THEIVENDRAM Hariharani, TR3

RAPPORT PFMP N°4

23 janvier au 17 février 2023

BACCALAUREAT PROFESSI0NNEL SYSTEMES NUMREIQUES – RISC
(Réseaux Informatiques et Systèmes Communiquant)

Lycée Professionnel Gustave Ferrié

7 Rue des Ecluses St Martin, 75010 Paris

01 42 02 19 55

SOMMAIRE

I. REMERCIEMENTS

Il m'est agréable à remercier Mme. Patria AZZAM, ma mentor et collaborateurs en IT chez BNP Paribas et M. Cyril RIGHI, manager groupe SOC (Security Operation Center), pour m'avoir donnée l'opportunité de réaliser la première partie de mon stage parmi eux.

D'autre part, je remercie plus particulièrement Mme. Viktoria MIROSHNICHENKO, ma tutrice durant la première semaine et M. Pascal BOCQUET, mon tuteur durant les 3 dernières semaines, de m'avoir accueilli chaleureusement dans leurs groupes. Ils ont tenu le rôle de guide durant la cette insertion professionnelle. Ils ont tous su me rassurer et me donner les moyens de concrétiser des projets en autonomie, ainsi qu'en équipe à leurs côtés. Merci aux deux équipes pour son soutien et son écoute, chacun a su rendre mon stage plus agréable et instructif.

Je remercie par ailleurs M. GUILLEMEAU, mon professeur référent ainsi que tous mes enseignants pour toutes les connaissances qu'ils m'ont inculquées. Je souhaite que le travail réalisé soit à la hauteur de leurs espérances.

II. INTRODUCTION

Du 23 janvier au 17 février 2023, j'ai effectué ma 4e et dernière période de stage au sein de l'entreprise BNP Paribas, située à Montreuil, que j'ai réalisé dans le département SOC et OPS.

Plus largement, ce stage a été l'opportunité pour moi de comprendre mieux l'importance des exercices de crises cyber et les réponses aux incidents. Mes maîtres de stage étant très agréable, j'ai pu apprendre dans d'excellentes conditions.

L'élaboration de ce rapport a pour principale source, les différents enseignements tirés des tâches auxquelles j'étais affectées. Enfin, les nombreux entretiens que j'ai pu avoir avec les employés des différents services de la banque m'ont permis de donner une cohérence à ce rapport.

En vue de rendre compte de manière fidèle et analytique de la période passé au sein de la BNP Paribas, il paraît logique de présenter à titre préalable l'environnement informatique du stage. Enfin, il sera précisé les différentes missions et tâches que j'ai pu effectuer ay sein des deux départements, et les nombreux apports que j'ai pu en tirer.

