Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

CONCOURS INTERNE ET 3ème CONCOURS D'INGENIEUR DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2018 -

Mercredi 5 septembre 2018

Interne : Résolution d'un cas pratique à partir d'un dossier à caractère technique permettant d'apprécier les qualités d'expression, d'analyse et de synthèse du candidat et sa capacité à conduire un projet.

3ème concours : Résolution d'un cas pratique à partir d'un dossier à caractère technique faisant appel à des connaissances relatives à l'environnement et à la technique des systèmes d'information et de communication et permettant de vérifier les capacités d'analyse et de synthèse du candidat ainsi que son aptitude à dégager des solutions appropriées.

(Durée : 4 heures – Coefficient 1)

Le dossier documentaire comporte 27 pages.

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.

ECRIRE EN NOIR OU EN BLEU - PAS D'AUTRE COULEUR

SUJET

Vous êtes chef de projet à la DINSIC (Direction Interministérielle du Numérique et du Système d'Information et de la Communication de l'Etat), chargé de la mise en place d'une offre interministérielle de service de soutien aux utilisateurs. Dans le cadre de la mutualisation de ses supports et ressources informatiques, l'Etat souhaite homogénéiser ses procédures et ses organisations.

Les structures actuelles sont hétérogènes notamment en termes d'outillages et de qualité de service. Trois ministères A, B et C, déjà connectés au Réseau Interministériel de l'Etat (RIE), souhaitent être pilotes de cette offre de service pour leurs sites situés en Ile-de-France. Vous trouverez ci-après les schémas de présentation de l'organisation actuelle de leur Chaîne de Soutien aux Utilisateurs (CSU) y compris le VIP (Very Important Person, personne très importante).

L'objectif consiste à déterminer le ministère qui portera en interne le centre de service unifié qui s'appuiera sur un catalogue d'offres interministérielles pour une mise en service au 1er janvier 2020.

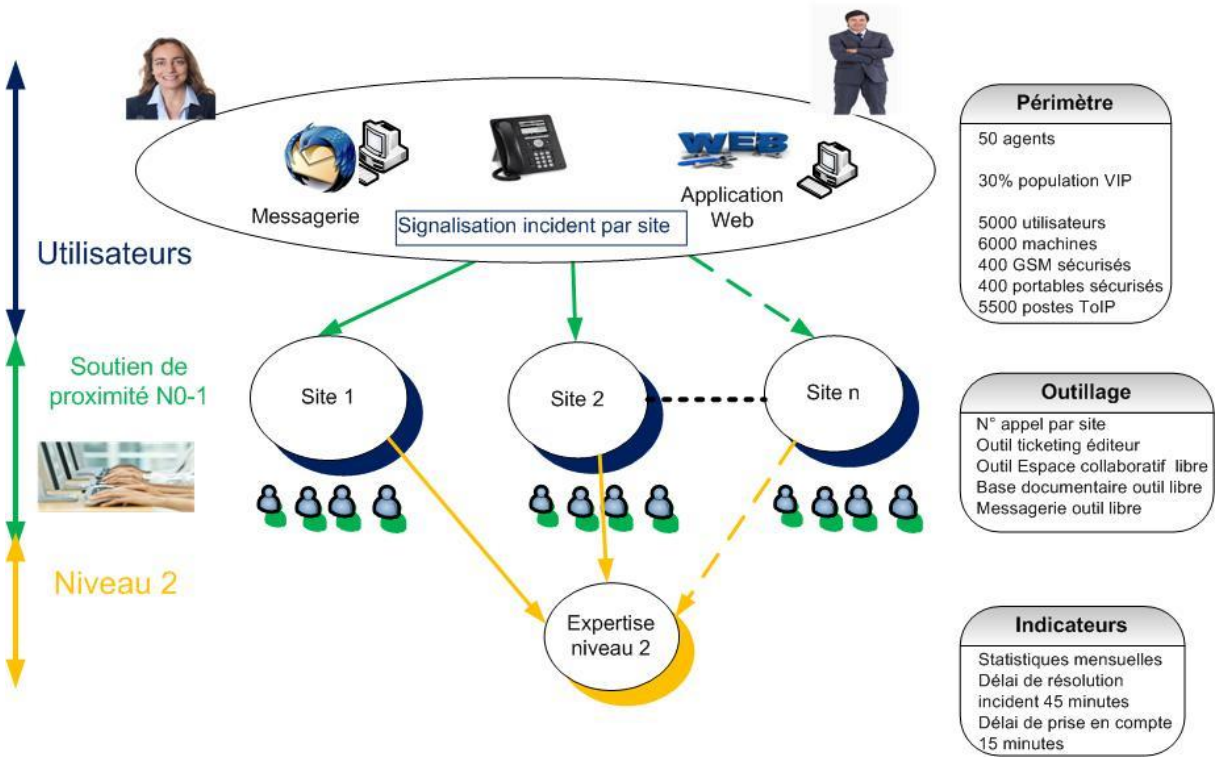
L'externalisation de cette prestation de soutien aux utilisateurs n'est pas retenue et le projet pilote doit se faire à isopérimètre en termes de ressources humaines.

Vous proposerez :

- une solution technique étayée en présentant ses avantages et ses inconvénients,
- un plan d'actions opérationnel (planning détaillé, identification des acteurs du projet et notamment du ministère que vous recommanderez pour porter le centre de service unifié).

Votre proposition tiendra compte des contraintes de sécurité, de qualité de service et d'accompagnement aux changements.

Ministère A chaîne de soutien



Périmètre

50 agents

30% population VIP

5000 utilisateurs
6000 machines
400 GSM sécurisés
400 portables sécurisés
5500 postes ToIP

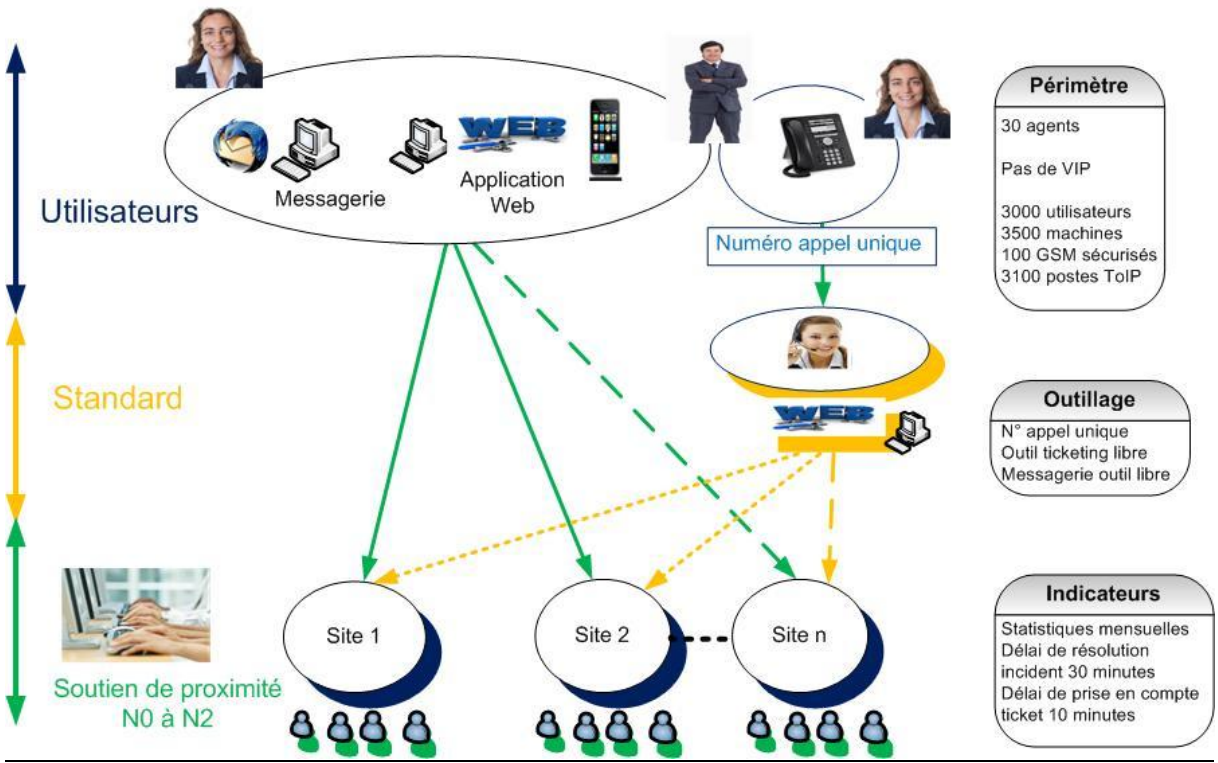
Outillage

N° appel par site
Outil ticketing éditeur
Outil Espace collaboratif libre
Base documentaire outil libre
Messagerie outil libre

Indicateurs

Statistiques mensuelles
Délai de résolution incident 45 minutes
Délai de prise en compte 15 minutes

Ministère B chaîne de soutien



Périmètre

30 agents

Pas de VIP

3000 utilisateurs
3500 machines
100 GSM sécurisés
3100 postes ToIP

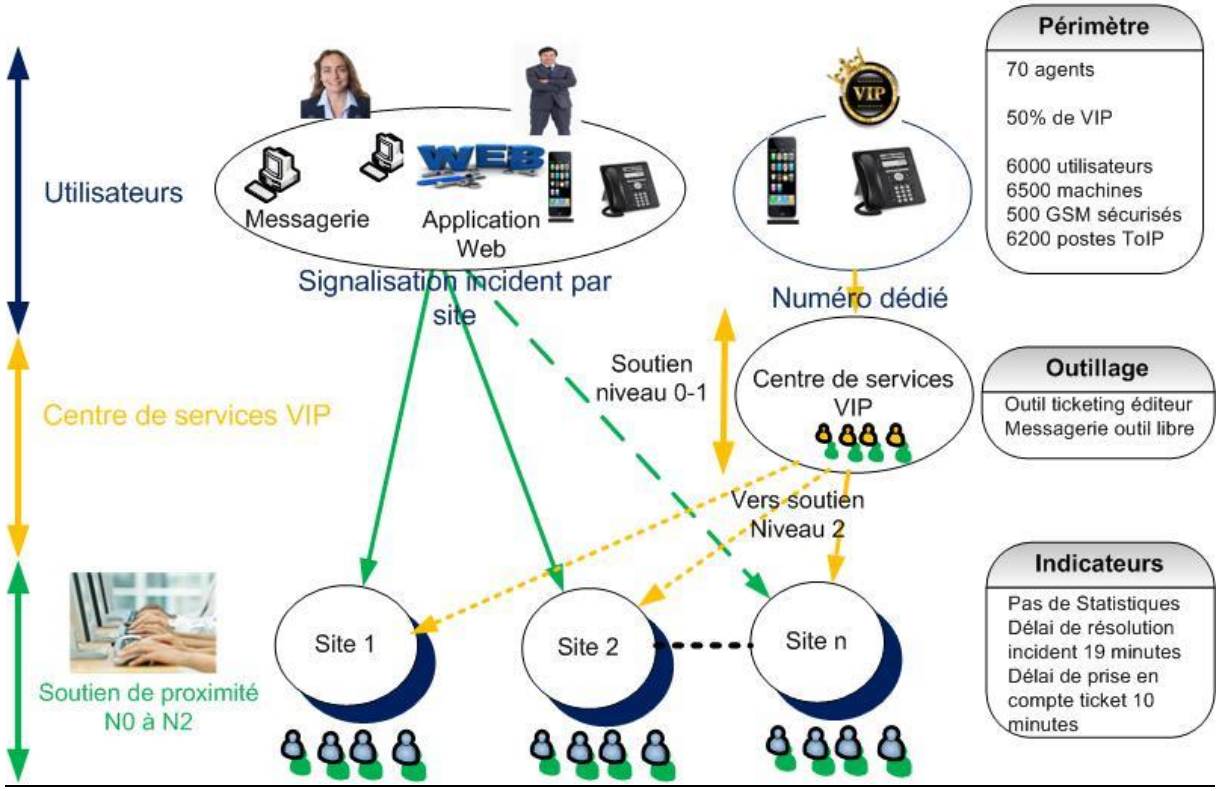
Outillage

N° appel unique
Outil ticketing libre
Messagerie outil libre

Indicateurs

Statistiques mensuelles
Délai de résolution incident 30 minutes
Délai de prise en compte ticket 10 minutes

Ministère C chaîne de soutien



Dossier documentaire :

Document 1

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE MINISTRE DES FINANCES
ET DES COMPTES PUBLICS

LE SECRETAIRE D'ETAT
CHARGE DU BUDGET

LE SECRETAIRE D'ETAT
CHARGE DE LA REFORME
DE L'ETAT ET DE LA
SIMPLIFICATION

Paris, le 30 OCT. 2014

à

Mesdames et Messieurs les ministres,

Mesdames et Messieurs les secrétaires d'Etat

Objet : Modernisation de la chaîne de la dépense de l'Etat

Une nouvelle étape de modernisation de la chaîne de la dépense de l'État a été décidée par le comité interministériel pour la modernisation de l'action publique (CIMAP) du 18 décembre 2013.

