PROJET PRINTCORP

Dossier technique par l'entreprise ReNewIT

écrit par SALLARD Axel

BRC Groupe 1 - Metz Numeric School

TABLE DES MATIÈRES

Liste des compétences mobilisées

Bloc 1 - Analyse des besoins et conception d'infrastructures systèmes et réseaux

- ☐ Analyser les caractéristiques et spécificités de l'entreprise (types d'activités, effectifs, localisation des acteurs, etc.) afin de cadrer le besoin en fonction des types d'utilisations.
- ☐ Établir et analyser un audit d'infrastructures systèmes et réseaux en mettant en place des indicateurs, interprétant la documentation et analysant les contrats de services en cours afin de réaliser un état des lieux de l'existant.
- ☐ Proposer des solutions en intégrant les aspects budgétaires et les contrats de services afin de répondre aux besoins de l'entreprise.
- ☐ Concevoir des infrastructures systèmes et réseaux dans un environnement hybride (Infrastructures propres à l'entreprise, cloud public et/ou cloud privé) en respectant les contraintes imposées par le système d'information (S.I.) pour bénéficier de la flexibilité offerte par les solutions cloud et fournir un service hautement disponible et sécurisé.
- ☐ Rédiger la documentation en tenant en compte les besoins des destinataires afin de formaliser une démarche qualité.

Bloc 2 - Implémentation, configuration et déploiement des systèmes et réseaux informatiques dans le respect des normes de sécurité

- ☐ Installer et paramétrer les services réseaux locaux ou à distance en vérifiant la conformité des installations par rapport aux cahiers des charges pour assurer la haute disponibilité et la sécurité du service.
- ☐ Installer et paramétrer des bases de données coté serveur (accès, partages) en vérifiant la conformité des installations par rapport aux cahiers des charges pour assurer la haute accessibilité et la sécurisation des données.
- ☐ Automatiser et industrialiser les procédures de déploiement et d'exploitation en adoptant une démarche DevOps, en vue d'optimiser les coûts, la rapidité de mise en œuvre et les performances des systèmes et réseaux.
- ☐ Paramétrer les dispositifs réseaux (serveurs, routeurs incluant les services de sécurité), en vue d'installer et de configurer les postes clients.
- ☐ Configurer les postes clients en réseaux, les services transverses et les services avancés, dans le but de faciliter leur administration et d'assurer la continuité et la sécurité du service.

Bloc 3 - Surveillance du bon fonctionnement, de la performance et de la sécurité des systèmes et réseaux informatiques

- ☐ Identifier les risques inhérents au système d'information et aux réseaux de l'entreprise, les différents types de rupture de charge et de menaces d'intrusion, en vue de configurer les alertes utiles à la surveillance des systèmes et réseaux.

- ☐ Concevoir une réponse globale et coordonnée aux alertes sur le système d'information, en impliquant les utilisateurs dans la démarche, afin de minimiser les dommages éventuels.

- ☐ Organiser les contrôles d'accès dans le cadre plus global de la sécurité des systèmes d'information et des réseaux, en cohérence avec les différentes catégories d'utilisateurs, afin de prévenir tous risques d'interventions inopportunes.

- ☐ Évaluer et mesurer en continu la performance des systèmes et réseaux au moyen d'indicateurs pertinents, en vue d'optimiser la qualité de service.

Bloc 4 - Gestion des incidents, opération de maintenance et gestion des évolutions des systèmes et réseaux

- ☐ Concevoir une organisation raisonnée des opérations de maintenance, de façon à préserver la continuité d'activité, afin d'anticiper sur les incidents et de faciliter leur gestion.

- ☐ Élaborer les parades adaptées aux menaces d'intrusion et de pertes de données, en vue d'assurer une gestion rapide et économe des incidents.

- ☐ Assurer l'amélioration continue des systèmes et réseaux de l'entreprise, en réalisant des audits réguliers de l'activité en vue de proposer et mettre en œuvre les solutions appropriées.

Project Summary

The PrintCorp project is not only about **upgrading IT systems**, it's really about giving the company a fresh start. PrintCorp decided to work with ReNewIt, an IT partner, to **modernize** its whole infrastructure and make it more secure, faster and easier to use for everybody.

The project is not just technical, it's also about people. Employees are trained, supported and they get clear documentation so they don't feel lost with the new tools. Security and reliability are very important, but the goal is also to make daily work smoother and less complicated.

To stay on track, the project follow the **Prince2 method** with milestones and deadlines. Cloud and local solutions are mixed together, so PrintCorp can have flexibility while keeping control on sensitive datas.

In the end, this transformation is more than technology — it's about helping PrintCorp grow, adapt and stay competitive. With the help of ReNewIt, the company is building an IT environment that workers can trust everyday, and that will support the future of the business.

Cahier des charges – Projet PrintCorp

Contexte

PrintCorp est une entreprise spécialisée dans la vente et la maintenance d'imprimantes professionnelles. Avec la croissance de ses activités, l'infrastructure informatique actuelle montre ses limites : lenteurs, risques de panne, sécurité insuffisante et outils trop dispersés. Ces difficultés freinent la productivité des équipes et compliquent la gestion quotidienne.

Objectif du projet

L'idée est de moderniser en profondeur le système d'information de PrintCorp afin qu'il soit :

- plus **fiable**,
- plus **sécurisé**,
- plus **simple à utiliser** pour les collaborateurs.

En d'autres termes, il s'agit de bâtir une infrastructure qui soutienne la croissance de l'entreprise, tout en garantissant la protection des données et la continuité de service.

Périmètre

Le projet couvrira plusieurs volets :

- La modernisation des serveurs et du réseau, avec une ouverture vers le cloud.
- Le renforcement de la sécurité, notamment sur la gestion des accès et la protection des données.
- La mise en place d'un meilleur suivi des incidents pour réagir plus vite et éviter les interruptions de service.
- La création d'une base documentaire claire et partagée pour centraliser les informations IT.
- L'accompagnement des utilisateurs, avec de la formation et de la sensibilisation à la cybersécurité.

Contraintes

Le chantier devra être réalisé sans bloquer l'activité de PrintCorp. Il faudra aussi tenir compte du budget et des délais (environ un an), tout en respectant les normes en vigueur. Enfin, les solutions choisies devront être évolutives pour suivre le développement de l'entreprise.

Livrables attendus

À la fin du projet, PrintCorp doit disposer :

- d'une nouvelle infrastructure fiable et sécurisée,
- d'outils de supervision et de gestion des incidents,
- d'une documentation claire et accessible,
- d'un plan de formation adapté aux équipes,
- et d'un rapport garantissant la conformité et la qualité du système déployé.

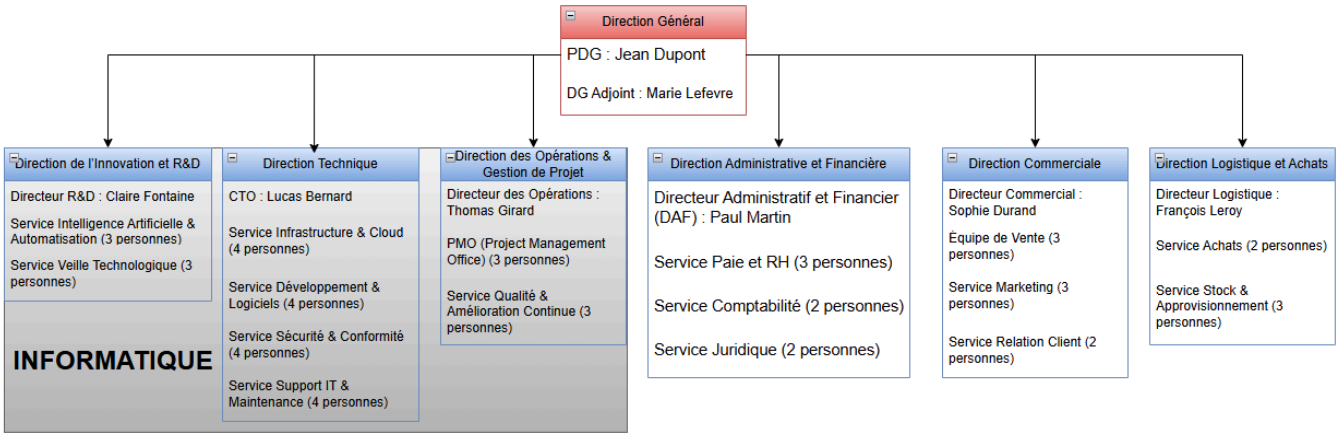
Introduction

ReNewIT est une entreprise spécialisée dans la fourniture de services pour l'implantation ou le renouvellement de parcs informatiques (ESN). Nous intervenons directement chez nos clients moyennant rémunération. Un audit de leur infrastructure informatique est réalisé à l'aide d'outils tels que NinjaOne, avec l'accord préalable du client. En collaboration avec ce dernier, nous établissons un cahier des charges détaillant les aspects du projet (coût, ressources, durée et date de livraison). L'ancien matériel est soit recyclé, soit reconditionné, faisant de ReNewIT un acteur engagé dans la gestion durable des équipements.

La société a eu un chiffre d'affaire annuel de : **1,5 millions d'euros**

L'entreprise possède 50 employés dans divers postes.

Voici un organigramme de la société :



I. Présentation de l'entreprise - Bloc 1

A. Historique de PrintCorp.

L'entreprise PrintCorp, spécialisée dans les **solutions d'impression** industrielle et de services digitaux.Fondée en 1998 à Paris, elle s'adresse principalement aux secteurs de la **logistique**, de la **production industrielle**, et du commerce de détail, où **l'efficacité** et la précision des impressions jouent un rôle stratégique.Elle a récemment ouvert trois nouvelles antennes internationales (New York, Berlin, et Singapour).Forte de sa présence sur cinq sites à travers le monde.

L'année dernière, PrintCorp a réalisé un chiffre d'affaires de 45 millions d'euros. 10% de cette somme ont été alloués au département informatique et investis dans le projet de restructuration de son infrastructure informatique (soit 4,5 millions d'euros).

Ses secteurs d'activité principaux sont :

- Solutions d'impression industrielle :
- Services numériques :

B. Présence géographique et organisation des sites.

L'entreprise est structurée autour de **cinq sites principaux** :

- **Siège social à Paris (France)** : Gestion stratégique, R&D, direction financière et IT.
- **Bureau régional à New York (États-Unis)** : Développement commercial pour le marché nord-américain, marketing, et support technique.
- **Centre logistique et de production à Berlin (Allemagne)** : Fabrication et gestion des stocks pour les clients européens.
- **Bureau régional à Singapour** : Développement des marchés asiatiques, support technique, et gestion administrative régionale.
- **Centre de données et de supervision à Montréal (Canada)** : Hébergement des infrastructures numériques globales, maintenance des systèmes IT, et gestion des sauvegardes.

C. Clients et partenariats.

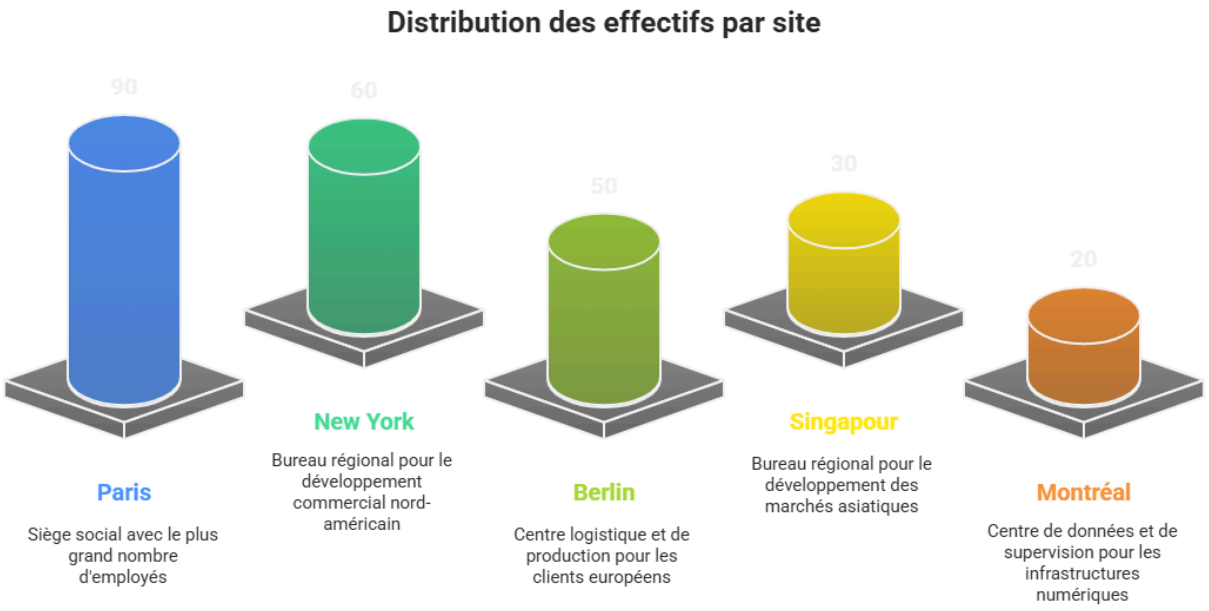
PrintCorp fournit des solutions d'impression optimisées pour la **logistique** (étiquettes et suivi des colis), **l'industrie manufacturière** (intégration en ligne de production) et le **commerce de détail** (tickets, étiquettes de prix, affichage numérique). Grâce à des partenariats avec des leaders technologiques, l'entreprise développe des solutions innovantes, connectées et évolutives, adaptées aux besoins de ses clients.

