveau de maturité. Cette matière sert ensuite de base à l'élaboration d'un plan d'action.

Les résultats de l'ensemble de ces points sont présentés et discutés avec le client lors de la restitution. Après validation de ce diagnostic, un travail de priorisation des actions à mener est établi sur la base des recommandations fournies. L'établissement d'un macro-planning avec la direction constitue la dernière étape de cette phase.

LES AXES D'ANALYSE

Les axes d'analyse englobent un grand nombre de dimensions que nous considérons comme intéressantes à explorer dans le cadre d'un diagnostic. Notre expérience nous a prouvé qu'aucune de ces dimensions n'est à négliger, même si, dans la plupart des cas, l'effort va être réalisé sur quelques axes essentiels à la contribution de la fourniture du service.

LES PERSONNES : Quelles sont les personnes sur lesquelles s'appuyer au sein de l'entité SIC et à l'extérieur ? Qui sont les sponsors ? Quel est le niveau de formation de vos équipes ? Nous regardons également le dimensionnement de votre service IT et la maturité du management.

LES PROCESSUS : Quels sont les processus en place et leur niveau de description ? Une démarche d'amélioration continue est-elle en place ? Nous mesurons l'écart entre la théorie et «le terrain". Enfin, nous vérifierons qu'ils sont connus et utilisés par vos agents.

LES OUTILS : Quels outils sont déployés dans votre DSI ? Votre SI est-il urbanisé ? Nous vérifierons également le niveau de maîtrise technique du système d'information par vos ressources internes.

LES AXES D'ANALYSE

L'ORGANISATION: L'organisation est-elle adaptée à vos exigences de gestion efficace et efficiente ? Quelles sont les compétences clés et comment sont-elles réparties au sein de l'entité? Quelle est la justification de chaque fonction de l'organigramme ? Ne pourrait-on pas imaginer une autre organisation plus en accord avec vos besoins/attentes ?

LA COMMUNICATION: Comment l'entité communique t'elle ? Quels sont les médias utilisés, les porteurs et la fréquence de vos communications ? Quelles sont les cibles, internes ? Externes ? Quel est l'impact attendu ? Pourquoi communiquer ?

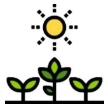
LE REPORTING : Analyse du reporting des responsables de service de l'entité. Analyse du contenu, de la fréquence, de la fiabilité et de la véracité des indicateurs de performance sur les activités de gestion des services. Nous vérifions également la diffusion et la pertinence des indicateurs diffusés.

LA DOCUMENTATION : Analyse de la maturité du processus de documentation. Savoir si le niveau de documentation est suffisant, utile et partagé avec vos collaborateurs.

LES AXES D'ANALYSE

SERVICES ET RELATION CLIENT : Existe-t-il un catalogue de services ? Quel est son niveau d'utilisation ? S'il existe, quel est le principe utilisé pour la création des conventions de service ? Qui sont les interlocuteurs privilégiés de l'entité côté client ? La relation est-elle formalisée et/ou documentée ?

LE BUDGET : Il s'agit d'analyser les principes de suivi et de contrôle budgétaire. Quels sont les montants ? Quelles sont les périodes budgétaires ? Avez-vous mis en place des systèmes de contrôle de gestion ?



LA CULTURE D'ENTREPRISE : Comment l'organisation fonctionne t'elle pour mener à bien ses projets ? Existe-t-il une culture d'entreprise ? La culture est-elle favorable à une progression rapide en fonction des enjeux ? Une forte résistance au changement est-elle à prévoir ?

LES SOUS-TRAITANTS : Quels sont vos contrats de sous-traitance ? Quels sont les engagements de vos prestataires et votre niveau de contrôle ?

LES 10 RÈGLES D'OR

1 / MENER UNE ANALYSE DE RISQUES EN PRENANT EN COMPTE L'ÉCOSYSTÈME du périmètre concerné. Identifier les actifs métier essentiels à protéger, cartographier les parties prenantes de l'organisation, préciser les menaces, identifier les exigences légales et réglementaires et définir des scénarios stratégiques.

2 / RÉDIGER UNE EXPRESSION DE BESOIN EXHAUSTIVE prenant en compte les besoins métier et les exigences de sécurité, définies notamment par l'analyse des risques, pour permettre à la maîtrise d'oeuvre de mener à bien les travaux de conception et de développement.

3 / S'APPUYER SUR UN PRESTATAIRE D'HÉBERGEMENT DE CONFIANCE pour les traitements et les données les plus sensibles (e.g. SecNum*Cloud* pour les hébergements *cloud*). Cloisonner également les systèmes d'information (SI) dédiés à l'événement et ceux des autres clients de l'infrastructure.

4 / S'ASSURER DES BONNES PRATIQUES DE DÉVELOPPEMENT ET DE CONCEPTION (sécurisation des infrastructures, des applications et des terminaux, etc.) et mettre en place des audits réguliers, en interne comme chez les sous-traitants.

5 / MAÎTRISER ET PROTÉGER LES INTERCONNEXIONS entre les SI étudiés et des SI tiers. Elles conditionnent la surface d'exposition aux menaces et aux attaques.

6 / SÉCURISER LA GESTION DES IDENTITÉS, LES MÉCANISMES D'AUTHENTIFICATION ET LES CONTRÔLES D'ACCÈS.

7 / PROTÉGER LES RESSOURCES D'ADMINISTRATION. Par essence critiques, la mutualisation avec d'autres fonctions (e.g. la bureautique) est à proscrire, puisque cela accroît significativement le risque de prendre rapidement le contrôle de l'ensemble d'un SI.

8 / MAINTENIR LES SYSTÈMES D'INFORMATION EN CONDITIONS DE SÉCURITÉ en assurant la mise en oeuvre des correctifs de sécurité des socles techniques utilisés, avec une attention particulière aux services exposés sur Internet, souvent ciblés comme vecteur initial de compromission.

9 / ASSURER ET PROTÉGER LES SAUVEGARDES DES DONNÉES ET DE L'INFRASTRUCTURE. Les sauvegardes hors ligne et hors site et les processus de restauration sont structurants pour remédier à une situation de crise et recouvrer rapidement une capacité technique de production.

10 / ACTIVER UN DISPOSITIF DE DÉTECTION DES INCIDENTS DE SÉCURITÉ ET DE GESTION DE CRISE. Il permet d'identifier rapidement une menace et de mener les actions conservatoires et de remédiation utiles avant d'arriver à une situation de compromission. Il est également primordial de définir des procédures de gestion de crise cyber.

EN SAVOIR PLUS

RETROUVEZ L'INTÉGRALITÉ DES RÈGLES ET TOUTES LES RESSOURCES UTILES POUR GARANTIR LA SÉCURITÉ DES SERVICES NUMÉRIQUES SUR LE SITE DE L'ANSSI :

Pour toute question, contacter **conseil-technique@ssi.gouv.fr**

3.5. AUDIT DU SUPPORT UTILISATEURS ET DE LA GESTION DU PARC

La mission de la fonction support est orientée autour de deux axes :

- fournir l'assistance et le support aux utilisateurs des systèmes d'information et améliorer en permanence leur niveau de satisfaction ;
- améliorer la performance globale des systèmes.

La performance d'un centre d'assistance (*help-desk*) ainsi que ses répercussions sur la productivité des utilisateurs doivent être évalués. Elle doit permettre d'identifier les domaines sur lesquels il semble possible d'accroître la productivité des utilisateurs, notamment les besoins en formation.

Il est nécessaire que la fonction de support d'une part anticipe ses besoins et dimensionne convenablement ses équipes et, d'autre part, contribue à la mise en place de règles de gestion du matériel et des applications informatiques de l'organisation en analysant le retour d'expérience.

Les aspects relatifs à la gouvernance et à la sécurité sont traités dans les fiches 3.1 et 3.2. Les points de contrôle proposés ci-dessous leur sont complémentaires.