La simplification et l'optimisation des modalités d'exécution de la dépense, ainsi que la rationalisation des organisations qui en ont la charge, doivent permettre à la fois de respecter les engagements de l'Etat de réduire les délais de paiement, de réaliser des gains de productivité, et d'améliorer la qualité des comptes de l'Etat.

1. Le respect du processus de dépense défini dans le cadre de la mise en œuvre du système d'information financière de l'Etat

Le strict respect du processus de la dépense

Un audit de l'inspection générale des finances mené en 2013 a constaté que le processus relatif à l'exécution de la dépense, tel qu'il avait été conçu et décrit dans le cadre de la mise en place du système d'information financière de l'Etat (« SI Chorus »), était encore imparfaitement mis en œuvre. Afin d'atteindre les objectifs d'amélioration assignés à l'administration, il est impératif que ce processus, soit désormais strictement appliqué par l'ensemble des acteurs de la chaîne de la dépense. Les axes d'amélioration prioritaires feront l'objet d'une déclinaison opérationnelle détaillée, ambitieuse et réaliste dans le cadre des plans d'action ministériels.

La mise en place d'un pilotage de la performance de la chaîne de la dépense par le responsable de la fonction financière ministérielle

Pour optimiser la chaîne de la dépense, il est nécessaire que le responsable de la fonction financière ministérielle en pilote le fonctionnement et s'assure de sa performance. Pour ce faire, il s'appuie sur les responsables de programme et les ordonnateurs secondaires, et peut solliciter l'appui technique des contrôleurs budgétaires et comptables ministériels et de l'ensemble des comptables assignataires des dépenses de son périmètre ministériel.

D'ores et déjà, nous attendons de ces responsables qu'ils rappellent, sans délais, les règles relatives à la chaîne de la dépense et qu'ils identifient et partagent les bonnes pratiques mises en œuvre dans leur ministère. Cette communication devra s'accompagner d'actions de formation et d'animation ministérielles. Par ailleurs, l'accélération du déploiement des dispositifs de contrôle interne est de nature à conforter cette démarche.

Le ministère des finances et des comptes publics, notamment la direction générale des finances publiques, la direction du budget et l'agence pour l'informatique financière de l'Etat (AIFE), accompagnera l'ensemble des ministères. Par ailleurs, il mobilisera les contrôleurs budgétaires et comptables ministériels ainsi que l'ensemble des comptables assignataires des dépenses de l'Etat.

Une stratégie d'amélioration des indicateurs de qualité du processus de la dépense

Des indicateurs ont été définis dans le cadre d'une concertation interministérielle, menée dans le cadre du Comité d'Orientation Stratégique (COS) du système d'information financière de l'Etat, et leurs résultats sont fournis mensuellement par l'AIFE aux ministères pour chacun de leurs services. Chaque ministère devra déterminer, pour ces indicateurs, des objectifs chiffrés adaptés à ses services et les assortir d'une stratégie permettant d'atteindre les cibles. Ces indicateurs devront faire l'objet d'un suivi rigoureux par le responsable de la fonction financière ministérielle et seront examinés régulièrement au niveau interministériel dans le cadre du COS.

2. La dématérialisation des actes de gestion et des échanges

L'ordonnance n°2014-697 du 26 juin 2014 relative au développement de la facturation électronique rend progressivement obligatoire la dématérialisation des factures dans le cadre de l'exécution de la commande publique. Au plus tard en janvier 2017, tous les services de l'Etat doivent être en capacité technique et organisationnelle de traiter les factures en mode dématérialisé. Dès 2017 pour les plus grandes entreprises, et au plus tard en 2020, les fournisseurs adresseront directement et exclusivement leurs factures sous forme électronique aux services utilisateurs de Chorus. Cette mesure vise à alléger la charge administrative pesant sur les opérateurs économiques, tout en facilitant les travaux des administrations. Elle permettra d'éviter des traitements manuels à faible valeur ajoutée qui représentent un coût significatif et offrira des gains de temps dans l'envoi et le traitement des factures.

La réussite d'un tel dispositif implique le strict respect du processus de la dépense et une adaptation des pratiques. Dans cette perspective, nous vous demandons d'intensifier dès 2014 la dématérialisation des factures en provenance de vos fournisseurs, en préconisant le recours au portail Chorus factures, en développant l'Echange de Données Informatisé (EDI) avec les fournisseurs raccordés, et en recourant de manière plus intensive à la numérisation pour unifier les chaînes de traitement des factures. D'ici au 1er décembre, vous présenterez, dans le cadre de vos plans d'action ministériels, les engagements pris sur ces différents axes pour la période 2014-2017.

Plus largement, l'État a engagé une démarche volontariste s'appuyant sur son système d'information financière, qui dispose d'un ensemble de fonctionnalités permettant la dématérialisation quasi complète de la chaîne d'exécution de la dépense : les actes de gestion et la validation des étapes de l'exécution et du contrôle de la dépense peuvent être traités électroniquement sans matérialisation des pièces et documents.

Le décret n°2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique ouvre aussi, de la manière la plus large, la possibilité de dématérialiser les pièces justificatives. Nous attendons des acteurs de la chaîne de la dépense qu'ils développent rapidement le recours à cette dématérialisation.

La dématérialisation des pièces des marchés dès leur publication et lors de la réception des offres électroniques doit notamment être une priorité de vos ministères.

Les échanges entre services d'actes de gestion sous une forme dématérialisée, et en particulier par formulaire, devront être intensifiés.

Chaque ministère déterminera des objectifs chiffrés de dématérialisation aux différents stades de la chaîne de la dépense.

3. La rationalisation du processus d'achat

L'amélioration de la chaîne de la dépense et de l'organisation de la fonction financière est étroitement liée à la démarche de modernisation de la politique des achats de l'Etat décidée par le CIMAP du 2 avril 2013.

C'est pourquoi le service des achats de l'Etat devra, en lien avec l'AIFE, prendre en compte dans les travaux qu'il conduit avec vos administrations la nécessaire articulation entre le processus des achats et la fonction financière. En particulier, les besoins résultant de la démarche de rationalisation de la fonction financière de l'Etat et ceux issus de l'organisation de la fonction achats devront être mis en cohérence.

Il convient de rappeler qu'afin de fluidifier la chaîne d'exécution de la dépense, chacune des étapes du processus d'achat doit être respectée. Il est notamment essentiel que les appels d'offres soient publiés sur la plate-forme des achats de l'Etat (PLACE) et que l'intégration dans Chorus des marchés notifiés soit réalisée systématiquement par les acheteurs au travers du lien Place-Chorus. En outre, en amont comme en aval, des actions doivent être entreprises afin de réduire le nombre d'actes. Une attention particulière devra être portée à la diminution du nombre de factures de faible montant unitaire, dont les coûts de traitement sont élevés au regard des sommes à régler.

La mutualisation des achats entre services de l'Etat et leur anticipation doivent être intensifiées, chaque fois que cela est possible, avec pour premiers objectifs d'optimiser les coûts et de limiter les dépenses de faible montant.

Les meilleures modalités de règlement ou de facturation doivent également être étudiées en amont de la commande. Ainsi, il conviendra de recourir de façon plus systématique au règlement par carte d'achat pour les approvisionnements ponctuels, de faible montant. La définition d'un plan de facturation pourra également être favorisée. Enfin, devra être encouragé le regroupement périodique (mensuel, trimestriel, ...) des factures par les fournisseurs.

L'attention de tous les acheteurs ministériels devra également être appelée sur la nécessité de recourir à l'ensemble des leviers de dématérialisation mis à leur disposition et d'inclure dans les appels d'offres toutes les clauses nécessaires pour y parvenir : obligation de déposer des réponses électroniques et des pièces justificatives dématérialisées, de produire des factures dématérialisées, de recourir largement au plan de facturation, de réguler le nombre de factures émises en cas de fortes volumétries par une périodicité adaptée, etc.

4. Des organisations permettant une plus grande fluidité du processus de dépense

L'organisation de la fonction financière mise en place dans le cadre du déploiement du nouveau système d'information financière de l'Etat (« SI Chorus ») repose sur des services prescripteurs et des centres de services partagés agissant pour le compte des ordonnateurs, et des services placés sous l'autorité des comptables.

L'optimisation du rôle des centres de services partagés

Les Centres de Services Partagés (CSP) ont été conçus pour améliorer l'efficacité, la qualité et l'efficience des traitements, en regroupant des ressources capables de mobiliser des compétences spécifiques pour l'exécution des dépenses en environnement Chorus.

La répartition des tâches entre les services prescripteurs et les centres de services partagés doit donc faire l'objet de contrats de services, précisant les modalités pratiques du fonctionnement de la chaîne de la dépense et les niveaux de prestation auxquels ils s'engagent, en termes de délai et de contenu des informations transmises. Des objectifs ministériels devront être définis en ce sens. Un contrat de services type sera établi, dans le cadre de la concertation interministérielle, afin de disposer d'un modèle unique et partagé, dont la déclinaison locale devra respecter les lignes directrices.

La généralisation des services facturiers

Les travaux préalables au déploiement du SI CHORUS ont conduit, dès 2007, à définir une organisation cible incluant la généralisation des services facturiers à l'ensemble du périmètre des administrations de l'Etat. Le CIMAP du 18 décembre 2013 a décidé que cette extension devrait être achevée en 2017.

Cette généralisation est une contribution essentielle à la diminution des délais de paiement et à la réduction des coûts de la chaîne de la dépense, et permettra sur l'ensemble du périmètre de la commande publique de faciliter la mise en œuvre de l'obligation de dématérialiser les factures.

Chaque ministère doit, en concertation avec la direction générale des finances publiques, présenter les voies et moyens ainsi que le calendrier permettant d'atteindre opérationnellement cet objectif. Les exceptions tenant à une nature particulière de dépenses ou de marché ou à leur confidentialité devront être explicitées.