D. Mission sur l'avenir.

Durant les **5 prochaines années**, PrintCorp renforce son **infrastructure** IT avec le cloud et la cybersécurité. Elle développe des produits **intelligents** capables d'auto-diagnostic. L'entreprise mise sur l'innovation pour optimiser la maintenance de ses solutions. Elle investit dans des **technologies d'impression durables**. Son objectif est de rester compétitive tout en réduisant son impact environnemental.

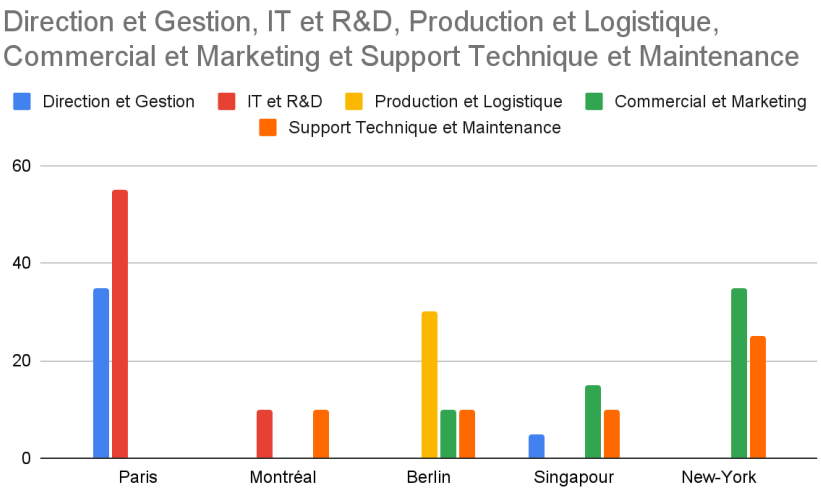
II. Effectifs et sites - Bloc 1

A. Répartition des employés par site.



B. Analyse des ressources humaines.

Voici une petite synthèse des différentes fonctions sur les sites :



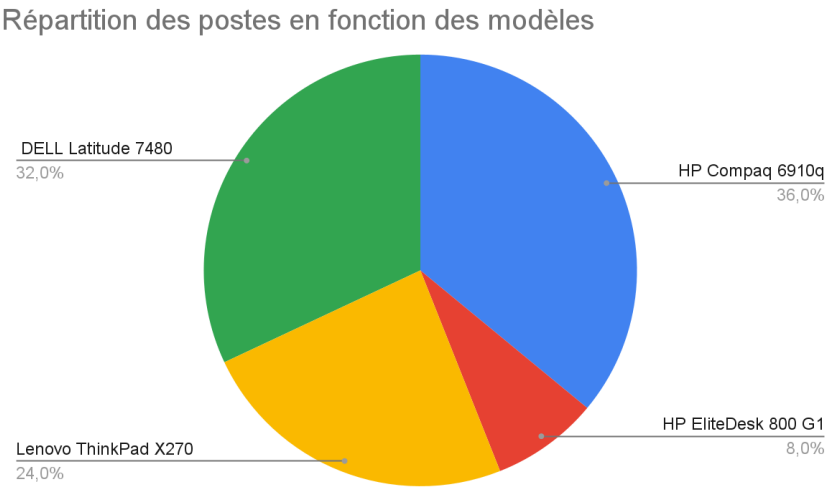
III. État actuel du système d'information - Bloc 1

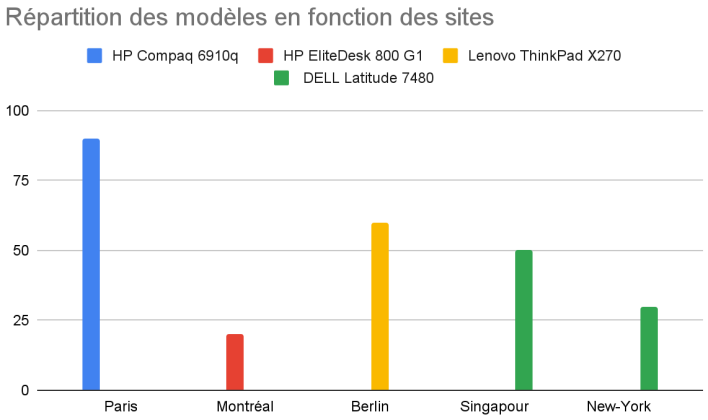
A. Infrastructure technologique existante.

L'entreprise nous à fourni un audit (en annexe page 42) fait par leurs soins .

Afin d'approfondir notre analyse du système d'information du client, un audit complet a été réalisé à l'aide de NinjaOne (comparatif en annexe 43), par notre entreprise. Cet audit a révélé une hétérogénéité du parc informatique. Pour plus de détails, voir annexe (page 47).

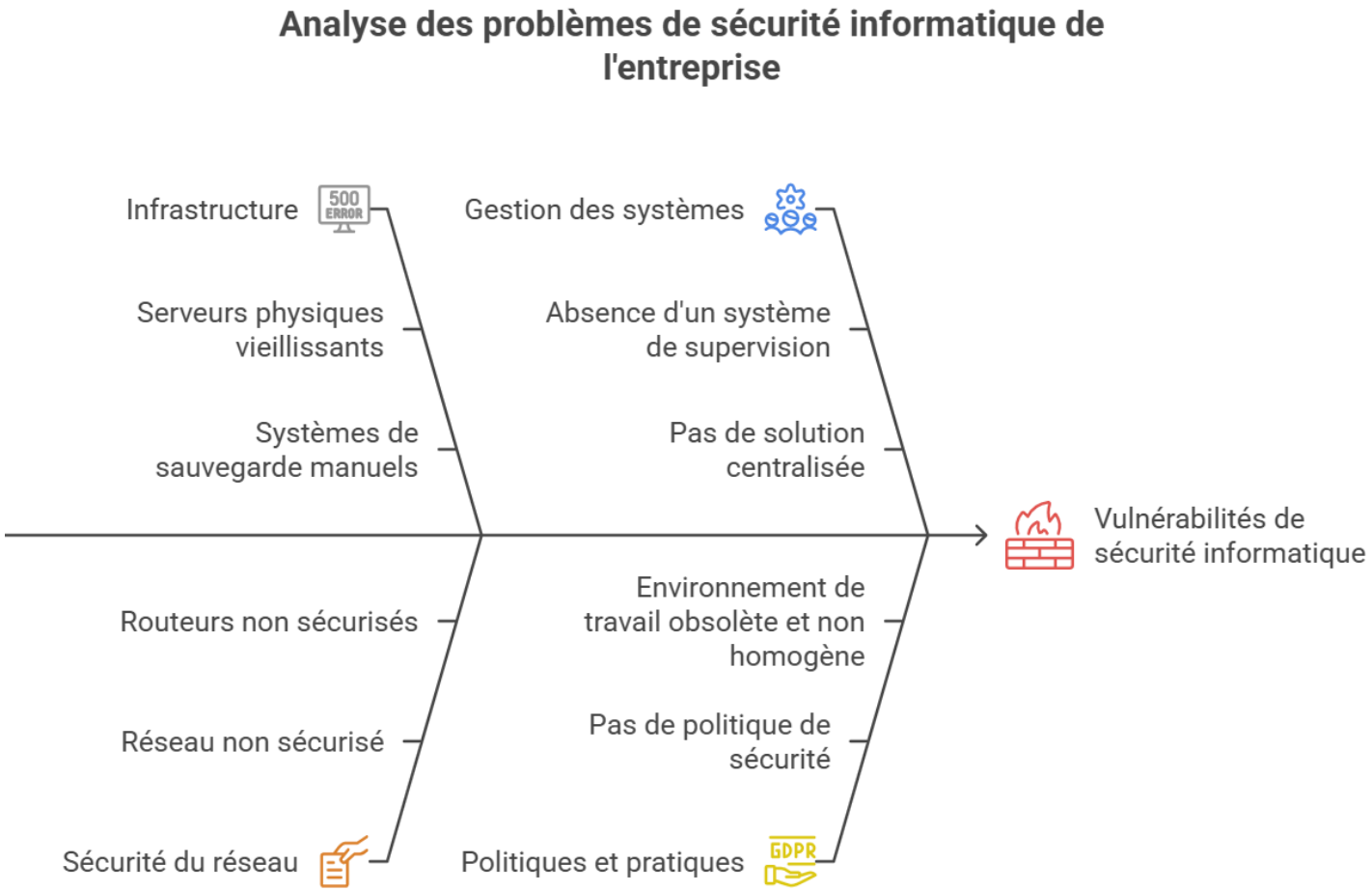
Sur les **250 postes clients**, nous avons identifié :





Ainsi que du matériel réseau (routeurs, switch, serveur, pare-feu) soit obsolètes soit inexistant. Cela prouve l'état déplorable de l'informatique de la société à l'heure actuelle.

B. Limites, problèmes et expérience utilisateurs.



L'audit révèle une infrastructure obsolète avec des serveurs vieillissants, un réseau non sécurisé et une absence de supervision. Les sauvegardes, l'accès aux fichiers et la collaboration manquent de solutions centralisées. La sécurité et la modernisation des outils sont insuffisantes, nécessitant une refonte complète.