III. PRESENTATION DE L'ENTREPRISE

a. Coordonnées

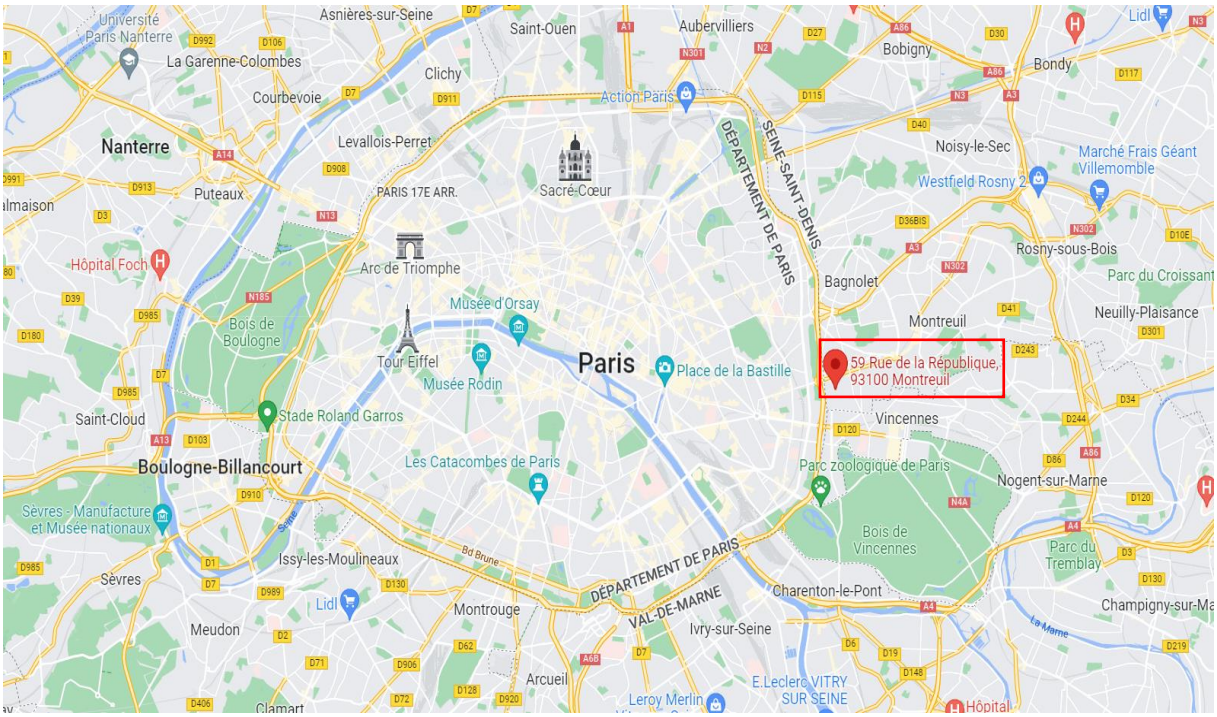
Nom : BNP Paribas – Valmy 1

Adresse : 59 Rue de la république, 93100 Montreuil

N° de téléphone : 06 33 30 36 66

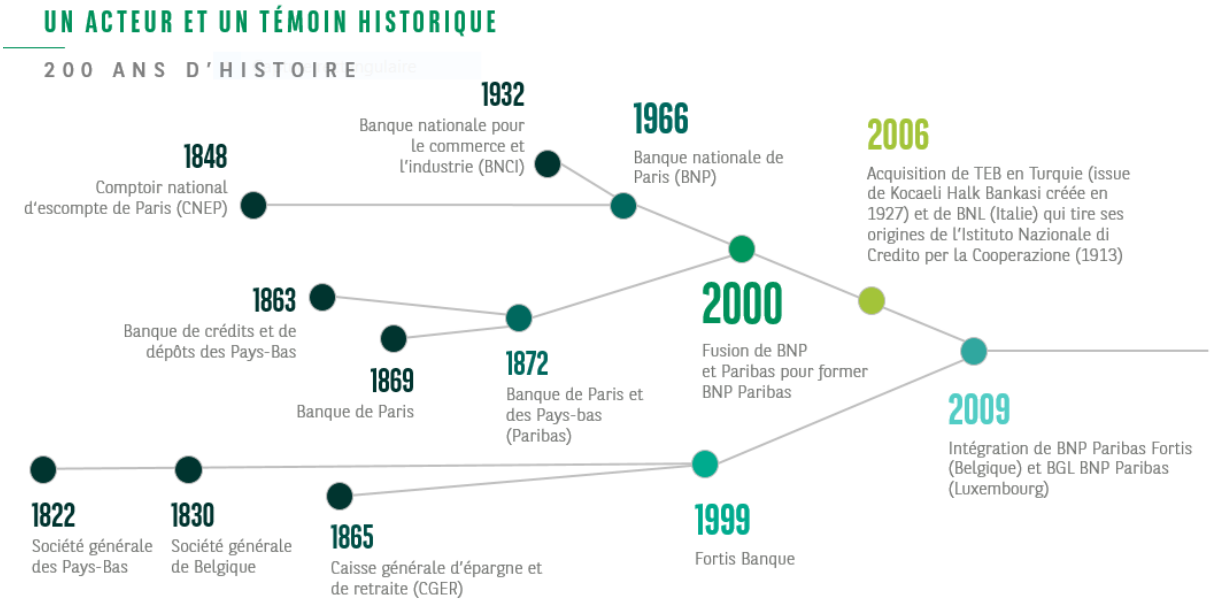
N° de Siret : 662 042 449 000 14

b. Situation géographique

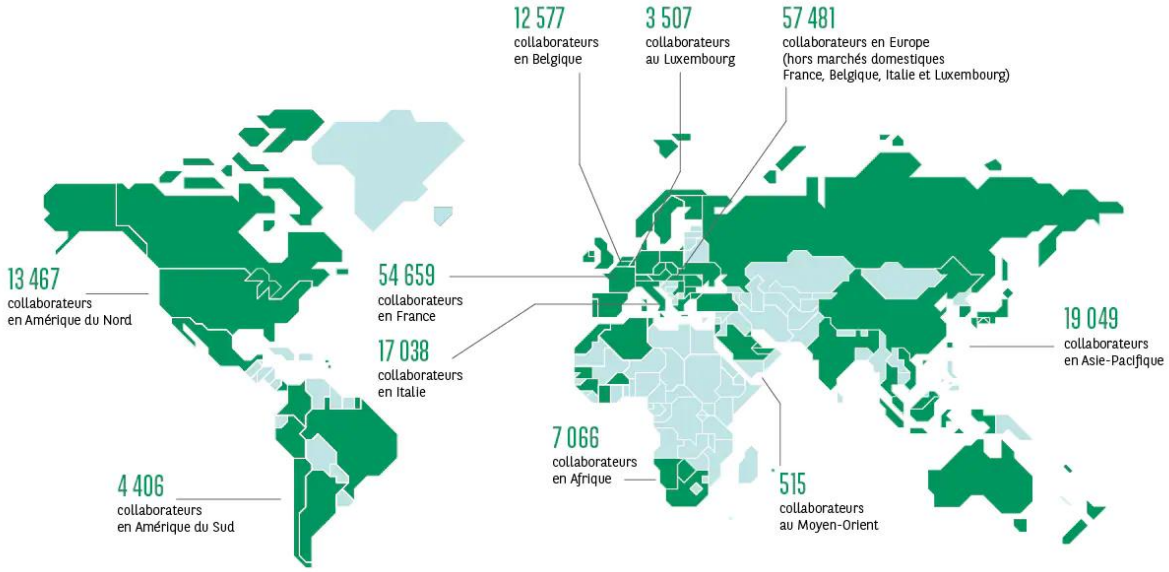


c. Histoire de BNP Paribas

L'histoire de BNP Paribas début au XIXème siècle, alors que les banques ancêtres du Groupe naissent et se développent. Entrainées par le formidables essor industriel de l'Europ, elles drainent l'épargne nécessaire au financement du développement économique. En remontant aux sources du Groupe, ce sont près de 25 siècles d'histoire du secteur de la banque, mais aussi d'histoire de l'Europe, voire du monde, que l'on peut parcourir.

