



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

- SESSION 2022 -

Mardi 10 mai 2022

Concours 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 ou de la candidate 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 ou de la candidate ainsi que son aptitude à dégager des solutions appropriées.

(Durée: 4 heures – Coefficient 1)

Le dossier technique comporte 36 pages (hors la page d'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 entraînera 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 BLANC OU D'EFFACEUR SUR LES COPIES.**
- 3. ÉCRIRE EN NOIR OU EN BLEU – PAS D'AUTRE COULEUR.**
- 4. IL EST RAPPELÉ AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAÎTRE SUR LA COPIE.**

SUJET

En qualité d'ingénieur des systèmes d'information et de communication, vous travaillez au sein de l'un des cinq ministères du périmètre ATE (Administration Territoriale de l'Etat).

Votre ministère a été chargé par la DINUM (Direction Interministérielle du Numérique) de piloter le projet de mise en place d'une CSU (Chaîne de Soutien Utilisateur) interministérielle pour l'ensemble des applications informatiques nationales de ces 5 ministères.

Vous avez été désigné chef de projet par votre directeur pour déployer une solution normée ITIL de gestion de tickets (traitements de demandes, incidents,...) sur l'ensemble de ces applications.

Dans le cadre de votre mission de pilotage et de coordination de ce projet, votre directeur des systèmes d'information vous demande de lui fournir une note qui devra présenter :

- Les enjeux de l'implémentation ITIL en terme d'assistance aux utilisateurs ;
- La gouvernance que vous mettrez en place ainsi que la méthode de conduite que vous utiliserez.

Vous décrierez notamment :

- comment vous organisez votre projet ;
 - la constitution de votre équipe ;
 - le planning général associé qui illustre explicitement les principales phases.
- Une description, dans ses grandes lignes, de la solution technique qui sera mise en œuvre en précisant :
- le logiciel retenu en justifiant votre choix ;
 - l'architecture déployée en explicitant en particulier la solution d'hébergement choisie ;
 - les actions relatives aux domaines SSI et RGPD que vous mettrez en œuvre tout au long de votre démarche projet.

Dossier technique :

| | | |
|-------------|---|----------------|
| Document 1 | « Création des secrétariats généraux communs départementaux au 1 ^{er} janvier 2021 » Source : Communiqué de presse du SGCD - Préfecture du Loir-et-Cher | Page 1 |
| Document 2 | « Gestion des services IT » Source : easyvista.com - bestpractices-si.fr | Pages 2 à 9 |
| Document 3 | « Memento, la gestion de projet » Source : Document interne Ministère de l'intérieur | Pages 10 et 11 |
| Document 4 | « Exploiter l'informatique à l'heure d'Itil » Source : O1net.Entreprises | Pages 12 et 13 |
| Document 5 | « Les 5 meilleurs logiciels helpdesk 2020 » Source : L'Express | Page 14 |
| Document 6 | « Tests et guides d'achats spécial logiciels helpdesk – comment choisir le bon produit » Source : L'Express | Pages 15 à 18 |
| Document 7 | « Le Cloud Computing » Source : Document interne Ministère de l'intérieur | Pages 19 et 20 |
| Document 8 | « Les documents de référence du S.I. de l'État » Source : DNUM | Pages 21 à 27 |
| Document 9 | « Protection des données – Adoptez les 6 bons réflexes » Source : www.cnil.fr | Page 28 |
| Document 10 | « L'offre du cloud externe dit C3 » Source : Ministère de l'Intérieur | Pages 29 à 33 |
| Document 11 | - « La démarche d'homologation de sécurité au ministère » - « La démarche d'intégration de la SSI dans les projets » Source : Ministère de l'Intérieur | Pages 34 à 36 |



COMMUNIQUÉ DE PRESSE

Blois, le 11 janvier 2021

Création des secrétariats généraux communs départementaux au 1^{er} janvier 2021

L'administration territoriale se réforme pour améliorer la qualité du service à l'utilisateur

Depuis le 1^{er} janvier, les nouveaux secrétariats généraux communs permettent dans chaque département de regrouper l'intégralité des fonctions "supports" des préfectures et des directions départementales interministérielles¹ (DDI). Ces fonctions concernent les ressources humaines, le budget, la logistique ou encore l'informatique. Précédemment, elles étaient éclatées entre chaque entité, chaque préfecture ou direction disposant de son ou de ses propres services en charge des moyens.

Alors que l'État territorial est plus fortement attendu que jamais autour des enjeux de la résilience sanitaire, économique ou encore environnementale, il est apparu nécessaire de moderniser l'exercice des fonctions supports des services déconcentrés. Prévu par l'instruction du Premier ministre du 12 juin 2019 qui a lancé la réforme de l'organisation territoriale de l'État, les secrétariats généraux communs aux préfectures et aux DDI ont vu ainsi le jour le 1^{er} janvier 2021, dans l'ensemble des départements de métropole, ainsi qu'en outre-mer (Guadeloupe, Martinique, La Réunion, Mayotte).

Armés par plus de 6 000 agents, rattachés au ministère de l'Intérieur, les secrétariats généraux communs auront vocation à assurer d'une manière plus efficace, plus lisible et plus simple la gestion RH, financière, immobilière, système d'information et logistique des préfectures, des sous-préfectures ainsi que des DDI.

En Loir-et-Cher, le SGCD regroupera 53 agents. Certains viennent du ministère de l'Intérieur, d'autres de l'agriculture, ou encore des affaires sociales. Les métiers sont très variés : informaticiens, standardistes, comptables, techniciens de maintenance, archiviste, gestionnaires des ressources humaines... tous au service de la préfecture et des sous-préfectures, de la DDT et de la DDCSPP. Les équipes seront réparties à Blois sur 2 sites : à la préfecture place de la République et au sein de la future cité administrative mail Pierre Charlot. Depuis un an les agents et leurs cadres se préparaient activement à cette réorganisation, avec l'objectif de simplifier et de gagner en qualité de service. En piste depuis le 4 janvier 2021, le nouveau service est prêt à répondre aux multiples besoins humains et fonctionnels des administrations.

Les mutualisations rendues possibles par cette nouvelle organisation, porteuse de simplification et de gains d'efficacité, permettront de conforter l'exercice des métiers des services déconcentrés de l'État. Un support plus efficace, c'est le gage d'un meilleur service rendu à l'utilisateur du service public.

¹ Au nombre de 230, les DDI sont : les directions départementales des territoires (et de la mer dans les territoires littoraux) ; les directions départementales de la cohésion sociale ; les directions départementales de la protection des populations ; dans certains départements, notamment en Loir-et-Cher, ces deux dernières constituent une direction départementale de la cohésion sociale et de la protection des populations unique.

Contacts presse

Service départemental de la communication interministérielle
02.54.81.55.80 – 02.54.81.55.82 | pref-communication@loir-et-cher.gouv.fr
www.loir-et-cher.gouv.fr | @prefet41

GESTION DES SERVICES IT



ITSM vs ITIL, quelle différence ?

La gestion des services IT (ITSM) est une approche stratégique permettant de concevoir, de distribuer, de gérer et d'améliorer la manière dont la technologie de l'information (IT) est utilisée au sein d'une entreprise. L'ITSM est conçu pour optimiser la planification des ressources (à la fois software et Hardware), de fluidifier la gestion des problèmes et de rapprocher l'ensemble des collaborateurs de l'entreprise. Attention car le sigle ITSM est souvent associé à l'acronyme ITIL, pourtant il s'agit bien de deux choses différentes.

ITIL (Information Technology Infrastructure Library) fournit des bases pratiques et flexibles pour soutenir les organisations dans leur parcours vers la transformation numérique, en les aidant à aligner leurs ressources numériques et physiques pour rivaliser dans un environnement toujours plus complexe.

L'ITSM inclut l'implémentation de services dans l'entreprise entière alors que la norme ITIL fournit des processus standard pour la prestation de services informatiques. Les administrateurs peuvent choisir de n'implémenter que certaines parties de la norme ITIL et d'utiliser également d'autres structures.

Les 8 principes de base d'ITIL v4

1. Considérer l'utilisateur comme un client

« L'utilisateur » interne ou externe des services informatisés est considéré comme un « client » avec lequel la DSI contractualise au travers de conventions de service (Service Level Agreement ou SLA).

2. Positionner la DSI comme un prestataire de services

La DSI doit s'organiser non plus uniquement autour du développement des applications mais également autour de la fourniture de services. Devenant la Direction des Services Informatisés, elle doit acquérir l'image et assumer le rôle d'un prestataire de services recourant lui-même à des prestataires externes. Le développement des applications ne constitue qu'une étape intermédiaire, certes fondamentale, pour fournir le service attendu. Il s'agit là d'un changement de paradigme supposant une transformation culturelle et organisationnelle profonde.

3. Optimiser la qualité et les coûts des services informatiques

ITIL a pour objectif final l'amélioration de la qualité. Mais également la réduction des coûts des services informatiques et par voie de conséquence du TCO (Total cost of ownership, coût total de possession).

4. Capitaliser sur les «meilleures pratiques»

Quelles que soient la taille de l'entreprise ou la technologie informatique utilisée, les problématiques des entreprises relatives aux services informatiques sont très semblables. Au lieu de réinventer la roue, il est préférable de capitaliser sur des pratiques issues de réflexions approfondies et d'utilisations opérationnelles éprouvées. ITIL représente aujourd'hui l'approche la plus complète et la plus structurée disponible pour traiter de ces problématiques.

5. Penser « organisation » et « processus »

ITIL est avant tout une démarche organisationnelle et procédurale. Elle identifie et décrit les processus clés permettant de maîtriser la qualité et le coût des services informatiques.

6. Adopter une démarche structurée

Pour développer ou améliorer les processus de gestion des services informatiques, ITIL recommande d'adopter une démarche structurée : analyse de l'existant, fixation des objectifs à atteindre, planification, développement des outils, formation, essais, revue de projet. ITIL préconise d'aborder les questions relatives aux services informatiques de production et de soutien le plus en amont possible c'est à dire dès la phase de développement des applications.

7. Rationaliser les services de front office

Les services de soutien sont directement en relation avec les utilisateurs/clients. Il s'agit d'améliorer, d'une part, la coordination et les synergies entre les équipes, et, d'autre part, de simplifier l'interface avec les clients. ITIL préconise la constitution d'un front office dénommé Service Desk pour assurer un contact central entre les utilisateurs et le back-office de la gestion des services informatiques. Ce groupe de personnes prend en charge les incidents et les demandes des utilisateurs. Il assure l'interface nécessaire pour la gestion des changements, des problèmes, des nouvelles versions, etc. ITIL accorde une importance capitale à la qualité et au dimensionnement de ce Service Desk au delà du concept usuel mais trop réducteur de groupe d'assistance (Help Desk).

8. Informatiser la gestion des services informatiques

Dans la mesure où ITIL propose une approche basée sur des processus, il est souhaitable d'informatiser ceux-ci. Il existe désormais sur le marché bon nombre de logiciels performants pour gérer les incidents, les configurations, les évolutions, etc. en conformité avec les pratiques d'ITIL.

Comment mettre en place un processus de gestion des incidents informatiques ?

De la sortie imprimante bloquée à l'application hors service, nombreux sont les incidents, plus ou moins critiques, que votre système informatique éprouve. D'où l'intérêt de mettre en place un processus de **gestion des incidents**.

Mais comment vous assurer de la performance de votre **procédure de gestion des incidents** ? Quelles étapes de résolution définir et comment déterminer les rôles de chacun dans votre processus ? Est-il possible d'apporter une solution satisfaisante à l'utilisateur, conforme à votre **SLA** (*Service Level Agreement*), et dans des délais raisonnables ?

Définition de la gestion des incidents

La norme ITIL

Les incidents rencontrés en informatique sont, la plupart du temps, gérés en accord avec la norme **ITIL**, ou *Information Technology Infrastructure Library*.

Mais de quoi s'agit-il exactement ?

Projet développé dans les années 1980 par l'Office public britannique du commerce, ITIL est un ensemble de documents énumérant les bonnes pratiques à appliquer dans la gestion des services informatiques de manière étendue. L'objectif est d'apporter un support méthodologique aux professionnels, avec une intention d'amélioration continue.

Le **processus ITIL** aborde plusieurs thématiques (organisation du **système d'information**, gestion des configurations, gestion des changements, etc.), dont celle de la gestion des incidents, définie de la sorte :

Un incident se définit par tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.

Cette définition englobe différents types d'incidents.

Catégorisation des incidents

Nous pouvons classer les incidents en trois types :

- Les **incidents logiciel ou application**. Exemples :
 - erreur programme freinant l'utilisateur,
 - ralentissement de l'application, etc.
- Les **incidents concernant le matériel**. Exemples :
 - sortie imprimante bloquée,
 - disque dur bientôt saturé, etc.
- Les **demandes de service**. Exemples :
 - oubli de mot de passe,
 - demande de documentation particulière, etc.

Notez que la demande de service est un cas à part. Elle ne constitue pas un incident à proprement parler. Mais son traitement s'intègre au processus, d'où l'assimilation.

La priorisation des incidents

D'autre part, si nous rencontrons différents types d'incidents, il existe également plusieurs degrés de priorité, en fonction de la gravité de l'incident et de l'urgence à le traiter.

Comment savoir si l'incident rencontré est critique ou mineur ?