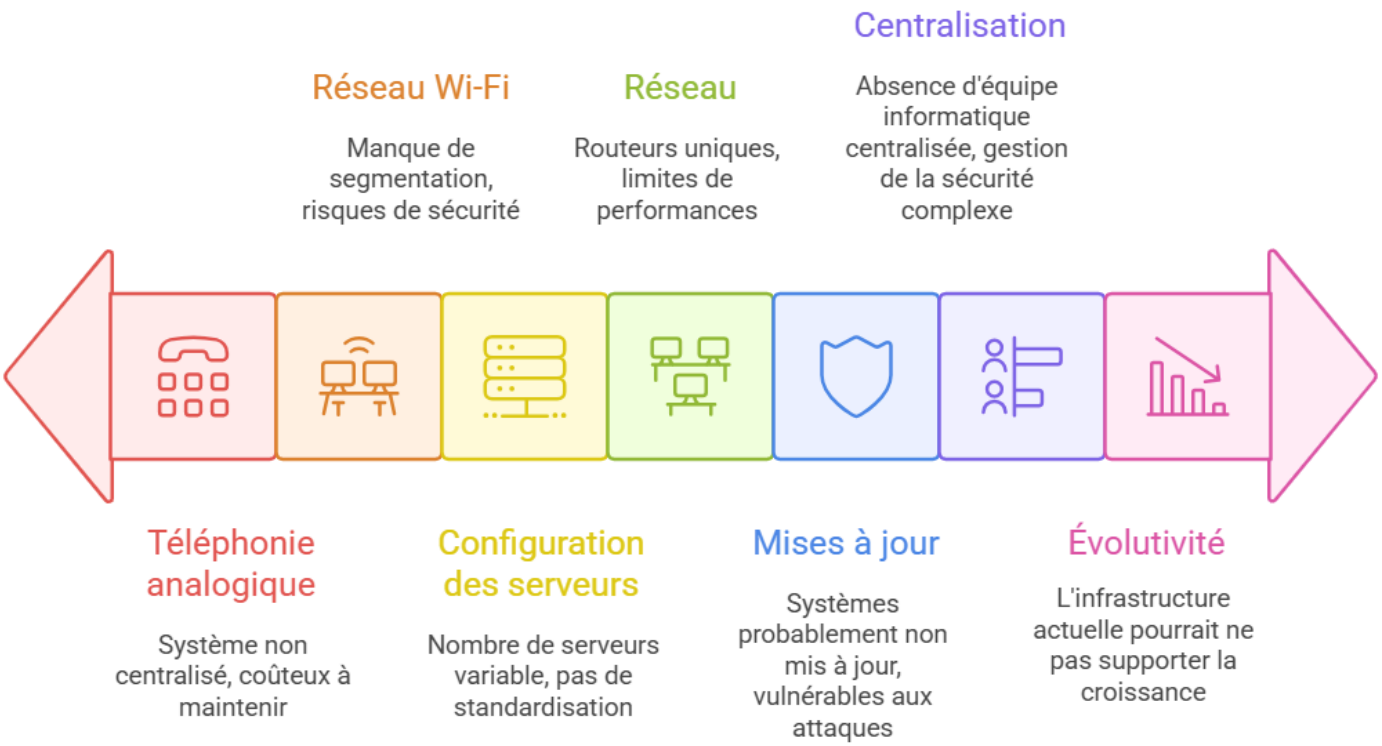
Expérience utilisateur

Après interrogation des utilisateurs, voici les principaux points néfastes selon eux :
🔴 Lenteurs, erreurs, manque de connectivité, sécurité insuffisante.
🔴 Beaucoup de tâches manuelles répétitives et perte de temps.
🔴 Manque de centralisation et d'automatisation, ce qui nuit à la productivité.

On retrouve des plaintes plus détaillées en annexe (page 45).

C. Analyse du parc informatique.

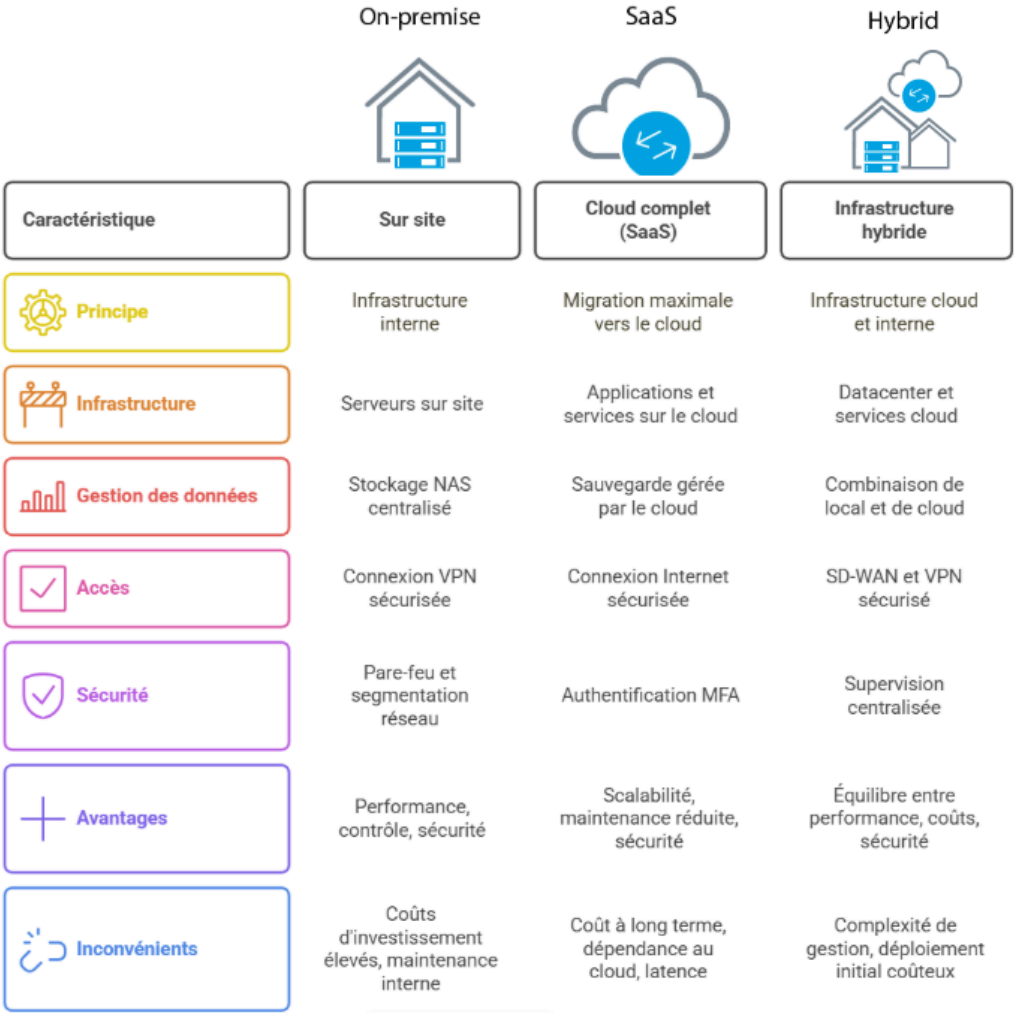
L'étude du parc informatique de PrintCorp révèle une hétérogénéité marquée entre les différents sites, tant en termes de taille que de configuration.



En conclusion, le parc informatique de PrintCorp présente des opportunités d'amélioration significatives. En investissant dans une modernisation de son infrastructure, l'entreprise pourra améliorer sa productivité, réduire ses coûts et renforcer sa sécurité.

D. Solutions émises

D'après l'analyse du parc informatique du PrintCorp, 3 solutions émergent :



Caractéristique	Sur site	Cloud complet (SaaS)	Infrastructure hybride
Principe	Infrastructure interne	Migration maximale vers le cloud	Infrastructure cloud et interne
Infrastructure	Serveurs sur site	Applications et services sur le cloud	Datacenter et services cloud
Gestion des données	Stockage NAS centralisé	Sauvegarde gérée par le cloud	Combinaison de local et de cloud
Accès	Connexion VPN sécurisée	Connexion Internet sécurisée	SD-WAN et VPN sécurisé
Sécurité	Pare-feu et segmentation réseau	Authentification MFA	Supervision centralisée
Avantages	Performance, contrôle, sécurité	Scalabilité, maintenance réduite, sécurité	Équilibre entre performance, coûts, sécurité
Inconvénients	Coûts d'investissement élevés, maintenance interne	Coût à long terme, dépendance au cloud, latence	Complexité de gestion, déploiement initial coûteux

Choix recommandé : **Solution Hybride**
La solution hybride est la plus adaptée à PrintCorp car elle permet de :

- Exploiter le datacenter de Montréal tout en modernisant l'infrastructure.
- Réduire la dépendance aux fournisseurs cloud tout en bénéficiant de leur scalabilité.
- Renforcer la sécurité et assurer une résilience accrue.
- Garantir une meilleure performance locale pour les services critiques.

Le déploiement pourra se faire en plusieurs phases, avec une transition progressive vers le cloud pour optimiser les coûts et la sécurité.

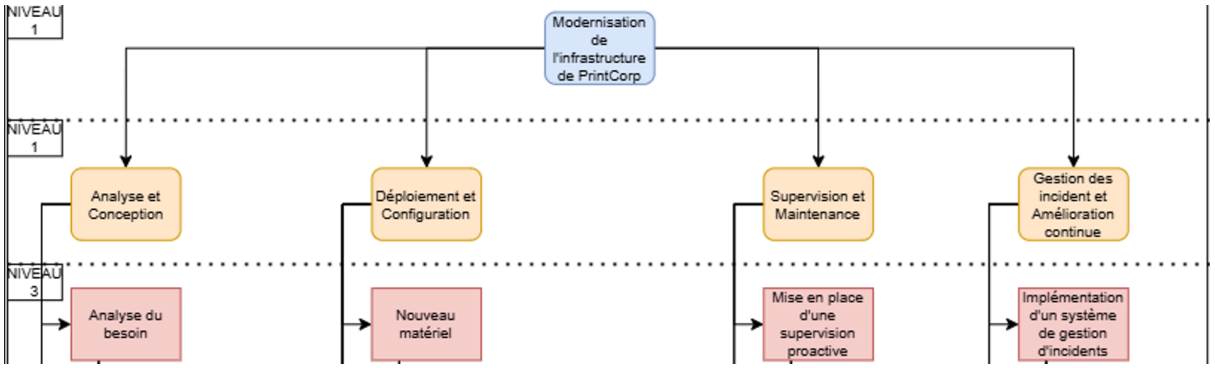
IV. Méthodologie de projet - Bloc 1

Maintenant que la solution hybride est choisie, nous allons mettre en place une gestion de projet efficace pour répondre à la problématique du client.

A. WBS (Work Breakdown Structure)

Une matrice WBS ou organigramme de gestion de projet est un outil de management utilisé pour définir et gérer les tâches d'un projet.

Pour le cas de PrintCorp, on a pu définir 4 structures de niveau 2.
Voici la matrice (vous pouvez retrouvez le tableau complet en annexe page 48) :



B. Diagramme de Gantt et Matrice RACI

Nous avons pu élaborer un diagramme de Gantt (en annexe page 64) par rapport au tableau WBS ci-dessus :

Le projet débutera donc le 2 Janvier 2025 pour finir en Décembre 2025. Celui-ci a pour but de moderniser l'ensemble de l'infrastructure de la société PrintCorp.

Les différentes tâches devront être respectées en temps et en heure sous peine de malus pour la société ReNewIT.

Pour accompagné ce diagramme, une matrice RACI a été mis en place (vous pouvez retrouver la matrice RACI entière en annexe page 49) :

Tâches WBS	DG	DAF	IT	Opérations (PMO)	Commercial	R&D & Innovation	Logistique & Achats
1. Analyse et Conception	A	C	R	C	C	C	I
1.1. Analyse des besoins	A	C	R	C	C	C	I
1.2. Conception de l'architecture	A	C	R	C	I	C	I
1.3. Documentation et validation	A	C	R	C	I	I	I

C. KPI

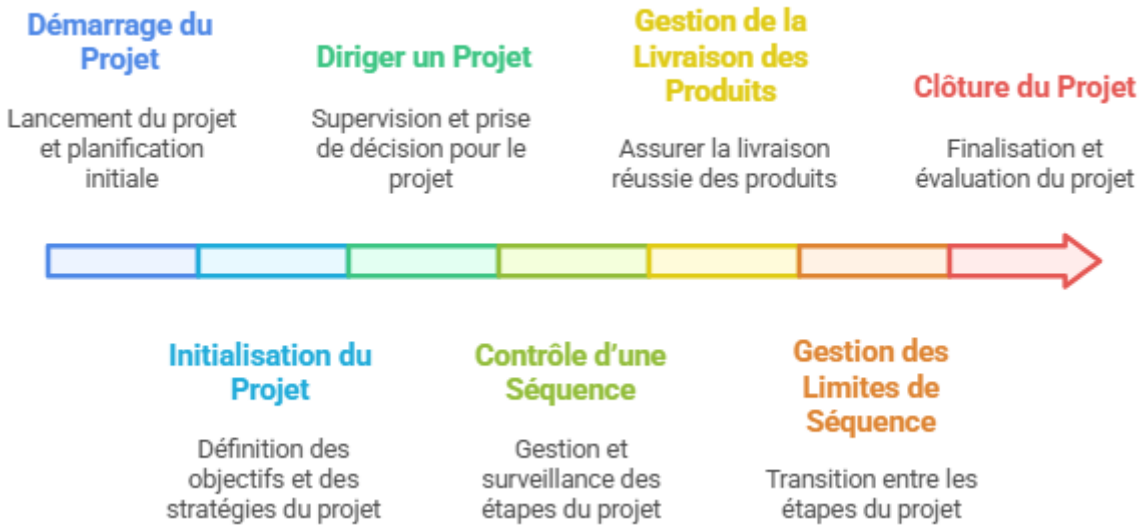
Key Performance Indicator (ou KPI) signifie « indicateur clé de performance » et désigne, dans un contrat informatique et plus spécialement dans un contrat d'externalisation, un indicateur destiné à mesurer les performances c'est-à-dire à vérifier si le prestataire exécute ses obligations conformément aux niveaux de services contractuellement convenus.