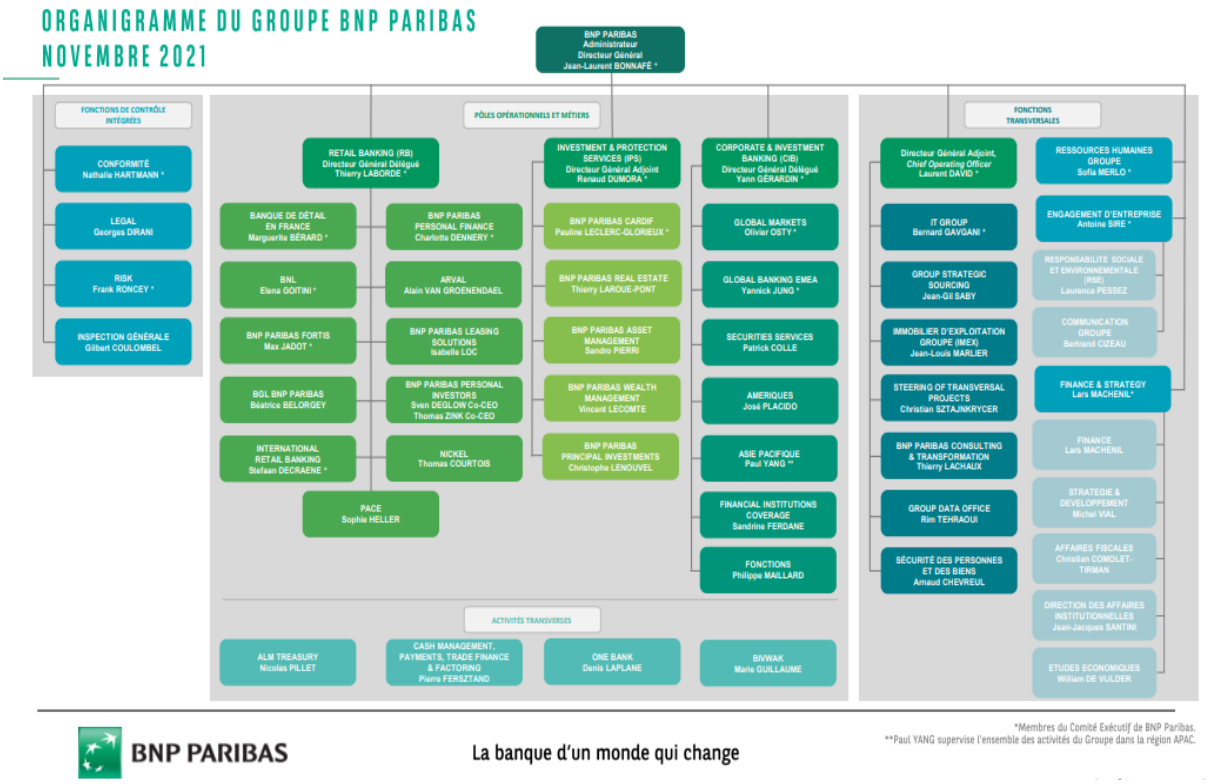


BNP Paribas est présent dans 68 pays avec plous de 193 000 collaborateurs dont près de 148 000 en Europe. Le groupe accompagne tous ses clients – particuliers, associations, entrepreneurs, grandes entreprises et institutionnels – dans la réussite de leurs projets grâce à ses solutions de financement, d'investissement, d'épargne et de protection.



Partenaires (exemple)	Concurrents (exemple)
• Handisport • Festival Cinema • Etc.	• Société générale • Crédit agricole • Etc.

d. Organigramme de l'entreprise



Dans cet organigramme, on y trouve tous les membres du comité exécutif de BNP Paribas. BNPP est une organisation très complexe. On peut voir aussi les différentes filiales de cette entreprise.

Chez BNPP, il y a 3 pôles opérationnels :

1. Domestic Markets (DM) qui regroupe :
   4 banques de détails dans la zone euros :

- BDDF en France
- Fortis en Belgique
- BNL en Italie
- BGL eau Luxembourg

4 métiers spécialisés :

- Arval : spécialisé dans la location de voiture
- Leasing : offre des solutions locatives et du financement
- PI (Personal Investigator) : propose des solutions d'épargne et du courtage en ligne
- Nickel : présente des services bancaires alternatif