La rationalisation des procédures financières concernant les DDCS et DDCSPP

Il convient de rationaliser la procédure concernant les opérations financières des directions départementales de la cohésion sociale (DDCS), des directions départementales de la protection des populations (DDPP) et des directions départementales de la cohésion sociale et de la protection des populations (DDCSPP), qui relèvent actuellement, en fonction de leur nature, de plusieurs centres de services partagés.

Conformément à la décision du CIMAP du 18 décembre 2013, ces opérations seront unifiées en 2015, en transférant les dépenses de chaque type de DDI vers la structure qui traite d'ores et déjà le plus grand nombre d'actes. En conséquence, l'exécution des opérations financières des DDCSPP et des DDPP sera rattachée au "bloc 2" (CSP communs aux ministères de l'écologie et de l'agriculture) et l'exécution des opérations financières des DDCS au "bloc 3" (CSP communs aux ministères économique et financiers, aux ministères sociaux et au ministère de la culture).

Les ministères et les services comptables concernés veilleront à procéder en temps utile aux opérations nécessaires à la mise en œuvre de cette décision.

5. Une démarche déclinée dans des plans d'action ministériels et faisant l'objet d'une concertation interministérielle

Une concertation interministérielle s'est engagée sur l'ensemble des volets précédemment évoqués.

Vous devez décliner dans un plan d'action les différents objectifs rappelés par la présente circulaire.

Chaque plan ministériel d'action devra comporter :

1. un volet relatif à l'amélioration du processus de la dépense incluant des objectifs chiffrés d'évolution des indicateurs, des engagements précis de progression de la dématérialisation sous toutes ses formes et une déclinaison ministérielle de rationalisation du processus achat ;
2. un volet organisationnel dressant le schéma d'organisation cible des centres de services partagés et la trajectoire de généralisation des services facturiers à l'horizon 2017.

Les plans d'action, sur la base des premières versions présentées en juin 2014, devront être finalisés au plus tard le 1er décembre 2014 et transmis au COS pour examen. Les arbitrages nécessaires afin d'assurer le respect des orientations de la présente circulaire seront le cas échéant proposés au Premier ministre.

Les plans d'action seront ensuite actualisés annuellement.

Leur mise en œuvre sera suivie par le COS, placé auprès du ministre des finances et des comptes publics et du secrétaire d'Etat chargé du budget, et qui associe des représentants de chacun des ministères. Il sera rendu compte régulièrement de l'avancement des travaux au Premier ministre.

Vous nous saisirez des difficultés que vous pourriez rencontrer dans l'application des instructions qui précèdent.

Michel SAPIN Christian ECKERT Thierry MANDON

Document 2

Sources : https://www.myrhline.com/actualite-rh/les-centres-de-services-partages-retour-d-experience-avec-air-france.html

Les centres de services partagés, retour d'expérience avec Air France

Les CSP, centres de services partagés, se développent en France depuis plusieurs années. En mutualisant les ressources et les activités, ils ont pour but de permettre aux entreprises ayant mis en place un tel système d'améliorer la performance de la fonction RH tout en réduisant les coûts dans la plupart des cas. Un tel projet peut, néanmoins présenter des risques, notamment sur le plan social et peut-être vécu comme une perte d'autonomie.

My RH Line a rencontré Laurent Guillaume, Responsable du Centre d'expertise et se services partagés d'Air France

My RH Line : Pourquoi avez-vous décidé la mise en place d'un CSP ?

Guillaume Laurent : Nous menions, comme dans beaucoup d'entreprises, une réflexion plus globale sur les fonctions support dans un objectif de productivité accrue. Parmi tous les projets qui ont été lancés à ce moment-là, il y en a également eu un sur la paie. A cette période, en 2006, la paie était traitée par 19 services de paie en Métropole avec une logique à la fois géographique et métier.

L'objectif de ce projet était de les regrouper, dans un premier temps, au sein d'un CSP à la fois pour des objectifs de productivité, et d'homogénéisation de traitement car nous nous apercevions au fil du temps qu'il y avait eu des petites dérives dans chaque service de gestion dans l'application des règles. Nous avions un objectif d'équité de traitement.

Le troisième objectif était un accompagnement informatique. Nous étions en train de lancer en parallèle un projet de e-service. Dans le cadre de la modernisation, nous avons donc décidé de mener en parallèle la partie informatique et la partie organisationnelle.

My RH Line : Comment étiez-vous organisés auparavant ?

Guillaume Laurent : Nous avions différents petits services en proximité qui étaient totalement indépendants les uns des autres, avec une coordination autour des outils et de la réglementation mais dont le management et les méthodes de travail étaient totalement indépendants les uns des autres. Comme toujours, dans ce genre de situation, au fur à mesure du temps, les différences sont de plus en plus fortes et il y avait un vrai sujet à étudier sur l'homogénéité de traitement.

My RH Line : Quel a été l'apport de ce CSP pour l'entreprise et pour les salariés ?

Guillaume Laurent : Le CSP est en place depuis presque 3 ans. Les objectifs principaux sont en passe d'être atteints en termes de productivité et d'homogénéité de traitement. Cela a apporté une économie de masse salariale à la taille de l'objectif fixé autour de la fonction paie. En termes d'équité de traitement, il y a un moins de possibilités de contentieux sur l'équité par rapport aux salaires.

Nous avons également perçu un gain d'image en termes de modernisation.

Au point de vue du salarié géré par le CSP, la réponse est un peu plus ambivalente. Pour le salarié, le premier ressenti a été celui d'une dégradation de qualité de services. Auparavant, la personne disposait d'un service de gestion avec un gestionnaire qu'il connaissait depuis des années et qui connaissait parfaitement son dossier. Il pouvait aller le voir pour faire le point. Et du jour au lendemain, ce même dossier se trouve géré par un service à distance. Le salarié ne connaît pas le gestionnaire et doit s'adresser à un call center.

Le collaborateur a eu le sentiment de passer dans un mode un peu plus déshumanisé et distant. Ce sentiment a été très fort au début mais aujourd'hui, 3 ans après, nous avons beaucoup moins de remontées, les salariés se sont habitués à ce mode de relation. Nous avons travaillé sur le fait que ça ne se traduise pas par une baisse de qualité mais uniquement une différence de relation : au lieu d'avoir le numéro de son agent de gestion, il a celui du call center.

My RH Line : Quelle a été la démarche projet et comment Northgate Arinso vous a accompagné ?

Guillaume Laurent : La mise en place d'un CSP est un projet très complet car on touche à la fois à l'organisation, à l'outil, au processus et au management. Il faut ajouter à cela une partie immobilière car on regroupe dans un même lieu des services qui étaient auparavant dispersés.

Il s'agit donc d'un projet très complet qui touche à un sujet sensible, la paie. `

Il se divise en plusieurs phases :

- la phase traditionnelle d'analyse de l'existant, de définition d'organisation qui a duré une année
- la partie présentation, officialisation devant les instances CCE, CE et CHSCT. Cette partie est la plus sensible car sur ce genre de projet de productivité les syndicats sont très regardants. Les échanges ont été relativement vifs pour finir sur des votes globalement négatifs. Mais j'ai néanmoins gardé un souvenir positif de ces moments-là car cela a été l'occasion de montrer notre vision du projet et de les rassurer. Pour finir, l'impact en termes de relation sociale a été moins important que prévu.
- Enfin, la partie conduite du changement, à la fois pour le salarié qui devient une sorte de "client" auquel il faut expliquer la nouvelle façon de procéder et désamorcer la déception qui va en découler et en interne. Nous n'avons pas recruté au démarrage mais procédé à la mobilité des salariés qui étaient dans les petits services. Pour eux c'est un gros changement : de lieu de travail, de management, de collègues et aussi de portefeuille de salariés. Jusqu'alors, ils connaissaient par cœur les salariés, ils ont donc dû se réapproprier un nouveau "portefeuille". Cela prend plusieurs mois.

Ce qui était aussi important en termes de changement est la partie call center car cela était très nouveau.

Nous avons bénéficié d'un accompagnement d'Arinso très orienté sur le pilotage du projet avec ses différents lots, interdépendants et divers.

Ils nous ont accompagnés, également, sur la partie call center qui est assez nouvelle dans le monde RH. J'ai apprécié leur expertise sur les outils dédiés spécifiques du call center, des outils de téléphonie et de gestion de demandes. Nous avons pu ouvrir le CSP tout de suite avec l'organisation call center et cela dans un temps relativement court

My RH Line : Vous accompagnent-ils toujours ?

Guillaume Laurent : Non, aujourd'hui nous sommes passés en régime de croisière. La première année a été difficile, mais aujourd'hui nous sommes tout à fait sortis des difficultés. Nous travaillons plus sur des améliorations à la marge. Nous n'avons, à aucun moment, ressenti le besoin de remettre en question le modèle organisationnel décidé au début et nous n'avons pas ressenti le besoin d'avoir recourt à un consultant dans ce régime de croisière.

My RH Line : Quels sont vos projets RH ?

Guillaume Laurent : Je ne vais pas parler au niveau RH global mais au sein du CSP qui a un périmètre très lié à la paie et à la gestion administrative.

Il y a plusieurs points que nous pouvons toujours améliorer.

La fluidité des processus est à améliorer dans le sens où nous sommes en relation avec le monde RH, les managers, les salariés. Il y a une automatisation des processus à pousser un peu plus dans la remontée d'information.

En terme organisationnel, il faut absolument que nous réfléchissions à nos services de gestion en province qui sont restés dans l'ancien modèle.

En termes de contrôle, nous avons créé un pôle support pour développer les contrôles et les formations. Nous passons d'un mode de contrôle assez artisanal à un mode un peu plus professionnel à base de requêtes, et de comparaisons de paie (mois m-1 et mois m). Nous pouvons, sans doute, encore nous améliorer pour pister les risques d'erreur au plus fin.

My RH Line : Souhaitez-vous intégrer d'autres fonctions RH au CSP ?

Guillaume Laurent : Aujourd'hui ce n'est pas prévu, nous n'avons, en particulier, pas travaillé sur l'intégration de ce qui se fait parfois à savoir le suivi administratif de la formation.

Je pense qu'il serait intéressant d'intégrer certaines tâches administratives qui sont encore faites par les RH de proximité qui ont gardé un certain nombre de fonctions administratives. Maintenant que le CSP fonctionne bien, je serai assez favorable pour les inclure progressivement au CSP car il permet de par sa taille et son volume de travailler sur des automatisations, des mailings, des comparaisons de fichiers.

Avec la création de ce CSP, qui gère 30 000 salariés, nous avons acquis un poids plus fort pour la discussion sur la réglementation et surtout dans le débat budgétaire à propos des outils.

Je suis satisfait de l'organisation et cela justifie les difficultés inévitables du départ. Il ne faut pas les sous-estimer mais cela vaut le coup de tenir le cap car l'organisation a des vertus en elle-même. Je m'aperçois aujourd'hui que nous allons pouvoir continuer à générer des gains de productivité n régime de croisière, car se met en place une organisation vertueuse de travail sur les processus d'homogénéisation.

Propos recueillis par Anne-Sophie Duguay

A propos d'Air France :

Air France-KLM est le premier transporteur aérien en Europe avec plus 74,5 millions de passagers et 24 milliards d'euros de chiffre d'affaires en 2008-09.

Air France-KLM dessert 244 destinations dans 105 pays au travers le monde. Son réseau aérien, le plus important entre l'Europe et le reste du monde, est efficacement coordonné et équilibré autour des hubs de Roissy-Charles de Gaule et Amsterdam-Schiphol. Avec son nouveau partenaire Alitalia, Air France-KLM développe le premier réseau coordonné du Nord au Sud de l'Europe.