Pendant le projet, les utilisateurs de PrintCorp rencontreront divers motifs récurrents de KPI, qui reflètent les défis et améliorations progressives de l'expérience utilisateur. Voici une liste complète :

Catégorie	KPI	Objectif
Qualité & Performance	Taux de résolution des tickets	≥ 90%
Qualité & Performance	Temps moyen d'assignation	≤ 1h
Qualité & Performance	Temps moyen de résolution	≤ 8h
Qualité & Performance	Résolution au 1er contact	≥ 70%
Qualité & Performance	Taux de tickets rouverts	≤ 5%
Qualité & Performance	Conformité SLA globale	≥ 95%
Qualité & Performance	Délai de première réponse dans SLA	≥ 90%
Satisfaction utilisateur	Nombre total d'incidents déclarés	≤ 100
Satisfaction utilisateur	Nombre de tickets créés (via portail/ITSM)	-
Satisfaction utilisateur	Incidents signalés par le service "Support IT"	≤ 30% du total
Satisfaction utilisateur	Taux de satisfaction utilisateur (post-ticket)	≥ 80%
Satisfaction utilisateur	Net Promoter Score (NPS)	≥ 30
Satisfaction utilisateur	Disponibilité des services critiques (Uptime)	≥ 99.5%
Efficience & Coûts	Coût moyen par ticket (€)	≤ 15 €
Efficience & Coûts	Coût par utilisateur (€)	≤ 100 €

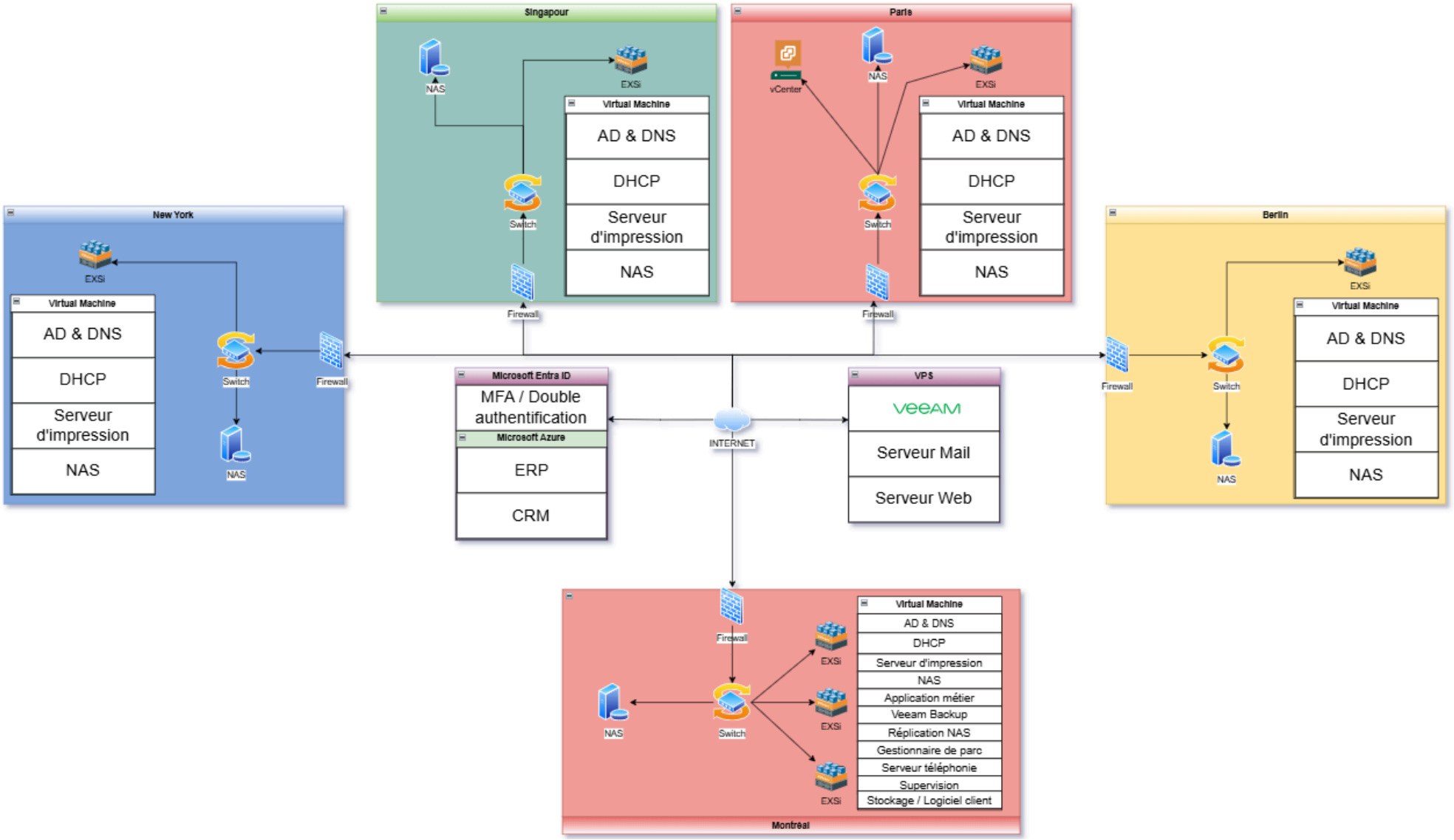
D. Méthodologie PRINCE2

Pour le projet PrintCorp, nous allons suivre la méthodologie PRINCE2 qui se distingue en 7 étapes distinctes. Vous retrouverez le détail complet des étapes en annexe (page 51).



E. Présentation de la solution

Maintenant, nous allons pouvoir étudier la solution hybride proposée par ReNewIT pour la refonte de l'infrastructure de PrintCorp.


Singapour
NAS
EXSi
Virtual Machine
AD & DNS
DHCP
Serveur d'impression
NAS
Switch
Firewall
Paris
vCenter
NAS
EXSi
Virtual Machine
AD & DNS
DHCP
Serveur d'impression
NAS
Switch
Firewall
New York
EXSi
Virtual Machine
AD & DNS
DHCP
Serveur d'impression
NAS
Switch
Firewall
NAS
Berlin
EXSi
Virtual Machine
AD & DNS
DHCP
Serveur d'impression
NAS
Firewall
Switch
NAS
Microsoft Entra ID
MFA / Double authentification
Microsoft Azure
ERP
CRM
INTERNET
VPS
Veeam
Serveur Mail
Serveur Web
Firewall
NAS
Switch
EXSi
EXSi
EXSi
Virtual Machine
AD & DNS
DHCP
Serveur d'impression
NAS
Application métier
Veeam Backup
Réplication NAS
Gestionnaire de parc
Serveur téléphonie
Supervision
Stockage / Logiciel client
Montréal

V. Mise en place des solutions - Bloc 2

A. Conception et déploiement d'une nouvelle infrastructure.

Suite à l'analyse du parc informatique de l'entreprise, nous avons pu déceler des lacunes dans de nombreux domaines critiques. De plus, le matériel que cela soit réseau ou système est plus que obsolète :

- Pannes fréquentes : liées à des serveurs physiques en fin de vie.
- Absence de centralisation : ce qui complique la gestion et favorise les erreurs.
- Sécurité quasi inexistante : pare-feux absents ou mal configurés, aucun suivi des connexions, mots de passe faibles.
- Téléphonie obsolète et réseaux Wi-Fi non segmentés.

Dans le cadre de notre intervention pour PrintCorp, la question de la protection des données personnelles s'est naturellement imposée. L'entreprise manipule quotidiennement des informations sensibles, tant sur ses clients que sur ses collaborateurs, ce qui rend indispensable le respect du **RGPD**. Nous avons donc revu l'ensemble des pratiques liées à la gestion des données, en veillant à limiter les traitements au strict nécessaire, à clarifier leur finalité, et à garantir la transparence auprès des utilisateurs internes.

Sur le plan technique, les accès aux systèmes ont été renforcés à travers une meilleure gestion des droits, l'usage de mots de passe robustes et des mécanismes de double authentification. Les données sont désormais sauvegardées de manière régulière, chiffrée, et les restaurations sont testées pour garantir leur fiabilité. Un registre des traitements a également été proposé à la DSI, afin d'assurer une traçabilité claire et conforme.

Même sans viser une certification formelle, nous avons structuré notre approche selon les principes de la norme **ISO/CEI 27001**. Cette démarche a guidé la mise en place de mesures de sécurité cohérentes, appuyées sur une analyse des risques, et ancrées dans un processus d'amélioration continue. Au-delà des aspects techniques, c'est toute une culture de la sécurité de l'information qui s'est mise en place, renforçant la résilience de PrintCorp face aux enjeux numériques actuels.

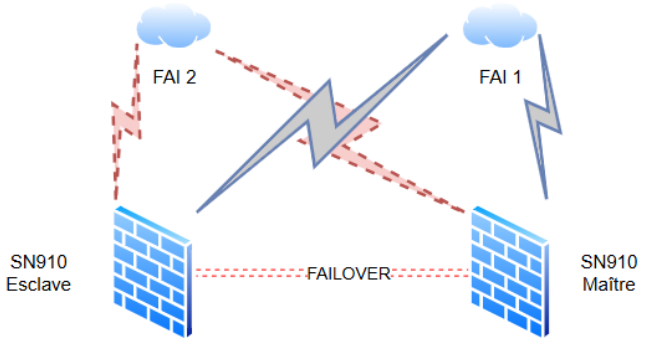
Matériel

Sur les 5 sites, le matériel utilisé sera le même pour une homogénéisation.
Certains sites auront des variations en fonction du risque comme Paris et Montréal. Les autres sont des sites avec des risques plus faibles.

1. Routeur/Firewall

Actuellement, l'entreprise utilise des routeurs fournis par les FAI. Ces routeurs ne sont clairement pas adaptés à une entreprise de cette taille.

Élément	Description
Équipement choisi	Pare-feux StormShield SN910
Fonctionnalités principales	- Fonction de routeur - Pare-feu performant
Fonctionnalités supplémentaires	VPN site-à-site puissant et fiable / Adapté aux besoins de PrintCorp
Avantage du fournisseur	Entreprise française offrant un support technique en français, facilitant le dépannage
Coût estimé	5 000 € à 10 000 € par unité
Architecture prévue	Firewalls installés en binômes (mode FAILOVER) / Connexion via deux liens fibres de deux opérateurs pour garantir la résilience



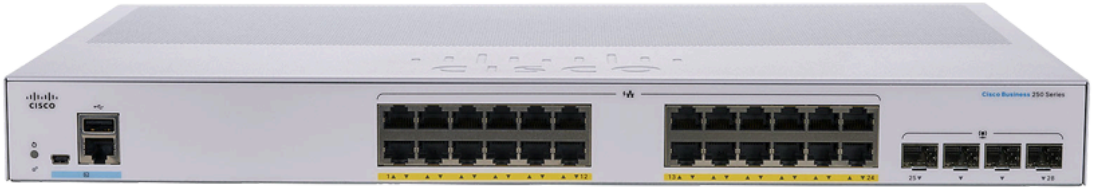
2. Switch

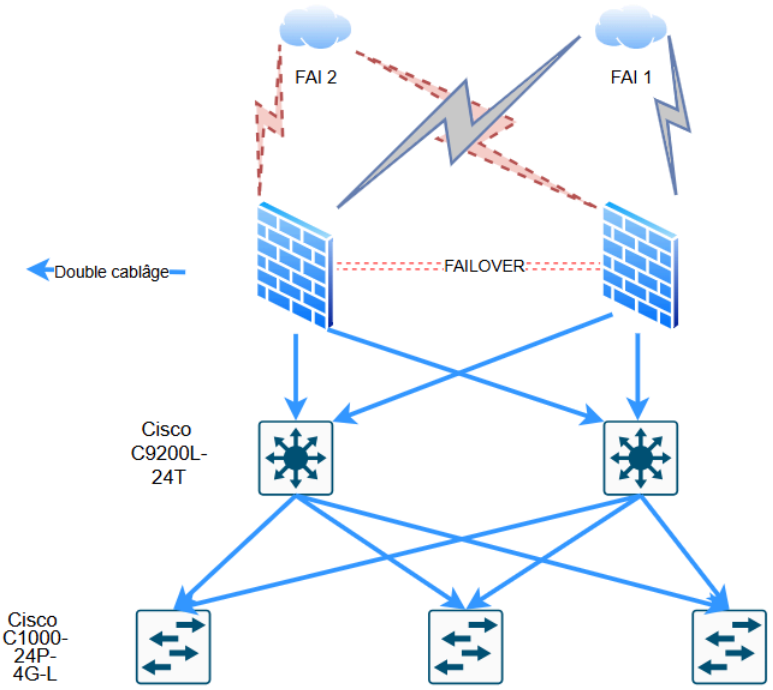
On peut déjà différencier les switch du core réseau (salle serveur) et ceux du reste du bâtiment