C'est à l'entreprise, par exemple à la **DSI** (direction du système d'information), de déterminer sa propre priorisation, en tenant compte de divers paramètres comme :

- la perte financière pour l'entreprise générée par l'incident,
- l'impact de l'incident sur des utilisateurs VIP,
- le non-respect des réglementations et des lois auquel l'incident peut conduire, etc.

En d'autres termes, ce sont **l'impact sur l'activité de l'entreprise**, et **l'urgence à mettre en place une solution** qui déterminent la classification des priorités.

| | IMPACT | | | |
|---------|--------|---------------------------------|--|-----------------------------|
| | | Élevé (organisation entière) | Moyen (service ou > 5 utilisateurs) | Bas (1 à 5 utilisateurs) |
| URGENCE | Urgent | P1 - Majeure | P2 - Élevée | P3- Normale |
| | Normal | P2 - Élevée | P3- Normale | P4- Basse |

Le tableau en exemple ci-dessus montre une proposition de matrice de priorisation des incidents. En fonction des cas de figure, l'incident est affecté à un type de priorité. Celui-ci sera par la suite relié à un délai de résolution qui décroît à mesure que l'incident est critique. Par exemple, vous pouvez déterminer qu'un incident P4 nécessite deux jours de traitement, alors qu'un P1 doit être résolu en deux heures.

Gestion des incidents ITIL ≠ gestion des problèmes ITIL

Enfin, il arrive de confondre gestion des incidents avec **gestion des problèmes**. Pourtant, ils impliquent des procédures différentes.

Selon ITIL, la gestion des problèmes sert à :

Minimiser l'impact négatif sur les activités de l'entreprise des incidents et problèmes causés par des erreurs dans l'infrastructure informatique, et prévenir la réapparition des incidents induite par ces erreurs.

➔ Autrement dit, la gestion des problèmes s'effectue davantage de manière proactive, alors que la gestion des incidents relève plus d'une démarche réactive.

Les deux processus fonctionnent néanmoins en parallèle, la gestion des problèmes opérant grâce à l'identification d'incidents récurrents.

Bénéfices de la gestion des incidents et difficultés

Les bénéfices

Peut-être vous demandez-vous pourquoi il est si important de mettre en place un processus tant normé pour gérer vos incidents.

Parce qu'il en découle nombre de bénéfices pour votre entreprise. La gestion des incidents :

- réduit plus rapidement l'impact, parfois critique, des incidents sur l'entreprise et le business,
- simplifie grandement le processus en évitant, par exemple, les allers et retours d'emails,
- permet d'identifier les incidents récurrents, et d'ainsi déployer le processus de gestion des problèmes évoqué plus haut,
- améliore la qualité de la **base de connaissances** métiers grâce à la mise en place de base de données destinées au **traitement des incidents**,
- apporte de la transparence au sein de la structure quant à la résolution des incidents,
- améliore la satisfaction des utilisateurs et la productivité de tous les acteurs de l'entreprise.

Il est important de garder à l'esprit qu'un processus de gestion des incidents va au-delà de la simple résolution d'un problème informatique. Il constitue un solide soutien aux fonctions business de l'entreprise, en diminuant le nombre de ralentissements ou arrêts des activités qui impacteraient le chiffre d'affaires.

Les difficultés

Cependant, malgré tout le bien fondé d'une politique de gestion des incidents structurée, certaines difficultés sont à prévoir lors de sa mise en pratique. Citons par exemple :

- le manque d'engagement des collaborateurs, parfois réfractaires aux changements. Conséquence ? Une mauvaise application de la méthode, et donc des résultats moins satisfaisants ;
- le manque d'engagement de la direction. Il peut mener à des freins tels qu'un manque de moyens (matériel et ressources) pour la bonne conduite du processus ;
- le manque de connaissance des utilisateurs, qui parfois court-circuitent les procédures mises en place.

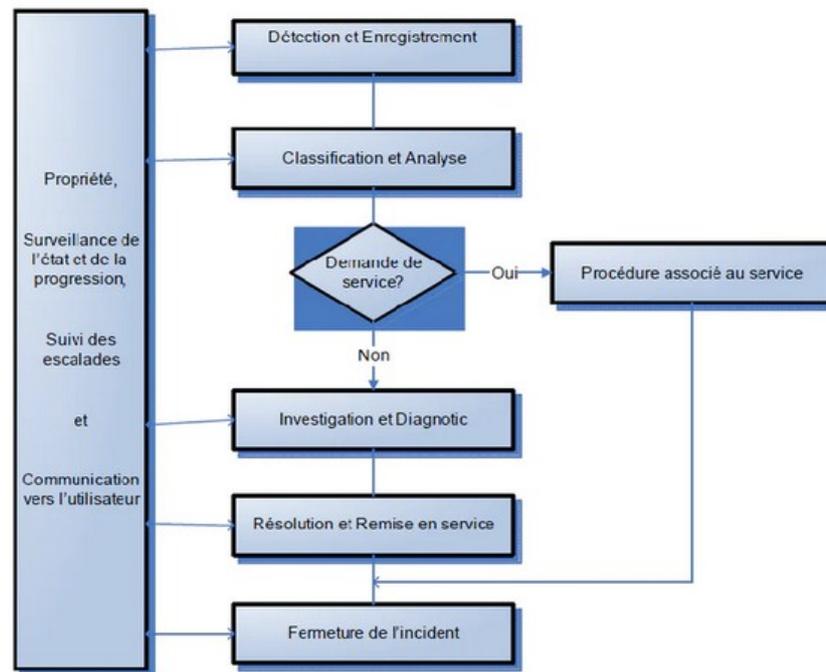
Parce que ces barrières mettent en péril les procédures préalablement définies, il est important « d'éduquer » les différentes parties prenantes impliquées directement ou indirectement dans la gestion des incidents.

Vous vous assurez ainsi une meilleure gestion du processus, que nous allons maintenant décrire plus en détails.

Le processus de gestion des incidents

Les différentes activités du processus

Schéma figurant le processus de gestion des incidents et les différentes activités associées :



Source : researchgate.net

La détection et l'enregistrement

Le service responsable enregistre les détails afférents à l'incident sur l'outil choisi (logiciel, tableur, formulaire, etc.) et le signale aux équipes de support chargées de le traiter selon la procédure.

La classification et l'analyse

L'incident est classifié selon l'ordre de priorité défini en amont, en fonction de l'impact sur l'activité et de l'urgence de la situation.

Notez que s'il s'agit d'une demande de service, vous devez suivre la procédure associée au service.

L'investigation et le diagnostic

Toutes les informations relatives à l'incident sont analysées, dans l'objectif de procéder à la résolution et à la remise en service dans les délais.

Sachez que parfois, le premier niveau de service ne peut résoudre l'incident : il se déclenche alors une **escalade des incidents** sur des **niveaux de service** supérieurs, sur laquelle nous reviendrons ultérieurement.

La résolution et la remise en service

La résolution de l'incident prend diverses formes :

- l'incident est réparé immédiatement. Il a été résolu et les activités reprennent leur cours normal.

- une solution de contournement a été trouvée. En effet, la gestion des incidents doit mener au rétablissement rapide des services. Si le système n'est pas parfait, mais qu'il rend la situation « acceptable », le processus est respecté.

Notez que si les causes sous-jacentes d'un incident sont inconnues, mais qu'elles semblent partager la même origine, il est recommandé d'initier un processus de gestion des problèmes. Rappelons que les flux de gestion des incidents et des problèmes sont souvent croisés.

La fermeture de l'incident

Pour clore convenablement un incident, les équipes en charge du processus mènent un certain nombre d'actions :

- elles prennent soin de consigner tous les détails de l'incident et le temps passé dessus,
- elles informent l'utilisateur de la résolution,
- elles veillent à ce que tous les détails de la solution soient clairs et lisibles.

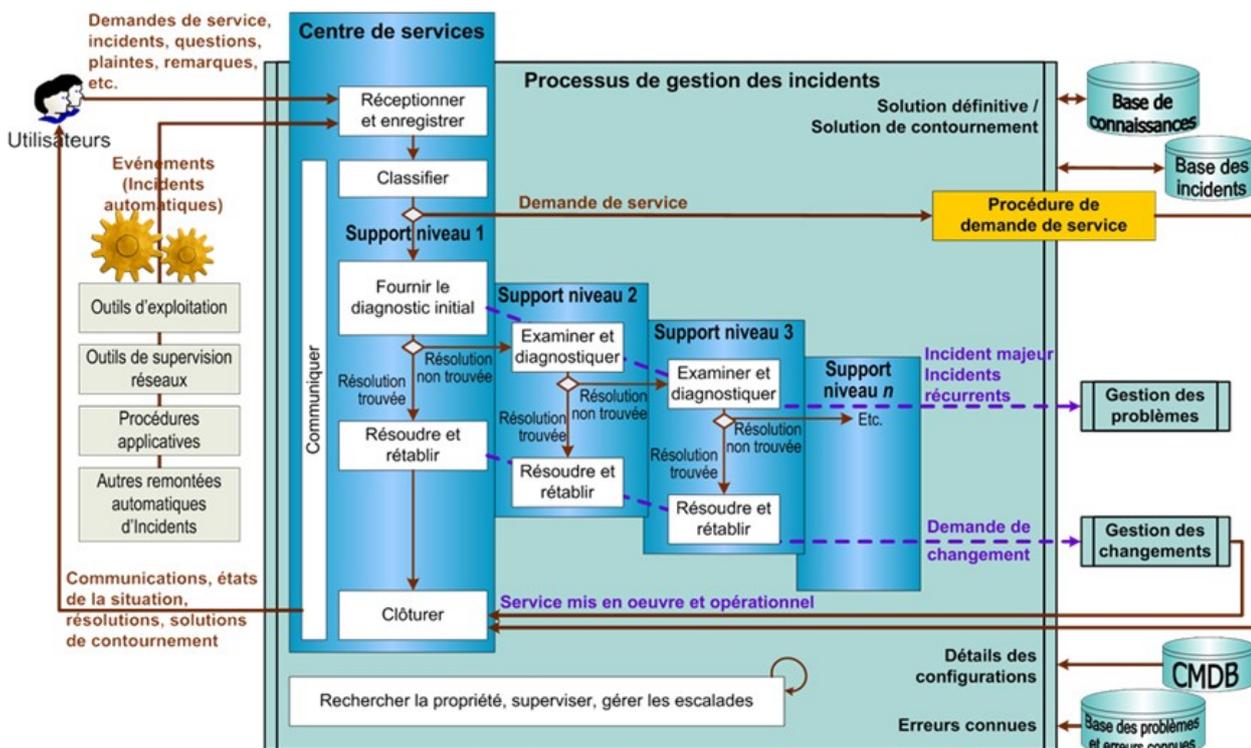
Grâce à ce niveau de détails, vous diminuez le risque de conflit entre les différentes parties prenantes.

L'escalade des incidents

Nous avons vu que l'escalade des incidents survient lorsque la résolution est transférée à un niveau supérieur.

En règle générale, cette manœuvre intervient lorsque les personnes en charge de la gestion au premier niveau ne possèdent pas l'expertise nécessaire, ou lorsque le délai initialement prévu est dépassé.

Dans ce cas, le schéma du **cycle de vie** de l'incident diffère un peu :



Nous constatons qu'au moment de la résolution de l'incident, le travail est transféré au niveau de support supérieur, et ce jusqu'à ce qu'il puisse être clôturé. Cette escalade conduit parfois jusqu'à l'éditeur du logiciel ou au fabricant du matériel.

Les acteurs de la gestion des incidents

Différents acteurs sont impliqués dans la gestion des incidents. S'ils diffèrent d'une organisation à l'autre, nous identifions toutefois quelques rôles fondamentaux :

- le demandeur/l'utilisateur : il signale l'incident en spécifiant clairement de quoi il s'agit. L'équipe technique peut également le solliciter en fin de processus pour répondre à des enquêtes.
- les différents niveaux de support : en fonction de leur niveau, les équipes de support apportent les solutions nécessaires à la résolution de l'incident, et réaffectent parfois l'incident non résolu au niveau supérieur.
- le gestionnaire d'incident : garant de la bonne conduite de la gestion des incidents, il planifie le processus et peut recommander des axes d'amélioration.
- le propriétaire du processus : il assume, au sein de l'entreprise, les responsabilités du processus de gestion des incidents de manière générale. Il peut également se charger de la définition des **KPIs** (*Key Performance Indicators*), ou **indicateurs clés**.

Les KPIs de la gestion des incidents

Pour mesurer l'efficacité de votre processus de gestion des incidents, référez-vous à des KPIs.

C'est à vous de les définir, en accord avec vos objectifs et la configuration de votre structure. Toutefois, certains KPIs ont fait leurs preuves, comme :

- le nombre total d'incidents décomptés,
- le temps de résolution moyen d'un incident,
- le nombre d'incidents récurrents,
- le nombre d'incidents en suspens, ou backlog des incidents,
- le coût moyen de traitement d'un incident.