Points de contrôle
1. Fonction support : audit fiabilité et sécurité
1.1. Quelle structure de centre d'assistance (*help-desk)* (HD) est mise en place ?
1.2. Existe-t-il une procédure de gestion des demandes, diffusée et connue des utilisateurs ?
1.3. Quelle est la procédure d'escalade mise en place ?
1.4. Quelle est la couverture géographique du HD ?
1.5. Quelle est la couverture fonctionnelle du HD ?
1.6. Un outil est-il implémenté pour la prise d'appel et le suivi des tickets ?
1.7. Quelles sont les critères à renseigner pour la qualification des tickets ?
1.8. Existe-t-il une liste de questions à dérouler lors d'un appel afin d'identifier au mieux la demande de l'utilisateur ?
1.9. Les problèmes sont-ils gérés ? Si oui quel est le processus ?
1.10. Les incidents de production de nuit sont-ils saisis aussi dans l'outil ?
1.11. Quels sont les comités mis en place pour suivre les incidents et leur résolution ? Qui participe ? Comment sont suivies les actions ?
1.12. Si le HD est externalisé, existe-t-il un contrat de service ?
1.13. Quels sont les indicateurs pour suivre le contrat de service ?
1.14. Y-a-t-il un planning systématique concernant les mises en production ?
1.15. Interroger le DSI, le responsable HD, des utilisateurs, l'équipe HD – si possible, participer « à la vie du HD ».
1.16. Demander des extractions de la base de ticket : • vérifier le nombre, la complétude des critères, l'adéquation de la qualification, la description de l'incident ;

- analyser les délais de clôture ;
- analyser la criticité moyenne des tickets.

1.17. Demander les *reporting* de suivi.

2. Fonction support : audit d'efficacité et de performance

2.1. Existe-t-il une aide à la saisie pour la saisie des tickets ?

2.2. Existe-t-il des revues qualité pour la saisie des tickets ?

2.3. Quelle est la procédure de mise à jour de la base de connaissance ?

2.4. Les appels sont-ils enregistrés ?

2.5. Des études de satisfaction sont-elles réalisées auprès des utilisateurs ?

2.6. Existe-t-il une évaluation de l'équipe HD ? Notamment pour les prestataires pour évaluer leur niveau de connaissance ?

2.7. Les certifications (ITIL, ISO, COBIT) sont-elles encouragées au sein de la DSI, du HD en particulier ?

2.8. Interroger le DSI, le responsable HD, des utilisateurs, l'équipe HD – si possible, participer « à la vie du HD ».

2.9. Demander la stratégie de formation des utilisateurs et de l'équipe *Help-Desk*.

2.10. Demander les *reportings* de suivi.

2.11. Demander les études de satisfaction.

3. Gestion du parc matériel et logiciel : audit fiabilité et sécurité

3.1. Quelle est la procédure de déploiement des mises à jour, d'un nouveau logiciel ?

3.2. Quels sont les outils mis en place pour gérer les versions des logiciels ?

3.3. Quels sont les outils mis en place pour gérer le matériel informatique ?

3.4. L'installation des PC / portables est-elle faite à partir d'un master (configuration minimum et standardisée) ?

3.5. Existe-t-il un processus spécifique pour le suivi des mises à jour sur les portables ?

3.6. Le déploiement de nouveaux logiciels ou mises à jour est-il possible à distance ? (utile pour les utilisateurs nomades).

3.7. Est-il possible pour le HD de prendre la main à distance ? Si oui, quelle est la procédure ?

3.8. Comment est géré le parc informatique ? Quel type de machine ? Quel outil ?

3.9. L'inventaire du parc informatique comprend-t-il la localisation des machines ?

3.10. Les logiciels "non officiels" sont-ils répertoriés et suivis ?

3.11. Les utilisateurs sont-ils sensibilisés à la sécurité informatique, notamment à l'installation de logiciel "non officiel" ?

3.12. Faire des copies d'écran ou d'extraction des outils de suivi des mises à jour/déploiement.
Vérifier sur les postes utilisateurs les versions antivirus, firewall, version Windows, version IE.

4. Gestion du parc matériel et logiciel : audit d'efficacité et de performance

4.1. Comment est effectué l'inventaire des licences (logiciel, version, date de mise en production, nombre d'utilisateurs) ?

4.2. Outils de type SAM (*Software Asset Management*) sont-ils déployés ?

4.3. Existe-t-il des revues régulières des licences ?

4.4. Existe-t-il une base de données de gestion de configuration de type CMDB (*Configuration Management DataBase*) ?

4.5. La DSI est-elle sensibilisée aux enjeux de la maîtrise des licences ? (notamment en cas de contrôle) ?

4.6. Des audits sont-ils réalisés ?

4.7. Une politique logicielle existe-t-elle ?

3.8. AUDIT DES MARCHES SPECIFIQUES AU DOMAINE INFORMATIQUE

Ce paragraphe est consacré aux marchés spécifiques au domaine informatique. Il a vocation à compléter le guide des bonnes pratiques des achats de services informatiques du service des achats de l'État (SAE), qui reste la référence.

Les risques propres à ces marchés sont notamment :

- l'imprécision des responsabilités des acteurs étatiques et privés, en raison de l'utilisation dans les marchés des notions de MOA, MOE, AMOA, etc. sans accord explicites des parties sur la portée de ces notions ;
- la complexité opérationnelle et juridique des prestations, notamment pour les fonctions partiellement externalisées ;
- la nature des prestations, qui peuvent aisément dériver vers un positionnement illicite des agents du prestataire vis-à-vis de l'administration ;
- l'insuffisante définition des livrables et l'imprécision – voire l'inexistence – des critères d'évaluation permettant d'attester objectivement la réalité du service fait.

3.8.1. ÉTUDE DES MARCHES D'ASSISTANCE TECHNIQUE

L'assistance technique (qui se retrouve fréquemment en conduite de projets sous la forme d'AMOA) est un besoin pour les services du ministère qui ne disposent pas de toutes les compétences pour mener à bien toutes les missions qui leur sont confiées. Néanmoins, les marchés passés dans ces domaines présentent différents risques :

- risque de perte de compétence pour les services ;
- risque de coût prohibitif pour les finances publiques ;
- risque pénal car ces marchés, s'ils sont mal rédigés, mal passés ou mal exécutés, courent le risque d'être requalifiés, par le juge, en prêt illégal de main d'œuvre ou en délit de marchandage.

Points de contrôle
1. Marchés d'AMOA
1.1 Les responsabilités respectives de l'administration et du titulaire sont clairement établies et le marché ou un document qui lui est annexé les précise.
1.2 Les équipes du titulaire et les représentants de l'administration connaissent et respectent ce document.
1.3 L'objet du marché est régulier : • la prestation, objet du marché, n'est pas irrégulière par nature (liquidation de factures, rédaction de marchés, …) ; • le marché n'a pas pour seul objet le prêt de main d'œuvre (ex : prix calculé selon un montant exprimé en hommes/jour).
1.4 Les obligations des parties sont conformes au droit : • les pièces du marché (CCTP, acte d'engagement) font apparaître des obligations de résultats du titulaire et non des obligations de moyens (ex : pas de jalons, pas ou peu de livrables, aucun résultat réellement exigé).
1.5 Les documents du marché ne montrent pas que le service a voulu s'attacher une personne précise (CV, nom de l'intervenant cité, …).
1.6 L'exécution du marché ne fait pas apparaître une rupture du lien hiérarchique entre l'employé et sa hiérarchie : • les agents du titulaire ne sont pas intégrés dans les équipes de l'administration ; • les agents du titulaire ne reçoivent pas leurs ordres de la hiérarchie du service prescripteur.
1.7 L'exécution du marché ne fait pas apparaître une intégration des agents du titulaire au sein de l'administration : • les agents du titulaire n'apparaissent pas nominativement dans les documents de l'administration (organigrammes, annuaires, PV de réunions, …) ; • les agents du titulaire n'utilisent pas abusivement les moyens de l'administration (accès au restaurant de l'administration au tarif "usager", utilisation d'une adresse de messagerie de l'administration, accès aux réseaux de l'administration, …) ; • les agents du titulaire ne sont pas répartis dans les locaux des services de l'administration sans séparation manifeste et identification précise (absence de badges et de locaux particuliers) ; • les agents du prestataire ne sont pas en poste depuis plus de **3 ans (durée indicative).**

3.8.2. ÉTUDE DES MARCHES D'ACQUISITION DE PRESTATIONS INFORMATIQUES SUR LA BASE D'UN FORFAIT

Le marché peut avoir pour objet la prestation de services dont le prix est fixé forfaitairement, à la date de conclusion du contrat. Même dans le cadre d'un forfait, le contrat peut détailler les sommes allouées au titre des redevances de licences, de maintenance, ou du prix de la formation éventuelle, des développements spécifiques…

Si le client a l'avantage de bénéficier d'un prix forfaitaire, il faut tenir compte d'un certain nombre de risques. Par exemple, le calendrier peut dériver, la charge de travail du prestataire peut être sous-évaluée, ou le référentiel trop imprécis peut enfermer l'administration dans un périmètre excessivement restreint.