Élément	Description
Équipement utilisé	Cisco C9200L-24T
Type d'équipement	Commutateur manageable de niveau 3
Fonctionnalités avancées	Routage statique / OSPF - Listes de contrôle d'accès (ACL) / Qualité de service (QoS)
Connectique	24 ports Ethernet Gigabit (RJ-45)
Coût estimé	800€ par unité

Pour les switch de distribution, on va utiliser Cisco C1000-24P-4G-L

Élément	Description
Équipement utilisé	Cisco C1000-24P-4G-L
Type d'équipement	Switch compact et silencieux, idéal pour les baies d'étage en environnement professionnel
Connectique	24 ports Gigabit PoE+ – permet d'alimenter téléphones IP, caméras, bornes Wi-Fi sans injecteurs externes
Fonctionnalités réseau	Gestion complète des VLANs / Compatibilité 802.1Q / Interface Web/CLI intuitive
Avantages	Facile à intégrer dans un réseau managé / Fiabilité et compatibilité Cisco assurées
Coût estimé	800€ par unité

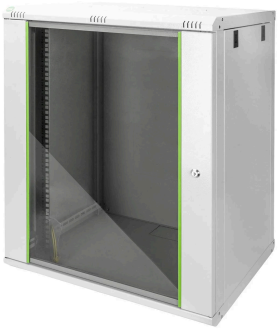




3. Baie de Brassage et Rack

Pour accompagner les équipements actifs installés dans l'infrastructure réseau de PrintCorp, nous avons sélectionné des baies adaptées aux différents environnements techniques de l'entreprise.

Élément	Description
Emplacement concerné	Baies d'étage ou locaux techniques répartis dans le bâtiment
Type de baie recommandé	Baies murales 22U – modèle Digitus DN-19 22U, format 600x600 mm
Capacité	Peut accueillir : - Un switch d'accès (ex. : Cisco C1000-24P-4G-L) - Un panneau de brassage
Caractéristiques physiques	- Porte vitrée verrouillable - Système de ventilation passive, compatible avec kit de ventilation active
Avantages	- Sécurité physique des équipements - Organisation du câblage - Bonne dissipation thermique pour le fonctionnement optimal des dispositifs réseau
Coût estimé	Entre 250 et 350 € HT par unité



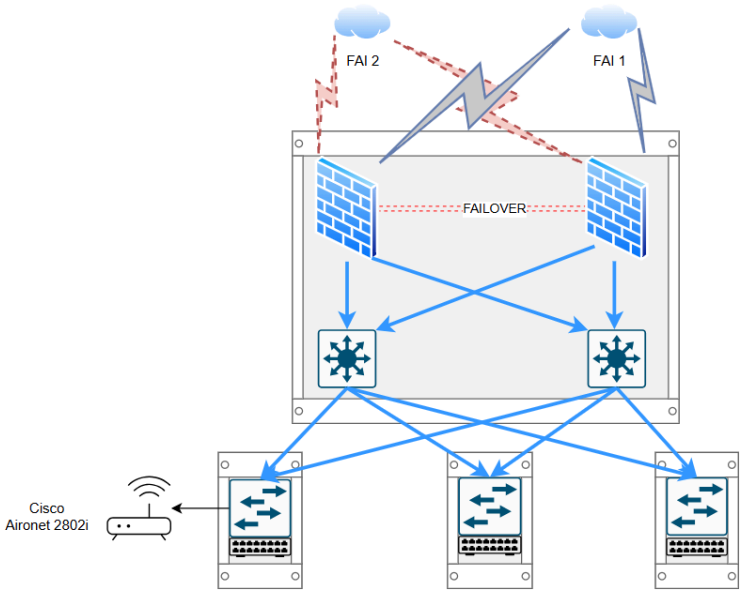
Élément	Description
Emplacement concerné	Salle serveur principale de chaque site
Type de baie recommandé	Baie sur pied 42U, format 800x1000 mm, marque Digitus
Capacité d'accueil	- Switchs cœur de réseau (Cisco C9200L) - 2 pare-feux StormShield SN910 (mode redondance) - Serveurs virtualisés - Équipements de sauvegarde - PDU intelligents - Onduleur
Avantages	Permet de regrouper tous les équipements critiques dans une seule baie pour une meilleure organisation, sécurité et maintenance
Coût estimé	Entre 700 et 1 200 € HT par unité

Pour le câblage réseau de PrintCorp, nous avons retenu des patch panels 19 pouces, 1U, en catégorie 6 FTP, offrant 24 ports RJ45. Ce format s'adapte parfaitement aux switchs d'étage tout en garantissant un câblage propre et organisé. Le blindage FTP assure une protection contre les interférences, tandis que la numérotation claire et la barre de maintien facilitent la maintenance.

En salle serveur, plusieurs unités peuvent être empilées selon les besoins, tout en respectant les standards professionnels.
Entre 40 à 70€ HT par unité

4. Borne WiFI

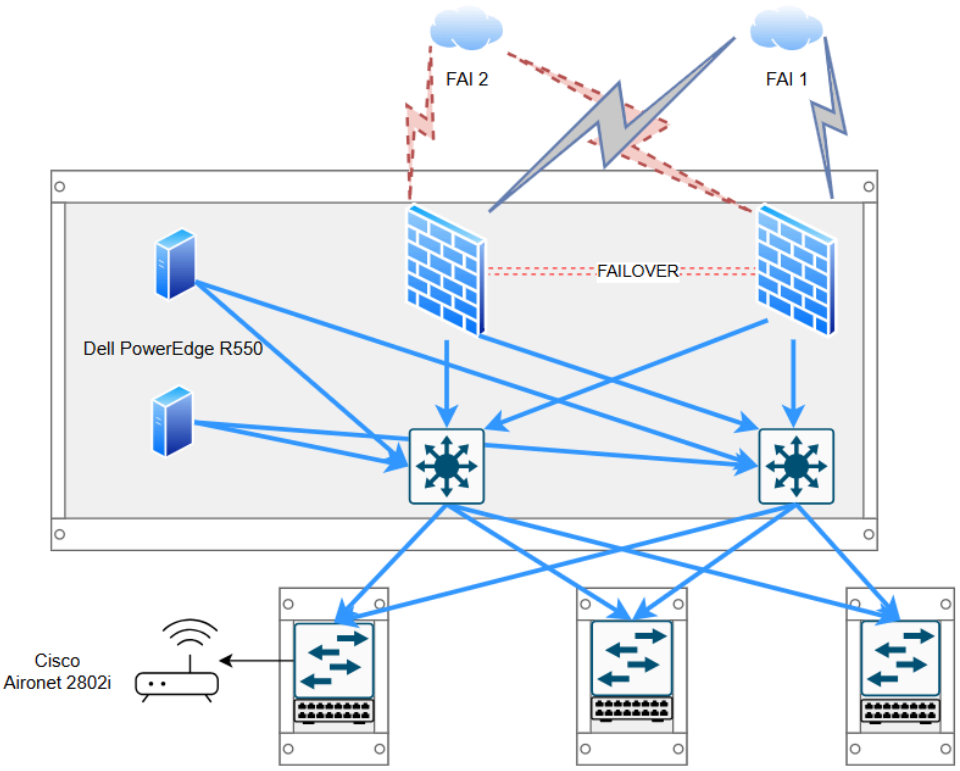
Concernant les bornes Wi-Fi, nous avons fait le choix de conserver les équipements existants, dont l'état général a été jugé très satisfaisant à l'issue de l'audit. Il s'agit de modèles Cisco Aironet 2802I, encore tout à fait adaptés aux usages actuels et pleinement compatibles avec l'infrastructure réseau déployée. Une réinitialisation complète est prévue afin d'intégrer ces bornes au nouveau plan d'adressage et à la configuration de sécurité mise en place. Ce choix permet à la fois de préserver des équipements performants et de réduire les coûts de remplacement sans compromis sur la qualité du service.



5. Serveur

Chaque site sera équipé au minimum, d'un cluster de 2 serveurs pour pallier les problèmes physique de matériel et la continuité d'activité. Sur le site de Montréal, le nombre de serveurs et de clusters sera plus important (data center). Le modèle choisi sera le Dell PowerEdge.

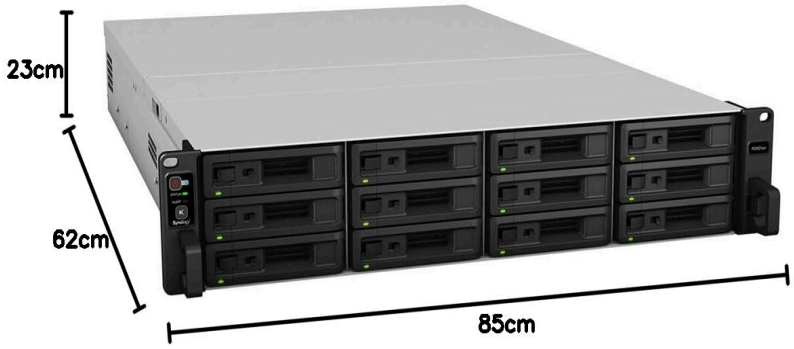
Élément	Description
Serveur recommandé	Dell PowerEdge R550
Caractéristiques techniques	- 2 processeurs Intel Xeon Silver - Jusqu'à 512 Go de RAM DDR4 ECC - Prise en charge de plusieurs services simultanés (AD, fichiers, impression, etc.)
Stockage	- Jusqu'à 8 disques (2,5" ou 3,5") - Capacité totale : 64 To en RAID - Allie performance et sécurité des données
Connexion réseau	Chaque serveur sera connecté à deux switchs pour garantir la redondance
Coût estimé	Entre 4 500 et 6 000 € HT par unité (selon la configuration)

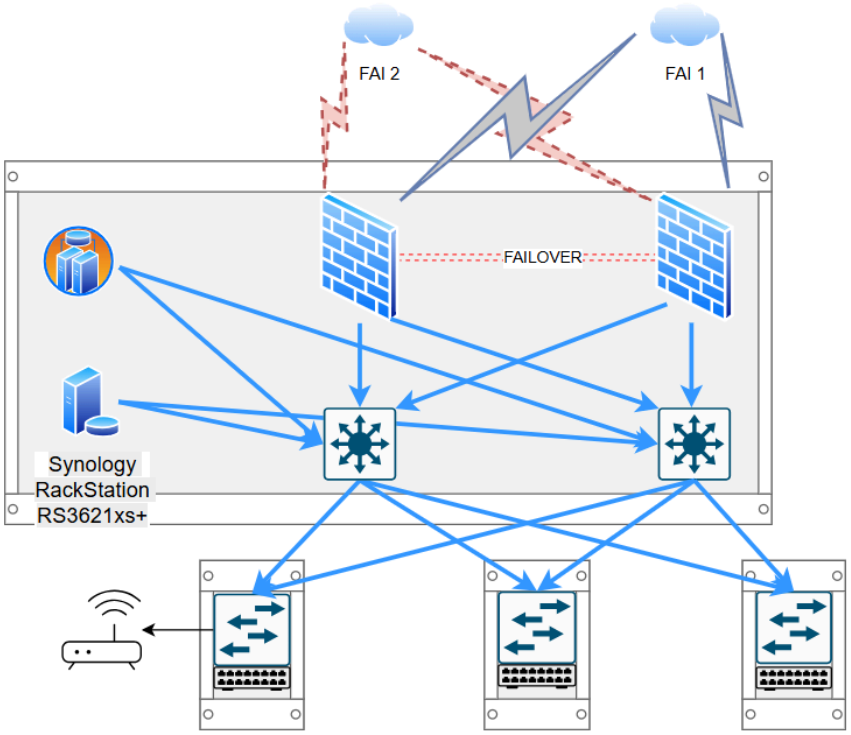

FAI 2
FAI 1
FAILOVER
Dell PowerEdge R550
Cisco
Aironet 2802i

6. NAS ou serveur de fichier

Pour être conforme à l'architecture de sauvegarde 3-2-1, qui consiste à avoir 3 copies de stockage dont 2 types de stockages différents ainsi que 1 hors site (VPS).
Nous allons mettre en place une NAS Local sur chaque site ainsi qu'une réplication de chaque NAS sur le site de Montréal et sur le VPS.
Pour le modèle, nous avons choisi le Synology RackStation RS3621xs+