Partenaire privilégié des acteurs majeurs du secteur aérien, Air France-KLM est un des membres fondateurs de l'alliance aérienne internationale SkyTeam qui lui permet d'étendre et de consolider sa présence sur tous les plus grands marchés du secteur aérien à travers 169 pays.

107 000 collaborateurs (63 000 pour la société Air France seule) participent au dynamisme de ses activités dont les principaux métiers sont le passage, le fret et la maintenance. Le groupe développe également des activités complémentaires comme le catering et le transport de loisir.

A propos de Northgate Arinso :

Véritable partenaire global de services RH, NorthgateArinso est un des leaders reconnus dans le monde. Il offre une gamme complète de solutions innovantes aux entreprises de toute taille, parmi lesquelles bon nombre de sociétés présentes dans le classement «Global Fortune» 500 et les organisations du secteur public.

NorthgateArinso assiste les Directions des Ressources Humaines dans l'optimisation des services rendus à leurs employés, grâce à des processus adaptés et une technologie de pointe, couvrant ainsi tous les domaines clés tels que l'administration du personnel, la paie, les avantages, le recrutement, la formation et la gestion des talents.

Les 4500 employés de NorthgateArinso sont dédiés à l'excellence des Ressources Humaines au travers des 4 activités suivantes : le conseil RH (HR Business Consulting), l'externalisation des services RH, l'implémentation des systèmes ERP RH, et la mise à disposition de solutions de pointe. NorthgateArinso est l'un des cinq premiers fournisseurs mondiaux de services RH et est présent dans 32 pays sur 5 continents. Pour plus d'informations, veuillez consulter le site web : www.northgatearinso.com

Extrait de la documentation du site GLPI : http://glpi-project.org/DOC/FR/

GLPI

GLPI (gestionnaire libre de parc informatique) est une solution open-source d'ITSM (information technology service management=gestion de services informatiques) et de centre d'assistance (service desk). GLPI permet d'effectuer un inventaire (avec un logiciel tel qu'OCS Inventory) de postes, périphériques réseaux, imprimantes... GLPI permet aussi la gestion des licences (date d'expiration, informations commerciales...), le service desk, des rapports statistiques, réservation de matériel, une FAQ et bien d'autres fonctionnalité qui en font un outil puissant pouvant être mises en place dans une SI et ce peu importe la taille de l'entreprise.

Les fonctionnalités de cette solution aident les Administrateurs IT à créer une base de données regroupant des ressources techniques et de gestion, ainsi qu'un historique des actions de maintenance. La fonctionnalité de gestion d'assistance ou helpdesk fournit aux utilisateurs un service leur permettant de signaler des incidents ou de créer des demandes basées sur un actif ou non, ceci par la création d'un ticket d'assistance.

L'inventaire régulier d'ordinateurs, des imprimantes périphériques en réseau et composants associés est réalisé par le serveur OCS via une interface OCS inventory avec un agent installé sur chaque équipement.

Fonctionnalités	Specificités
Inventaire	Inventaire d'ordinateurs, des imprimantes périphériques en réseau et composants associés via une interface composée de OCS Inventory
	Gestion administrative, des contrats et des documents en relation avec les éléments d'inventaire
ServiceDesk ITIL Compliant	Gestion des problèmes dans plusieurs environnements par le biais de la création de tickets, la gestion des tickets, l'assignation et la planification des tickets, etc.
	Gestion des problèmes, des projets et des changements
Utilisateurs finaux	Historique des interventions
	Enquête de satisfaction
	Commentaire des requêtes
Techniciens	Suivi des mails de demandes d'intervention
	Gestion des demandes d'intervention
	Remontée des incidents
Statistiques	Rapports dans différents formats (PNG, SVG, CSV)
	Statistiques globales
	Statistiques par catégories (par technicien, matériel, utilisateur, catégorie, priorité, lieu…)
Management	Gestion des statuts d'équipement et réservation
	Gestion des contrats et documents
	Système basique de gestion de la base de connaissances
	Gestion des demandes d'assistance pour tout type d'inventaire d'équipements
	Gestion des informations financières et commerciales (achat, garantie et extension, amortissement)
Réservation Gestion des réservations	Interface utilisateur (calendrier)
Base de Connaissances	Gestion des articles de la base de connaissances et de la foire aux questions (FAQ)
	Gestion des contenus par cible (profiles, groupes, etc.)
Rapports	Génération de rapports liés aux dispositifs (type de dispositif, contrats associés, informations commerciales)

Authentifier les utilisateurs

GLPI s'interface avec des annuaires LDAP afin d'authentifier les utilisateurs, de contrôler leur accès, de récupérer leurs informations personnelles et d'importer des groupes. Tous les annuaires compatibles LDAP v3 sont supportés par GLPI. C'est donc aussi le cas pour Microsoft Active Directory (AD).

Profils GLPI

Plusieurs profils sont pré-enregistrés dans GLPI dont les suivants :

- Admin : Ce profil dispose de droits d'administration sur l'intégralité de GLPI. Certaines restrictions lui sont appliquées au niveau de la configuration des règles, des entités ainsi que d'autres rubriques pouvant altérer le comportement de GLPI.
- Supervisor : Ce profil reprend les élements du profil Technician en y ajoutant des élément permettant la gestion d'une équipe et son organisation (attribution de tickets...)
- Technician :Ce profil correspond à celui utilisé pour un technicien de maintenance. Il a accès à l'inventaire en lecture et au helpdesk afin de traiter des tickets.
- Hotliner : Ce profil correspond à celui que l'on pourrait donner pour un service de Hotline. Il permet de saisir des tickets et de les suivre mais pas d'en être en charge comme peut l'être un technicien.
- Observer : Ce profil dispose de droits de lecture sur toutes les données d'inventaire et de gestion. Au niveau de l'assistance, il pourra déclarer un ticket ou s'en voir attribuer mais ne pourra administrer cette rubrique (*attribuer un ticket, voler un ticket...*). Il ne dispose cependant d'aucun droit lié à l'administration ou à la configuration de GLPI.

Règles métier (Business rules)

GLPI dispose d'un moteur de règles qui permet d'effectuer un certain nombre d'actions et d'associations de manière automatique.

Par exemple, le moteur sert pour :

- l’affectation d'une machine à une entité
- associer un profil à un utilisateur
- donner des catégories à un logiciel
- le routage de tickets dans des entités
- actions automatiques à la création des tickets

Le moteur se comporte de manière différente en fonction des types de règles :

- arrêt après la première règle vérifiée
- déroulement de toutes les règles
- déroulement des règles avec passage du résultat aux suivantes

Exemple de règles métier pour les tickets :
- Les tickets des sites 1-8 seront étiquettés VIP (quelque soit la catégorie)
- Les tickets des sites 1-8 de catégorie "Electrique" ou "Climatisation" seront attribués aux techniciens électriciens.

GLPI implémente un mécanisme de routage des tickets ouverts par courriel, afin de les créer dans la bonne entité. Celui-ci se base sur le moteur de règles. Les critères disponibles sont des entêtes du courriel (priorité, from, to, in_reply_to), ainsi que les données du ticket (sujet et corps).

Les critères disponibles sont tous les attributs du ticket (titre, description, statut, catégorie, urgence, impact, priorité, source de la demande, type de matériels, demandeurs groupe/utilisateur/lieu, attribué à fournisseur/groupe/technicien, type de matériels, entité) ainsi que d'autres liés aux collecteurs de courriels (entêtes...).

Les actions possibles sont de modifier certains attributs du ticket (statut, catégorie, urgence, impact, priorité, demandeurs groupe/utilisateur/lieu, attribué à fournisseur/groupe/technicien). Il est aussi possible d'attribuer un ticket à

un matériel en fonction de données présentes dans le ticket (attribution sur l'adresse IP, le nom complet et le domaine, l'adresse MAC).

Remarque : les règles métier pour les tickets ne sont jouées qu'à la création du ticket. Lors de la modification de celui-ci, aucun mécanise automatique n'est lancé.

Important : le moteur joue toutes les règles les unes après les autres. Le résultat des règles précédentes est passé à la règle en cours. Cela veut dire que si une règle précédente modifie un attribut utilisé par la règle courante, c'est la valeur modifiée de celui-ci qui sera traité.

Dans le cas d'une utilisation de GLPI en multi-entités, les règles métier pour les tickets peuvent être récursives, c'est à dire qu'elles peuvent être définies sur une entité avec une application sur l'entité même et sur les sous-entités. 3 onglets sont accessibles : *règles appliquées (nom entité)* qui sont toutes les règles des entités parentes jouées, *règles locales* qui représente la liste des règles définies pour l'entité en cours, règles applicables dans les sous-entités qui sont toutes les règles appliquées après celles de l'entité courante.

Un type de règles permet d'affecter automatiquement une machine provenant d'un outil d'inventaire à une entité et un lieu. Un certain nombre de critères sont disponibles : ceux reprenant des champs génériques (nom, description, numéro de série, domaine, adresse IP, sous-réseau) mais aussi des champs venant de l'outil d'inventaire si celui-ci les propose. Les actions disponibles sont d'ignorer l'import de la machine, de l'affecter à une entité (statiquement), de l'affecter à une entité en utilisant le résultat d'une expression rationnelle ou de l'affecter à un lieu défini.

Pour qu'un utilisateur puisse accéder à une entité, il faut qu'il matche :

- soit une règle qui donne affectation à une entité et affectation d'un profil
- soit une règle qui donne affectation à une entité ET une autre qui donne affectation d'un profil

Si une règle indique juste l'affectation d'un utilisateur à une entité, alors le profil par défaut sera appliqué automatiquement pour celle-ci.

Il est possible de combiner les 2 types de règles :

- une règle A définissant l'accès à une entité 1
- une règle B définissant l'accès à une entité 2
- une règle C affectant un profil P1 à l'utilisateur
- une règle D définissant l'accès à l'entité 3 avec le profil P2

Le moteur va exécuter les règles dans l'ordre suivant :

- affectation à l'entité 3 avec profil P2
- affectation à l'entité 1 avec profil P1
- affectation à l'entité 2 avec profil P1

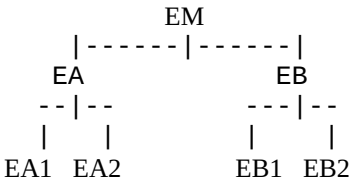
Entités

La notion d'entité est une notion clé dans GLPI. Elle peut s'apparenter à la notion de hiérarchie, de service au sein d'une administration d'une entreprise ou d'un système d'information. Elle permet d'isoler des ensembles organisés de manière hiérarchique dans une instance unique de GLPI (une seule installation de GLPI). Le terme choisi est volontairement neutre, afin de pouvoir s'adapter à chaque système d'information. Une seule instance de GLPI composée de plusieurs entités permet la consolidation des données et des règles communes. L'utilisation des entités permet un cloisonnement relativement étanche entre les unités organisationnelles. Dans les cas où ce cloisonnement étanche n'est pas souhaité, il est préférable d'utiliser les fonctionnalités offertes par les groupes. La segmentation en entités peut avoir plusieurs finalités : isoler le parc informatique de chaque service afin de limiter la vision du parc à certains groupes ou utilisateurs ; isoler le parc informatique de différents clients, reproduire la hiérarchie existante au sein de votre Annuaire informatique (LDAP, Active Directory)... Cette notion est très intéressante pour une entreprise dont la gestion est hiérarchique et où les personnes doivent avoir une vision du parc dépendant de leur appartenance à un service.