Exemple de 2 solutions ITSM « opensource »

| | |
|--|---|
| <p>GLPI est un logiciel de gestion de services basé sur des technologies open source. Il vous aide à planifier et à gérer facilement les changements informatiques, à résoudre efficacement les problèmes, à automatiser vos processus métier et à prendre le contrôle de votre infrastructure informatique.</p> <p>Fonctionnalités clés de GLPI :</p> <ol style="list-style-type: none">1. Bureau de service2. Gestion des actifs et inventaire automatique3. Rationalité du contrôle de la qualité des données4. Gestion administrative et financière du patrimoine5. Inventaire des logiciels et gestion des licences6. Connaissances et questions fréquemment posées7. Statistiques et rapports8. Intégration profonde9. Inventaire des appareils basés sur Android | <p>ITop s'adapte aux besoins des entreprises du numérique (hébergeurs, prestataires de services, éditeurs de logiciels) pour gérer de multiples clients, contrats et engagements. iTop est l'élément central pour construire une solution qui couvre tous les environnements clients tout en protégeant la confidentialité nécessaire à chaque organisation.</p> <p>Basé sur l'expérience des professionnels de l'infogérance, iTop est conçu pour gérer la complexité des infrastructures mutualisées. iTop vous donnera la possibilité d'analyser l'impact d'un incident ou d'un changement sur les différents services, contrats ou clients que vous devez honorer. iTop est au cœur des activités opérationnelles des centres de services. En constituant un référentiel partagé par toutes les équipes, iTop vous permet de proposer des offres personnalisables pour chaque client. Dans une logique de centre de contrôle avec une solution déportée.</p> |
|--|---|

Performance et satisfaction utilisateur

Nous pouvons conclure que la gestion des incidents, normée par ITIL, est une procédure à intégrer rapidement à votre système d'information, tant elle permet d'apporter une réponse claire et rapide aux problèmes. De plus, elle conduit progressivement à une diminution du nombre de ces incidents en alimentant vos processus de gestion des problèmes, et par là même vos actions préventives.

Et bonne nouvelle, tout le monde ressort gagnant de la mise en pratique d'une telle méthode de travail :

- Les équipes techniques travaillent plus efficacement et en toute transparence.
- Les utilisateurs sont moins impactés par des bugs et sont davantage satisfaits par votre produit.
- L'entreprise essuie moins de pertes en cas d'incident critique.

Enfin, rappelons qu'une bonne gestion des incidents va de pair avec l'utilisation d'outils pertinents, qui viennent en soutien de votre processus et font gagner un temps précieux aux équipes.

L'ITSM : un accélérateur de transformations

Si on parle beaucoup de transformation digitale, en réalité, celle-ci recouvre plusieurs réalités qui sont à la fois humaines, technologiques et organisationnelles. Dans un monde qui va toujours plus vite et où les tendances naissent et meurent rapidement, il est fondamental de disposer d'un système qui vient accompagner la transformation. En interne, il y a toujours un processus à améliorer et à fluidifier, une erreur à corriger ou une manière de faire différemment. L'ITSM vient faciliter cette transformation en continu, car elle s'adapte aux outils et aux technologies actuels et futurs. Ainsi, que l'on parle d'intelligence artificielle, d'automatisation, de chatbots ou d'agents virtuels, l'ITSM est capable de gérer la transformation de l'expérience utilisateur (pour une plus grande facilité d'utilisation et un service à forte valeur ajoutée), des processus et des technologies (pour une meilleure visibilité des services et rationaliser des processus complexes), et des coûts et risques (pour une meilleure gestion des données quelle que soit la structure organisationnelle en place).

Quel futur pour ITIL et l'ITSM ?

ITIL se met à jour à son propre rythme, mais nul doute que les changements culturels et sociétaux que nous vivons viendront l'influencer. Le futur d'ITIL se construira sur les nouveaux processus nourris par l'intelligence artificielle. Cette dernière sera en mesure de dire ce qui fonctionne ou non, et ce qui va fonctionner ou non, tout en proposant des axes de développement sur lesquels travailler. En augmentant les capacités humaines grâce à l'analyse prédictive, l'intelligence artificielle contribue à refaçonner le monde des systèmes d'information, ce dont l'ITSM profitera.

ITSM et prédiction (source : IT Operations – Gartner)

Alors que l'intelligence artificielle et l'apprentissage automatique ont déjà fait leur marque dans les secteurs du commerce électronique et de l'automobile, l'informatique commence tout juste à adopter ces tendances. La gestion des services informatiques (ITSM) peut potentiellement bénéficier de l'intelligence artificielle, car les agents du centre de services effectuent une grande variété de tâches transactionnelles. Mais attention, il est important de comprendre les fondamentaux de l'IA, l'impact généré par son adoption et de mener des recherches préparatoires avant de la mettre en place. L'IA aide l'informatique à répondre aux attentes croissantes des utilisateurs en matière de rapidité de service et de technologie de pointe. La numérisation alimente l'IA pour exploiter les données et accélérer les performances opérationnelles.

- "D'ici 2019, 40% des initiatives de transformation numérique seront soutenues par l'apprentissage automatique et l'intelligence artificielle."
- "En 2020, 99% des initiatives d'IA dans l'ITSM échoueront, faute d'une bonne base en termes de gestion des connaissances."

(Sources : www.easyvista.com | www.bestpractices-si.fr)



MEMENTO : LA GESTION DE PROJET

| | |
|---|--|
| <ul style="list-style-type: none"> ■ les objectifs du projet sont définis en qualité, coût, délais et périmètres (fonctionnel, organisationnel, technique, prestation, SLA) ■ la note de cadrage définit l’engagement formel de tous les acteurs au lancement du projet ; objectif – périmètres – ressources – calendrier et comitologie ■ sa validation matérialise la fin de la phase d’initialisation ; par la suite, en cas d’écart sur les engagements qui y sont définis, le chef de projet alertera le COPIL ■ la réunion de lancement vise à faire partager la vision et l’engagement avec l’ensemble des acteurs du projet et à poser les premières règles du jeu ■ le chef de projet (CDP) fait avancer ses réunions, grâce à des questions ouvertes ; il prépare l’introduction de sa réunion jusqu’à la première question ■ le découpage en tâches est effectué dès le lancement du projet en impliquant les experts bien avant leurs interventions sur l’exécution des tâches ■ la liste des tâches montre des phases et des produits, structurés selon le cycle projet (V, agile, intégration de progiciel) ■ le couple MOA/MOE choisit le cycle le mieux adapté en fonction des enjeux et du contexte ■ un projet peut piloter plusieurs sous-projets (par phase ou lot) ayant des cycles différents et mixés (agile/V) ■ le CDP arrête de découper lorsqu’il ne peut désigner un responsable engagé sur : activité/livrables/délais/coûts/qualité/risque ■ les ressources sont affectées sur l’optimum de leur Savoir-Vouloir-Pouvoir ; s’il y a inadéquation avérée sur 2 des critères il convient d’alerter la hiérarchie ■ l’équilibre contribution rétribution permet de maintenir la motivation des collaborateurs. ■ la délégation est un geste managérial ; elle fixe l’objectif et les contrôles ; elle peut s’accompagner de la fiche de délégation visée par les parties ■ les règles du jeu : devoir d’engagement, de conseil, d’alerte et droit à l’erreur ■ chaque CDP a un style de management à adapter selon le projet et la situation | |
| <p>- cadrer le projet et définir les objectifs (but) et les enjeux (valeur) selon les composants projets</p> | <p>- Triangle d’or <u>Qualité-Coût-Délai</u> - Au centre du triangle, le <u>Périmètre</u></p> <p>- exécuteurs et commanditaires du projet : MOA, AMOA, MOE et PMO</p> |
| <p>- gouvernance claire ; la note de cadrage doit inclure le cahier des charges, objectif, démarche, contraintes, acteurs, ressources</p> <p>- le CDP (Chef De Projet) constituer une équipe projet avec une vision commune sur le projet</p> <p>- le CDP ou le référent technique équipe peut faire appel ponctuellement à des experts internes ou sous-traitants pilotés</p> <p>- le CDP partage largement sur les règles de fonctionnement et formaliser les décisions dans le compte-rendu</p> <p>- le CDP a un devoir d’alerte</p> | <p>- 6 périmètres caractérisant le projet :</p> <ul style="list-style-type: none"> • fonctionnel • technique • organisationnel • SLA (contrat de service) • prestation (engagement) • sites <p>- découpage du projet en sous-projet (avec tâches/jalons) selon méthodologie adaptée au produit Cycle V (par phase ou déterministe), AGILE (par lot ou incrémentale) ou autre</p> <p>- élaboration de la matrice des responsabilités (RACI) servant d’annuaire et identifiant les rôles de chaque intervenant/acteur sur le projet</p> <p>- alignement stratégique des ressources/tâches (S-V-P) et planning (GANTT)</p> <p>- afficher une date de fin prévisible</p> <p>- évaluer le coût du projet : ratio entre l’estimé et le négocié</p> |

| | |
|--|---|
| <p>- les achats publics sont encadrés par des textes (code des marchés publics) et des principes (libre accès, égalité, transparence...), à appliquer et à adapter pour chaque sous-projet RACI en lien avec le SAE (Service Achat de l'État)</p> <p>- La passation d'un marché public est soumise à des règles de procédure et de publicité. D'une part, l'acheteur doit se conformer à une procédure, qui est déterminée en fonction de la valeur de l'achat et de son objet. D'autre part, il doit appliquer des règles de publicité, qui varient elles aussi en fonction de l'acheteur, de la valeur estimée et de l'objet de l'achat.</p> <p>- les 3 procédures formalisées : l'appel d'offres, la procédure avec négociation et le dialogue compétitif</p> | <p>- si projet > 9 M€ : nécessité de réaliser une étude (ou analyse de risque interministérielle) MAREVA pour appréhender la valeur du projet (élaboration de notes stratégique et de rentabilité économique) => optimisation COÛT VALEUR</p> <p>- marché public de services : Il peut s'agir de services matériels (entretien des locaux) ou immatériels (projet informatique)</p> <p>- procédure en fonction des seuils-Marché passé par l'État :</p> <ul style="list-style-type: none"> • ≤ 40k€HT choix libre (sans publicité ni mise en concurrence) • MAPA, entre 40k€ HT et 140k€HT • Procédure formalisée > 140k€HT |
| <p>- établir une comitologie idoine, l'ODJ, la fréquence des réunions avec participants identifiés</p> <p>- rendre compte à sa hiérarchie et au commanditaire</p> <p>- instances de pilotage :</p> <ul style="list-style-type: none"> • comité direction • comité pilotage • comité fonctionnel et technique | <p>- le CDP passe en suivi de projet</p> <p>- il anime les réunions de suivis, assure le pilotage opérationnel du projet :</p> <ul style="list-style-type: none"> • s'assure de la réalisation effective des travaux (%Avancement) via TdB • suit les risques projets • prépare les arbitrages à faire rendre par le COPIL • apporte le soutien nécessaire à l'équipe projet |
| <p>■ <i>Un risque est un événement aux conséquences négatives pour le projet (sur QDCP)</i></p> <p>■ <i>Criticité : risque = probabilité x impact</i></p> <p>■ <i>Maîtriser les risques : identifier, mesurer, agir (préventif et curatif) ; suivre le plan de maîtrise optimise et l'équilibre qualité risques</i></p> <p>■ <i>Le suivi des risques est fait à chaque comité opérationnel ou stratégique</i></p> | |
| <p>- anticiper et réagir en situation de crise</p> <p>- en cas de besoin, alerter permet d'escalader pour obtenir plus de moyens</p> | <p>- Identifier les signes qui caractérisent une crise et adapter une stratégie ou plan d'urgence :</p> <ul style="list-style-type: none"> • acteurs à l'origine de la crise • chiffrer les conséquences • négocier un délai • retex en sortie de crise (capitaliser) |
| <p>- accompagner le chargement</p> | <p>- l'accompagnement (essentiel pour un succès) se caractérise par :</p> <ul style="list-style-type: none"> • redéfinition des processus métiers • la formation • la communication • le soutien |
| <p>- capitaliser (à formaliser lors du bilan projet)</p> | <p>- collecte tout au long du projet ; technos, outils, codes, procédures, docs, compétences, tiers, relations et management projet</p> |



Exploiter l'informatique à l'heure d'Itil

La mise en oeuvre d'Itil dans les entreprises améliore la qualité des services informatiques délivrés. Son utilisation par les DSI marque l'avènement d'une culture orientée utilisateur.

Francisco Villacampa
01net.

Les utilisateurs ne se privent plus pour exiger des outils informatiques qu'ils répondent à leurs besoins professionnels. A charge pour les DSI d'assumer. Dans ce contexte, la bibliothèque Itil (*Information Technology Infrastructure Library*) constitue un auxiliaire utile. Conçue à la fin des années quatre-vingt-dix, elle comprend un ensemble de méthodes et de procédures, destinées à l'amélioration de la qualité des services délivrés par la DSI.

Itil concourt donc à ce titre à la réalisation globale des activités de l'entreprise. Parmi d'autres objectifs, Itil préconise un pilotage rigoureux du changement et du cycle de vie de l'infrastructure informatique. Cela dans une évidente optique de rationalisation des coûts. Dans ce cadre, il est normal que les éditeurs spécialisés dans la gestion de l'infrastructure fassent valoir la 'compatibilité' Itil de leurs logiciels. Cette tendance concerne les éditeurs de logiciels de gestion de parc ou d'actifs, dont Peregrine Systems, BMC, HP, LANDesk, PS'Soft, Apsynet, EasyVista, etc.

Car la compatibilité Itil permet à ces derniers de faire valoir la prise en charge des aspects qualitatifs du système d'information, et non plus simplement ses aspects techniques et financiers. Cette prise en charge est notamment assurée par l'apparition de centres de services, ou 'service desk', dont la vocation est d'aller plus loin que le simple recensement de pièces informatiques et leur gestion financière.