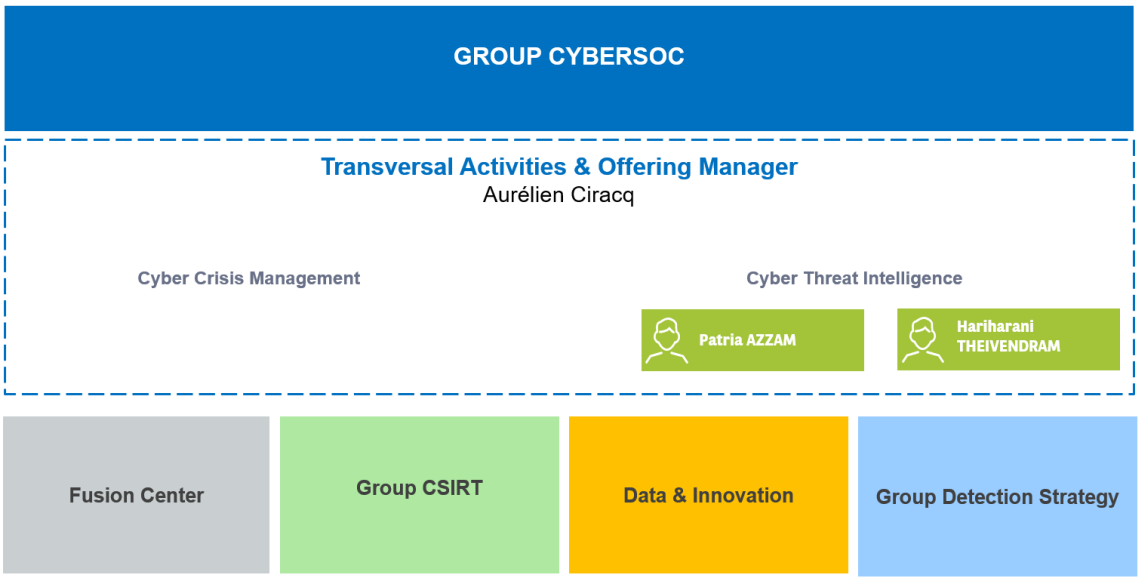
2. **International Financial Services (IFS) qui regroupe :**
   2 activités :

- PF (Personal Finance) : qui propose aux clients des solutions de crédit
- Cardif : qui propose des solutions d'épargne et de protection

3. **Corporate Investment Banking (CIB) qui offre des solutions sur mesure :**

- Corporate Banking : dans les domaines des financements, de la gestion de trésorerie et du conseil financier aux entreprises
- Global Markets : dans le domaine des marchés capitaux
- Securities Services : dans les services de conservation et administration de titres.

e. Organigramme de l'équipe SOC



Lors de mon stage, j'ai travaillé avec le groupe CYBER SOC. Voici les rôles des différentes activités du département :

- **Fusion center :** gère la gouvernance et gestion des risques de cyber-fraud (la fraude est une attaque commise dans l'intention de voler de l'argent à des clients ou à l'entreprise).

- **CSIRT (Computer Security Incident Response Team) :** s'occupe de faire la réponse aux incidents de sécurité cyber.

- **Data & Innovation :** pilote la collecte, la transformation et l'enrichissement des données dans le but d'augmenter les capacités d'investigation et de détection ainsi que d'automatiser tous les processus de pré et post détection.

- **Detection Strategy** : gère la gouvernance du programme Cyber SOC afin d'améliorer les capacités de détection du Groupe.

- **Transversal Activities & Offering Management** : définit et maintient la feuille de route des différents services du SOC. Cette activité inclut en plus :

    - **Cyber Threat Intelligence** : collecte d'information sur les incidents de cybersécurité qui ont touché d'autres entreprises pour améliorer la capacité de détection du Groupe.
    - **Cyber crisis management** : préparation d'un exercice d'entraînement, pour tester la procédure déjà défini afin d'être prêt lors d'une vraie attaque.

IV. COMPTE-RENDU D'ACTIVITES

Pendant mon stage, j'ai pu participer à divers :

Rencontres avec :

- Les membres de l'équipe SOC.
- Les membres de l'équipe OPS.

Au cours de mon stage, j'ai étudié divers sujets :

- **Cyber crisis management :** un exercice cyber est planifié pour que les collaborateurs puissent être prêt lorsqu'il y a une attaque. Cela permet de ne pas trop paniqué lors d'un vrai incident.
- **ITIL :** un référentiel de bonnes pratiques pour une gestion efficace des services IT les plus couramment utilisés.
- **DRP (Disaster Recovery Plan) :** est un document contenant l'ensemble des procédures et dispositifs à mettre en place en cas de sinistre pour réduire le temps d'arrêt du système informatique.

Formations :

J'ai participé aux formations ci-dessous qui sont obligatoire pour tous les employés :

- **Sensibilisation sur la cybersécurité**
- **Sécurisation des bureaux**

Le badge d'un collaborateur chez BNP Paribas est très important car c'est son passeport et il doit l'avoir toujours sur soi. Ce badge couvre plusieurs niveaux de sécurité :

- **Les accès physiques** : pouvoir badger à l'entrée du bâtiment, la circulation entre les étages.
- **Les accès logiques** : utiliser pour la connexion du poste professionnelle et authentification sur les applications de travail par le certificat présent sur la carte à puce. Lorsque l'on quitte le bureau, il faut toujours :
    1. **Verrouiller les fenêtres.**
    2. **Fermer la session de l'ordinateur.**

En retirant le badge, la session se verrouille automatiquement. Il est préférable d'attacher un antivol au cas où il y a une intrusion malveillante.

3. **Ranger les documents confidentiels dans les placards et fermer à clefs.**

Si on a plus besoin de certains documents (papiers), il faut les détruire.

V. ETUDE DE CAS

a. CCTP

- **Contexte :** dans le cadre de l'IT , je souhaite étudier l'ITIL.
- **Objectif à atteindre :** expliquer ce qu'est l'ITIL et son rôle.
- **Description fonctionnelle du besoin :** rédiger un document sur le rôle de l'ITIL.

b. Introduction

Qu'est-ce que l'ITIL?