Élément	Description
Équipement recommandé	Synology RackStation RS3621xs+ (NAS rackable 2U)
Processeur & Mémoire	- Intel Xeon D-1531 (6 cœurs / 12 threads, 2.2 GHz Turbo 2.7 GHz) - 8 Go DDR4 ECC (extensible à 64 Go, 4 slots)
Capacité de stockage	- 12 baies SATA 3,5"/2,5", jusqu'à 108 To bruts - Extensible à 324 To+ avec 2 unités d'extension RX1217(RP)
Connectivité	- 4 ports LAN Gigabit - 2 ports 10 GbE (RJ45) - 1 port PCIe Gen3 x8 (ajout de cartes réseau / SSD NVMe) - 2 ports USB 3.2 Gen 1
Usages	Idéal pour la sauvegarde centralisée, la virtualisation et le stockage collaboratif multisite
Coût unitaire (NAS seul)	Entre 3 500 à 4 500 € HT
Coût des disques durs	Seagate IronWolf Pro 8 To : 300 à 400 € par disque
Déploiement prévu	5 NAS (1 par site)
Coût total estimé	20 000 à 30 000 € (NAS + disques durs inclus)





7. Câblage réseau

Pour chaque site de PrintCorp, un budget d'environ 5 000 € est prévu pour le câblage réseau. Ce montant couvre l'installation complète de câbles Cat6 pour le réseau cuivre standard ainsi que de fibre optique pour les liaisons inter-baies ou équipements nécessitant de hautes performances (comme les NAS, serveurs ou switches cœur de réseau). Ce budget inclut également, si nécessaire, le tirage des câbles vers les prises murales RJ45, afin de garantir une infrastructure propre, évolutive et conforme aux normes professionnelles.

8. Imprimantes

PrintCorp est une société spécialisée dans les solutions d'impression professionnelle. Grâce à son cœur de métier, l'entreprise bénéficie de partenariats établis avec plusieurs constructeurs d'imprimantes reconnus, ce qui lui permet de disposer d'un parc d'équipements performants et adaptés à ses besoins. Il n'est donc pas nécessaire de renouveler ces imprimantes, qui seront simplement intégrées à l'architecture réseau existante. Cette intégration garantira leur accessibilité depuis les différents sites et assurera leur bon fonctionnement au sein du nouvel environnement informatique.

9. Ordinateurs utilisateurs

Élément	Description
Projet concerné	Équipement informatique pour 250 utilisateurs
Matériel prévu	300 ordinateurs portables HP ProBook 450 G10 (dont 50 en spare)
Caractéristiques techniques	- Intel Core i5 - 16 Go de RAM - SSD 512 Go - Adapté à la bureautique avancée, la visioconférence et les applications professionnelles
Répartition	- 250 postes utilisateurs - 50 machines de réserve (spare)
Prix unitaire public	850 € HT
Prix unitaire négocié (-18 %)	697 € HT
Extension de garantie	HP Care Pack J+1 – 4 ans sur site à 85 € HT par machine
Dispositif complémentaire	Mise en place d'un contrat de renouvellement sur 4 ans - Remplacement/évolution du matériel en fin de cycle - Reprise possible des anciennes unités

Ainsi, le **prix global de l'opération** s'élève à :

- **Prix unitaire par PC avec garantie 4 ans** : **697 € + 85 € = 782 € HT**
- **Prix total pour 300 machines** : **234 600 € HT**

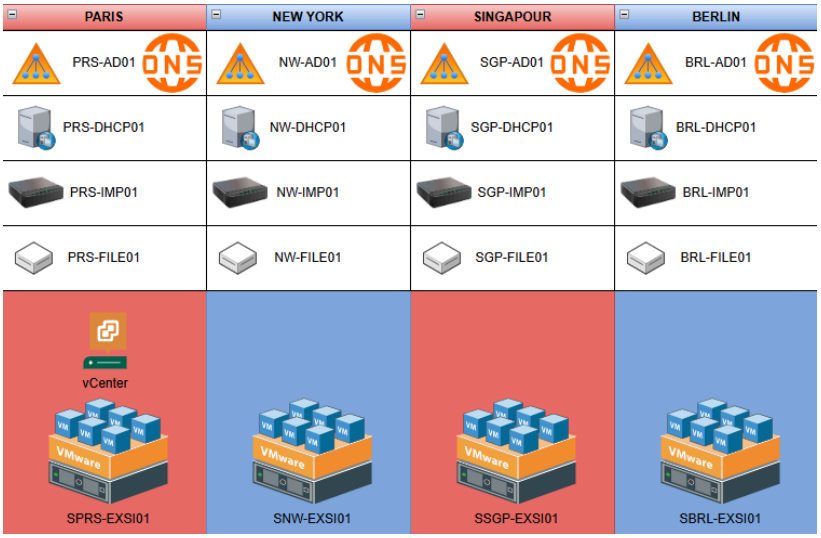
10. Résumé des coûts

Matériel	# Nombre requis	# Prix unitaire	# Prix total
Firewall	10	10 000,00 €	100 000,00 €
Switch	25	800,00 €	20 000,00 €
Rack	7	350,00 €	2 450,00 €
Baie d'étage	15	1 000,00 €	15 000,00 €
Baie de brassage	15	70,00 €	1 050,00 €
Serveur	14	6 000,00 €	84 000,00 €
NAS + Stockage	5	6 000,00 €	30 000,00 €
Ordinateur	300	782,00 €	234 600,00 €
Cablage réseau	1	5 000,00 €	5 000,00 €
			492 100,00 €

Virtualisation

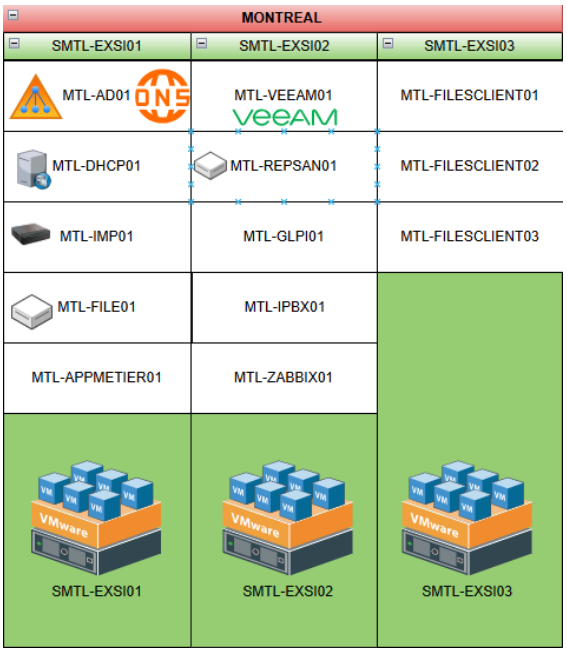
1. Paris/Berlin/Singapour/New York

Comme déjà mentionné, chaque site aura un cluster de 2 serveurs à sa disposition pour accueillir les services indispensables pour la bonne continuité de l'activité sur l'ensemble de la société.

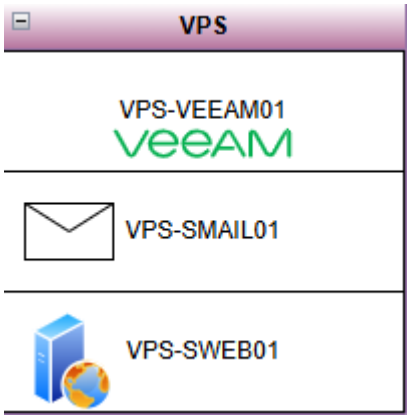


2. Montréal

Pour Montréal, on aura 3 clusters de 2 serveurs. Chacun d'eux aura son utilité pour la continuité de l'activité comme le stockage des clients ou la réplication.



3. VPS

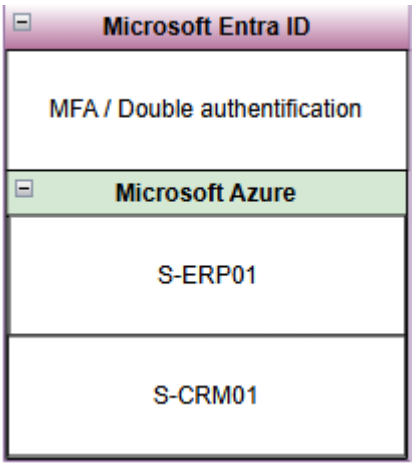


Un VPS, ou **serveur privé virtuel**, est un ordinateur virtuel que vous pouvez utiliser à distance, comme si c'était votre propre serveur. Il est hébergé dans un centre de données (dans le "cloud", souvent), mais vous avez un accès complet pour y installer ce que vous voulez.

Dans notre cas, les services web, mails ainsi qu'une réplication des données via Veeam pour une architecture en 3-2-1.

Il sera hébergé chez OVH afin de diversifier nos fournisseurs et ainsi réduire les risques liés à une dépendance unique en cas de problème.

4. Microsoft Azure



Le choix de Microsoft Azure pour l'hébergement de notre ERP et CRM offre une infrastructure fiable, évolutive et hautement disponible, parfaitement adaptée aux besoins critiques de notre entreprise. Grâce à cette plateforme cloud, nous bénéficions d'une sécurité renforcée, de sauvegardes automatiques et d'une gestion centralisée des données.