Un utilisateur peut être attaché à plusieurs entités avec des droits différents. Ces droits peuvent aussi être conservés sur les entités filles. Une entreprise qui gère plusieurs clients peut définir une entité par client

Une fois plusieurs entités créées dans GLPI, l'inventaire de votre parc, les utilisateurs, les profils ou encore le service d'assistance devient fonction des entités. Autrement dit, on peut affecter un ordinateur à une entité, déclarer un ticket sur une entité, créer des profils, gérer des habilitations spécifiques à chaque entité. L'affectation automatique des utilisateurs et des matériels est possible grâce au paramétrage de règles.

On considère la hiérarchie suivante :



L'entité mère (`EM`, ou nativement appelée `Entité Racine` dans GLPI) possède deux filiales (`EA` et `EB`) qui possèdent à leur tour deux départements chacune (`EA1`, `EA2`, `EB1` et `EB2`). Chaque entité possède une vision de son parc et des entités qui lui sont affiliées.

- `EM` a une vision de son parc et de toutes les entités.
- `EA` a une vision de son parc et de `EA1` et `EA2`.
- `EA1` ne voit que son parc.

Un utilisateur peut être rattaché à plusieurs entités avec des droits différents. Ces droits peuvent être conservés sur les entités filles ou non. Pour reprendre l'exemple précédent, un utilisateur ne pourra ne déclarer un ticket qu'au sein de son service, se rapportant uniquement au matériel qui lui est rattaché ou à un matériel de son service (une imprimante, un écran...).

Inversement, un utilisateur disposant d'habilitations plus étendues pourra consulter l'ensemble des matériels, tickets ou autres objets. Et ce, sur toutes les entités sur lesquels ses droits sont applicables.

Par défaut, GLPI s'installe avec une entité générique, appelée `Entité Racine`. Il est donc mono-entité. Cette entité peut être renommée simplement en modifiant celle-ci.

Il est possible de définir des profils de transferts pour les mutations d'éléments entre entités.

Cette fonctionnalité permet notamment de passer d'un GLPI mono entité à un GLPI multi-entités en utilisant les transferts. L'idée de la multi-entité est d'ajouter une couche supplémentaire pour créer des ensembles avec des droits qui leur sont propres. Ces ensembles s'appellent des entités. Ces droits peuvent aussi être conservés sur les entités filles.

Groupes

Les regroupements peuvent être faits selon :

- les utilisateurs, pour gérer des groupes de compétences pour Helpdesk par exemple
- les services : pour rassembler du matériel, des tickets et des utilisateurs

La notion de groupe permet de rassembler des utilisateurs dans des groupes afin d'attribuer des matériels à ces groupes et permettre un suivi de ces matériels communs.

Si vous utilisez l'authentification externe, vous pouvez importer directement vos utilisateurs dans des groupes créés préalablement dans GLPI.

De la même manière qu'il est préférable de définir les entités hérarchie avant de commencer la configuration de GLPI, il est important d'étudier les profils par défaut de l'application, car ceux-ci répondent à des besoins génériques. Les règles d'affectation des droits et les profils permettent de déléguer la gestion quotidienne des habilitations au répertoire LDAP. En général on associe un profil GLPI à l'appartenance LDAP. Une règle d'attribution permet d’attribuer une entité et/ou

un profil à une personne. GLPI permet de faire correspondre les groupes GLPI créés dans la base avec ceux qui proviennent de l'annuaire LDAP.

La localisation permet de définir géographiquement les équipements et les utilisateurs. Elle peut être définie par une structure arborescente. Exemple: 20 rue de Paris> Bâtiment à 1 étage> Salle 225.

La récursivité consiste à rendre visible dans les sous-entités un objet. Cela permet de traiter les problèmes d'objets totaux / locaux. Par exemple, un fournisseur présent dans toutes les entités sera déclaré dans l'entité mère.

Collecteur

Le collecteur permet d'utiliser la messagerie électronique pour créer des tickets et ajouter des suivis aux tickets déjà existants. Un collecteur permet d'importer un courriel depuis une boîte, et de le transformer en ticket dans GLPI. Un mécanisme de routage permet d'affecter celui-ci à une entité de destination. Un collecteur est associé à une adresse de messagerie. Les tickets créés peuvent avoir comme date de création celle du courriel initial ou celle de l'import dans GLPI (en fonction de l'option définie dans le collecteur).

Gestion de l'inventaire

Un moteur de règles spécifique permet de contrôler le processus d'import et de liaison des machines depuis un outil d'inventaire. Ce moteur a pour vocation de définir des règles qui permettent d'importer, de lier ou de refuser des ordinateurs. Un certain nombre de critères sont disponibles : des champs génériques (nom, description, numéro de série, domaine, adresse IP, sous-réseau) mais aussi des champs venant de l'outil d'inventaire si celui-ci les propose, l'entité de destination de la machine ainsi qu'un statut servant à rechercher une machine déjà présente dans GLPI.

Base de connaissance

La base de connaissances répond à deux objectifs principaux : Le premier est de centraliser des connaissances internes aux différents techniciens. Le second est de mettre à disposition des utilisateurs des informations (FAQ publique) leur permettant de résoudre seuls des problèmes simples. Vous pouvez créer des catégories et sous-catégories afin d'indexer vos connaissances.

Création de règles d'affectation des machines aux entités

Il faut définir les règles métier permettant d'affecter les machines dans les différentes entités. L'utilisation du plugin mass_ocs_import permet de contribuer à la vérification et à l'affinement des règles. En effet, il possède un onglet qui liste les machines non importées, avec l'affichage des données provenant d'OCS. Ainsi, on peut détecter quels critères ne vérifient pas la règle métier.

Dans le cas d'un environnement avec beaucoup d'entités, il pourrait être intéressant d'utiliser la procédure suivante:

- déployer l'agent OCS sur une seule machine de l'entité
- vérifier que le processus de synchronisation fonctionne et que la machine est intégrée dans GLPI
- comparer les données remontées dans GLPI à celles inventoriées par OCS

Si les données sont correctes, lancer le déploiement des agents OCS sur les autres machines.

Dans le cas des affectations de machines à des entités, le moteur de règles s'arrête à la première règle trouvée. Il est donc conseillé de placer en tête de liste les règles qui seront appliquées le plus souvent (c'est-à-dire les règles d'affectation aux plus grandes entités).

Migration vers GLPI depuis un autre système de gestion du parc

L'installation d'OCS et GLPI peut intervenir dans les cas suivants:

- installation d'un système de gestion de parc dans un environnement vierge

- migration d'un système de gestion de parc existant (libre ou propriétaire).

Il est possible de récupérer des données du système existant, afin de ne plus les saisir manuellement dans GLPI. Ce processus utilise l'injection plugin de fichiers CS (data_injection). Il faut un fichier CSV par type de données à importer dans GLPI. Par exemple un fichier pour les machines et un autre pour les équipements réseau. Il est conseillé de mettre en place une plate-forme de qualification avec une copie de la base de production et le plugin data_injection afin tester les données à injecter. Afin d'éviter de polluer la base de production en cas d'erreur.

Exemple: Vous récupérez d'un outil précédent l'information financière des machines existantes (date d'achat, période de garantie, etc) ainsi que les connexions à un réseau (nom du réseau + port). Vous exportez avec cet outil les équipements réseau (hubs, commutateurs) et les numéros de port qui n'ont pas été pris en compte par OCS. Procédure:

1. Injectez vos équipements réseau en indiquant les numéros de ports de chaque équipement
2. GLPI créera les équipements et les ports associés (si vous injectez un switch 16 ports, alors 16 ports seront créés automatiquement dans GLPI)
3. Injectez chaque ordinateur en indiquant le réseau et le port auquel il est connecté
4. GLPI va créer l'ordinateur et le raccorder au port.

Configurer les SLAs

Un SLA (Service Level Agreement ou accord de niveau de service) est la formalisation d'un contrat négocié entre le ServiceDesk et le client définissant le niveau de service attendu et donc au délai maximum pour résoudre un incident ou une demande (J+1, H+4...). Des niveaux d'escalades peuvent être définis au sein d'un SLA. Chaque niveau déclenche des actions automatiques permettant la résolution du ticket dans les meilleurs délais. Un niveau se déclenche avant ou après la date d'échéance du SLA en fonction du délai défini. Par exemple, un jour avant l'échéance, le ticket est affecté au support de niveau 2 et sa priorité passée à Haute. Les SLAs sont associés aux tickets via le moteur de règles des tickets. L'association du SLA au ticket permet le calcul automatique de sa date d'échéance. Plusieurs SLAs peuvent ainsi être définis et affectés suivant des critères précis. Par exemple, le SLA 1 sera affecté si le ticket est associé à une catégorie spécifique et le SLA 2 pour les autres catégories.

Statistiques

Il est possible de visualiser des statistiques selon une période paramétrable :

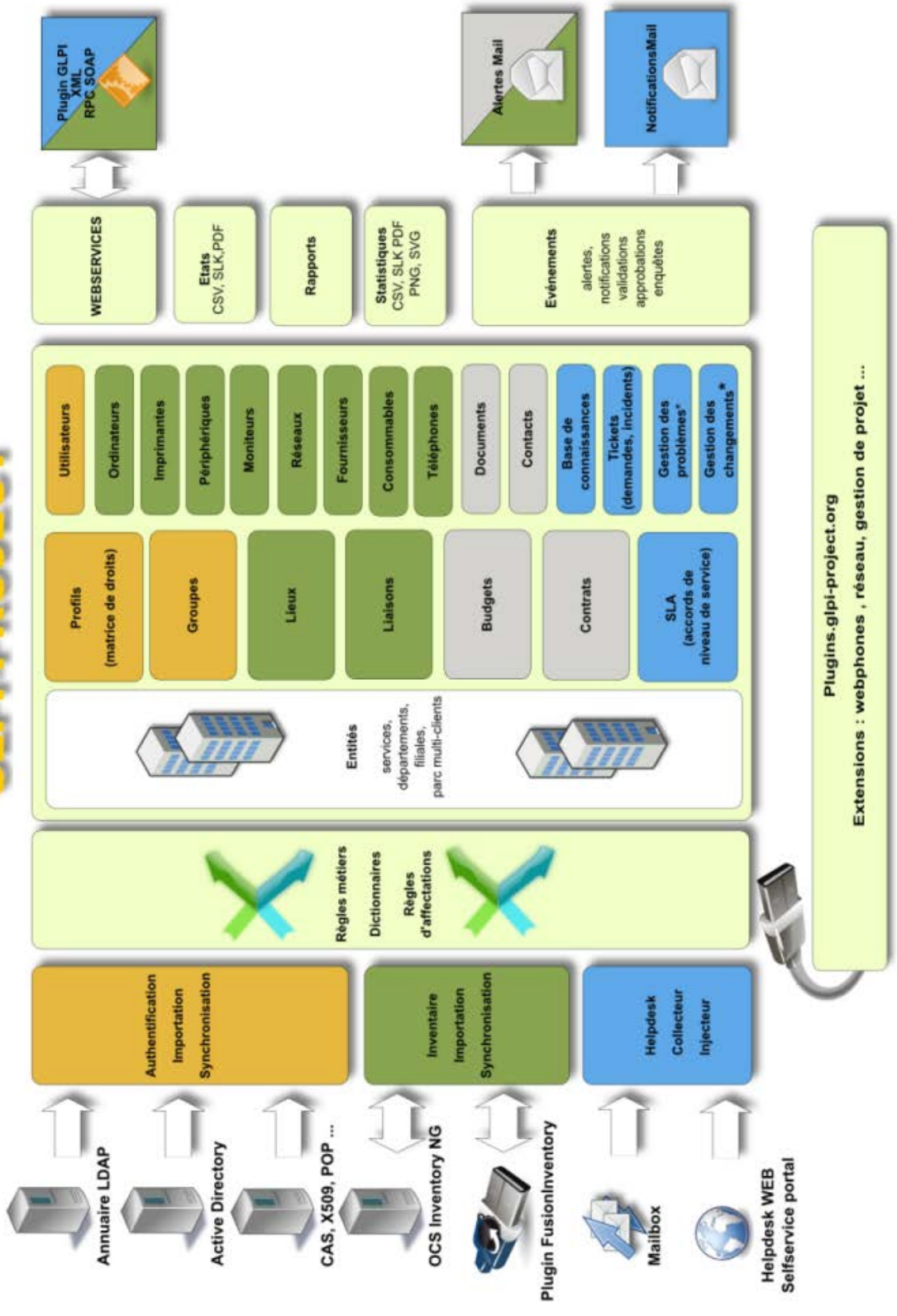
- **Globales :**
  Affiche des statistiques générales sur les tickets : Nombre de tickets ouverts, résolus, clos et résolus en retard ; Nombre d'enquêtes de satisfaction ouvertes ou avec une réponse ainsi que le degré de satisfaction moyen ; Les délais moyens de prise en compte, résolution et clôture du ticket ; La durée réelle moyenne de traitement du ticket.