L' ITIL (ou Information Technology Infrastructure Library), est un référentiel de bonnes pratiques pour une gestion efficace des services IT les plus couramment utilisés. Elle permet aux organisations et aux individus de passer à l'informatique optimiser :

- De fournir un ITSM (IT service management) en phase avec la vision et la stratégie globale de l'entreprise.
- D'améliorer l'efficacité et de réduire les coûts des prestations de services informatiques.
- De créer un point de contact entre le fournisseur de service et les utilisateurs.
- De guider les initiatives de transformation digitale.
- D'aider les entreprises à afficher une croissance plus rapide grâce à des processus définis, et soutenus par la technologie adéquate
- D'optimiser les ressources en révisant continuellement les processus existants

Les bénéfices de l'ITIL pour l'entreprise

L'ITIL permet aux entreprises d'être plus agiles, et constitue un excellent complément aux autres bonnes pratiques et aux cadres méthodologiques. Elle agit comme vecteur de la gestion efficace des services informatiques, et apporte de nombreux bénéfices, tels que :

- **L'amélioration de la qualité de service**

L'outil ITIL permet d'augmenter la qualité de service d'une entreprise, en améliorant l'efficacité de ses équipes et la qualité de leur travail, et en garantissant la cohérence entre les différents niveaux de service.

- **L’optimisation des coûts**

L’optimisation des coûts doit être effectuée en vérifiant que les ressources sont priorisées et utilisées efficacement, en fonction des demandes de l’entreprise et de ses clients.

- **La gestion optimisée des risques**

L’ITIL permet d’avoir un ITSM proactif, permettant ainsi d’éviter les incidents majeurs et de garder les risques sous contrôle. Grâce à un ITSM soutenu par l’IA (Intelligence Artificielle), il devient possible de prédire les événements futurs, en se basant sur les tendances passées.

- **L’alignement des objectifs de l’entreprise**

L’alignement stratégique est le processus à travers lequel une entreprise va repenser l’organisation et le fonctionnement de ses systèmes d’information et de production, pour les adapter de la façon la plus parfaite à sa stratégie.

ITIL v4

Depuis sa création par l’agence britannique de télécommunication en 1980, plusieurs versions de l’ITIL ont été publiées. Il a fallu en effet s’adapter à l’évolution des technologies d’information sur cette quarantaine d’années , ce qui a abouti à l’ITIL v4, sortie en février 2019.

ITIL v4 est une version améliorée de l'ITIL v3, plus adaptée à l'environnement technologique actuel. Tandis que l'ITIL v3 comporte 26 processus du cycle de vie des services, ces processus sont remplacés par 34 bonnes pratiques dans la version 4. Cette dernière version donne également la possibilité aux fournisseurs de services de personnaliser leurs processus.

Le référentiel ITIL consiste en cinq étapes qui font partie du cycle de vie du service. Chaque étape consiste en un ensemble de processus ou de fonctions qui sont alignés avec la structure de l’organisation informatique. Les sociétés choisissent d’adopter les processus qui conviennent à leurs équipes. L’ITIL est donc souple en termes d’adoption. Voici les étapes du cycle de vie du service ITIL.

- **Gestion des changements ITIL**

Les entreprises implémentent de nouveaux projets ou de nouvelles applications au quotidien. Il est important d'analyser les risques et les impacts avant d'effectuer les activités prévues. En fonction du risque et de l'impact, les validations des changements sont planifiées en incluant les parties prenantes appropriées. La gestion des changements enregistre chaque détail du changement qui est demandé pour permettre le bon suivi et l'audit. Elle est aussi essentielle afin que l'organisation puisse déployer efficacement les nouvelles implémentations sans qu'il y ait de période d'indisponibilité. La revue post implémentation est effectuée pour garder le contrôle.

- **Gestion des incidents ITIL**

Les utilisateurs s'attendent à observer des opérations harmonieuses, sans aucune perturbation. Toutefois, dans la réalité, il s'agit d'un défi à relever avec la complexité des composants de l'infrastructure et des applications disponibles. Une approche proactive de la gestion des incidents permet d'éviter la redondance des tickets et également d'éliminer l'apparition d'incidents majeurs. L'automatisation gère la classification et l'allocation des tickets afin que les agents du centre de services puissent se concentrer sur des activités à priorité plus élevée. La gestion des incidents ITIL fonctionne en relation étroite avec la base de données de gestion des configurations (CMDB) pour associer l'actif relatif à l'incident.

- **Gestion des problèmes ITIL**

Les problèmes répétitifs sont gérés par l'équipe de gestion des problèmes qui analyse la cause première et trouve une solution permanente. Le gestionnaire de problèmes effectue l'analyse de la cause première et suggère une solution de contournement jusqu'à ce qu'une solution permanente soit déployée. La gestion proactive des problèmes est adoptée par un grand nombre d'organisations pour éviter tout dommage éventuel qui serait causé par des pannes majeures et pour garantir la disponibilité du service. Il est recommandé de bien comprendre la différence entre la gestion des incidents et la gestion des problèmes pour attribuer clairement les rôles et les responsabilités.

L'ITIL est le Système de Valeur des Services

À travers le concept du système de valeur des services (SVS), et grâce à un bloc solide de 4 dimensions essentielles à la gestion des services, l'ITIL v4 met l'accent sur la flexibilité et sur l'efficacité.

Le système de valeur des services met en lumière l'influence des outils informatiques dans la création de valeur pour l'entreprise. Cet outil est composé de 6 éléments, qui peuvent être combinés pour s'adapter à toutes les configurations :

- La chaîne de valeur des services ITIL (planification, amélioration etc.)
- Les pratiques de gestion ITIL
- Les principes directeurs ITIL (ou objectifs)
- La gouvernance organisationnelle
- L'amélioration continue (initiatives, évaluations etc.)