L'utilisateur devient client

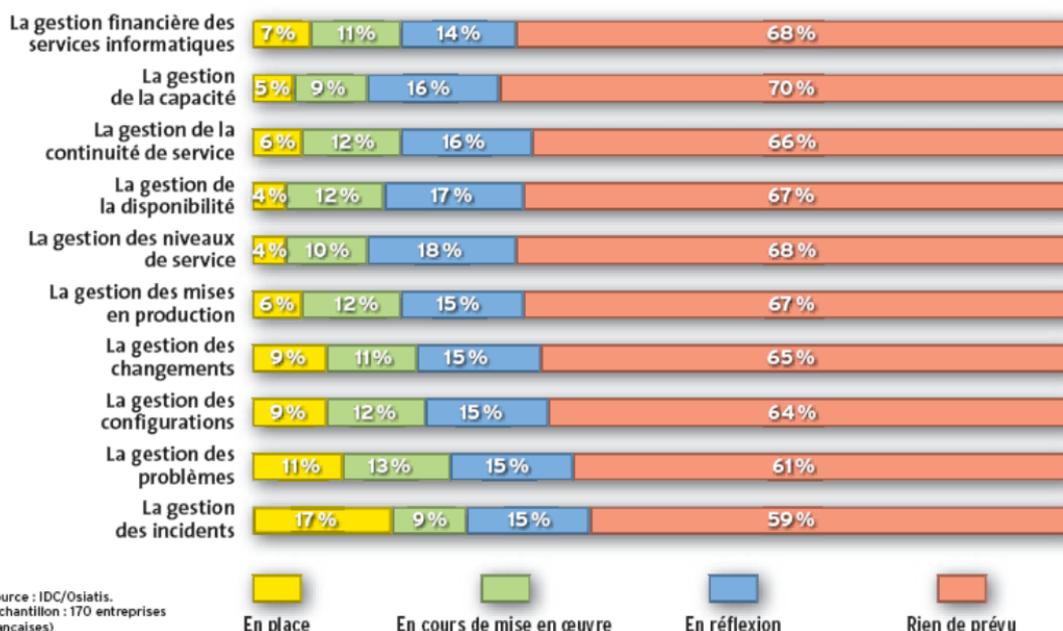
Les logiciels qui se proclament compatibles Itil doivent a minima assurer une assistance adaptée aux besoins de l'utilisateur (service support). Cela comprend 'la gestion des configurations techniques, des changements, des incidents et des problèmes', explique Francis Ronez, satisfaction. D'autres recommandations existent en matière de gestion de la sécurité, de l'activité métier, des infrastructures et des applications. En entreprise, la mise en place de pratiques Itil se traduit souvent par une réorganisation de l'assistance utilisateur.

' Nous souhaitons rationaliser le fonctionnement de notre département informatique. Le logiciel Kim'Hotline de Kimoce nous a permis de transformer l'aide directe fournie à l'utilisateur par téléphone ou courriel, en point d'entrée unique de gestion des changements et des configurations informatiques, témoigne Sophie Zerr, responsable du SI au sein du conseil général de la Manche. Nous commençons à travailler sur la qualité de service délivrée. ' Précisons que les recommandations ne sont pas des normes et que 'Itil n'a pas lieu d'être au-delà de l'exploitation informatique', prévient Olivier Barre, responsable ingénierie OS chez Mondadori France.

Enfin, soulignons qu'il n'existe pas de certification ou de norme Itil capable de garantir qu'un logiciel de gestion de parc ou d'inventaire sera capable de prendre en charge une gestion qualitative du système d'information. ' ISO/CEI 20000 certifie les entreprises qui ont mis en place l'ensemble des processus de gestion de service [et non pas les logiciels, NDLR]', souligne Francis Ronez, administrateur de l'itSMF France, l'association principale de promotion d'Itil. Quant au certificat Pink Elephant, il garantit en théorie que le logiciel répond aux recommandations Itil. Toutefois, ce certificat payant est onéreux, ce qui explique sa rareté.

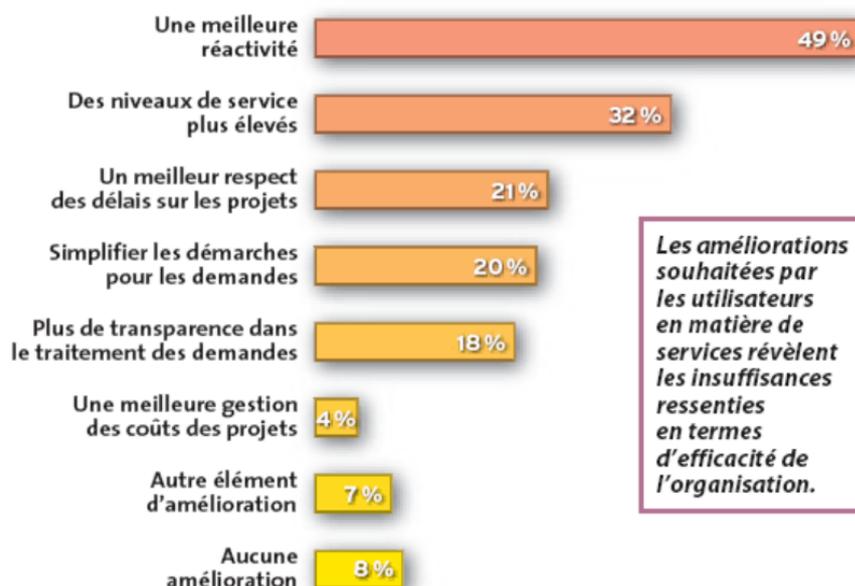
LA GESTION DES INCIDENTS ET DES PROBLÈMES EST PRIORITAIRE

Où en êtes-vous dans la mise en œuvre d'ITIL sur...



LES UTILISATEURS ATTENDENT UNE PLUS GRANDE RÉACTIVITÉ

Quelles améliorations des services du département informatique les utilisateurs attendent-ils ?



Source : IDC/Osiatis. (Question posée aux directions informatiques)

Logiciels helpdesk: Test et comparatif

Les 5 meilleurs logiciels helpdesk 2020

Guide d'achat - L'Express

| | Vainqueur du comparatif | | | | |
|--|--|---|---|---|---|
| |  zendesk |  freshdesk |  freshservice |  GENESYS |  LiveChat |
| Nom | Zendesk | Freshdesk | Freshservice | Genesys PureCloud | LiveChat |
| Évaluation ① Comment évaluons-nous Avis aux utilisateurs | Score:9,46 "Remarquable" | Score:9,33 "Excellent" | Score:8,58 "Excellent" | Score:8,57 "Excellent" | Score:8,04 "Très bien" |
| Atouts | <ul style="list-style-type: none"> ⊕ palette de fonction très complète ⊕ interface conviviale ⊕ options de paiement flexibles | <ul style="list-style-type: none"> ⊕ facilite la définition des SLA ⊕ nombreuses ressources d'aide et de formation de haute qualité ⊕ version basique gratuite | <ul style="list-style-type: none"> ⊕ interface très conviviale ⊕ nombreuses fonctions automatisées ⊕ saisie automatique du portefeuille de logiciels et de matériels | <ul style="list-style-type: none"> ⊕ répartition maligne des appels ⊕ système de requête des données clients ⊕ outils de gestion à distance intégrés | <ul style="list-style-type: none"> ⊕ interface très conviviale ⊕ intégration facile sur le site ⊕ service d'assistance joignable à toute heure |
| Inconvénients | <ul style="list-style-type: none"> ⊖ tarification peu claire ⊖ peu entraîner des frais annexes élevés | <ul style="list-style-type: none"> ⊖ le service VoIP intégré est assez cher ⊖ le chatbot d'assistance est uniquement en anglais | <ul style="list-style-type: none"> ⊖ peu de canaux de communication ⊖ les outils de gestion de projet laissent à désirer | <ul style="list-style-type: none"> ⊖ pas de billetterie ⊖ pas de base de connaissances | <ul style="list-style-type: none"> ⊖ se résume à un chat ⊖ dispositifs de sécurité uniquement disponibles dans la formule premium |
| Coût par agent / par mois | 5 - 199 € | \$19 - 99 | 20 - 75 € | 60 - 112 € | \$16 - 149 |
| Version d'essai | 30 jours | 21 jours | 21 jours | Sur accord préalable | 30 jours |
| Version gratuite | ⊗ | ⊙ | ⊗ | ⊗ | ⊗ |
| Version web (SaaS) | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Version auto-hébergée | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ |
| REST API | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Langues | 28 | 34 | 30 | 18 | 45 |
| Limite pièces jointes | 1 - 20 Mo | 15 - 20 Mo | 15 Mo | n/c | n/c |
| Espace de stockage total | n/c | n/c | n/c | 17,5-42,25 Go / utilisateur | n/c |
| Open Source | ⊗ | ⊗ | ⊗ | ⊗ | ⊗ |
| Système de billetterie | ⊙ | ⊙ | ⊙ | ⊗ | ⊙ |
| Téléphone | ⊙ | ⊙ | ⊗ | ⊙ | ⊗ |
| SMS | ⊙ | n/c | ⊗ | ⊙ | ⊗ |
| E-Mail | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Formulaire web | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Chat | ⊙ | ⊙ | ⊗ | ⊙ | ⊙ |
| Facebook | ⊙ | ⊙ | ⊗ | ⊗ | ⊙ |
| Twitter | ⊙ | ⊙ | ⊗ | ⊗ | ⊗ |
| Autres réseaux sociaux | intégrations | intégrations | ⊗ | ⊗ | ⊗ |
| Base de connaissances | ⊙ | ⊙ | ⊙ | ⊗ | ⊗ |
| Forum | ⊙ | ⊙ | ⊗ | ⊗ | ⊗ |
| Gestion des SLA | ⊙ | ⊙ | ⊙ | ⊙ | ⊗ |
| Branding, respect de la charte graphique | ⊙ | ⊙ | ⊙ | ⊗ | ⊙ |
| Rapports et statistiques | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Appis mobiles | Android, iOS | Android, iOS | Android, iOS | Android, iOS | Android, iOS |
| Application de bureau | Fournisseur tiers | ⊗ | ⊗ | Windows | Windows, macOS |
| Blocs de texte | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Macros | ⊙ | ⊙ | ⊙ | ⊙ | ⊗ |
| Raccourcis clavier | ⊙ | ⊙ | ⊙ | ⊗ | ⊙ |
| Rôles d'utilisateurs | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Champs personnalisables | ⊙ | ⊙ | ⊙ | n/c | ⊗ |
| Enregistrement automatique | ⊙ | ⊙ | ⊗ | n/c | ⊗ |
| Serveurs situés en UE | n/c | n/c | ⊗ | Allemagne | UE et Etats-Unis |
| Chiffrement SSL | ⊙ | ⊙ | ⊙ | ⊙ | ⊙ |
| Conformité ISO27001 | ⊙ | ⊙ | ⊙ | ⊙ | ⊗ |
| Authentification à double facteur | ⊙ | ⊗ | ⊗ | ⊙ | ⊙ |
| Liste blanche d'IP | ⊙ | ⊙ | ⊙ | ⊗ | ⊙ |

Qu'est-ce qu'un centre de service ?

Le service desk, ou centre de service informatique, est **le premier point de contact** entre les utilisateurs et une organisation IT. Selon ITIL (Information Technology Infrastructure Library), le centre de service est le point de contact unique (SPOC - Single Point Of Contact) entre le **prestataire de services** (IT - Information Technology) et les **utilisateurs pour les activités quotidiennes**.

Toujours selon ITIL, les services informatiques sont définis comme un “ensemble de capacités organisationnelles permettant de fournir de la valeur à des clients sous forme de services.” Un IT service desk classique gère les **incidents** (interruptions de service) et les **demandes de services** (tâches routinières reliées au service) tout en traitant les communications des utilisateurs au sujet d'événements tels que les pannes ou les changements prévus dans les services.

Quelle est la différence entre un Service Desk et un support client ou un centre d'appels ?

Les entreprises utilisent souvent les termes « centre d'appels », « support client » et « centre de services » de manière interchangeable, ce qui peut créer de la confusion. ITIL considère les centres d'appels et les supports clients comme des centres de services limités qui n'offrent qu'une partie de ce que le centre de services informatiques peut apporter. Pour beaucoup d'entreprises, la définition ITIL n'est pas conforme aux pratiques opérationnelles, ce qui rend la distinction nettement plus compliquée. Voici des explications des fonctions du support client et du centre d'appels pour vous aider à faire la différence avec un centre de services informatiques.

Support client

Un support client est une ressource centralisée conçue pour fournir au client ou à l'utilisateur interne des renseignements et du support associés aux processus, produits et services de l'entreprise. Des exemples classiques de support client comprennent : les centres de support technique, les fonctions de support produit/garantie, les comités d'entreprises pour les employés et les centres de service pour installations. Le support client peut être fourni par différents canaux, notamment des sites physiques, des numéros verts, des sites web, la messagerie instantanée ou l'e-mail.

Centre d'appels

Un centre d'appels ou centre de contacts est un centre qui gère les contacts et les interactions clients. Le bureau est chargé de gérer un grand volume de demandes généralement par téléphone (mais peut aussi inclure les lettres, les fax, les réseaux sociaux, la messagerie instantanée ou les e-mails). Les centres d'appels entrants sont souvent utilisés pour des cas comme le support produit, le service client, le traitement de commandes et les services téléphoniques 24h/24, 7j/7. Les centres d'appels sortants sont utilisés pour des cas comme le télémarketing, le recouvrement de créances et les études de marché. Une entreprise peut avoir plusieurs centres d'appels qui prennent en charge différents aspects des opérations business (y compris l'IT) et ils peuvent être gérés soit en interne, soit par un sous-traitant.