Points de contrôle
2. Marchés de prestation sur la base d'un forfait
2.1 S'agissant des licences, le marché prévoit les droits concédés par l'éditeur et les conditions d'accès au code source en cas de résiliation.
2.2 Le contrat précise quels documents constituent le référentiel des spécifications afin de déterminer le champ des prestations entrant dans le montant du marché fixé forfaitairement.
2.3 Le marché distingue le traitement des évolutions qui pourront entraîner une facturation complémentaire, dans des conditions prévues entre les parties, et celles, simples précisions ou adaptations, qui resteront incluses dans le prix établi forfaitairement.
2.4 Un mécanisme de pénalités de retard sanctionne le non-respect du calendrier (y compris les jalons intermédiaires), ou un bonus est prévu si le prestataire atteint ses objectifs dans des délais plus courts que prévu.
2.5 Les jalons intermédiaires ne sont pas artificiels.
2.6 Le marché précise bien quels sont les prérequis (disponibilité du personnel du client, configuration matérielle, …).

Volet III - 12 chantiers numériques

Chantier opérationnel		Objectif à atteindre	Information communiquées à la suite du COPIL du 22 novembre 2022	Bilan à date présenté lors du COPIL du 23 mai 2023
Chantier numérique "SI ATE"	1	Elaborer un tableau de bord « SI ATE » en lien avec les autres ministères de l'ATE conformément aux décisions du CITP de juillet 2021	**Chantier abouti.** Le tableau de bord du SI ATE mis en place au 1er trimestre 2022 est désormais diffusé mensuellement.	**Situation confirmée.** Le tableau de bord de mars 2023 a été publié. **Le tableau de bord d'avril sera publié entre le 15 et le 17 mai 2023.**
	2	Converger sur des outils collaboratifs communs dans l'ATE	**Chantier abouti.** Les opérations de migration d'OCMI vers les nouveaux outils collaboratifs, ont été planifiées et se sont déroulées tout au long de 2022.	**Situation confirmée.** La reprise vers de nouveaux outils collaboratifs (RESANA et OSMOSE) s'est poursuivie au début de l'année 2023 et a abouti. **OCMI a été définitivement décommissionné depuis le 4 mai 2023.**
	3	Converger sur des solutions de publication communes dans l'ATE (intranet et internet)	**Chantier abouti.** Les portails intranet des services de l'Etat dans les départements ont été dotés d'un onglet SGC-D et SGC NUM au 1er trimestre 2022 et une doctrine a été élaborée	**Situation confirmée.** La doctrine a été diffusée. **Situation inchangée.**
	4	Mettre en place un socle informatique commun de l'ATE en améliorant l'offre Web et la visio-conférence	Amélioration de l'offre de service de web et visioconférence **Chantier abouti** Possibilité d'organiser des réunions mixtes (présentiel et distanciel) depuis toutes les salles de réunion de l'ATE. Déploiement de terminaux de visioconférence en **2022.**	**Situation confirmée concernant les acquisitions financées par la centrale au moment de la crise sanitaire.** Un besoin complémentaire a été émis par les départements pour un coût prévisionnel total de l'ordre de 6 M€. Le portage de ce besoin complémentaire est examiné dans le cadre du renforcement de la relation SIDSIC/SGAMI/SGAR et de l'exécution déconcentrée des budgets SIC et dans le cadre d'une priorisation du besoin (la totalité du besoin complémentaire ne pourra pour autant pas être validé). **La situation est inchangée.** On peut néanmoins signaler que le niveau de dialogue SIDSIC-SGAMI-SGAR ne semble pas partout montrer le même niveau de maturité ; retours réguliers des SIDSIC qui indiquent ne pas arriver à faire prendre en compte des besoins nouveaux priorisés. **Le fonctionnement a été rappelé à l'ensemble des acteurs concernés.**
	5		Améliorations fonctionnelles de COMU **Chantier abouti au 1er semestre 2022.** 100% des utilisateurs de COMU ont bénéficié des améliorations fonctionnelles (gestion des micros, main levée, 2800 connectables). L'accès en web depuis internet pour des partenaires extérieurs ou en région sera déployé d'ici à la fin 2022.	**La situation est inchangée. Le service est techniquement opérationnel. La communication informant de la disponibilité du service sera lancée prochainement.** Le service permettant l'accès à des partenaires externes a été ouvert en février ; un plan de communication est en préparation. Les pré-requis techniques ont été finalisés comme prévu fin 2022. Il y a en cours la mise en oeuvre de pré-requis fonctionnels comme celui consistant à demander aux détenteurs de mettre un code de protection sur les conférences existantes. L'accès depuis un navigateur au travers le RIE pour les ministères de tutelle et leurs directions régionales (y compris en télétravail) sera ouvert dans le même temps.
	6	Mettre en place un socle informatique commun de l'ATE en mettant à niveau les infrastructures	Dotation de cartes agents MIOM pour l'ensemble des agents des SGC **Chantier abouti.** Les cartes agent permettent depuis juillet 2022 une connexion partagée aux différents SIRH ATE.	**Situation confirmée** - un sondage serait peut-être utile pour vérifier qu'il n'y a pas de régressi**on.**
	7		Dotation d'adresse mel ICASSO pour l'ensemble des agents des SGC-D. **Chantier abouti.** L'ensemble des agents des SGC-D dispose d'une adresse mel ICASSO.	**Situation confirmée.**
	8		Intégration numérique des agents des ex UD DIRECCTE dans les DDETS-PP. **Chantier en cours.** Au 15 novembre 2022, 86 départements ont remis des postes NoeMI à leurs agents ex UD Direccte. Remise prévue d'ici **février 2023 pour les derniers départements.**	**Chantier en cours de finalisation** Tous les départements (sauf le 44 qui finalise d'ici à la fin mai 2023) ont terminé la remise des postes de travail pour la totalité des agents ex UD Direccte. S'agissant de la reprise des autres éléments d'infrastructure (serveurs de partage de données notamment) 14 départements doivent encore faire aboutir leurs travaux (départements suivants : 01, 02, 06, 07, 13, 22, 24, 41, 44, 46, 58, 67, 68, 95)

Chantier numérique "SI ATE"	**9**	Mettre en place un socle informatique commun de l'ATE en : - achevant le déploiement de PC portables VPN pour toutes les activités télétravaillables ; - déployant la nouvelle messagerie collaborative de l'Etat - modernisant les infrastructures locales	Equipement des agents dont les activités sont télétravaillables **Chantier abouti.** 100 % des agents aux activités télétravaillables sont équipés depuis la fin 2021. Les départements ont tous un taux d'équipement au moins égal à 50 % des effectifs.	**Situation confirmée.**
	10		Déploiement de la nouvelle messagerie de l'Etat **Chantier en cours.** Échéance : **1er semestre 2023.**	**Les travaux se poursuivent.** La nouvelle messagerie de l'Etat sera déployée auprès des premiers pilotes du périmètre MIOM à la mi-année 2023, avant généralisation à partir de la fin 2023. Les DDI au sein de l'ATE seront concernées dans un deuxième temps entre 2024 et début 2025.
	11		Modernisation des infrastructures locales des DDI **Chantier en cours.** 96 % des DDETS-PP sont en voie d'achèvement, 21 % des DDT-M ont terminé leur migration complète. Echéance : **fin de l'année 2022 pour les DDETS-PP ; fin du 1er semestre 2023 pour les DDT-M.**	**Chantier en cours de finalisation** Sur le périmètre DDETS-PP, la finalisation de la migration du périmètre sera atteinte d'ici à fin du 1er semestre sur l'ensemble du territoire métropolitain (reste quelques reliquats en cours d'élimination, quelques serveurs à reprendre dans le champs ex UD Direccte et le cas particulier des abattoirs). Sur le périmètre DDT : le volet postes de travail sera achevé d'ici fin juin 2023 ; le volet autres éléments d'infrastructures sera achevé d'ici à la fin d'année 2023. **L'objectif de terminer la migration vers le SI ATE sur l'ensemble du territoire métropolitain d'ici à la fin d'année 2023 demeure atteignable.**
	12	Doter les agents des DDI en cartes agents	**Travaux en cours.** Echéance : **horizon 2024.**	**Chantier en cours** Un administrateur général de l'Etat chef de projet a été nommé en février 2023 (M. Eric Tison) Le financement de l'AMOE sera assuré par le P354, la possibilité d'un cofinancement à hauteur de 50% du FTAP est recherchée. Le périmètre du besoin et le calendrier de mise en œuvre sont en cours de définition. Le déploiement de la carte agent dans les DDI sera progressif, avec une première étape de mise en œuvre d'ici la fin 2024.