Ce système de valeur des services (SVS) s'appuie sur 4 dimensions, qui doivent être prises en compte dans le cadre de chacun de ses 6 éléments :

- Organisations et personnes
- Information et technologie
- Partenaires et fournisseurs
- Flux de valeur et processus

Mise en place des pratiques ITIL

Le référentiel ITIL est composé de cinq étapes qui font partie du cycle de vie du service ITIL, et qui peuvent être ajustées à la structure de chaque organisation informatique. L'ITIL offre donc une certaine liberté d'adaptation aux fournisseurs de services. Ils pourront passer par ces cinq étapes dans l'ordre souhaité :

- **Stratégie des services IT**

Cette étape aide les organisations à se fixer des objectifs réalistes, et à développer une stratégie permettant de répondre aux besoins et aux priorités des clients.

- **Conception des services**

Cet aspect concerne la conception des processus ITIL, de la technologie, de l'infrastructure et de la gestion des services.

- **Transition des services**

Ici, l'accent est mis sur le maintien de l'état actuel du service pendant le déploiement des changements organisationnels, afin d'éviter la perturbation des services en cours.

- **Exploitation des services**

Cette étape permet de vérifier que les tâches opérationnelles quotidiennes s'effectuent sans encombre. Elle prend en charge la surveillance de l'infrastructure et des services reliés aux applications.

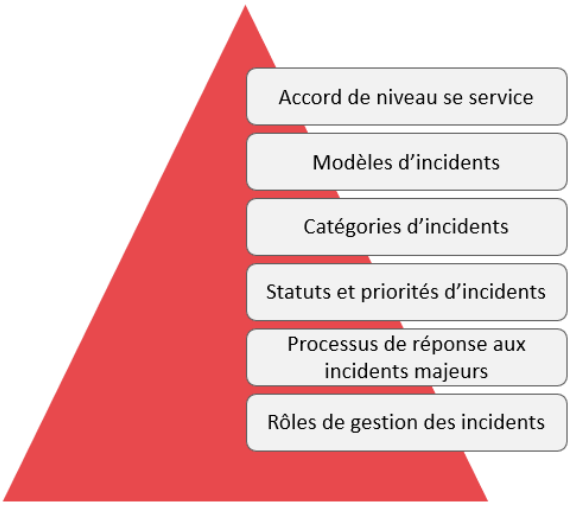
- **Amélioration continue des services**

L'amélioration continue des services fait partie de la vérification de la qualité qui a pour but l'amélioration continue des processus de façon progressive. Elle s'effectue tout au long du cycle de vie du service.

Définir la gestion

Dans cette situation, selon le référentiel ITIL, un incident peut être défini comme tout événement ne faisant pas partie du fonctionnement normal d'un service (ou d'un équipement), et qui cause ou peut causer une interruption ou une altération de sa qualité. En conséquence, la gestion des incidents permet de rétablir rapidement le fonctionnement normal du service et de minimiser l'impact de ceux-ci sur l'entreprise. L'action doit être menée tout en assurant le niveau de disponibilité et de service défini dans le contrat de services. A retenir qu'il s'agit de traiter les conséquences et non les causes.

Il ne faut pas confondre « gestion des incidents » et «gestion des problèmes». Il faut bien faire la distinction puisque l'objectif de la gestion des incidents est axé sur le niveau de l'utilisateur, elle sert à rétablir un service normal le plus rapidement possible, soit agir « en mode pompier ». Alors que la gestion des problèmes permet de résoudre la cause profonde des incidents dans le but d'empêcher que de futurs incidents ne se produisent.



La gestion des incidents

Classification des incidents

Les incidents sont classés en fonction :

- **De leur priorité (faible, moyenne et élevée)**

▫ **Faible** : n'interrompent pas les utilisateurs finaux, ils peuvent généralement terminer le travail malgré l'incident.
▫ **Moyenne** : sont des problèmes qui touchent les utilisateurs finaux, mais la perturbation est légère ou brève.
▫ **Elevée** : affectent un grand nombre d'utilisateurs finaux et empêchent le bon fonctionnement d'un système.

On constate le volume et l'ampleur d'un incident sur une entreprise en mesurant le nombre d'utilisateurs ou le nombre de systèmes touchés par un dysfonctionnement. Lorsqu'un incident présente un impact majeur pour un grand nombre d'utilisateurs, on considère qu'il s'agit d'un incident hautement prioritaire.

- **De leur type**

▫ **Matériel** : Problème de réseaux et autres pannes du système.

▫ **Logiciel** : Bug d'application ou problème de disponibilités de service.

▫ **Sécurité** : Accès non autorisé d'un domaine ou tout autre menace qui compromet et viole les données.

A noter qu'un problème de performances résulte souvent de n'importe quelle combinaison de ces domaines.

Priorité des incidents

Cette structure n'est pas systématique. De nombreuses entreprises adaptent cette hiérarchie et combinent les niveaux de support en fonction de leur capacité de ressources, de leur capacité financière et de leur « philosophie ».

- **Niveau 1 :**

Il fournit généralement un support ou une assistance rudimentaire grâce à la base de connaissances et de solutions identifiées Ce niveau comprend l'identification, l'enregistrement, la hiérarchisation et la catégorisation des incidents, ainsi que la décision de passer au niveau deux du soutien si besoin. Il tente donc de résoudre l'incident s'il en est capable, cela permet d'augmenter la satisfaction de l'utilisateur final. Par exemple : un ordinateur ne fonctionne pas, l'utilisateur demande assistance et on l'invite à vérifier si la barre de prise est bien branchée. Ce niveau gère aussi les réinitialisations de mots de passe et les dépannages informatiques.