La distinction est surtout centrée sur ce que la fonction couvre et la façon dont ils sont structurés :

- Un **support client** porte principalement sur la mise à disposition de support pour « aider » et « réparer ». Les supports clients ne sont pas nécessairement centrés sur le service IT et peuvent être utilisés pour supporter des exceptions aux opérations normales qui se produisent partout dans l'entreprise. Ils peuvent être soit des sites physiques qui interagissent directement avec les demandeurs en personne, ou des sites distants/virtuels qui utilisent des technologies telles que le téléphone, l'e-mail, le chat ou autres pour fournir un contact virtuel.
- Le **centre d'appel** a la portée la plus étendue en ce qui concerne les problèmes qu'ils gèrent, notamment les aspects techniques et non techniques. Les centres d'appels n'interagissent pas en personne avec les demandeurs et impliquent toujours une forme de technologie intermédiaire pour permettre le contact.
- Le **Service Desk** se concentre non seulement sur le support de services IT, mais gèrent aussi les services « d'aide » réactifs, ainsi que les tâches quotidiennes, comme l'approvisionnement des ressources, la gestion des accès, etc. Les centres de service IT peuvent être des sites physiques, auxquels les utilisateurs peuvent avoir accès en personne, ou opérer à distance, comme un centre d'appels. Ceux qui connaissent bien l'ITIL pourraient dire que le support client est tactique, alors qu'un centre de services est stratégique – cela varie en fonction des organisations.

Quel est le rôle du centre de services informatiques?

Le rôle principal d'un Service Desk est de servir de premier point de contact pour la surveillance et la prise en charge des incidents :

- En **répondant aux demandes** et aux questions des utilisateurs
- En fournissant un **canal de communication** entre d'autres fonctions de la gestion de services et la communauté des utilisateurs.

En plus de ces fonctions principales, le centre de service IT joue souvent un rôle actif en ce qui concerne:

- La capture des **demandes de changement**
- La maintenance des **contrats de support** avec les parties tierces
- La **gestion des licences** logicielles
- L'assistance dans la **gestion des problèmes**.

Dans certaines organisations, le centre de services est intégré à d'autres processus business tels que :

- L'accueil des **nouveaux employés**, l'intégration des **acquisitions**, la gestion de **l'accès aux données**, l'accueil et le départ des **fournisseurs/partenaires**, le **reporting** et la gestion des métriques, la gestion **d'entreprise**, la surveillance de **l'infrastructure et des services**

Quels sont les avantages d'un centre de services informatiques?

Réduction des coûts et extensibilité

La réduction des coûts et l'extensibilité sont les deux avantages les plus couramment recherchés par les entreprises lors de la mise en œuvre d'un centre de services informatiques. Un centre de services bien géré, avec le bon personnel, peut gérer la plupart du travail quotidien du département informatique. Le Service Desk fournit aux organisations une option relativement bon marché permettant de transférer le travail simple des équipes coûteuses d'ingénieurs et d'experts, leur permettant ainsi de se concentrer sur les activités qui rapportent plus de valeur à l'entreprise. Le centre de services peut aussi permettre à l'entreprise de fournir du support « follow the sun » aux activités mondiales et aux communautés d'utilisateurs réparties dans le monde.

Rester à l'écoute des utilisateurs

Le IT Service Desk est le point de départ de beaucoup de processus et de services clés pour l'IT et, en tant que tel, est souvent l'interface principale entre les utilisateurs, les processus business et les services informatiques qui les soutiennent. Surveiller cette interaction permet d'obtenir des informations précieuses sur la satisfaction des utilisateurs, leur sentiment vis-à-vis des services, ainsi que les fonctions et les besoins non satisfaits qui pourraient être comblés par les services informatiques à l'avenir.

Alerte précoce des problèmes potentiels

Du fait de la grande quantité de problèmes et de demandes qui sont pris en charge par le centre de services, en ayant à sa disposition les bonnes données et les bons outils permettant d'évaluer les tendances et les évolutions, l'organisation peut se servir du centre de services comme un outil de suivi pour identifier les problèmes de service et les traiter de manière anticipée. Le « système d'alerte précoce » qu'offre le centre de services permet la gestion proactive des problèmes, la maintenance préventive et les changements de services afin de réduire l'impact des pannes et des dégradations de service sur les utilisateurs.

Les meilleures pratiques du service desk:

Les entreprises opèrent des centres de services informatiques depuis de nombreuses années, ce qui a permis d'identifier les meilleures pratiques.

L'engagement par rapport aux clients

- Analysez le comportement des clients et leurs attentes pour être sûr de comprendre leurs besoins
- Proposez un portail libre-service pour les utilisateurs 24h/24 (même lorsque votre centre de services est fermé)
- Utilisez les SLA et les classifications de priorité/sévérité pour différencier les requêtes afin de gérer les plus urgentes en premier

- Essayez de résoudre les problèmes dès le premier point de contact et évitez les transferts, les escalades et les rappels
- Menez des enquêtes de satisfaction client de façon régulière pour savoir ce que pensent les clients des services qu'ils reçoivent

La gestion du centre de services & le reporting

- Utilisez les rapports en temps réel, les tableaux de bord et les statistiques du support client pour surveiller les opérations et lancer des actions de correction avant que les incidents ne deviennent des problèmes
- Vérifiez que les processus de transfert et d'escalade soient clairs et bien compris pour éviter de manquer des SLA
- Exploitez les capacités d'analyse de votre système ITSM pour réduire le temps et les efforts passés à générer des rapports
- Assurez-vous que la direction fasse directement l'expérience de l'exploitation du centre de services directement afin d'apprécier la valeur du personnel du centre de services et les défis qu'ils rencontrent
- Traitez le personnel du centre de services comme des professionnels de la communication et de la résolution de problèmes en leur donnant les outils dont ils ont besoin pour réussir

Utiliser la technologie pour aider le centre de services informatiques

- Etablissez des capacités de workflow de demande de service dans votre logiciel de support pour orchestrer les escalades et les transferts
- Fournissez des capacités d'automatisation pour les requêtes utilisateurs courantes (accès, réinitialisation du mot de passe, etc.)
- Utilisez votre logiciel service desk pour faciliter et enregistrer les communications entre les agents et les demandeurs
- Intégrez vos systèmes de Service Desk dans votre ITSM au sens plus large afin de fournir à vos agents un accès plus étendu aux informations sur l'environnement informatique

La gestion des connaissances

- Mettez en place un système de gestion des connaissances pour collecter les connaissances là où de nombreuses personnes pourront y accéder
- Fournissez directement les réponses aux questions fréquemment posées (FAQ) par les utilisateurs – évitant ainsi le besoin de contacter un agent
- Actualisez régulièrement vos fichiers de connaissances en les révisant et en les épurant fréquemment

Le logiciel de centre de service:

Aussi appelé logiciel Service Desk, cet outil efficace a besoin d'une solide base technologique pour fournir aux agents les outils et les informations permettant de répondre efficacement aux besoins des demandeurs.

Système de tickets du support client

Le système de tickets du support client est la plateforme transactionnelle clé pour le centre de services informatique – orchestrant aussi bien les incidents que les demandes de service dans toutes les fonctions du centre de services et les équipes de support élargies. Les fonctions principales du système de tickets comprennent :

- La gestion du workflow, les alertes/escalades, le routage automatique, la gestion des contrats/SLA

Gestion des connaissances

La connaissance est la ressource la plus précieuse du centre de services et pour optimiser la performance opérationnelle, il faut créer des données de la meilleure qualité possible. Un système de gestion des connaissances est essentiel pour canaliser cette ressource et s'assurer que la connaissance organisationnelle est disponible à ceux qui en ont besoin. Les fonctions principales d'un système de gestion des connaissances comprennent :

- Une base de données des connaissances (KMDB), les workflows de gestion des connaissances pour soutenir le cycle de vie des connaissances, une base de données des problèmes/ erreurs connues (KEDB), des vues différentes des données pour les agents et les utilisateurs, une recherche par mots-clés évocateurs basés sur la description de l'incident.

Libre-service pour l'utilisateur final

Un grand nombre de problèmes et de requêtes qui génèrent des appels au Service Desk sont des requêtes que les utilisateurs peuvent solutionner par eux-même en ayant accès aux informations et aux outils pertinents. Les capacités de support libre-service permettent aux utilisateurs de résoudre leurs problèmes plus rapidement, sans avoir à attendre un agent. Ils économisent aussi de l'argent à

l'entreprise en diminuant le besoin d'agents supplémentaires pour gérer les demandes simples dans le centre de services informatiques. Certaines des fonctionnalités libre-service les plus courantes comprennent :

- La recherche dans la base de connaissances, les diagnostics en libre-service, les processus courants automatisés, le formulaire de demande de service.

Gestion du Service Desk et reporting

Les fonctions de gestion et de reporting sont essentielles au sein du centre de services lorsque les chefs de service cherchent à optimiser les coûts opérationnels, identifier au préalable les problèmes impactant l'entreprise (incidents majeurs), gérer la satisfaction client et garantir le respect des SLA. La technologie peut jouer un rôle important dans les fonctions de gestion en permettant aux responsables du centre de services d'avoir une vue d'ensemble de leurs opérations et des données nécessaires pour prendre des décisions éclairées. Certaines des capacités principales de gestion et de reporting du centre de services sont :

- Les capacités de gestion des incidents majeurs, les tableaux de bord pour la performance et la disponibilité des services, les rapports de mesure sur les agents/la gestion des appels, les rapports sur le respect des SLA, les analyses des problèmes connus

Intégration du centre de service avec d'autres fonctions ITSM

Le service desk fonctionne comme un élément des opérations de gestion de service au sens large. Même si le centre de service IT peut fonctionner de façon indépendante, la performance et la valeur seront augmentées en intégrant le logiciel de service desk avec d'autres parties du système ITSM de l'entreprise. Certaines des intégrations les plus intéressantes comprennent :

La base de données de la gestion de la configuration (CMDB)

Donnant aux agents l'accès au réseau complexe des interdépendances techniques et aux informations des composants de configuration pour leur permettre de mieux évaluer les impacts des incidents

La gestion des changements

Un grand nombre de problèmes technologiques sont causés par des changements planifiés. En donnant aux agents accès au système de gestion des changements, ils seront capables d'identifier les incidents associés plus rapidement

La surveillance

Les surveillants de service et d'infrastructure donnent une visibilité en temps réel sur la santé de l'environnement informatique et donnent l'alerte lorsque quelque chose ne va pas. En intégrant les capacités de surveillance avec le système du centre de services, beaucoup d'incidents peuvent être identifiés sans que l'utilisateur n'ait besoin d'appeler et de signaler un problème

La gestion des problèmes

Le meilleur moyen de gérer les incidents est d'éviter qu'ils se produisent. Intégrer les capacités de gestion des problèmes permet non seulement d'aider les agents du centre de services de comprendre quels problèmes connus sont déjà en train d'être traités, mais permet aussi aux équipes de gestion des problèmes de se concentrer sur ceux qui causent le plus grand nombre d'incidents.

La gestion des actifs

Les interactions du centre de services avec les utilisateurs sont un moment idéal pour vérifier et mettre à jour les informations de gestion des actifs. Donner aux agents la possibilité de voir et de mettre à jour les données de gestion des actifs peut être un moyen efficace d'améliorer la qualité de cet ensemble de données importantes de l'ITSM.

Résumé

Le **centre de services informatique** est un élément essentiel de la **fonction ITSM** des entreprises modernes. A mesure que le rôle de la technologie en tant que partie intégrante des processus commerciaux et des expériences utilisateurs s'élargit, il est essentiel de s'assurer que les **services IT** fonctionnent correctement et sont accessibles à ceux qui en ont besoin. Le centre de service IT **centré sur l'utilisateur**, avec ses workflows bien définis, sa richesse de connaissances sur l'organisation et ses connexions avec le reste de l'organisation informatique est le **lien critique entre les utilisateurs et l'organisation informatique**.

Chaque organisation est unique et votre Service Desk, ainsi que les outils que vous utilisez, doivent être **totalelement en phase avec les besoins de votre entreprise**.

Le cloud computing se définit par la mise à disposition d'un parc de machines, de réseau et de logiciels. Les clients utilisent un réseau informatique (en général à travers Internet) facilité par le fournisseur qui en assure la maintenance. Il existe trois modèles de services de cloud computing adaptés aux différents besoins : IaaS, PaaS et SaaS. Quels services incluent ces modèles et à qui sont-ils destinés ? Explications.

Les aspects du Cloud Computing

IaaS (Infrastructure as a service) : externalisation de l'infrastructure matérielle

L'IaaS offre au client une infrastructure externe. Le fournisseur prend en charge l'installation des serveurs de fichiers, les réseaux et le stockage des données. De cette façon, le client n'a pas besoin d'acheter les équipements liés à ces ressources : il les loue au prestataire. En revanche, le client est responsable de ses applications, de ses données et du système d'exploitation.

PaaS (Platform as a service) : externalisation de l'infrastructure matérielle, des applications et des données

Le PaaS inclut les services de l'IaaS mais va encore plus loin : outre les serveurs, le stockage et les réseaux, le prestataire fournit également l'ensemble des applications middleware : système d'exploitation, base de données, serveur web... En d'autres termes, le client loue l'exploitation des serveurs et les outils intégrés.