12

Document 5

Adresse de l'article https://www.lagazettedescommunes.com/634398/creation-des-secretariats-generaux-communs-aux-prefectures-et-directions-departementales-interministerielles/

RÉFORME TERRITORIALE

Création des secrétariats généraux communs aux préfectures et directions départementales interministérielles

Léna Jabre | TO non parus au JO | Publié le 08/08/2019

La circulaire n° 6104-SG du 2 août 2019 relative à la constitution de secrétariats généraux communs aux préfectures et aux directions départementales interministérielles [1] expose les objectifs, le périmètre des missions et les modalités d'organisation des secrétariats généraux communs aux préfectures et aux directions départementales interministérielles. La constitution de secrétariats généraux communs consiste à rassembler pour les conforter, les professionnaliser et susciter des démarches de simplification et de modernisation des procédures et permettre que les responsables des services déconcentrés puissent ainsi consacrer davantage de temps à la conduite des politiques publiques.

Ainsi, les secrétariats généraux communs (SGC) répondent à trois principes directeurs d'organisation :

- le caractère interministériel du SGC, inhérent à la logique de mutualisation;
- une gouvernance collégiale autour du préfet de département qui réunira les responsables des services concernés et devra définir les modalités d'action, de suivi et les priorités du SGC, dans le respect des obligations et spécificités de chacun des services concernés;
- le maintien de la capacité des directeurs à piloter leur service, d'exercer leurs missions en leur conférant une autorité fonctionnelle sur le SGC.

Le périmètre des missions de ces secrétariats est départemental. Le périmètre de l'ensemble de ses missions, qui recoupent entre autres la gestion des ressources humaines, la logistique, l'immobilier, les ressources informatiques, est défini dans une annexe à la circulaire.

Ce secrétariat est un service à vocation interministérielle, chargé des fonctions support, placé sous 1' autorité du préfet, secondé par le secrétaire général de la préfecture : un projet de texte réglementaire permettant la création de ces services est en cours de préparation.

Les SGC devront être mis en place dans tous les départements entre le 1er janvier et le 30 juin 2020, sous la coordination du préfet de région, en associant étroitement les préfets de département et les directeurs des services concernés et en veillant au dialogue social.

A suivre : un rapprochement des régimes indemnitaires, des règles de gestion en matière de ressources humaines et de l'action sociale dont l'état d'avancement sera porté à connaissance ultérieurement.

REFERENCES

Circulaire du 2 août 2019, n°6104-SG

POUR ALLER PLUS LOIN

- Mise en œuvre de la réforme de l'organisation territoriale de l'Etat

Source : https://pi.interieur.rie.gouv.fr/home-dnum/infrastructure-et-dev/securite-et-surete/sauvegarde-et-recuperation-de-donnees/

Produits de l'Intérieur > Infra et développement > Sécurité et sûreté > Sauvegarde et récupération de données

Protégez vos données lors des incidents, qu'il s'agisse de pannes matérielles, d'erreurs humaines ou de cyber-attaques. L'offre de sauvegarde et de récupération de données assure l'intégrité de ces dernières, et vous permet une récupération simple et complète de votre système d'information.

Capable de prendre en charge vos applications, vos systèmes d'exploitation, vos bases de données et vos serveurs de stockage en réseau (NAS), notre solution vous aide à centraliser vos politiques de sauvegarde.

Cette offre de service s'adresse aux entités du Ministère de l'Intérieur, dès lors que les données sont hébergées par la DNUM sur la plateforme Isocèle.

Prérequis

- La plateforme d'hébergement doit être à la DNUM, hors Cloud et hors SIPN
- Le déploiement d'un agent de sauvegarde peut être nécessaire en fonction des options définies pour la sauvegarde ou la récupération
- La version du système d'exploitation, du moteur de bases de données, ou de l'application doivent être supportées par la solution de sauvegarde. Un document listant les compatibilités vous sera fourni

Services

Serveurs

Systèmes d'exploitations Windows, Linux, Unix, AIX, etc.

Volumes de serveurs de stockage en réseau (NAS).

Hyperviseurs

Hyperviseurs Hyper-V, KVM, VMware.

Bases de données

MS-SQL Windows, MySQL, Oracle, PostgresSQL, DB2, Hbase, Informix, MariaDB, SQL Lite, Sybase.

Applications

Lotus Notes, MS Excahnge, SAP, Share point.

Avantages

Flexibilité

Une solution unifiée pour tous les environnements.

Sécurisation

Intégrité et disponibilité des données garanties.

Simplicité

La mise à jour de la solution de sauvegarde, l’optimisation des services et l’enrichissement sont assurés sans intervention de votre part.

Cas d'utilisation

Conformité et performance

Respectez vos objectifs de Perte de Données Maximale Autorisée (PDMA) et de Durée Maximale d’Interruption Autorisée (DIMA). Assurez les engagements pris dans les accords de services.

Résilience

Réduisez les risques en cas d’attaque par un rançongiciel ou un logiciel malveillant grâce à une protection contenue de vos données.

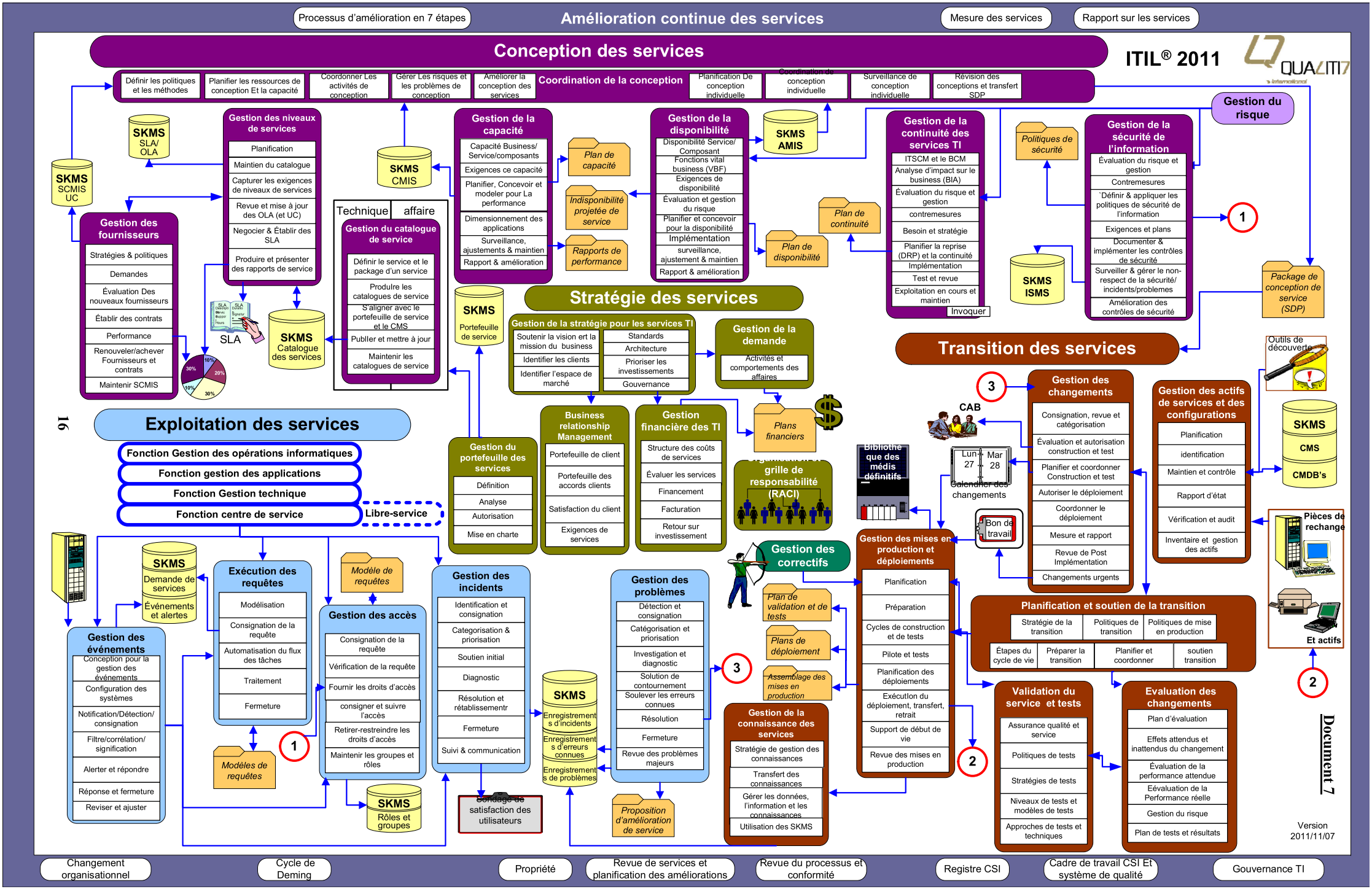
Niveau de service

- Service de sauvegarde supervisé et disponible 24h/24
- Récupération sur demande
- Journaux des tâches de sauvegarde et de restauration disponibles
- Logiciel de sauvegarde : déploiement des montées de versions tel que préconisé par l’éditeur + mises à jour de sécurité préconisées par l’éditeur

Tarification

Coût forfaitaire annuel calculé en fonction du volume de données concernées.