- **Par ticket :**
  Affiche des statistiques sur les éléments des tickets, sélectionnés via un menu déroulant. Par exemple : demandeur, technicien assigné, impact, etc. Le tableau obtenu présente les éléments suivants : Nombre de tickets ouverts, résolus, clos et résolus en retard ; Nombre d'enquêtes de satisfaction ouvertes, nombre de réponses aux enquêtes et degré de satisfaction moyen ; Durée entre l'ouverture du ticket et la première action sur celui-ci (suivi, tâche ou solution); Délai moyen de résolution et de clôture du ticket; Durée réelle moyenne et totale de traitement du ticket; Durée réelle des interventions programmées par les personnes qui prennent en charge les tickets (intervention programmée signifie le temps alloué par un technicien sur les tâches liées aux tickets).

- **Par intitulé :**
  Affiche des statistiques sur les éléments des ordinateurs. Par exemple : Modèle, Système d'exploitation, modèle de carte-mère, etc. Les éléments statistiques obtenus sont les mêmes que pour les statistiques sur les tickets.

- **Par matériel :**
  Affiche le nombre de tickets affectés à chaque matériel, trié par nombre de tickets.

Source : https://blogauvraymarvin.wordpress.com/2016/01/14/mise-en-place-de-glpiocs-et-customisation-du-css/



Sources : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
https://www.advens.fr/ressources/blog/nouveau-top-ten-owasp-2017-notre-analyse

OWASP Top 10 2017

Pour rappel, le TOP 10 de l'OWASP (Open Web Application Security Project) est un projet visant à maintenir à jour la liste des 10 principales vulnérabilités des applications Web. Ce classement 2017 succède à celui de 2013 mais contrairement aux années précédentes, il n'est plus uniquement basé sur la « vision » de l'OWASP sur le sujet. Le processus méthodologique a été entièrement revu. Il repose ainsi sur les remontées de 500 utilisateurs et de 40 sociétés spécialisées dans le domaine de la sécurité des applications.

Le Top 10 de l'OWASP a pour but d'informer sur l'existence de ces vulnérabilités et de fournir des guides simplifiés sur les bonnes pratiques pour s'en prémunir. Ces guides sont disponibles sur le site de l'OWASP et s'adressent notamment aux développeurs, architectes, chef de projets, managers. Le tableau suivant permet d'apprécier les évolutions entre les deux derniers classements :

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Sans surprise, le risque numéro 1 demeure l'attaque par Injection, notamment celle qui permet l'exécution de code à distance : Injection SQL, NoSQL, LDAP, … jusqu'aux injections de code au niveau système qui sont les plus dévastatrices.

En deuxième position, les risques liés à une gestion incorrecte de l'authentification ou du suivi des sessions. On parle ici de compromission de mot de passe, de clé ou de jeton d'authentification ou de session.

En milieu de tableau, demeurent les problèmes liés à la défaillance des systèmes de contrôles d'accès aux ressources. On notera que les références directes non sécurisées ont été fusionnées avec le manque de contrôle d'accès fonctionnel, ce qui de prime abord apparaît logique. Toutefois, les références directes restent un vrai problème qui n'est pas formellement connexe avec le contrôle d'accès. Nombre d'avis ont recommandé de maintenir la séparation de ces deux vulnérabilités.

Enfin, les problèmes de mise à jour des composants et les mauvaises configurations restent elles-aussi aux mêmes places que précédemment. L'usage des scanners de vulnérabilités n'est manifestement toujours pas industrialisé dans les organisations vulnérables.

Les évolutions

L'exposition de données sensibles passe de la 6ème à la 3ème place sans qu'il soit possible si cette évolution reflète l'actualité en matière de fuites de données ou traduit l'influence de la mise en application attendue du RGPD.

La vulnérabilité par attaques CSRF disparaît : seules 5% des applications y resteraient vulnérables. N'importe quel Framework de développement intègre effectivement par défaut une protection contre ce type de risque qui demeure efficace si l'application ne souffre pas de Cross Site Scripting. Cette vulnérabilité XSS dégringole de manière cependant surprenante de la 3ème place à la 7ème place. Le contournement de système d'authentification, l'injection de code côté client, le contournement de protection CSRF, le phishing, sont toujours autant de vecteurs d'attaques facilités par le Cross Site Scripting. L'OWASP semble vouloir réduire le XSS à la défiguration de site, les redirections et l'usurpation de session.

La vulnérabilité 2013 « A10 – Redirection et transferts non validés » disparaît elle-aussi, bien que toujours présente dans 8% des applications, car elle ne traduit pas un risque aussi important que ceux ajoutés dans le Top 10 2017 :

- A4 : 2017 - XML External Entities (XXE) dont l'apparition surprend car nombre d'observateurs auraient tendance à classer ces vulnérabilités dans les attaques par injection (injection XML dans le cas présent). Ce classement en quatrième place peut être motivé par son impact important en cas d'exploitation réussie de cette vulnérabilité.
- A8 : 2017 – Insecure deserialization. La sérialisation permet de faire passer des objets ou des structures de données plus ou moins complexes entre deux programmes en les transformant dans un format « sérialisé », compréhensible par les deux parties. Les problèmes surviennent au moment de reconstituer, c'est à dire « dé-sérialiser », l'objet d'origine : un attaquant envoyant des données malicieuses spécifiquement sérialisées pourra tenter d'exploiter des vulnérabilités sur le système en charge de la dé-sérialisation. Ce type d'attaque est souvent basé sur des conversions de type et peut notamment conduire à des élévations de privilèges, ou encore des attaques par injection.
- A10 : 2017 – Insufficient Logging & Monitoring. Surprenant que cette vulnérabilité n'ait pas intégré plus tôt le Top 10 OWASP compte tenu du nombre croissant d'applications qui négligent la traçabilité. Connexion, déconnexion, accès aux modules / fonctions sensibles, sont pourtant des évènements qu'il est indispensable de journaliser. La surveillance en général et celle des logs applicatifs en particulier est essentielle pour détecter tout dysfonctionnement de la sécurité. Qu'on utilise un produit de type SIEM ou, mieux, un service de type SOC pour surveiller ses applications est juste indispensable aujourd'hui. Dans son rapport, l'OWASP **rappelle qu'en moyenne 200 jours s'écoulent entre une intrusion et sa détection** – et que bien souvent la détection n'est pas faite par l'entreprise vulnérable, mais par l'un de ses partenaires ou clients. Rappelons enfin que le risque zéro n'existe pas et que tôt ou tard une vulnérabilité affectera vos systèmes. Ce qui compte ce n'est pas d'être invulnérable, mais de réduire au maximum le temps entre la détection de la vulnérabilité et sa suppression. Les logs sont souvent indispensables pour réduire cette période au maximum.

Rappelons que le risque zéro n'existe pas et que tôt ou tard une vulnérabilité va affecter tout système d'information. L'objectif n'est donc pas de concevoir un système invulnérable, mais plutôt de réduire au maximum le temps entre la détection de la vulnérabilité et sa suppression par conception ou procédure. Les logs et leur exploitation en temps réel sont indispensables pour réduire cette période au maximum.

Sources : http://ssi.minint.fr/index.php/maitrise-d-ouvrage/dissip
Archives "DISSIP" de la DSIC/VFSSI

La démarche d'intégration de la SSI dans les projets – DISSIP

I. Introduction

Conçu comme une mise en application du modèle DICATA (Disponibilité, Intégrité, Confidentialité, Accessibilité, Traçabilité et Authenticité), ce dernier se voulant une alternative plus complète aux habituels modèles DIC et DICT, le DISSIP procède d'une transposition "adaptée" du Guide ANSSI d'Intégration de la SSI dans les Projets (GISSIP). Il a été décidé de l'utiliser comme base de travail lorsque la Voie Fonctionnelle de la SSI (VFSSI) de la Direction des Systèmes d'Information et de Communication (DSIC) a été chargée de proposer une évolution du processus projet de la DSIC par intégration maitrisée et raisonnée de la SSI.

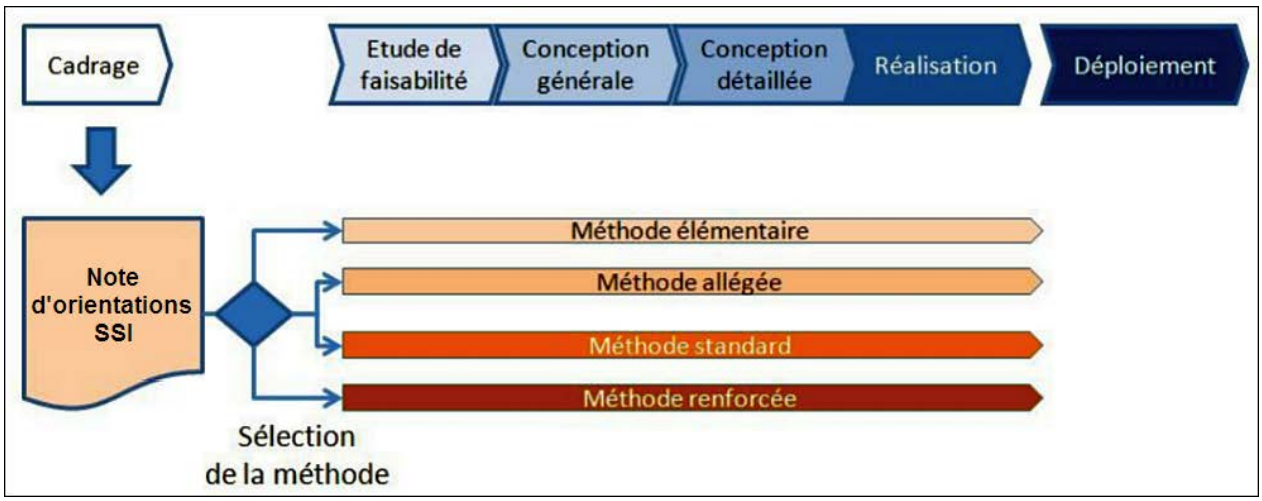
Si les systèmes d'information en mode projet constituaient la cible première du DISSIP, ce dernier a rapidement pu être exploité pour proposer une sécurisation des systèmes d'information en mode production. Au final, le DISSIP est devenu démarche ministérielle recommandée par le SHFD pour toute procédure de mise en conformité RGS ou d'homologation de sécurité d'un système d'information. Après deux premières versions adaptées au contexte du ministère de l'Intérieur par la DSIC, un groupe de travail ministériel (DSIC, ST(SI)², DGPN, DCSCGC, PP et SHFD) a poursuivi cet effort d'adaptation, de clarté et de facilité d'utilisation pour produire la troisième version du document qui a été adoptée en comité de pilotage ministériel SSI du 14 novembre 2016.