SaaS (Software as a service) : la formule « tout compris »

Le SaaS est le service le plus connu du grand public. Le fournisseur s'occupe de l'installation, de la configuration, du fonctionnement et de la maintenance de l'interface. Le client paye en général un abonnement mensuel et peut directement utiliser la plateforme que le fournisseur met à sa disposition.

IaaS, PaaS, SaaS : quel modèle choisir ?

Le choix de la solution la plus adaptée à une entreprise dépend de ses besoins, de ses compétences et de son budget. Il va de soi que le SaaS est plus cher que l'IaaS. Certaines entreprises préfèrent garder la main sur leurs applications, d'autres (en particulier les néophytes en informatique) jugent préférable de les remettre partiellement ou totalement entre des mains expertes.

Le mode SaaS, l'art du prêt-à-naviguer

La plupart des entreprises abritent leur infrastructure matérielle (serveurs, réseau, stockage) dans un espace physique sur leur lieu de travail. Une telle installation nécessite de la place, du temps et de l'expertise. Pour une entreprise, le mode SaaS (Logiciel As A Service) revient à remettre les clés de son infrastructure à un tiers, un prestataire qui va se charger de toutes les tâches liées au réseau, au stockage, à la sauvegarde et à l'actualisation des fichiers. Ainsi, le client n'a plus besoin d'investir dans des serveurs et des applications pour héberger ses données.

Le mode SaaS, une formule tout compris

Contrairement aux autres modèles d'usage du Cloud computing (IaaS, PaaS), le mode SaaS suppose une totale prise en charge des logiciels, de la maintenance et de l'infrastructure. Le fournisseur gère les serveurs, le réseau, le stockage, le système d'exploitation, les bases de données et les applications du client. Les employés de l'entreprise et les autres collaborateurs peuvent accéder aux logiciels à distance 24h/24, grâce à une connexion Internet.

Les avantages du mode SaaS

- Une meilleure maîtrise du budget. Nombreux sont les chefs d'entreprise qui avouent ne pas connaître les coûts liés à l'informatique (serveurs, ordinateurs, licences, personnel, etc.). En payant un abonnement fixe dont le montant est préalablement défini, les dépenses sont mieux maîtrisées.
- Un gain d'espace. L'externalisation des serveurs libère un espace non négligeable, qui peut être réutilisé à bon escient.
- Gain de temps. En mode SaaS, l'entreprise déploie plus rapidement ses applications. Par ailleurs, elle peut se concentrer sur des activités à plus haute valeur ajoutée.
- Externalisation totale de l'infrastructure matérielle et des applications. L'entreprise n'a plus à se soucier de ses serveurs ni de ses sauvegardes ; elle peut se consacrer entièrement à son activité.
- Le mode SaaS offre par ailleurs aux travailleurs nomades une grande flexibilité. Un simple ordinateur, une connexion Internet et un mot de passe leur permettent d'accéder à leurs fichiers. Les informations sont quant à elles stockées dans des serveurs distants ultra sécurisés.
- La réduction des coûts, notamment sur la consommation électrique
- La reprise d'activité rapide en cas de faille du système et la récupération des données en cas de sinistre ;
- La maintenance et mises à jour assurées par le prestataire.



LES DOCUMENTS DE RÉFÉRENCE DU S.I. DE L'ÉTAT

un service proposé par numerique.gouv.fr



STRATÉGIE DU SI DE L'ÉTAT

URBANISATION DU SI DE L'ÉTAT

RÉFÉRENTIELS

[Accueil](#) > [Référentiels](#) > [Socle Logiciels Libres](#) > [Présentation](#)

SOCLE LOGICIELS LIBRES

LE LOGICIEL LIBRE ET LA MODERNISATION DU SI DE L'ÉTAT

La modernisation des systèmes d'information de l'Etat passe notamment par le développement des usages et technologies innovantes et créatrices de valeur pour les utilisateurs, et par la maîtrise des coûts, ce qui implique en particulier de développer la réutilisation et la mutualisation, et d'ajuster au mieux les dépenses d'acquisition. L'approche de l'Etat privilégie l'efficacité globale, en dehors de tout dogmatisme, pour lui permettre de choisir entre les différentes solutions, libres, éditeurs ou mixtes. C'est l'objet de la circulaire du 19 septembre 2012, signée par le Premier ministre, qui recommande les voies du bon usage du logiciel libre dans l'Administration.

LA CONVERGENCE VERS DES LOGICIELS PRÉCONISÉS

Pour dégager le maximum d'efficacité aussi bien économique qu'en terme de qualité, il convient d'utiliser le logiciel libre de manière concertée et coordonnée. Un cadre de convergence des logiciels à privilégier dans le développement des systèmes d'information de l'Etat, défini en 2012, est maintenu en concertation interministérielle. Il touche en priorité les systèmes les plus déployés, sur les serveurs comme sur les postes de travail. Ce cadre ne fait pas obstacle à l'innovation par essai de nouvelles souches, qui pourront aider à l'évolution du cadre. Ce cadre ne rend pas non plus obligatoire l'évolution adaptative des applications existantes non conformes. Par contre il définit des versions de référence à privilégier et indique les solutions à abandonner, avec des réserves éventuelles pour des contextes d'usage particuliers. Il participe ainsi à la convergence progressive des contextes d'exploitation et à la mutualisation de certains moyens. A ce titre il doit être intégré dans tous les cadres technologiques des ministères et pris en compte à l'occasion de nouveaux développements et de refontes majeures.

LE SOCLE INTERMINISTÉRIEL DE LOGICIELS LIBRES (SILL)

Co-construit par des communautés d'agents publics informaticiens de l'État, des opérateurs et des collectivités territoriales, le socle interministériel des logiciels libres est le catalogue de référence des logiciels libres répondant aux besoins des administrations françaises recommandés par l'État. Son périmètre - ne couvrant pas la totalité du système d'information (SI) de l'État - classe les logiciels par thématiques : poste de travail, gestion de parc, exploitation de serveurs et de bases de données et environnements de développements. Sous forme d'un tableau, il permet d'identifier rapidement le logiciel et la version préconisés grâce à un classement par fonctionnalité ou par cas d'usage. Il est également possible de consulter l'état d'avancement du statut d'un logiciel, selon qu'il est en cours d'observation, recommandé ou en fin de recommandation. Il est mis à disposition sans garantie de l'État. Il peut être utilisé librement et gratuitement par tous, à titre public, professionnel ou privé. Il peut être copié et diffusé sans restriction. Il est mis à jour annuellement.



Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | |
|----------------------------|---|--|--|--|--------------------|-----------------|--------|----------------|-------------|----------------|---------|---|-------------------|--|
| Conception & Développement | Aide au développement | Environnement de développement | | Spring Boot | | | O | | | | 2.X | | | |
| | Environnement d'exécution | | | OpenJDK | | | R | | | | | 8 | | |
| | Environnement de développement intégré (IDE) | | | Eclipse | | | R | | | | | | 4.9 | |
| | | | Outil et/ou plugin de génération de tout ou partie du code | Outil et/ou plugin de génération de tout ou partie du code | Visual Studio Code | | | R | | | | dernière version | | |
| | | | Accelero | | | | R | | | | | 3.7.4 | | |
| | | Gestion des Anomalies | Outil de remontée de bug | | Manitis BT | | | R | | | | 1.X | | |
| | | Gestion du code source | Outil de gestion des configurations (serveur) | | Git | | | R | | | | dernière disponible | | |
| | | | Dépôt d'artefacts | | Nexus | | | R | | | | 3.1 | | |
| | | Installation, Packaging, Diffusion et Distribution | Gestionnaire de paquets pour Node.js | | Npm | | | R | | | | Dernière version compatible avec la version nodeJS préconisée | | |
| | | | Outil de gestion des dépendances | | Yarn | | | O | | | | 1.12.3 | | |
| | | | Outil de gestion des dépendances entre les différents composants d'un projet et cycle de vie | | Maven | | | R | | | | 3.5.2 | | |
| | | Modeleur | Environnement de développement | | IS Designer | | | O | | | | 1.9.0 | | |
| | Outils d'analyse, de Modélisation et de gestion de Patrimoine | Outil de maquettage IHM (statique et/ou dynamique) | | Pencil | | | FR | | | | 3 | | | |
| | Qualité et sécurité du code source | Couverture du code | | Jacoco | | | R | | | | 0.8.2 | | | |
| | | Tableau de bord d'indicateurs de qualité | | SonarQube Plugins : FindBugs CheckStyle Pmd | | | R | | | | 6.7 | | | |
| | | Vérification de la | | Asqatasun | | | O | | | | docker | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | |
|----------------------------|-----------------------|--|---|-----------------------------|-----------------------------|-----------------|--------|----------------|-------------|----------------|---------|---------------------|-------------------|--|
| Test & Intégration | Serveur d'application | conformité de l'application aux règles d'accessibilité | | Tanaguru | | | O | | | | 5.0.3 | | | |
| | | Environnement de développement | | Tomcat | | | R | | | | 9.0 | | | |
| | Test & Intégration | Automatisation des tests | | | Serveur NodeJS | | | R | | | | 8 | | |
| | | Automatisation des tests Web | | | Squash TA | | | R | | | | 1.11 | | |
| | | Automatisation des tests Web | | | Selenium Server | | | R | | | | 3.x | | |
| | | Base de données | | poste développeur | Selenium IDE | | | R | | | | 3.4 | | |
| | | Framework de tests backend | | | H2 | | | R | | | | 1.4.197 | | |
| | | Génération / Gestion des jeux de données | | | CodeceptJS | | | O | | | | 2.0.4 | | |
| | | Gestion des campagnes de tests | | | Jailer | | | R | | | | 8.2.x | | |
| | | Gestion des campagnes de tests | | | Testlink | | | R | | | | 1.9.14 | | |
| | | Navigateurs | | poste développeur | Squash TM | | | R | | | | 1.17.1 | | |
| | | Outil d'aide à la livraison (dépôt, intégration continue...) | | | Chromium | | | R | | | | dernière disponible | | |
| | | Outil d'aide aux tests techniques | | | Jenkins | | | R | | | | 2.x | | |
| | | Outil d'anonymisation des données | | Tests orientés Web Services | SoapUI | | | R | | | | 5.4.0 | | |
| | | Outil d'injection afin tester les couches basses | | | ARX Data Anonymization Tool | | | O | | | | 3.7.1 | | |
| | | Outil de gestion des tests unitaires | | | Fitness | | | FR | | | | 20161106 | | |
| Outil de monitoring | | | DbFit | | | FR | | | | 3.2.0 | | | | |
| Reprise des données | | Outil d'automatisation de la reprise de données | Junit | | | R | | | | 5.2 | | | | |
| Robot de test / Injecteurs | | | Javamelody | | | R | | | | 1.74.0 | | | | |
| | | | Talend Open Studio for Data Integration (BASIC) | | | R | | | | 7.0.1 | | | | |
| | | | Jmeter | | | R | | | | 5.0 | | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | | |
|------------------------------------|----------------------------|---|-------------------------------|------------------------|-----------------|-----------------|----------|----------------|-------------|----------------|----------------------|---------|----------------------|-----|---|
| | Suite bureautique | Courrielleur | Courrielleur | LibreOffice | MPL2 | | R | ODF 1.2 | 2 | 6.1 | 6.1 | | X | | |
| | | | | Thunderbird | MPL2 | 0 | R | s.o. | X | 60 | 60 | | | X | |
| | messagerie agenda contacts | Courrielleur pour Android | liste de diffusion/discussion | Client de Messagerie | K-9 Mail | apache V2.0 | K-9 Mail | O | | n | | 5.600 | 0 | 0 | |
| | | | | | Sympa | | | O | | | | | | | |
| | | messagerie instantanée | Rendez-vous | | Rocketchat | | | R | | | | | | | |
| | | | | | Framadate | | | O | | | | | | | |
| | navigateur web | bloqueur des publicités et des pisteurs | correction grammaticale | Navigateur | Ublock Origin | GPL3 | Firefox | R | | | 1.18 | 1.18 | 1.18 | X | |
| | | | | | Grammlecte | GPL3 | Firefox | R | s.o. | 2 | 0.6.5 | 0.6.5 | | | X |
| | | Pour utiliser ses codes | recherche | Navigation | Firefox ESR | MPL2 | 0 | R | HTML | X | ESR 60 | ESR 60 | ESR 60 | 60 | X |
| | | | | | KeepFox | GPL V2.0 | Firefox | O | 0 | 0 | 0 | 2.5 | 2.5 | 2.5 | 0 |
| Qwant | | | | | Licence MIT/X11 | Firefox | R | | X | | 5 | 5 | | | |
| ProjectLibre | | | | | CPA | | R | POD et XML | X | 1.7 | 1.7 | | | | |
| visiophonie | Outils Visioconférence | | | Freeplane | GPL2 | | R | 0 | X | 1.7 | 1.7 | | X | | |
| | | | | JITSI | | | R | | | | | | Version Distribution | | |
| Intégration & Echanges | Serveur d'impression | Serveur d'impression | | Cups | | | R | | | | Version Distribution | | | | |
| | Serveur SMTP | Messagerie system | | Postfix | | | R | | | | Version Distribution | | | | |
| Logiciel Système et Virtualisation | Haute disponibilité (OS) | Haute Disponibilité | | Pacemaker – corosync | | | R | | | | Version distribution | | | | |
| | | | | CentOS (souche Redhat) | | | R | | | | | 7.6 | | | |
| | Système d'Exploitation | Distribution GNU/Linux | Services déconcentrés | Ubuntu – Eole | | | R | | | | 2.7 | | | | |
| | | | | Debian | | | R | | | | | 9 | | | |
| | Virtualisation serveur et | Hyperviseur | Virtualisation serveurs | | KVM | | R | | | | Version Distribution | | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | | |
|---|---|---|---------------------|--------------------------------|-------------------------|-----------------|--------|----------------|-------------|----------------|----------------------|----------------------|-------------------|---|---|
| Opérations | jusqu'à plateforme | laaS – 2 | Infonuage | OpenStack | | | R | | | | 0 | | | | |
| | | Virtualisation de serveurs | Infra virtuelle | OpenNebula | | | R | | | | 5.6 | | | | |
| | | conteneurs logiciels. | | Docker | | | R | | | | Version Distribution | | | | |
| | Outils système & virtualisation | Déploiement | | | SaltStack | | | R | | | | Version Distribution | | | |
| | | | | | Ansible | | | R | | | | Version Distribution | | | |
| | | | | | CONSUL | | | O | | | | Version Distribution | | | |
| | | orchestration | | conteneurs | Packer | | | O | | | | Version Distribution | | | |
| | | | | conteneurs | Swarm | | | O | | | | Version Distribution | | | |
| | | | | conteneurs | Kubernetes | | | R | | | | Version Distribution | | | |
| | déploiement gestion d'actif et de configuration | Affichage de GLPI pour terminaux mobiles et tablettes | | | Rundeck | | | O | | | | Version Distribution | | | |
| | | | | | Mobile | GPL2+ | GLPI | O | s.o. | X | 1.1.6 | 0 | 0 | 0 | |
| | | Automatisation de l'import OCSInventory-NG | | | OCS Inventory <i>ng</i> | GPL2+ | GLPI | R | s.o. | 0 | 01/05/04 | 0 | 0 | 0 | X |
| | | | | Gestion parc | WAPT | GPLV3 | | O | | | X | 1.6 Community | 1.6 Community | | X |
| | | | | <i>Uninstall</i> | GPL2+ | GLPI | R | s.o. | 0 | 0 | 2.5.1 | 0 | 0 | X | |
| Escalade de tickets | | | Gestion des tickets | Escalation | GPL2+ | GLPI | O | s.o. | 0 | 0.85+1.0 | 0 | 0 | X | | |
| Export en pdf des fiches GLPI | | | | <i>PDF (impression de pdf)</i> | AGPL3 | GLPI | R | s.o. | 0 | 1.4 | 0 | 0 | 0 | 0 | |
| Gestion de parc et suivi d'incidents | | | GLPI | GPL2 | 0 | R | s.o. | 0 | 9.3 | 0 | 0 | X | | | |
| Gestion des stocks et demandes par une entité différente de celles définies | | | Geststock | GPL2 | GLPI | R | s.o. | 0 | 1.0.0 | | | X | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | | |
|---|-----------|---|------------------------------|--|-----------------|-----------------|---------|----------------|-------------|----------------|---------|------------|-------------------|---|---|
| Orchestration & logique métier | | pour la délégation de gestion. | | | | | | | | | | | | | |
| | | Injection de données dans GLPI à l'aide de fichiers CSV | glpi | Data Injection | GPL2+ | GLPI | R | s.o. | 0 | 2.6.4 | 0 | 0 | X | | |
| | | Inventaire, télédéploiement et découverte du réseau | OCS Inventory NG serveur | | | GPL2 | 0 | R | s.o. | 0 | 2.3 | 2.3 | | X | |
| | | | Agent OCS | | | GPL2 | OCS | R | s.o. | X | 2.3.1.3 | 2.3.1.3 | | X | |
| | | Notifications supplémentaires à celles incluses dans GLPI | Gestion parc | FusionInventory | | | AGPL3+ | GLPI | O | s.o. | 0 | 9.1+. 1 | 0 | 0 | 0 |
| | | | | Additional Alerts | | | GPL2+ | GLPI | O | s.o. | 0 | 1.9.0 | 0 | 0 | X |
| | | | | Behaviors (Compartements) | | | AGPLV3+ | GLPI | R | s.o. | 0 | 02/01/01 | 0 | 0 | X |
| | | Rapports supplémentaires à ceux inclus dans GLPI | | | | AGPL3 | GLPI | R | s.o. | 0 | 1.12 | 0 | 0 | 0 | |
| | | Serveur de services web permettant à une application externe d'interroger et de piloter GLPI. | | | | | GPLV2+ | GLPI | O | s.o. | 0 | 1.8 | 0 | 0 | |
| | | service level management | | Affichage graphique des délais de prise en compte des incidents + indicateurs sous forme de rapports | | | GPL2+ | GLPI | O | s.o. | 0 | 0 | 0 | 0 | 0 |
| | | | | Plugin GLPI-Survey (questionnaire) | | | AGPLV3+ | GLPI | O | | | 9.3.1.0 | 9.3.1.0 | | |
| | | Supervision / Hypervision | | Supervision Infrastructure | Infra virtuelle | Centreon | | | R | | | | 2,8 | | |
| | | | | Supervision Infrastructure et composants | Infra virtuelle | Shinken | | | R | | | | 2.4.3 | | |
| synchronisation réplication déduplication | | Synchronisation Sauvegarde | | | GPL3 | 0 | R | s.o. | X | 10.6 | 10.6 | 0 | X | | |
| | | Forum | Utilisé au sein d'une forge. | PHPBB | | | FR | | | | 3.0.9 | | | | |
| | | Plateforme de développement | | GitLab Community Edition | | | R | | | | 11.X | | | | |
| Orchestration & logique métier | | Portail de gestion de projet | | | | | R | | | | 3.X | | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