Un devis vous sera remis en amont de la mise en oeuvre.

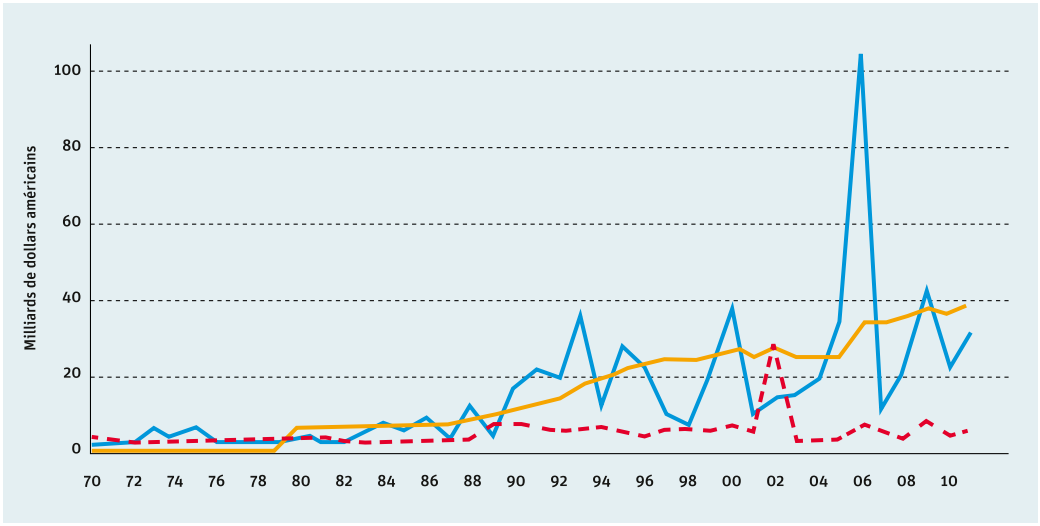

Processus d'amélioration en 7 étapes
Amélioration continue des services
Mesure des services
Rapport sur les services
Conception des services
ITIL® 2011
QUALITI7
Définir les politiques et les méthodes
Planifier les ressources de conception Et la capacité
Coordonner Les activités de conception
Gérer Les risques et les problèmes de conception
Améliorer la conception des services
Coordination de la conception
Planification De conception individuelle
Coordination de conception individuelle
Surveillance de conception individuelle
Révision des conceptions et transfert SDP
SKMS SLA/ OLA
SKMS SCMIS UC
SKMS CMIS
Gestion des niveaux de services
Planification
Maintien du catalogue
Capturer les exigences de niveaux de services
Revue et mise à jour des OLA (et UC)
Negocier & Établir des SLA
Produire et présenter des rapports de service
Gestion de la capacité
Capacité Business/ Service/composants
Exigences ce capacité
Planifier, Concevoir et modeler pour La performance
Dimensionnement des applications
Surveillance, ajustements & maintien
Rapport & amélioration
Plan de capacité
Indisponibilité projetée de service
Rapports de performance
Gestion de la disponibilité
Disponibilité Service/ Composant
Fonctions vital business (VBF)
Exigences de disponibilité
Évaluation et gestion du risque
Planifier et concevoir pour la disponibilité
Implémentation
surveillance, ajustement & maintien
Rapport & amélioration
Plan de disponibilité
SKMS AMIS
Plan de continuité
Gestion de la continuité des services TI
ITSCM et le BCM
Analyse d'impact sur le business (BIA)
Évaluation du risque et gestion
contremesures
Besoin et stratégie
Planifier la reprise (DRP) et la continuité
Implémentation
Test et revue
Exploitation en cours et maintien
Invoquer
Politiques de sécurité
Gestion de la sécurité de l'information
Évaluation du risque et gestion
Contremesures
`Définir & appliquer les politiques de sécurité de l'information
Exigences et plans
Documenter & implémenter les contrôles de sécurité
Surveiller & gérer le non-respect de la sécurité/ incidents/problèmes
Amélioration des contrôles de sécurité
SKMS ISMS
Gestion du risque
Package de conception de service (SDP)
Gestion des fournisseurs
Stratégies & politiques
Demandes
Évaluation Des nouveaux fournisseurs
Établir des contrats
Performance
Renouveler/achever Fournisseurs et contrats
Maintenir SCMIS
SLA
SKMS Catalogue des services
Technique
affaire
Gestion du catalogue de service
Définir le service et le package d'un service
Produire les catalogues de service
S'aligner avec le portefeuille de service et le CMS
Publier et mettre à jour
Maintenir les catalogues de service
SKMS Portefeuille de service
Stratégie des services
Gestion de la stratégie pour les services TI
Soutenir la vision ert la mission du business
Identifier les clients
Identifier l'espace de marché
Standards
Architecture
Prioriser les investissements
Gouvernance
Gestion de la demande
Activités et comportements des affaires
Plans financiers
Transition des services
Outils de découverte
Exploitation des services
Fonction Gestion des opérations informatiques
Fonction gestion des applications
Fonction Gestion technique
Fonction centre de service
Libre-service
Gestion du portefeuille des services
Définition
Analyse
Autorisation
Mise en charte
Business relationship Management
Portefeuille de client
Portefeuille des accords clients
Satisfaction du client
Exigences de services
Gestion financière des TI
Structure des coûts de services
Évaluer les services
Financement
Facturation
Retour sur investissement
Organisation et grille de responsabilité (RACI)
Bibliothèque des médis définitifs
CAB
Lun 27
Mar 28
Calendrier des changements
Bon de travail
Gestion des changements
Consignation, revue et catégorisation
Évaluation et autorisation construction et test
Planifier et coordonner Construction et test
Autoriser le déploiement
Coordonner le déploiement
Mesure et rapport
Revue de Post Implémentation
Changements urgents
Gestion des actifs de services et des configurations
Planification
identification
Maintien et contrôle
Rapport d'état
Vérification et audit
Inventaire et gestion des actifs
SKMS
CMS
CMDB's
Pièces de rechange
Et actifs
Gestion des correctifs
Gestion des mises en production et déploiements
Planification
Préparation
Cycles de construction et de tests
Pilote et tests
Planification des déploiements
Exécution du déploiement, transfert, retrait
Support de début de vie
Revue des mises en production
Plan de validation et de tests
Plans de déploiement
Assemblage des mises en production
Planification et soutien de la transition
Stratégie de la transition
Politiques de transition
Politiques de mise en production
Étapes du cycle de vie
Préparer la transition
Planifier et coordonner
soutien transition
Validation du service et tests
Assurance qualité et service
Politiques de tests
Stratégies de tests
Niveaux de tests et modèles de tests
Approches de tests et techniques
Evaluation des changements
Plan d'évaluation
Effets attendus et inattendus du changement
Évaluation de la performance attendue
Eévaluation de la Performance réelle
Gestion du risque
Plan de tests et résultats
Gestion des événements
Conception pour la gestion des événements
Configuration des systèmes
Notification/Détection/ consignation
Filtre/corrélation/ signification
Alerter et répondre
Réponse et fermeture
Reviser et ajuster
SKMS Demande de services
Événements et alertes
Exécution des requêtes
Modélisation
Consignation de la requête
Automatisation du flux des tâches
Traitement
Fermeture
Modèles de requêtes
Gestion des accès
Consignation de la requête
Vérification de la requête
Fournir les droits d'accès
consigner et suivre l'accès
Retirer-restreindre les droits d'accès
Maintenir les groupes et rôles
SKMS Rôles et groupes
Gestion des incidents
Identification et consignation
Categorisation & priorisation
Soutien initial
Diagnostic
Résolution et rétablissementr
Fermeture
Suivi & communication
Sondage de satisfaction des utilisateurs
SKMS Enregistrements d'incidents
Enregistrements d'erreurs connues
Enregistrements de problèmes
Gestion des problèmes
Détection et consignation
Catégorisation et priorisation
Investigation et diagnostic
Solution de contournement
Soulever les erreurs connues
Résolution
Fermeture
Revue des problèmes majeurs
Proposition d'amélioration de service
Gestion de la connaissance des services
Stratégie de gestion des connaissances
Transfert des connaissances
Gérer les données, l'information et les connaissances
Utilisation des SKMS
Document 7
Version 2011/11/07
16
Changement organisationnel
Cycle de Deming
Propriété
Revue de services et planification des améliorations
Revue du processus et conformité
Registre CSI
Cadre de travail CSI Et système de qualité
Gouvernance TI