II. Principes

L'objectif de la démarche est de s'insérer dans le processus projet classique et, dès la phase de cadrage, d'évaluer les enjeux du système d'information cible. Selon ces estimations, le DISSIP oriente vers une méthode adaptée permettant de d'atteindre les objectifs "métier" fixés par la MOA. La détermination de cette démarche repose sur la rédaction de la note d'orientations SSI qui demeure le premier livrable du DISSIP depuis sa toute première version. Quatre niveaux de pertinence ont été identifiés pour le DISSIPv3 :

- Elémentaire,
- Allégé,
- Standard,
- Renforcé.

A chaque niveau correspond une méthode à laquelle sont associés divers livrables dont le nombre et la teneur augmentent à mesure que l'on passe du niveau élémentaire au niveau renforcé.



Chacune des méthodes (élémentaire, allégée, standard, renforcée) permet d'obtenir le niveau d'assurance requis au niveau visé, en introduisant les livrables à différents jalons du processus projet. Le regroupement final de ces livrables constitue le dossier de sécurité du système cible, c'est-à-dire l'ensemble des pièces à étudier pour juger du niveau de maîtrise des risques du système. En cas d'homologation de sécurité, ce dossier devient le dossier d'homologation qui doit être présenté en commission.

III. Le dossier d'homologation

Le document SHFD de présentation du DISSIPv3 précise que "*l'homologation est l'attestation formelle que les besoins de sécurité ont été identifiés et traités de manière à ce que les risques résiduels soient maîtrisés et acceptables*". Cette décision atteste ainsi que le système d'information cible atteint ses objectifs et qu'il est par conséquent apte à être mis en production. En référence à l'objectif 5 de la PSSI-MI, ce document rappelle que "*l'homologation est obligatoire pour tous les systèmes d'information et elle conditionne leur mise en production*".

Le rapporteur de la démarche d'homologation doit présenter le dossier de sécurité sur la base duquel la décision d'homologation pourra s'appuyer et, le cas échéant, l'avis de la commission d'homologation sera formalisé. La composition minimale de ce dossier est fixée par la Note d'orientations SSI en fonction du niveau de démarche identifié :

<table>
<tr><th>Phase</th><th colspan="4">Démarche SSI</th></tr>
<tr><td rowspan="2">Phase 1
"Cadrage"</td><td colspan="4">Note d'orientations SSI déterminant la démarche de SSI</td></tr>
<tr><td>Élémentaire</td><td>Allégée</td><td>Standard</td><td>Renforcée</td></tr>
<tr><td>Phase 2
"Etude de faisabilité"</td><td></td><td colspan="3">Note de stratégie de sécurité</td></tr>
<tr><td>Phase 3
"Conception générale"</td><td>Liste des bonnes pratiques SSI applicables dans le cadre du projet</td><td colspan="2">Première version du dossier d'exigences de sécurité (DES)</td><td>Première version de FEROS</td></tr>
<tr><td rowspan="3">Phase 4
"Conception détaillée"</td><td rowspan="3">Liste des bonnes pratiques SSI pertinentes</td><td colspan="2" rowspan="2">Version finale du DES</td><td rowspan="2">Version finale de FEROS
Première version de TdBSSI</td></tr>
<tr></tr>
<tr><td colspan="2">Première version de la revue de couverture des objectifs de sécurité</td></tr>
<tr><td rowspan="5">Phase 5
"Réalisation"</td><td colspan="4">Revue de conformité à la PSSI MI</td></tr>
<tr><td rowspan="4">Revue de conformité des bonnes pratiques pertinentes</td><td colspan="3">Revue de couverture des objectifs de sécurité</td></tr>
<tr><td rowspan="3"></td><td colspan="2">Document d'application de PSSI du SI incluant les PES
Cahier de recette et d'évaluation incluant l'éventuel rapport d'audit</td></tr>
<tr><td></td><td>Version finale de TdBSSI
Audit SSI</td></tr>
<tr><td></td><td colspan="2">PSSI du système cible</td></tr>
<tr><td rowspan="2">Décision de mise en production</td><td></td><td colspan="3">Support de présentation à la commission</td></tr>
<tr><td colspan="4">Dossier de sécurité incluant tous les livrables
Décision d'homologation formalisée</td></tr>
<tr><td>Phase 6
"Déploiement"</td><td colspan="4"></td></tr>
</table>

IV. Les principaux livrables

IV.1. Les bonnes pratiques SSI

Le référentiel des bonnes pratiques SSI liste l'ensemble des bonnes pratiques génériques qui devraient être mises en œuvre. Certaines peuvent traiter de thèmes hors du spectre du système d'information cible. Il convient donc d'identifier celles qui sont pertinentes dans le cadre envisagé puis de s'assurer de leur bonne mise en œuvre.

IV.2. Note de stratégie de sécurité

La note de stratégie de sécurité est un livrable intermédiaire de la phase d'étude de faisabilité qui n'a plus d'utilité en fin de projet. Il est la suite de la note d'orientations SSI, qu'il affine, et la préparation des analyses de risques (DES ou FEROS) dont il viendra alimenter la partie "étude du contexte". Ce livrable permet de valider que l'orientation déterminée en phase de cadrage est la bonne.

IV.3. Stratégie d'homologation

La stratégie d'homologation est le document qui présente le périmètre du système d'information qui sera homologué et désigne formellement son autorité d'homologation. Il précise la composition de la commission d'homologation et la constitution du dossier d'homologation.

IV.4. FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité)

La FEROS permet d'identifier les objectifs de sécurité à atteindre pour maîtriser les risques. L'expertise et le temps nécessaire pour conduire l'analyse de risques impliquent souvent le recours à une prestation qui va s'appuyer sur la démarche préconisée par l'ANSSI reposant sur la méthode EBIOS (Étude des besoins et identification des objectifs de sécurité).

IV.5. Dossier d'exigences de sécurité (DES)

Le DES est une version simplifiée de la FEROS. Il s'appuie sur la même méthodologie que EBIOS mais comporte moins de détail et se concentre sur l'essentiel. Il aboutit également à l'identification des objectifs de sécurité.

IV.6. Revue de couverture des objectifs de sécurité

Les analyses de risques, intégrées aux démarches de rédaction du DES ou de la FEROS, identifient des objectifs de sécurité permettant d'atteindre un niveau de risque maîtrisé. Ce document fait l'inventaire des mesures de sécurité prévues et les associent aux objectifs qu'elles contribuent à atteindre. L'effectivité de la mise en œuvre de ces mesures est également précisée de manière à pouvoir évaluer les risques résiduels. C'est un des livrables clef permettant de prendre une décision d'homologation.

IV.7. PSSI du système

En niveau « Standard » et « Renforcé », une PSSI du système d'information doit intégrer le dossier de sécurité. Elle doit être conforme à la PSSI du ministère de l'Intérieur et vient préciser certaines règles dans le contexte du système d'information cible. La PSSI du système est la liste des objectifs de sécurité structurés par thème. Il demeure possible de ne pas produire cette PSSI spécifique et de décider de s'appuyer sur la PSSI de l'Autorité d'emploi qui est nécessairement une déclinaison de la PSSI du MI qui est déjà une déclinaison de la PSSI de l'Etat. Quel que puisse être le choix pour la PSSI, les Procédures d'Exploitation de la Sécurité (PES) doivent être rédigées, validées et intégrées au dossier de sécurité.

IV.8. Procédures d'exploitation et de sécurité (PES)

Les PES sont des documents d'application des PSSI auxquelles est soumis le système d'information cible. Elles détaillent les mesures et procédures adaptées à ce système en précisant les modalités de mise en œuvre des PSSI.

IV.9. Tableau de bord SSI (TdBSSI)

Le tableau de bord SSI est formalisé avant la mise en production. Il détermine les indicateurs qui seront présentés périodiquement afin d'apporter l'assurance du maintien du niveau de sécurité pendant tout le cycle de vie du SI.

didsic' Info

Lettre d'information n°3 | Avril 2013

Document 6

Numéro Spécial

Nouvelle interface assistance utilisateurs

La Direction Interministérielle Départementale des Systèmes d'Information et de Communication (DIDSIC) des Bouches du Rhône est, entre autre, chargée d'assurer le maintien des Systèmes d'information et de communication des différentes Directions Départementales Interministérielles (DDI), de la Préfecture du département et de ses Sous-Préfectures. Pour cela, la DIDSIC se dotera de nouveaux outils de gestion afin de maintenir un haut niveau de qualité de service, et d'assurer l'égalité de traitement entre tous les agents, quel que soit leur lieu d'exercice.

Dans cette perspective, l'année 2013 sera une année charnière avec la mise en mise en œuvre de l'application GLPI (Gestion Libre de Parc Informatique) qui est une application web permettant la gestion d'un parc d'équipements, des tickets d'incident et des demandes ainsi qu'une base de connaissance et un suivi statistique de l'activité.
Sa mise en œuvre opérationnelle est prévue le 02 mai 2013.
La gestion des tickets s'organisera autour d'un centre de service (CS13) qui sera le point de contact unique entre les utilisateurs et la DIDSIC (prestataire de service).

1 Comment accéder à l'application ?

Vous êtes sur un site de la préfecture,
saisir l'adresse http://glpi-national.dsic.mi dans votre navigateur Internet ou cliquer sur signalement incidents SIC du portail intranet de la préfecture.

vous êtes sur le site d'une DDI, accéder à l'outil au travers du portail intranet de la préfecture ou
en DDCS et DDPP saisir l'adresse http://glpi-national.intermin.ader.gouv.fr dans votre navigateur Internet,

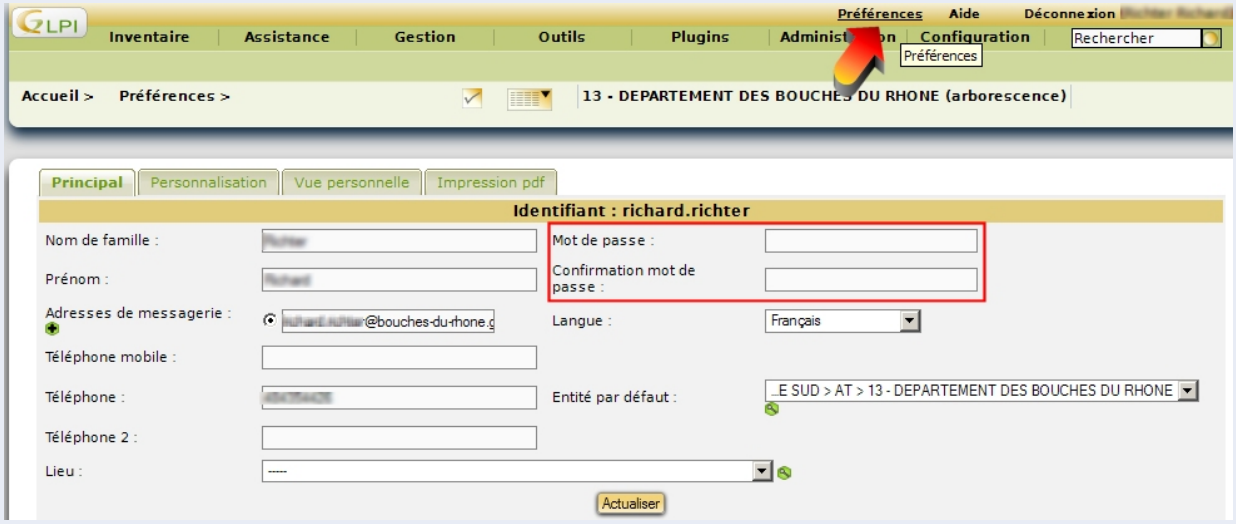
en DDTM
saisir l'adresse http://glpi-national.intermin.ader.gouv.fr dans votre navigateur Internet ou cliquer sur signalement incidents SIC du portail intranet de la DDTM13

Saisir son identifiant (prenom.nom) et le mot de passe (Provence13) en respectant la casse. Ce mot de passe devra être modifié à la première connexion

Pour changer son mot de passe : cliquer sur **Préférences**, saisir son mot de passe, la confirmation du mot de passe et cliquer sur **actualiser**. Le mot de passe est changé

Bureau : BEQS - E-mail : pref-didsic-beqs@bouches-du-rhone.gouv.fr

Mise en œuvre opérationnelle prévue le 02 mai 2013.