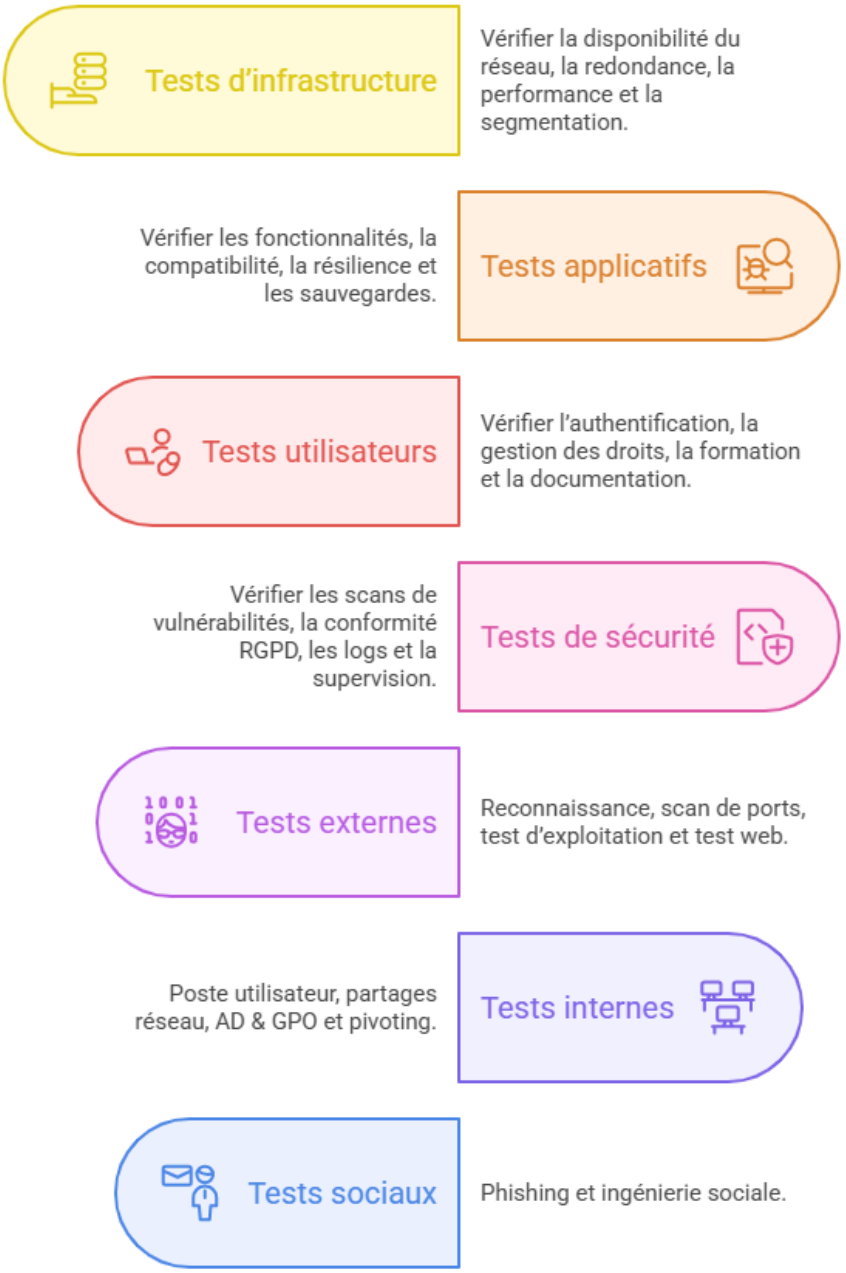
En complément, l'utilisation de **Microsoft Entra ID** pour la gestion des identités et l'authentification multifacteur (MFA) permet de sécuriser efficacement l'accès aux applications sensibles, tout en garantissant une expérience utilisateur fluide et conforme aux meilleures pratiques de cybersécurité.

5. Coût de la virtualisation

Pour calculer le coût, il nous faut définir le prix des licences ainsi que du VPS et Microsoft Azure.

Logiciels et licences	235 000€
Cloud public et VPS	30 000€/an

Définition du programme de test



B. Automatisation et industrialisation

1. Déploiement de poste

Le déploiement des postes de travail s'effectuera à l'aide de la technologie PXE (Preboot Execution Environment), qui permet d'automatiser efficacement l'installation des systèmes d'exploitation et des applications sur les machines des collaborateurs.

En configurant le service **Windows Deployment Services (WDS)**, associé au **kit ADK (Assessment and Deployment Kit)**, sur le contrôleur de domaine principal situé à **Montréal**, nous pourrons procéder à un **mastering centralisé** des postes de manière automatique.

De cette façon, un agent **Zabbix** ainsi que **GLPI** sera installé via le master pour avoir un parc informatique à jour. Chaque PC aura un **identifiant unique** (code matériel) pour le différencier des autres.

Cette approche apportera un **gain de temps significatif**, une **réduction des coûts** liés aux interventions manuelles, ainsi qu'une **homogénéité accrue** de l'environnement informatique. Des prises réseau dédiées seront mises à disposition sur les sites de **Paris** et **Montréal** afin de permettre le démarrage PXE et ainsi faciliter le déploiement à distance.

2. Installation de logiciel via GPO

L'**installation automatisée des logiciels** via les **stratégies de groupe (GPO)** constitue un levier important pour la gestion centralisée des postes au sein de **PrintCorp**.

En intégrant les packages MSI directement dans les stratégies de groupe, les applications essentielles peuvent être déployées **automatiquement** lors de la connexion ou du démarrage des machines. Cette méthode assure une **homogénéité** logicielle sur l'ensemble du parc, réduit considérablement le temps de **configuration manuelle** et limite les risques d'erreurs ou d'oublis lors des installations.

Elle permet également de faciliter la maintenance et les mises à jour en regroupant la gestion des logiciels à un seul point de contrôle : le **contrôleur de domaine**.

3. Sauvegardes des données critiques

La sauvegarde **automatisée des données critiques** repose sur la création de **scripts planifiés**, exécutés régulièrement via le **Planificateur de tâches Windows** ou des outils tiers.

Ces scripts permettent de copier automatiquement les fichiers sensibles (documents internes, données client, configurations système, etc.) vers des emplacements sécurisés, comme des serveurs de sauvegarde, des partages réseau ou des unités de stockage externes. Le script (en annexe page 60) s'activera tous les jours à 2h00.

Cette solution réduit fortement les risques de perte de données en cas de défaillance matérielle, de suppression accidentelle ou d'attaque informatique, tout en assurant la continuité d'activité pour les équipes de PrintCorp.

C. Réseau et connectivité sécurisée (VPN, pare-feu).

Pour garantir un réseau et parc performant ainsi que le respect de l'ensemble des RGPD. Nous mettons en place un réseau permettant de valider l'ensemble du cahier des charges demandé par l'entreprise.

Réseau et interconnexion

Pour garantir une segmentation logique et sécurisée du réseau, chaque site de PrintCorp a été équipé de switchs managés de type Cisco, capables de gérer les VLANs selon la norme IEEE 802.1Q.

Un **VPN IPsec** site-to-site a été mis en place entre les pare-feu des sites et celui de Paris. Ce tunnel chiffré permet de faire transiter les flux VLAN entre les sites tout en conservant leur isolation. Les VLANs sont reconnus de part et d'autre grâce à la cohérence des IDs VLAN, et un OSPF (Open Shortest Path First) est configuré pour faire correspondre les sous-réseaux.

Cette configuration garantit à la fois une modularité, une sécurité des communications internes, et une interconnexion fiable entre les différents sites. Elle permet également à PrintCorp d'évoluer vers une architecture plus avancée à l'avenir, notamment avec l'intégration d'un contrôleur SDN ou d'un NAC (Network Access Control).

VI. Surveillance du bon fonctionnement et de la performance - Bloc 3

A. Échelles détaillées

Pour correspondre au nouveau SI, la mise en place d'une échelle correspondante est importante.

1. Tableau d'impact

Niveau	Intitulé	Description
I1	**Insignifiant**	Aucun impact sur les services. Perturbation négligeable.
I2	**Mineur**	Perturbation mineure sur un service non critique. Résolution rapide.
I3	**Modéré**	Interruption temporaire d'un service important. Impact utilisateur limité.
I4	**Majeur**	Arrêt prolongé d'un service critique, impact métier important.
I5	**Catastrophique**	Panne totale ou perte de données, arrêt de l'activité, atteinte à la réputation.

2. Tableau de probabilité

Niveau	Intitulé	Description
P1	**Très improbable** (≤ 5%)	Rare, jamais observé auparavant.
P2	**Peu probable** (6–20%)	Possible mais peu fréquent. 1 fois tous les 5–10 ans.
P3	**Probable** (21–50%)	Déjà observé dans l'organisation ou dans le secteur.
P4	**Très probable** (51–80%)	Situation courante, se produit régulièrement.
P5	**Quasi certain** (> 80%)	Pratiquement inévitable sans action corrective.

3. Seuil de criticité

Formule de criticité : Impact × Probabilité (max 25)

Voici maintenant la **nouvelle matrice des risques** pour l'entreprise PrintCorp selon ces grilles :

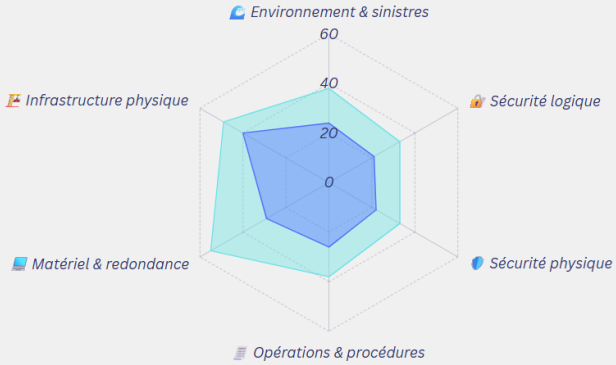
Score	Niveau	Couleur
1–4	Faible	🟢
5–10	Modéré	🟡
11–15	Élevé	🔶
16–25	Critique	🔴

	P1	P2	P3	P4	P5
I1	Faible 🟢	Faible 🟢	Faible 🟢	Faible 🟢	Modéré 🟡
I2	Faible 🟢	Modéré 🟡	Modéré 🟡	Modéré 🟡	Modéré 🟡
I3	Faible 🟢	Modéré 🟡	Modéré 🟡	Élevé 🔶	Élevé 🔶
I4	Faible 🟢	Modéré 🟡	Élevé 🔶	Critique 🔴	Critique 🔴
I5	Modéré 🟡	Modéré 🟡	Élevé 🔶	Critique 🔴	Critique 🔴

Définition du risque acceptable/inacceptable :

En vert : acceptable (1-10)
En rouge : inacceptable (11-25)

B. Etude de cas : Montréal



Vous pouvez retrouver une étude du cas de Montréal complète en annexe (page 55).

Mais pour résumé, voici le comparatif avant/après :

1. Expérience utilisateur

Suite à la mise en place du plan de prévention dans la salle serveur de PrintCorp à Montréal, l'expérience utilisateur des employés s'est nettement améliorée.

La disponibilité accrue des services IT, permise par l'installation d'un onduleur (UPS) et d'un groupe électrogène, a fortement réduit les interruptions liées aux coupures de courant ou aux incidents électriques. Les temps d'accès aux ressources réseau sont devenus plus stables, même en période de forte sollicitation ou de conditions climatiques dégradées. De plus, la fiabilité des sauvegardes et la réactivité des équipes IT en cas d'incident ont renforcé la confiance des utilisateurs internes dans les outils numériques de l'entreprise.

En résumé, ce plan a permis de **sécuriser** l'environnement de travail des collaborateurs, **d'optimiser** leur productivité au quotidien, et de garantir une continuité de service essentielle à la performance globale de PrintCorp.

2. Evolution des KPI

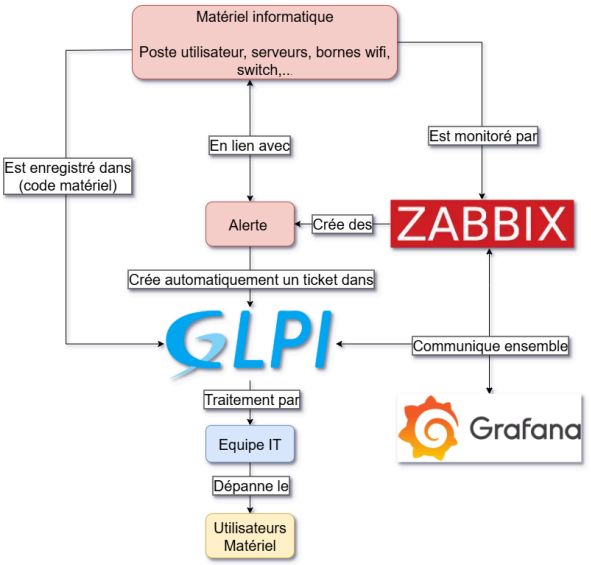
Au cours du projet, nous avons étudié l'évolution des KPI défini et voir si les **objectifs** précédemment évoqué ont été **atteints** :

Catégorie	KPI	Objectif	Mois précédent	Mois en cours	Évolution	Statut
Qualité & Performance	Taux de résolution des tickets	≥ 90%	86%	92%	+6%	Atteint
Qualité & Performance	Temps moyen d'assignation	≤ 1h	01:20	00:45	-35 min	Atteint
Qualité & Performance	Temps moyen de résolution	≤ 8h	10:15	7:30	-2:45	Atteint
Qualité & Performance	Résolution au 1er contact	≥ 70%	64%	75%	+11%	Atteint
Qualité & Performance	Taux de tickets rouverts	≤ 5%	9%	6%	-3%	En progrès
Qualité & Performance	Conformité SLA globale	≥ 95%	88%	93%	+5%	En progrès
Qualité & Performance	Délai de première réponse dans SLA	≥ 90%	82%	94%	+12%	Atteint
Satisfaction utilisateur	Nombre total d'incidents déclarés	≤ 100	135	95	-40	Atteint
Satisfaction utilisateur	Nombre de tickets créés (via portail/ITSM)	-	98	97	— Stable	OK
Satisfaction utilisateur	Incidents signalés par le service "Support IT"	≤ 30% du total	45%	28%	-17%	Atteint
Satisfaction utilisateur	Taux de satisfaction utilisateur (post-ticket)	≥ 80%	72%	84%	+12%	Atteint
Satisfaction utilisateur	Net Promoter Score (NPS)	≥ 30	18	36	+18	Atteint
Satisfaction utilisateur	Disponibilité des services critiques (Uptime)	≥ 99.5%	98.8%	99.7%	+0.9%	Atteint
Efficience & Coûts	Coût moyen par ticket (€)	≤ 15 €	17,50 €	13,80 €	-3,7 €	Atteint
Efficience & Coûts	Coût par utilisateur (€)	≤ 100 €	108 €	96 €	-12 €	Atteint

C. Surveillance, accessibilité et sécurité

Voici le plan global de surveillance sur le parc ainsi que sa gestion :

La définition d'alertes sur Zabbix est une étape importante. Les alertes seront définies sur des données précises du matériel comme la température, le stockage. Lorsque la condition devient vraie, Zabbix envoie une alerte qui crée automatiquement un ticket sur GLPI. L'équipe IT gère le problème, plus ou moins rapidement en fonction de la gravité du risque.