Socle interministériel des logiciels libres 2019

| SECTEUR | COMPOSANT | FONCTIONNALITÉ | CAS D'USAGE | LOGICIEL | LICENCE | LOGICIEL PARENT | STATUT | FORMAT ASSOCIÉ | Win X86/x64 | GNU/Linux MIMO | Version | ANDROID | VERSION FRANÇAISE | |
|------------|------------------------------|------------------------------------|------------------------|---------------------|----------------------|-----------------|--------|----------------|-------------|----------------|----------------------|--------------------------|-------------------|--|
| Réseau | moteur SIG | informations géographiques | | Umap, OpenStreetMap | | | O | | | | | | | |
| | | Système d'information géographique | | Qgis | GPL | | R | | X | 3.4 | 3.4 | | X | |
| | outil collaboratif | blogue | | | WordPress | | | O | | | | | | |
| | | enquête | | | Limesurvey | | | O | | | | | | |
| | | forum | | | Discourse | | | R | | | | | | |
| | | microblogue | | | Mastodon | | | O | | | | | | |
| | | partage de fichiers | | | NextCloud | | | O | | | | | | |
| | | rédaction collaborative | | | LibreOffice en ligne | | | O | | | | | | |
| | | wiki | | | MediaWiki | | | O | | | | | | |
| | | Load Balancer | | | HAProxy | | | R | | | | Version Distribution | | |
| Sauvegarde | Pare-feu – Réseau | Load Balancer | | Eole AMON | | | R | | | | 2.7 | | | |
| | | Pare-feu réseau et web | Services décentralisés | | | | R | | | | | | | |
| | Serveur Web & 'Reverse Proxy | cache web | | | VARNISH | | | R | | | | Version Distribution | | |
| | | proxy | | | SQUID | | | R | | | | Version Distribution | | |
| | | Reverse Proxy | | | Nginx | | | R | | | | Version Distribution | | |
| | | Serveur Web & Reverse Proxy | | | Apache | | | R | | | | Version Distribution | | |
| Sécurité | Authentification | Sauvegarde Serveurs | Services décentralisés | BAREOS | | | R | | | | Version Distribution | | | |
| | | Antivirus : Orienté serveur | Serveur Bureauitique | ClamAV | | | R | | | | Version Distribution | | | |
| | Annuaire | Annuaire | | OpenLdap | | | R | | | | 2.4 | | | |
| | | Gestion de mots de passe | | OpenLdap | 0 | | O | | | | 0 | | | |
| | IAM | SSO | IAM | | KeepPass | GPL2 | 0 | R | X | 2.3 | 2.4 | Keepass2 Android Offline | X | |
| | | | SSO | | KEYCLOAK | | | O | | | | 4 | | |
| | | | | LemonLDAP:NG | | | R | | | | Version Distribution | | | |

Les lignes en *italique* correspondent à des extensions, des modules complémentaires ; le logiciel parent est alors indiqué dans la colonne « Logiciel parent ».

Statut

R = recommandé
O = en observation
FR = en fin de recommandation

Colonne Windows

2 = versions x86 et x64
x = non précisé

Colonne GNU/Linux

version distribution = version courante de la distribution GNU/Linux utilisée
i = inutile ; fonctionnalité existante nativement

PROTECTION DES DONNÉES ADOPTÉZ LES 6 BONS RÉFLEXES



1 NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF



Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».

Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

4 FIXEZ DES DURÉES DE CONSERVATION



Vous ne pouvez pas conserver les données indéfiniment.

Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi. Elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

2 SOYEZ TRANSPARENT



Les administrés doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

5 SÉCURISEZ LES DONNÉES ET IDENTIFIEZ LES RISQUES



Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques. Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données. Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

3 ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES ADMINISTRÉS



Vous devez organiser des modalités permettant aux administrés d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

6 INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE



La conformité n'est pas gravée dans le marbre et figée.

Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en œuvre. Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.

La stratégie du « Cloud au centre »



Cadre de la stratégie interministérielle :

- 2018 : l'affirmation d'un SI de l'Etat (décret du 25 octobre 2018) et l'amorce d'une stratégie autour de l'informatique en nuage « cloud computing » (circulaire du 8 novembre 2018).
- La doctrine 2021-2022 « cloud au centre »

Les règles pour l'hébergement des futurs SI :

- Le **principe** « cloud au centre » implique que les futures applications devront être hébergées sur le Cloud.
- Par **exception**, les projets visant un choix hors Cloud devront être justifiés

Enjeu 1 : transformation numérique de l'Etat

Le Cloud computing est vu comme un facilitateur du changement de pratiques dans la production de services numériques (agilité, scalabilité, devops, développement continu)

Enjeu 2 : souveraineté et sécurité numérique de l'Etat

Le Cloud computing ne doit pas entraver l'autonomie de prise de décision, ni d'action de l'Etat, pas plus que sa sécurité numérique. L'Etat doit maîtriser ses données et ses traitements

Enjeu 3 : opportunité industrielle pour l'Etat français et l'Europe

L'adoption du Cloud computing par la sphère publique doit être une opportunité pour l'écosystème français et européen, et permettre aux acteurs publics d'accéder à une offre compétitive au niveau européen sinon mondial

Le Cloud interne de l'Etat dit « C1 »



C'est quoi ?

Des **infrastructures entièrement maîtrisées** par l'Etat :

- Hébergement
- Ingénierie
- Exploitation
- Supervision

Des offres portées sur le **RIE**, garant de la continuité de l'Etat.

Une offre Cloud C1 proposée par deux ministères :

- Le MI = offre **Cloud PI** (+ niveau de sécurité « Diffusion restreinte »)
- Le MINEFI = offre **NUBO** (associé au visa de sécurité SecNumCloud)

Avantages & inconvénients

Les + :

- Ouverture complète en interministériel sur le RIE
- Possibilité de mettre en place l'administration et l'exploitation par les équipes DNUM selon l'offre souscrite
- Cloud PI : niveau de sécurité « Diffusion restreinte »
- Des offres qui continuent de s'enrichir... pour le **Cloud PI Gen2, bientôt** :
 - une couche d'orchestration de conteneurs ;
 - De nouvelles capacités de stockage ;
 - Des perspectives en matière de calcul hautes performances et d'intelligence artificielle (GPU)
 - De nouveaux outils logiciels accessibles en tant que service pour faciliter le développement des applications
- Un modèle non commercial (pas soumis aux mêmes risques qu'une société)

Les - :

- Seulement 2 offres de Cloud C1
- Manque de services associés par rapport à certaines offres externes

L'option C3 sécurisée dit « C3 sécurisé »



C'est quoi ?

Des offres externes sécurisées grâce au visa de sécurité SecNumCloud et au label « Cloud de confiance »

- Garanties sur les compétences du prestataire, de son personnel, sur la qualité de la prestation
- Garanties sur la protection des données avec la localisation des infrastructures en Europe et le portage des offres Cloud par des acteurs européens
- Liste mise à jour mensuellement <https://www.ssi.gouv.fr/liste-produits-et-services-qualifies>

Avantages & inconvénients

Les + :

- Confiance pré-établie à l'égard du prestataire en matière de bonnes pratiques de sécurité relevant de l'hygiène informatique
- Certification sur les performances
- Une protection technique et juridique maximale pour la protection des données
- Raccordable au RIE (sans résilience)

Les - :

- Toutes les offres commerciales ne sont pas certifiées par l'ANSSI
- Tâches d'administration et d'exploitation relevant du client sans possibilité de délégation à la DNUM
- Le projet et le contrat doivent permettre la réversibilité et la portabilité multi-clouds du traitement applicatif

L'offre de cloud externe dit « C3 »



C'est quoi ?