2 Quels avantages au niveau utilisateurs ?

- La possibilité de déclarer directement un incident via une interface simplifiée.
- Dès la création du ticket d'incident, l'obtention d'un N° de dossier.
- À partir du tableau de bord utilisateur, un suivi de l'évolution du dossier.
- Après le passage du technicien, l'obtention d'un message de résolution d'incident.
- La possibilité d'effectuer une réclamation dans les 48H00 après avoir reçu le mail de résolution d'incident.

3 Quels avantages au niveau des directions ?

- Avoir une meilleure vision du parc de leurs équipements et des incidents survenus sur ce dernier.
- Obtenir des indicateurs sur le parc des équipements, des incidents.
- Vérifier la qualité de service rendu.
- Aide à la planification de la programmation annuelle.

4 Quels avantages au niveau DIDSIC ?

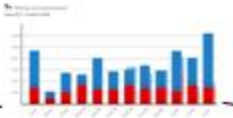
- Avoir un outil unique au niveau de la DIDSIC pour la gestion des équipements et les actions de support.
- Avoir une vision départementale du parc à maintenir.
- Avoir un meilleur suivi et pilotage de la résolution des incidents et des demandes.
- Avoir la possibilité de gérer les contrats et les fournisseurs.
- Avoir une meilleure vision des types d'incidents et des solutions.
- Aide à la formalisation des demandes relatives à la programmation annuelle.
- Production d'indicateurs à la demande de la préfecture, des DDI et mesure de la qualité du service rendu.

Centre de Services, se poser les bonnes questions

Document 7

Profils techniques

Horaires



Indicateurs de Qualité de service statistiques

Compétences

Centre de services

Missions

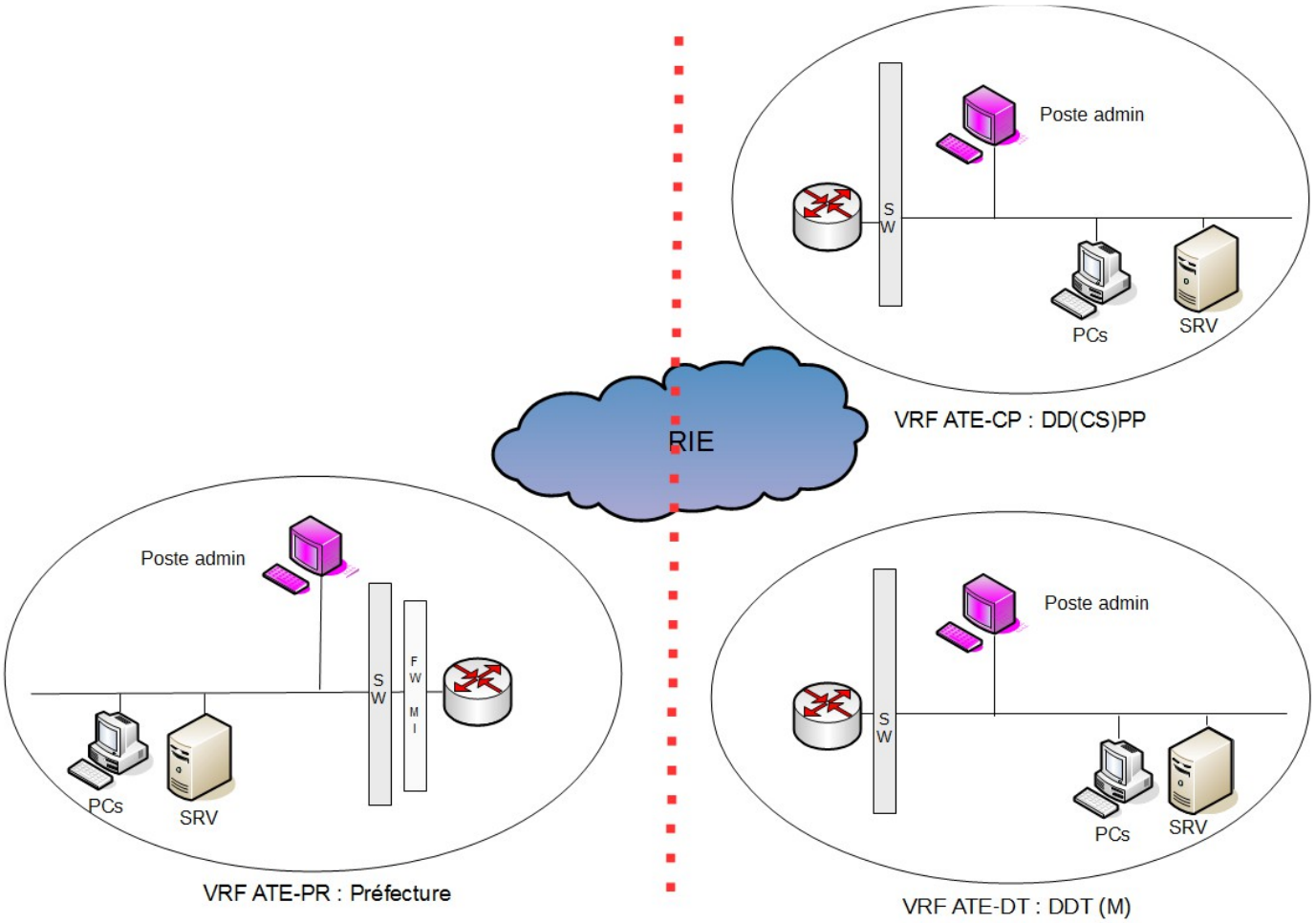
VIP

Outillage

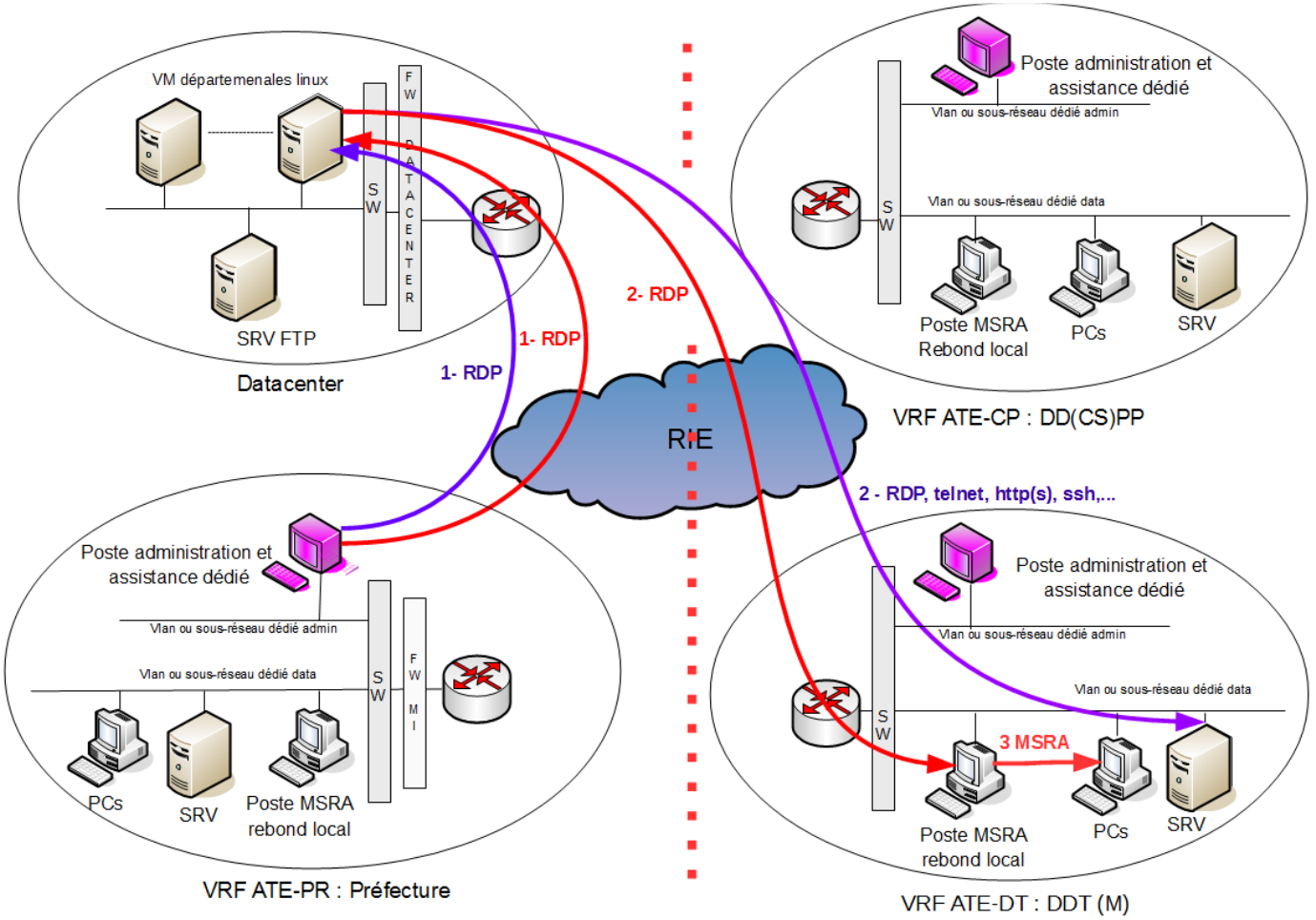
Parcours utilisateur

Dimensionnement

L'architecture existante



L’architecture cible



L’offre de service MI

Une VM linux par département en hébergement centralisé

- Les postes d’administration connectés un subnet dédié
- Séparer les fonctions
  - d’administration
  - d’assistance à distance
- Un espace sftp par département
- MSRA, seul outil d’assistance reconnu
  - Natif et gratuit sur les postes windows
  - Maîtrise de la connexion par le télé-assisté
  - Deux modes de fonctionnement
    - À l’initiative du technicien
    - À l’initiative du télé-assisté

La fiche pré-requis

- Mettre en place des sous-réseaux d'administration sur chaque site pour le contrôle d'accès (/28 ou /29 ou IP fixe possible)
- Dédier le poste d'administration à ces deux seules fonctionnalités (recommandations ANSSI) :
  - Prise de main à distance
  - Administration à distance
- Installer un serveur physique ou virtuel (ou un poste simple) MSRA dédié dans chaque entité, raccordée à AD, et indiquer leur adresse IP fixe pour chaque entité
- Définir la liste des techniciens (administrateurs ou assistants) et leurs droits pour chaque domaine (MI-DDT-DDCSPP)
- Confirmer les réseaux des entités (pour ouverture des flux)