> Retour sommaire principal

1 POURQUOI ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

1.1 QUELQUES BONNES RAISONS D'ENTREPRENDRE UNE DÉMARCHE DE CONTINUITÉ D'ACTIVITÉ

PRINCIPAUX CHOCS MONDIAUX



Pertes dues aux catastrophes mondiales 1970-2010 (Source : Swiss Re, Guy Carpenter & Company LLC).

➡ La nature, la fréquence et le coût des crises ont sensiblement évolué au cours des vingt dernières années. On comprend sans doute mieux aujourd'hui à quel point sont étroitement imbriquées les différentes dimensions de ces événements qui perturbent très fortement le fonctionnement de nombreuses organisations, publiques et privées, avec des conséquences allant jusqu'à la cessation définitive d'activité. Les retours d'expérience des grandes crises récentes montrent que les organisations ayant entrepris une démarche préalable visant à garantir la continuité de leur activité sont les plus résilientes face aux événements déstabilisants.

➡ Bien qu'il soit utopique de chercher à tout prévoir et maîtriser, le responsable d'une organisation – publique ou privée – se doit de concevoir et mettre en œuvre des stratégies de protection permettant d'éviter certains événements, ou tout du moins d'en limiter

les effets directs sur les objectifs de l'organisation, et d'assurer la continuité d'activité malgré la perte de ressources critiques. Cet impératif conditionne la situation financière de l'organisation, son image dans la société et naturellement la responsabilité personnelle du dirigeant. Les établissements de crédit, les entreprises d'investissement, les établissements de santé, les opérateurs d'importance vitale doivent déjà répondre à l'obligation légale de plan de continuité d'activité.

➡ Les contraintes économiques imposent de devoir justifier les dépenses - y compris celles qui concernent les actions à entreprendre dans le domaine de la sécurité - et de pouvoir prioriser ces dépenses dans le cadre d'une stratégie globale. Il faut par conséquent disposer d'outils méthodologiques permettant d'optimiser l'efficience de ces actions, en cohérence avec les objectifs de l'organisation. Des outils existent déjà pour couvrir séparément plusieurs domaines indissociables : la gestion de risque, la gestion de crise, l'intervention, le maintien et la reprise d'activité. La démarche de continuité d'activité est le moyen d'associer de manière globale et cohérente tous ces domaines.

1.2 QU'EST-CE QU'UN PCA ?

La gestion de la continuité d'activité est définie[1] comme un « processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs».

Un plan de continuité d'activité (PCA) a par conséquent pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit permettre à l'organisation de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image...) et de tenir ses objectifs.

Le règlement n° 97-02 du Comité de la réglementation bancaire et financière du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement donne la définition suivante : **le PCA représente l'ensemble des mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise, puis la reprise planifiée des activités.**

1/ Définition de la norme ISO 22301 : 2012(F).

> Retour sommaire principal > Retour sommaire fiches pratiques

COMMENT LANCER UNE DÉMARCHE DE CONTINUITÉ D'ACTIVITÉ ?

OBJECTIF

La réalisation d'un plan de continuité efficace et robuste nécessite d'impliquer de nombreux responsables, de conduire des travaux transverses à l'organisation, d'assurer la cohérence des analyses et d'effectuer des arbitrages de niveau stratégique.

➡ **Condition première du succès, la direction de l'organisation doit s'impliquer fortement dans la démarche.**
Dès le lancement, il s'agira de communiquer en expliquant les finalités et de mobiliser les responsables des métiers et des processus. Par la suite et durant toute la phase d'élaboration du PCA, la direction devra valider les résultats successifs :
- Description du contexte, des objectifs et obligations de l'organisation.
- Cartographie des processus clés pour la continuité, des niveaux de service et d'interruption acceptables.
- Cartographie des risques et identification de ceux qui justifient un traitement prioritaire, compte tenu de l'attitude de l'organisation face au risque.
- Stratégie de continuité avec l'optimisation des coûts de continuité tenant compte du coût de l'interruption d'activité, du niveau de continuité souhaité et du risque résiduel.
- Moyens et procédures nécessaires à la mise en œuvre et au suivi du plan de continuité (y compris sa composante de reprise d'activité).

➡ **Les autres conditions du succès sont :**
- Un travail préalable pour formaliser les activités et processus de l'organisation avec la nomination de responsables des métiers et des processus.
- La désignation d'un chef de projet à l'autorité reconnue, et d'une équipe projet qui marqueront le lancement officiel de la démarche. Cette désignation doit s'accompagner d'un mandat précisant les objectifs, les périmètres géographique et fonctionnel, ainsi que les principaux jalons de la mission.
- Une fois la stratégie de continuité établie et validée par la direction de l'organisation, doivent être impliqués, le moment venu, les correspondants du PCA, les responsables des métiers et processus, ainsi que tous les acteurs concernés par la mise en œuvre d'actions spécifiques, afin de mettre en place les ressources et procédures nécessaires.
- L'exercice du PCA pour vérifier son réalisme et son efficacité.
- L'accompagnement à la conduite du changement dans le cadre de cette démarche.

Il est recommandé de :
- Confier le pilotage du projet au responsable chargé de la gestion des risques au sein de l'organisation. À défaut, le responsable en charge du métier le plus impliqué dans les activités essentielles de l'organisation, ou le responsable chargé de l'écoute des clients, peuvent être désignés.
- Donner au responsable du projet PCA l'autonomie et l'autorité, éventuellement par délégation, sur l'ensemble des responsables de l'organisation et des acteurs concernés par les effets contre lesquels on cherche à se protéger.
- Maintenir en place la structure de gestion de PCA une fois que la première version a été validée.

Il est déconseillé de :
- Confier le pilotage d'un projet de PCA à un responsable informatique ou au responsable des services généraux, qui n'auront pas la vision « métier » de l'organisation.