- **Niveau 2 :**

Il passe par un processus similaire mais répond à des demandes plus complexes qui nécessitent de plus de formation, de compétences ou d'accès à la sécurité pour être satisfaites. Le support de niveau 2 peut rendre visite à l'utilisateur final si besoin, ce que le personnel du Service Desk ne peut pas faire.

- **Niveau 3 :**

Ce niveau concerne les incidents majeurs, ceux qui perturbent réellement le fonctionnement d'une entreprise, comme un problème de réseau. Les techniciens tentent de définir les causes profondes à l'aide de codes et de spécifications. Une fois la cause profonde identifiée, des correctifs aux incidents sont apportés, documentés puis communiqués aux techniciens de niveau 1 et de niveau 2 comme références futures.

- **Niveau 4 :**

Les incidents concernés par le niveau 4 relèvent de la responsabilité de services externalisés, soit les fournisseurs. Par exemple, si le logiciel Skype dysfonctionne, seule l'entreprise Microsoft pourra résoudre l'incident.

c. Problème : Comment fonctionne le processus de gestion des incidents ?

Étape 1: Identification de l'incident

Idéalement les incidents sont identifiés à un stade très précoce par la surveillance automatisée des évènements, donc avant même qu'ils n'entraînent des répercussions sur un utilisateur. Cependant, ce n'est pas toujours le cas. Parfois, les incidents sont identifiés par l'utilisateur touché qui le signale au Service Desk.

Étape 2 : Enregistrement de l'incident

Afin de tenir un registre historique complet, tous les incidents, quelle que soit la méthode utilisée pour les identifier et les signaler, doivent être enregistrés avec tous les détails pertinents, par exemple :

- Numéro incident
- Statut de l'incident
- Date de détection de l'incident
- Département
- Description de l'incident

- Pièce jointe (si besoin)

Étape 3 : Classification et priorisation de l'incident

L'attribution de la priorité est essentielle pour déterminer comment, quand et par qui l'incident sera traité. Une fois enregistré, il faut effectuer une catégorisation de l'incident pour déterminer sa prise en charge, et pour donner la priorité aux ressources d'intervention. Par exemple, si un incident est classé comme une panne de système, l'incident sera considéré comme à priorité élevée, et sera directement confié à un niveau supérieur afin de ne pas perdre de temps.

Vous renseignerez les éléments suivants :

- Catégorie de l'incident
- Périmètre de l'incident
- Source de détection
- Impact
- Priorité (critique, haute, moyenne, faible)

Étape 4 : Recherche et diagnostic de l'incident

Au cours de cette étape, l'équipe mènera son enquête sur l'incident, elle devra décrire le problème le plus précisément possible. L'incident devra être diagnostiqué par toutes les parties concernées et ceci jusqu'à ce que le problème soit résolu. L'enquête et le diagnostic comprendront les mesures suivantes :

- Établir la cause exacte de l'incident.
- Comprendre l'ordre chronologique des évènements.
- Confirmer l'impact complet de l'incident.
- Identifier tout évènement qui aurait pu le déclencher (un changement récent ou une action de l'utilisateur par exemple).
- Rechercher les erreurs connues dans la base de connaissances CMDB afin de trouver rapidement une solution de contournement ou de résolution.
- Rechercher s'il existe des évènements antérieurs similaires (des incidents déjà enregistrés, des erreurs fréquentes, chercher dans la CMDB, dans les journaux d'erreurs, dans les bases de connaissances des fabricants et fournisseurs associés, etc.

Étape 5 : Affectation ou escalade d'incident

Au cours de cette étape, l'entreprise devra mettre en pratique ce qui a été expliqué précédemment. Initialement, le technicien du service desk tentera de résoudre l'incident. S'il n'est pas en mesure de fournir une solution, l'incident sera élevé au niveau approprié de soutien (niveau deux ou trois).

Si d'aventure un incident s'intensifiait, l'escalade devrait se poursuivre dans la chaîne de gestion. Les cadres supérieurs devraient être avisés de la situation afin qu'ils puissent se préparer à prendre toutes les mesures nécessaires, comme l'allocation de ressources supplémentaires ou la participation de fournisseurs par exemple.

Étape 6 : Résolution de l'incident et restauration du service

Une fois l'incident résolu, la solution pourra être implémentée (assurez-vous bien de disposer des autorisations nécessaires pour le faire) et testée pour confirmer la récupération du service. Si tout fonctionne, le service confirmera que le service de l'utilisateur a été restauré au niveau SLA(Service Level Agreement) requis. C'est-à-dire adapté aux besoins du clients.