- Des offres « sur étagère » disponible via la centrale d'achat **UGAP**
- Hébergement des SI hors RI, avec des interconnexions au RIE selon les offres
- Certaines offres vont vers un niveau de sécurité SecNumCloud

Avantages & inconvénients

Les + :

- Offres à l'état de l'art, sans prérequis de sécurité et de souveraineté
- Aucune contrainte liée à la sécurité ou à la souveraineté
- Flexibilité / gains opérationnels

Les - :

- Pas de raccordement au RIE (qui paraît peu probable)
- Cloisonnement des données
- Aucune possibilité de déléguer les tâches d'administration et d'exploitation ; le client doit l'assurer si elle veut une disponibilité H24
- Le projet et le contrat doivent permettre la réversibilité et la portabilité multi-clouds du traitement applicatif

Quelle offre Cloud choisir ?

Quelle offre Cloud correspond le mieux à votre besoin, à votre produit ?

Nous avons résumé dans le tableau ci-dessous les caractéristiques principales de chacune des offres de cloud. Parmi ces critères, la compatibilité avec des données sensibles ou personnelles, et le caractère essentiel du service rendu par le produit sont les facteurs indispensables à prendre en compte.

Caractéristiques des offres Cloud

| | CLOUD INTERNE | CLOUD COMMERCIAL | |
|--|------------------------|-------------------------------|-------------------------------------|
| | | CLOUD COMMERCIAL DE CONFIANCE | CLOUD COMMERCIAL GÉNÉRIQUE |
| Étendue du catalogue | | | |
| Adaptabilité des modèles économiques | | | |
| Compatibilité données sensibles | | | |
| Compatibilité services essentiels | | | |
| Compatibilité données personnelles non sensibles | | | |
| Certification HDS | | Selon le fournisseur | Selon le fournisseur |
| SecNumCloud | Garanties équivalentes | | |
| Droit exclusivement applicable | Union européenne | Union européenne | Selon le fournisseur |
| Haute résilience | | | |
| Localisation possible des données | France | France Union européenne | France Union européenne Monde |
| Expositions possibles des services | RIE * / Internet | Internet | Internet |
| Accès à l'espace d'administration | RIE * | Internet | Internet |

Principaux critères de choix

* RIE : Réseau interministériel de l'État

LA DÉMARCHE D'HOMOLOGATION DE SÉCURITÉ AU MINISTÈRE



Imprimer

Mis à jour : 15 avril 2021



Quoi de commun entre la mise sur le marché d'un nouveau vaccin, l'ouverture au public d'un établissement accueillant du public ou la mise en service d'un système d'information de l'État ?

Ces événements doivent toujours être précédés d'une décision d'homologation par une autorité publique afin d'établir la confiance nécessaire face à des enjeux de sûreté ou de sécurité.

Dans le domaine du numérique, l'homologation de sécurité joue en quelque sorte le même rôle qu'une recette fonctionnelle mais pour la couverture des besoins de sécurité : c'est l'aboutissement d'un processus qui aboutit à la décision formelle par le responsable de l'entité concernée, d'accepter ou de refuser les risques (on parle alors de refus d'homologation) sur la base d'un dossier rigoureux.

Ce corpus documentaire est constitué à partir :

- des principes et méthodes définies par l'ANSSI[1] dans le RGS[2] compatibles avec la norme internationale ISO 27001 ;
- de l'application d'une démarche d'intégration de la sécurité numérique dans les projets appelée démarche DISSIP[3], spécifique au ministère. Définie par le SHFD en concertation avec la chaîne fonctionnelle SSI, cette démarche aboutit à une liste de livrables adaptés à la sensibilité du système d'information considéré.

Une démarche d'homologation comprend typiquement 4 étapes :

- une phase de planification dite de stratégie, essentielle pour le succès de l'homologation lors de laquelle on identifie le périmètre de l'homologation, les besoins de sécurité à couvrir, ainsi que toutes les parties prenantes concernées en allant de la direction générale, à la maîtrise d'ouvrage, à la maîtrise d'œuvre, à l'hébergeur, jusqu'au RSSI métier ;
- une phase d'analyse des risques reposant sur la méthode EBIOS[4] élaborée par l'ANSSI. Equivalent du cahier des charges fonctionnelles, celle-ci permet d'identifier les scénarios d'attaques opérationnels susceptibles de se produire et d'en évaluer la gravité et la vraisemblance ;
- une phase de décision et de suivi de la mise en œuvre de ce plan d'actions lors de laquelle l'autorité se prononce en commission d'homologation sur son acceptation des risques.

Fondée sur le principe d'amélioration continue, l'homologation vit avec son temps et n'a cessé d'évoluer pour rester pertinente et garder toute son efficacité. Ainsi depuis la fin de l'année 2020, nous mettons en œuvre au sein du ministère la 4^e version de la DISSIP afin de prendre en compte à la fois l'évolution du contexte réglementaire qui s'est considérablement durci en France et en Europe depuis 10 ans, ainsi que l'évolution inéluctable des organisations projets, avec notamment le recours de plus en plus prononcé à l'externalisation. Comme changements notables dans cette nouvelle DISSIP citons le passage à la dernière version d'EBIOS, EBIOS Risk Manager, l'introduction optionnelle de campagnes de bug bounty pour les audits ainsi que des nouveaux livrables qualifiés relevant par exemple des PRA/PCA.

Gageons qu'à l'avenir la démarche d'homologation continuera d'évoluer pour mieux prendre en compte les pratiques de gestion agile des projets et faciliter la capitalisation de nos connaissances sur les risques portés par nos systèmes d'information.

- [1] Agence Nationale de la Sécurité des Systèmes d'Information.
- [2] Référentiel Général de Sécurité.
- [3] Démarche d'Intégration de la Sécurité des Systèmes d'Information dans les Projets.
- [4] Expression des Besoins et Identification des Objectifs de Sécurité.
- [5] Prestataire d'Audit de la Sécurité des Systèmes d'Information.

La démarche d'intégration de la SSI dans les projets

La démarche d'homologation permet de s'assurer que la sécurité a été prise en compte dans le projet conformément aux besoins du métier.

- en identifiant le besoin de sécurité
- puis en mettant en place des mesures de maîtrise des risques
- et enfin, en évaluant les risques résiduels et leur compatibilité avec les besoins exprimés.

La démarche d'intégration de la SSI dans les projets est la méthode qui permet d'optimiser l'effort consacré pour y parvenir.

Les projets les plus critiques nécessitent bien sûr une analyse de risques formelle, via la méthode EBIOS pour définir les objectifs de sécurité. En fin de projet, des contrôles de conformité puis des audits intrusifs permettent de s'assurer de l'effectivité des mesures prévues.

Tous les projets n'ont cependant pas les mêmes enjeux et il est important de **ne pas consacrer davantage de ressources que nécessaires** sur les projets les moins critiques afin de pouvoir **déployer les moyens requis sur les projets qui le justifient.**

La DISSIP est la méthode qui permet de sélectionner la démarche SSI permettant de mettre en œuvre la sécurité adaptée.

Tout projet doit donc commencer par une étape commune incontournable, la note d'orientation.

Ce rapide QCM, rempli avec l'aide du RSSI, permet d'évaluer les enjeux et de sélectionner la démarche appropriée.

Cette démarche précise alors les jalons et les livrables SSI à intégrer au processus projet.

Des modèles de documents sont disponibles.

En fin de projet, l'ensemble de ces livrables forme le dossier d'homologation qui sera utilisé pour prendre la décision d'homologation.

Détails

Mis à jour : 22 mars 2021

Une analyse de risques demande des compétences spécifiques de méthodologie, une connaissance de l'état de l'art tant en terme de menaces que de solutions et, bien sûr, du temps. Il est donc vraisemblable que vous externalisiez la prestation.

Cet article décrit les points clés d'une prestation réussie.

Choix du prestataire

Contrairement à d'autres prestations SSI, il n'existe pas de label pour les prestataires d'analyse de risques. Pourtant, la méthode employée et l'expérience du consultant sont déterminantes sur la qualité des livrables et leur exploitabilité dans la suite du projet. Il convient donc de s'appuyer sur un prestataire spécialisé dans ce domaine.

- Un accord cadre interministériel permet de passer facilement des bons de commandes pour des prestations d'analyse de risques. Conclure un marché ayant le même objet serait par ailleurs contraire aux principes de la commande publique (principe d'exclusivité de l'accord cadre).
- Il reste possible, dans le cadre d'un marché plus global d'assistance à maîtrise d'ouvrage ou de conception d'un SI, de demander au titulaire de réaliser également une analyse de risque. Le prestataire doit être alors compétent sur les deux domaines, ce qui limite alors la concurrence.

En tout état de cause, il est important que la phase de réalisation d'un SI se base sur un cahier des charges intégrant les conclusions de l'analyse de risque (exigences de sécurité). Ainsi les soumissionnaires sont en capacité d'apporter une réponse sur la base d'un besoin parfaitement défini et l'Administration est en capacité de sélectionner l'offre la plus avantageuse en intégrant la dimension SSI.

La suite de cet article traitera du premier cas.

Pré-réunion

Cette réunion qui a lieu avant l'émission du bon de commande est importante afin de dimensionner la prestation commandée en fonction des enjeux du projet. Elle permet notamment de définir le nombre d'entretiens réalisés et de réunions d'étapes en cours de prestation. Sous dimensionnée, une analyse risque d'être trop superficielle pour être utile ou passer à côté d'informations pertinentes faute de pouvoir s'entretenir avec toutes les parties prenantes. Les réunions d'étapes permettent d'éviter les « effets tunnels » en s'assurant de la bonne compréhension tout au long de l'avancement. Les livrables attendus doivent être confirmés.

Il est indispensable de confirmer la méthodologie. EBIOS est la méthode retenue pour toute l'administration. Certains prestataires utilisent des adaptations de la méthode EBIOS. Avec un vocabulaire différent, des étapes accélérées ou sautées, les livrables fournis risquent d'être difficilement compréhensibles, exploitables ou révisables lors d'une ré-homologation (évolution du SI ou arrivée à échéance)

Réunion de lancement de la prestation

Cette réunion permet la validation du calendrier, des contacts pour les entretiens. Les interlocuteurs peuvent être différents de la réunion précédente qui avait un caractère plus commercial. Il est donc important de repréciser que la conformité EBIOS Risk Manager est impérative. Tout ce qui n'est pas conforme strictement doit être refusé. En cas de doute, n'hésitez pas à solliciter la section Maîtrise des risques du SHFD (shfd-smr@interieur.gouv.fr). Cette réunion doit permettre de définir les moyens d'échanges et de chiffrage des futurs livrables.

La prestation devra suivre les modules de la méthode :

1. Cadrage et socle de sécurité
2. Sources de risques
3. Scénarios stratégiques
4. Scénarios opérationnels
5. Traitement du risque

Relecture des livrables intermédiaires.

Chaque atelier s'appuie sur les conclusions du précédent. La validation de chaque atelier est donc importante pour ne pas revenir sur des points préalablement traités. Pour cela il est nécessaire que les livrables intermédiaires soient relus et validés par les parties prenantes pour s'assurer qu'il n'y pas d'écart avec les attentes, d'incompréhension, de sur ou sous estimation. Bien que ces échanges puissent être réalisés par fichiers et courriels (protégés en confidentialité), des réunions d'étapes sont fortement recommandées dès que le nombre d'acteurs est important.

Le pilote de la prestation (normalement le RSSI) doit absolument s'assurer que figurent :

- les métriques et hypothèses retenues
- les valeurs métiers
- les événements redoutés
- la revue aux référentiels du socle de sécurité
- les **sources de risques et leurs objectifs visés**
- les **scénarios de risques stratégiques et opérationnels**
- les risques **bruts, actuels** et **cibles**
- les mesures de sécurité

Cette liste est non exhaustive mais comprend la plupart des points de divergence habituellement constatés. Le strict respect du vocabulaire est essentiel.

Le détail de chaque atelier de la méthode EBIOS Risk Manager est disponible sur le site de l'ANSSI : <https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/>

Le risque brut est l'estimation du risque en absence de mesure, le risque actuel prend en compte les mesures existantes et le risque cible prend en compte les mesures identifiées dans l'atelier 5 de l'analyse. Il est important que l'analyse de risques fasse apparaître ces deux notions. Ainsi, le projet peut s'adapter aux changements internes (ex changement de stratégie d'hébergement) ou externes (ex: remise en question d'une mesures de sécurité transverse, obsolescence d'une brique de sécurité...).

Un élément est également indispensable, d'une part car il apporte des éléments pour les arbitrages à venir, et d'autre part car il prévient les raccourcis tentants (Le cas très classique d'un début d'analyse rigoureux conduisant de façon opaque à une liste de mesures génériques qui ne sont pas forcément nécessaires et suffisantes dans le cadre étudié) : les liens entre les mesures et les scénarios de risques qui permettra d'évaluer la progression de la maîtrise du risque au fil de la mise en oeuvre des mesures initialement prévues.

Les livrables sont construits sur la base d'échanges avec différents experts (métier, SIC, SSI...) mobilisés pour l'analyse. Il est essentiel que chaque choix ou valeur soit justifié afin qu'une relecture des documents permettent la compréhension immédiate des choix et évite de les remettre en cause un peu hâtivement quelques temps plus tard.

A noter : Si cet article insiste sur l'indispensable rigueur méthodologique sur laquelle il n'est pas question de transiger, EBIOS reste une méthode souple. Chaque atelier peut être traité avec une granularité et une exhaustivité qu'il convient d'adapter aux enjeux du projet. L'expérience du consultant est déterminante sur ce point.

En résumé :

Une analyse de risques doit être accessible pour un lecteur ne connaissant pas le SI ou le milieu de la SSI. Les étapes s'enchaînent de façon logiques, transparentes et reproductibles.