FICHE GUIDE SYNTHÉTIQUE
POUR L'AUTO-ÉVALUATION DES BONNES PRATIQUES

ETAPES ET ACTIONS	OUI	NON	OBSERVATIONS
1. Définition du contexte, identification des objectifs et des activités essentielles.			
1.1. La direction est-elle fortement impliquée ?			
1.2. Un chef de projet doté des compétences, de l'autorité et de l'autonomie nécessaires a-t-il été nommé ?			
1.3. Le contexte et le périmètre de PCA ont-ils été précisés ?			
1.4. Les objectifs, les activités essentielles, les flux et les ressources critiques ont-ils été identifiés ?			
1.5. Les processus de l'organisation ont-ils été cartographiés ?			
1.6. Les flux entre les systèmes d'information supportant les processus ont-ils été cartographiés ?			
2. Déterminer les attentes de sécurité pour tenir les objectifs.			
2.1. Les systèmes de téléphonie, serveurs de fichiers et messagerie ont-ils été intégrés dans les systèmes critiques de l'organisation ?			
2.2. Les ressources critiques « dures » ont-elles été prises en compte ?			
2.3. Les ressources immatérielles ont-elles été prises en compte ?			
2.4. Les niveaux de fonctionnement en mode dégradé sont-ils explicités ? Ont-ils été validés en liaison avec le(s) « client(s) » ?			
2.5. Les niveaux dégradés de prestations des fournisseurs ont-ils été pris en compte ?			
2.6. L'échelle de mesure des conséquences d'interruption validée avec les responsables est-elle identique pour tous les processus ?			
3. Identifier, analyser, évaluer et traiter les risques.			
3.1. Si une analyse de risques préexistait, a-t-elle été reprise pour en vérifier la pertinence ?			
3.2. L'analyse des risques a-t-elle permis d'identifier ceux contre lesquels il est prioritaire de se protéger ?			
3.3. Le PCA global repend-t-il en autant de composantes les scénarios de risques retenus ?			
3.4. Le PCA prend-t-il en compte les risques opérationnels pour lesquels l'interruption d'activité résulte de la perte de ressources critiques ?			
3.5. Les partenaires des secteurs publics et privés susceptibles d'être concernés par les scénarios ont-ils été identifiés ?			
3.6. Les interdépendances et les effets en cascade ont-ils été pris en compte ?			
4. Définir la stratégie de continuité d'activité.			
4.1. Les objectifs de continuité sont-ils cohérents avec ceux de l'organisation, mesurables, et tiennent-ils compte des ressources nécessaires ?			
4.2. Les objectifs de continuité en mode dégradé et pour la reprise d'activité sont-ils cohérents avec les scénarios de risques retenus ?			
4.3. L'ordre de priorité des procédures, des ressources, de la reprise et du basculement progressif sur les systèmes normaux est-il identifié ?			
4.4. Les exigences vis-à-vis des « partenaires » ont-elles été prises en compte de manière réciproque ?			
4.5. Les services de l'État et les organisations partenaires du PCA sont-ils identifiés et connus ?			
4.6. La stratégie a-t-elle été validée par la direction ?			

Page suivante

> Retour sommaire principal > Retour sommaire fiches pratiques

5. Mettre en œuvre et assurer l'appropriation du plan			
5.1. Les actions de communication inhérentes au lancement, à l'appropriation et à la mise en œuvre du PCA ont-elles été prévues ?			
5.2. Les mesures à mettre en œuvre et les procédures associées sont-elles simples et accessibles ?			
5.3. Les dispositifs, moyens et ressources nécessaires à la mise en œuvre du PCA sont-ils disponibles et/ou en place ?			
5.4. Les personnels responsables sont-ils désignés, informés et formés aux procédures prévues dans le PCA ?			
5.5. Les indicateurs, les dispositifs itératifs de vérification, contrôles, exercices et évolution du plan sont-ils conçus et déclinés ?			
5.6. Les procédures de sauvegarde/récupération et les moyens critiques du PCA seront-ils contrôlés périodiquement ?			

FICHE MODÈLE DE RETEX

Pour chacune des étapes suivantes, décrire les faits, les problèmes rencontrés, les solutions utilisées pour les résoudre :

Caractéristique de l'événement :
- Caractéristique de l'incident initial.
- Facteurs aggravants.
- Cinétique.
- Périmètre.
- Activités affectées et caractéristiques (dysfonctionnement ou arrêt, durée).
- Phénomènes en cascade.

Alertes :
- Détection de signes précurseurs.
- Analyse.
- Alerte.
- Mobilisation.
- Décision d'activation de la cellule de crise (délais).

Gestion de crise :
- Délais de mise en œuvre.
- Fonctionnement.
- Acteurs.
- Connaissance de la situation.
- Anticipation.
- Décisions.
- Coordination.
- Communication.

Planification de la mise en œuvre du PCA :
- Activités affectées.
- Processus affectés et ressources perdues.
- Existence de plan disponible et adapté à la situation.
- Bonne mise à jour du plan.
- Connaissance du plan.
- Clarté et facilité de mise en œuvre du plan.
- Fonctionnement du dispositif d'appui, de l'expertise métier et processus.

Mise en œuvre du PCA :
- Bonne évaluation de la situation et de son évolution.
- Décisions connues.
- Pertinence des décisions.
- Mise en œuvre des procédures.
- Disponibilité des ressources pour mettre en œuvre le PCA.
- Respect des délais (DMIA pour les différents modes dégradés et les différentes activités essentielles affectées).
- Efficacité du PCA.

Implication des parties prenantes :
- Consultation des parties prenantes internes.
- Dialogue avec les services de l'État.
- Consultation des fournisseurs, des clients.

Respect des obligations :
- Aspects juridiques.
- Réglementation.

Communication associée au PCA :
- Communication interne.
- Communication avec les partenaires.
- Communication avec le public.
- Pertinence des messages.
- Réaction des médias.

Circulation de l'information :
- Information suffisante.
- Information utile.
- Bonne remontée de l'information terrain.
- Problèmes techniques (moyens de transmission).
- Traçabilité de l'information.
- Bonne communication entre les différentes entités.
- Constatation d'incohérences dans les informations.
- Connaissance du niveau de fonctionnement des activités essentielles.
- Connaissance du niveau de perte des ressources critiques.
- Connaissance de l'impact sur les partenaires externes.

Gestion du PCA :
- Maîtrise de la situation.
- Utilisation des indicateurs pertinents.
- Clarté des rôles des différents acteurs.
- Contribution des correspondants du PCA.

Page suivante

- Rôle du responsable du PCA.
- Bonne coopération des différents services.
- Bonne gestion de la cinétique.
- Régularité des points de situation en cohérence avec la cinétique des événements.
- Bonne utilisation des outils (points de non retour, point de décision...).
- Traçabilité des décisions.
- Difficultés de langage (vocabulaire technique).

➡ **Fonctionnement du PCA :**
- Activation conforme aux décisions.
- Efficacité des procédures.
- Bon fonctionnement des modes palliatifs et de secours.
- Actions rapides et dans les temps impartis des différents acteurs.
- Difficultés techniques rencontrées.
- Niveaux de services.

➡ **Gestion des ressources :**
- Conditions de travail.
- Disponibilité des ressources pour mettre en œuvre le PCA.
- Bon suivi de l'engagement des ressources.
- Bonne utilisation des ressources nécessaires pour le PCA.
- Fonctionnement des moyens externes.
- Relations avec les fournisseurs et sous-traitants.

➡ **Gestion du retour à la normale :**
- Anticipation.
- Décisions au bon moment.
- Disponibilité des ressources nécessaires.
- Reprise des données.
- Respect des délais.
- Coopérations avec les clients et fournisseurs.
- Bonne gestion des aides financières et des assureurs.

➡ **Conclusions :**
- Points positifs.
- Points négatifs.
- Problèmes rencontrés.
- Axes d'amélioration concernant :
  - Le PCA.
  - La formation.
  - La préparation.
  - Les relations avec les parties prenantes externes.

3
Étapes préliminaires à la mise en place d'un système de contrôle d'accès ou de vidéoprotection

Pour bien appréhender les besoins de sécurité relatifs au contrôle d'accès physique ou à la vidéoprotection, il est nécessaire en premier lieu d'établir une cartographie précise de tous les éléments qui détermineront les caractéristiques du système de contrôle mis en place. Parmi ces éléments, on retrouve entre autres :

- les sites à protéger/contrôler ;
- les valeurs métier [10] et biens supports [11] à protéger ;
- les zones incluses dans chaque site ainsi que leurs niveaux de protection attendus ;
- les flux de circulation des individus entre les zones ;
- les acteurs ;
- les processus organisationnels.

Certains de ces aspects ne sont évoqués que sommairement dans ce guide. Les lecteurs qui souhaiteraient accéder à plus d'information peuvent se référer aux référentiels du CNPP :

- « APSAD D83 – Contrôle d'accès – Document technique pour la conception et l'installation » [28] ;
- « APSAD R82 – Vidéosurveillance – Règle d'installation » [30].

3.1 Identification des sites à protéger/contrôler

L'identification détaillée des sites à protéger/contrôler est une étape importante préalable à la mise en place d'un système de contrôle d'accès physique ou de vidéoprotection. Cette étape permet de clarifier les contraintes qui pèsent sur le projet et de disposer des éléments nécessaires, entre autres, à la rédaction des appels d'offres. Les sites à contrôler doivent donc être référencés de manière exhaustive, en prenant en compte leurs particularités.