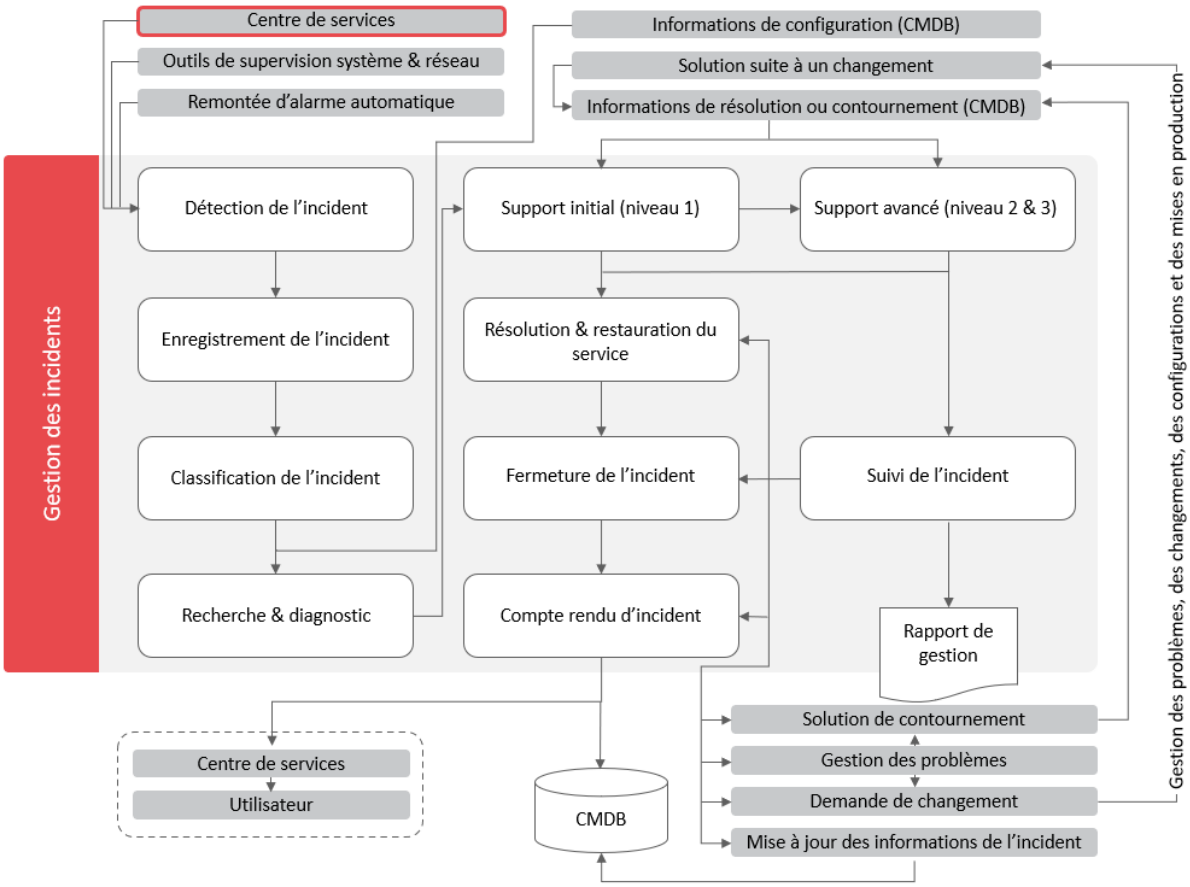
Étape 7 : Clôture de l'incident

Pour finir le service confirmera le correctif et fermera le ticket. Assurez-vous de recueillir une confirmation de bon fonctionnement de la part de l'utilisateur qui a déclaré l'incident avant de fermer le ticket.

L'analyste de l'incident devra rédiger le rapport d'incidence en s'assurant de décrire les éléments ci-dessous :

- Date de clôture effective
- Délai de traitement
- Source de l'incident : interne ou externe.
- Catégorie de l'incident
- Type d'incident
- Cause de l'incident
- Conséquence de l'incident
- Le ou les responsables du plan d'action
- Plan d'action d'amélioration continue

Enfin il faudra bien penser à mettre à jour la base de données.


Centre de services
Outils de supervision système & réseau
Remontée d'alarme automatique
Informations de configuration (CMDB)
Solution suite à un changement
Informations de résolution ou contournement (CMDB)
Gestion des incidents
Détection de l'incident
Support initial (niveau 1)
Support avancé (niveau 2 & 3)
Enregistrement de l'incident
Résolution & restauration du service
Classification de l'incident
Fermeture de l'incident
Suivi de l'incident
Recherche & diagnostic
Compte rendu d'incident
Rapport de gestion
Solution de contournement
Gestion des problèmes
Demande de changement
Mise à jour des informations de l'incident
Centre de services
Utilisateur
CMDB
Gestion des problèmes, des changements, des configurations et des mises en production

VI. SYNTHESE

Il va de soi que la différence entre le monde de l'école et celui de l'entreprise est très importante. Ce stage de 4 semaines au sein du groupe SOC et OPS et sur un site aussi important m'a permis de découvrir la réalité du monde de la sécurisation du réseau.

L'accueil de l'entreprise BNP Paribas étant bien préparé et détendu, cela m'a mis immédiatement en confiance avec les équipes. D'autant plus que mes tuteurs de stage m'ont apporté toute l'aide dont j'avais besoin. Une bonne ambiance règne dans les équipes et tous les personnels ont été très coopératifs et attentif à toutes mes questions. Le travail d'équipe est très important car tous les services sont liés et doivent communiquer entre eux.

Cette expérience est enrichissante tant du côté technique que du côté humain : c'était l'occasion de mener des projets, d'une manière totalement autonome avec une liberté de choix ainsi que d'acquérir des responsabilités, des connaissances, des capacités d'organisation, d'être précis et efficace et surtout constater des rapports humains.

Je remercie une fois de plus toutes les personnes que j'ai rencontrées pour m'avoir permis de mener à bien mes projets et de m'avoir accordé leurs confiances et leur sympathie durant cette période de stage.