Pour chaque site, les éléments suivants doivent être considérés :

10. Les « valeurs métier » définies dans la méthode EBIOS-RM [12] correspondent aux « biens essentiels » de la méthode EBIOS 2010 [14]. Il est utile de faire une distinction entre les valeurs métier qui, dans un système d'information, sont des biens immatériels (informations ou processus utiles à la réalisation des missions de l'organisme), et les biens supports dont ils dépendent pour le traitement, le stockage ou la transmission.
11. Les biens support définis dans la méthode EBIOS-RM [12] correspondent aux composantes du SI sur lesquelles reposent une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle.

- nom du site (pour l'identification) ;
- adresse (pour l'emplacement) ;
- nature du site (immeuble entier, quelques étages seulement, quelques pièces uniquement) ;
- caractère dédié ou partagé avec d'autres entités ;
- services à proximité (police, pompiers, etc.) ;
- risques naturels (zone inondable, zone sismique, etc.) ;
- nombre de personnes actuel et potentiel.

R2

Identifier les sites à protéger/contrôler

Il est nécessaire de référencer de manière exhaustive les sites à contrôler en prenant en compte leurs particularités.

3.2 Identification des valeurs métier et biens supports à protéger

Une fois les sites référencés, il convient d'identifier les valeurs métier et les biens supports à protéger. Cette identification, menée dans le cadre d'une analyse de risque, doit permettre également de définir le niveau de sensibilité de chaque site au regard du cadre règlementaire susceptible de leur être associé.

D'une manière générale, les valeurs métier représentent le patrimoine informationnel qu'une source de risque aurait intérêt à attaquer pour atteindre ses objectifs [12].

Les valeurs métier s'appuient sur des biens supports qui en assurent le traitement, le stockage et la transmission. Ainsi un serveur de calcul n'est pas une valeur métier mais un bien support, de même que les locaux, les systèmes informatiques, et les différents équipements. La valeur métier est le processus de calcul, et le serveur est le bien support qui permet l'exécution du processus.

L'ANSSI publie une méthode d'appréciation et de traitement des risques proposant notamment des outils permettant de recenser l'ensemble des valeurs métier et des biens supports : la méthode EBIOS *Risk Manager* [12].

R3

Identifier les valeurs métier et les biens supports à protéger

Il est recommandé d'identifier, au travers d'une analyse de risque, les valeurs métier et les biens supports sur lesquels elles s'appuient, pour déterminer les ressources qu'il convient de protéger, et définir le niveau de sensibilité associé à chaque site référencé.

12. Définition extraite du guide EBIOS *Risk Manager* [12].

3.3 Identification de zones

Après avoir réalisé l'inventaire des valeurs métier, des biens supports et de leur localisation, l'étape suivante consiste à distinguer des zones avec différents niveaux de protection attendus au sein des sites identifiés.

Niveau de protection attendu

Le niveau de protection attendu est associé au niveau de criticité des biens sensibles présents dans la zone. Plus les biens sensibles présents dans cette zone seront critiques, plus le niveau de protection attendu associé à la zone sera important.

Zone contrôlée

Une zone contrôlée est une zone *a priori* fermée, dont tous ses accès sont équipés de lecteurs de badges, ou placés sous vidéoprotection.

Il est recommandé d'établir une échelle précise et explicite des niveaux de protection attendus, avec leurs définitions associées. La numérotation à partir de zéro est tout à fait indiquée pour cet usage, le niveau 0 étant alors la zone considérée comme semi-publique, à l'intérieur de la limite de propriété.

Les niveaux de protection attendus supérieurs (1, 2, etc.) correspondent aux zones contrôlées, entourées de barrières physiques comprenant un nombre restreint de points d'accès, et situées dans l'enceinte des sites ou des bâtiments. Les niveaux de protection attendus les plus élevés correspondent aux zones névralgiques.

R4

Définir les zones incluant les systèmes de contrôle d'accès ou de vidéoprotection au niveau de protection attendu le plus élevé

Les zones où sont situés les éléments du système de contrôle d'accès ou de vidéoprotection (serveurs du centre de gestion du système, et stations de travail) doivent être définies au niveau de protection attendu le plus élevé.

Les sites à protéger doivent être découpés en zones classées par niveau de protection attendu selon l'échelle préalablement conçue. Ces zones n'ont pas à être découpées selon la configuration physique existante des lieux, mais bien selon le niveau de criticité des biens sensibles présents dans la zone : un tel projet peut nécessiter de conduire des travaux de réorganisation de cloisons, de bâtiments et de sites afin que la sécurité physique puisse être optimisée voire même rendue possible.

Si plusieurs zones sont regroupées pour ne former plus qu'une seule zone, la nouvelle zone ainsi formée sera du niveau de protection attendu égal au niveau de protection attendu le plus élevé des zones regroupées.

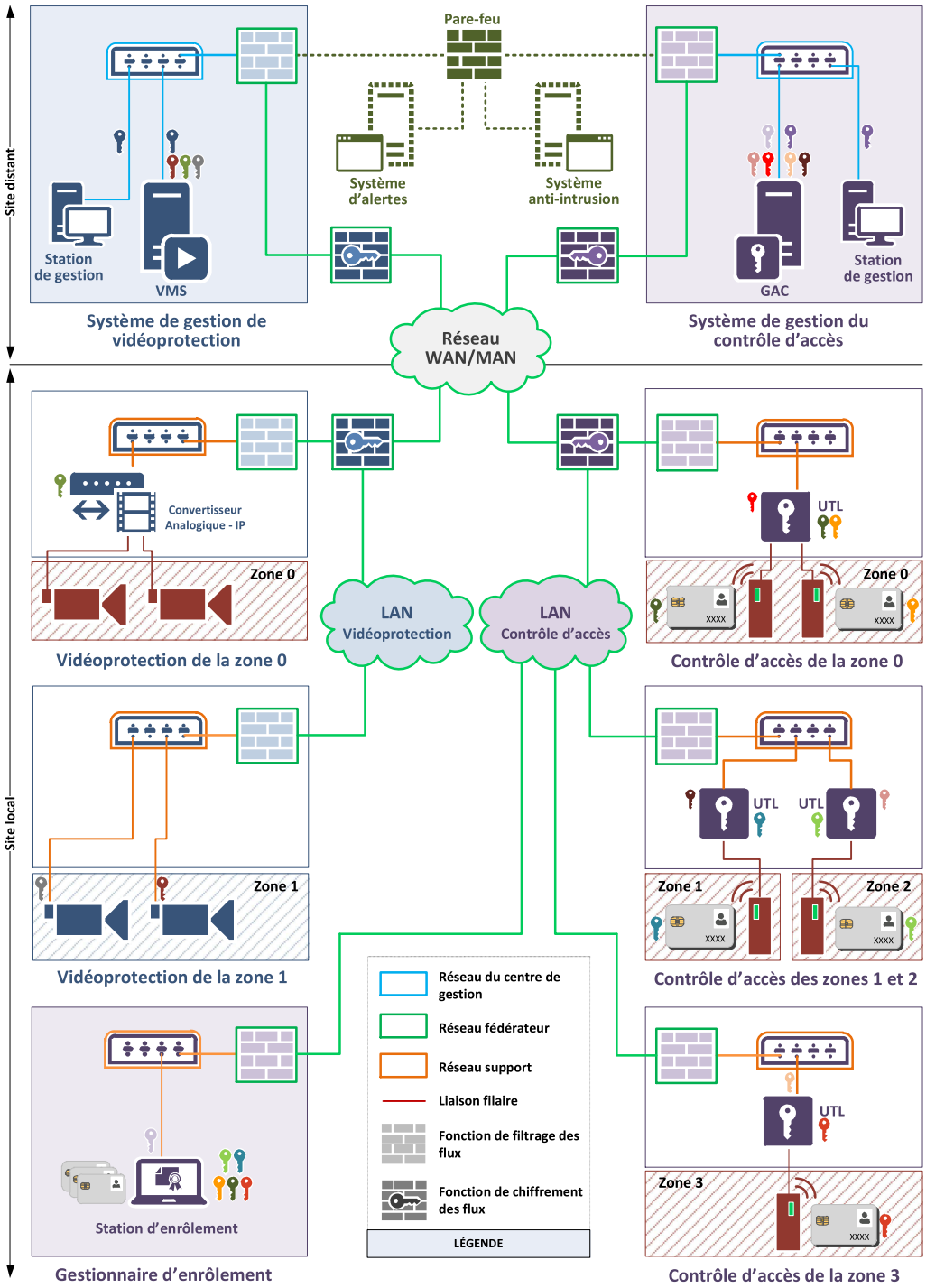


FIGURE 2.1 – Exemple d'architecture générale