Un serveur Grafana sera monté pour mettre en place des dashboard précis avec les informations de Zabbix et GLPI, pour une bonne visualisation. En effet, on peut prévoir des dashboard sur chaque site ou chaque salle serveur permettant une identification en avance d'un possible risque.

Voici les différent types d'alertes définis sur Zabbix ainsi que l'action attendu :

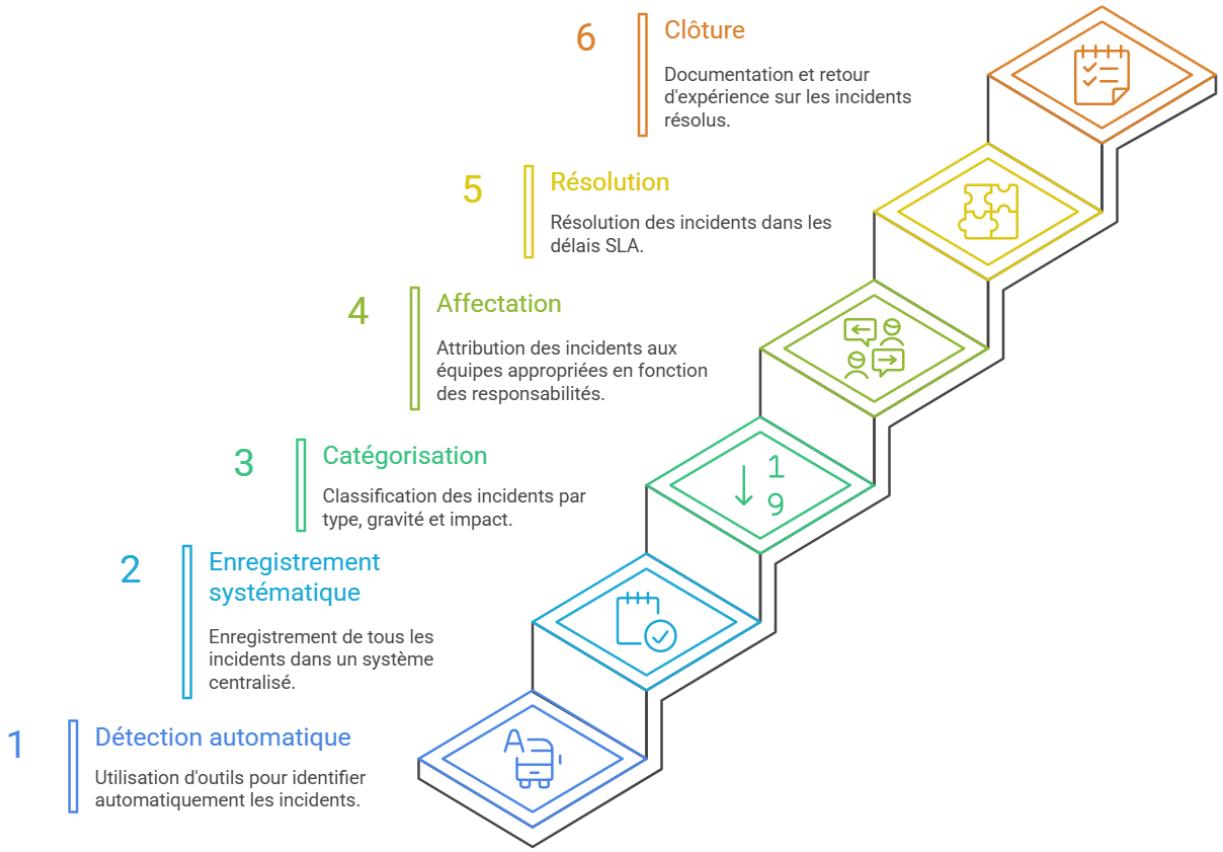
Nom de l'alerte	Seuil / Déclencheur	Gravité	Action attendue
Serveur de fichiers			
Température CPU élevée	Température > 75°C pendant 5 min	Élevée	Vérifier ventilation / climatisation
Espace disque critique	Espace disque libre < 10 % sur partition /data	Élevée	Nettoyage ou extension de volume
SMART disque en erreur	Détection d'erreurs SMART critiques	Critique	Remplacer le disque au plus vite
Latence disque élevée	Latence moyenne > 30 ms	Moyenne	Analyse I/O, vérifier RAID
Équipements réseau			
Perte de connectivité	Ping échoué 3 fois consécutives	Critique	Intervention physique ou redémarrage
Erreurs CRC port uplink	Erreurs CRC > 100 sur 5 min	Moyenne	Vérifier câble / port défectueux
Bande passante saturée	Utilisation > 95 % pendant 10 min	Élevée	Analyse du trafic, QoS, upgrade
Postes de travail / Imprimantes			
Espace disque système bas	Disque C: < 15 % libre	Moyenne	Nettoyage utilisateur / IT
Mémoire RAM saturée	Utilisation RAM > 90 % pendant 10 min	Moyenne	Fermer des applications ou upgrader la RAM
Périphérique déconnecté	Imprimante réseau injoignable	Moyenne	Vérifier câble ou redémarrer imprimante
Sauvegarde et sécurité			
Sauvegarde échouée	Statut job Veeam ou script = échec	Critique	Relancer sauvegarde, diagnostic logs
Taux d'échec élevé	> 3 sauvegardes échouées en 48h	Critique	Révision du plan de sauvegarde
Échec réplication distante	Plus de 24h sans réplication	Élevée	Vérifier connectivité avec le site distant
Supervision système			
Temps de réponse lent	Réponse HTTP > 2s pour l'intranet	Moyenne	Optimisation serveur web
Redémarrage anormal	Nombre de reboot > 1 sur 24h	Moyenne	Analyser journaux d'événements
MTTR dépassé	Temps de résolution incident > 2h	Moyenne	Suivi de la cellule support IT

Structuration des rôles et responsabilités

Chez PrintCorp, la réponse aux alertes est structurée autour d'une chaîne claire de responsabilités. L'équipe **Support IT de niveau 1** est chargée de traiter les alertes simples (utilisation mémoire excessive, perte de connectivité utilisateur), tandis que les incidents critiques sont automatiquement escaladés vers le **Niveau 2** (techniciens réseaux et serveurs) ou

le **Niveau 3** (équipe Infrastructure ReNewIt ou prestataires externes). Le **Responsable du Système d'Information** supervise le suivi global, valide les décisions de bascule en PRA, et assure le lien avec la direction générale.

PrintCorp s'appuie sur les bonnes pratiques ITIL pour organiser son processus de gestion des incidents :



Les incidents sont également analysés mensuellement pour identifier des causes racines récurrentes à traiter de façon préventive.

Mise en place d'une base de connaissances via GLPI

Cette base de connaissances sera mise à jour chaque semaine et **l'accès** aux données sera strictement contrôlé via des **groupes** d'utilisateurs prédéfinis. Un utilisateur ne pourra consulter que les informations correspondant aux **droits** accordés à son groupe. Elle facilitera la diffusion des connaissances liées au système d'information, avec pour objectif une extension progressive à d'autres services. Ce dispositif renforcera la **collaboration et le partage d'informations entre les équipes.**

Toutes les procédures d'intervention (pannes réseau, restauration de sauvegarde, gestion d'un poste HS, etc.) sont documentées sous forme de fiches PDF, disponibles sur les bases de connaissances. Chaque fiche suit un modèle commun : contexte, symptôme, étapes de diagnostic, actions à mener, escalade, vérification finale. Elles sont versionnées, validées par le DSI, et accessibles aux techniciens comme aux utilisateurs habilités.

Gestion des droits et politiques de sécurité

PrintCorp applique rigoureusement le **principe du moindre privilège** : chaque collaborateur dispose uniquement des droits nécessaires à ses fonctions. Tous les accès aux ressources critiques (serveurs, applications SaaS, consoles

d'administration) sont sécurisés par une **authentification multifacteur (MFA)** via des solutions comme Microsoft Entra ID. Des contrôles de permissions sont effectués trimestriellement avec revue des comptes inactifs ou à risque.

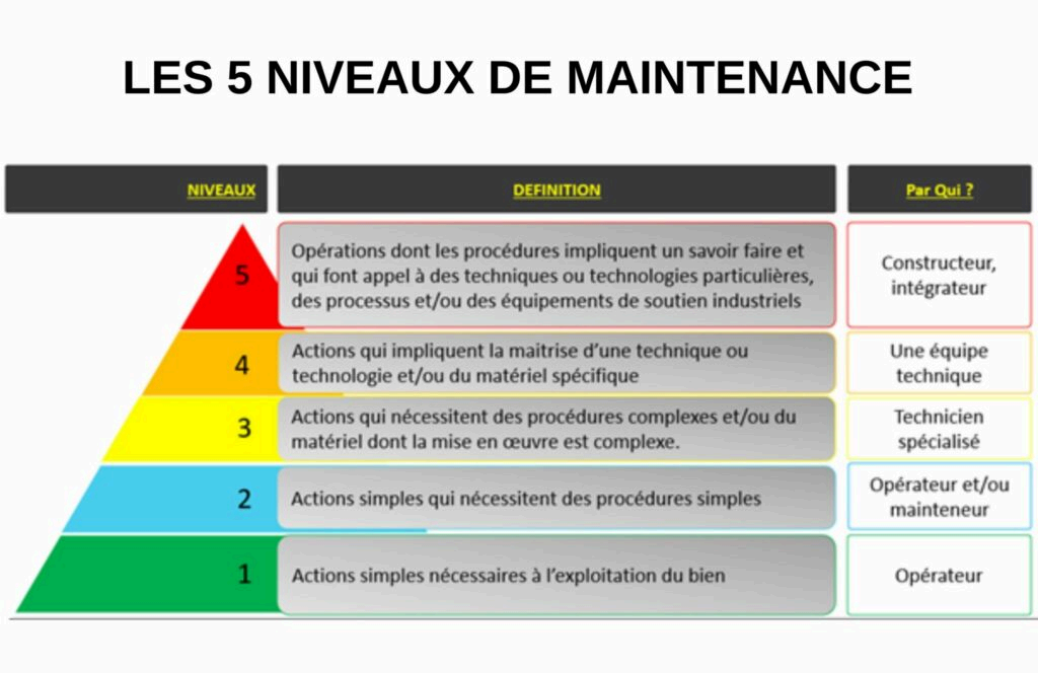
Implémentation des contrôles d'accès et audits

Les accès sont **centralisés via un Active Directory** synchronisé avec les systèmes cloud (Azure AD). Chaque demande de création/modification/suppression d'un compte fait l'objet d'un **ticket avec validation managériale**. Les journaux d'accès (logs) sont collectés et **audités régulièrement** pour détecter les anomalies (heures inhabituelles, connexions depuis l'étranger, etc.).

VII. Opération de maintenance et gestion des évolutions des systèmes et réseaux - Bloc 4

A. Niveau de maintenance

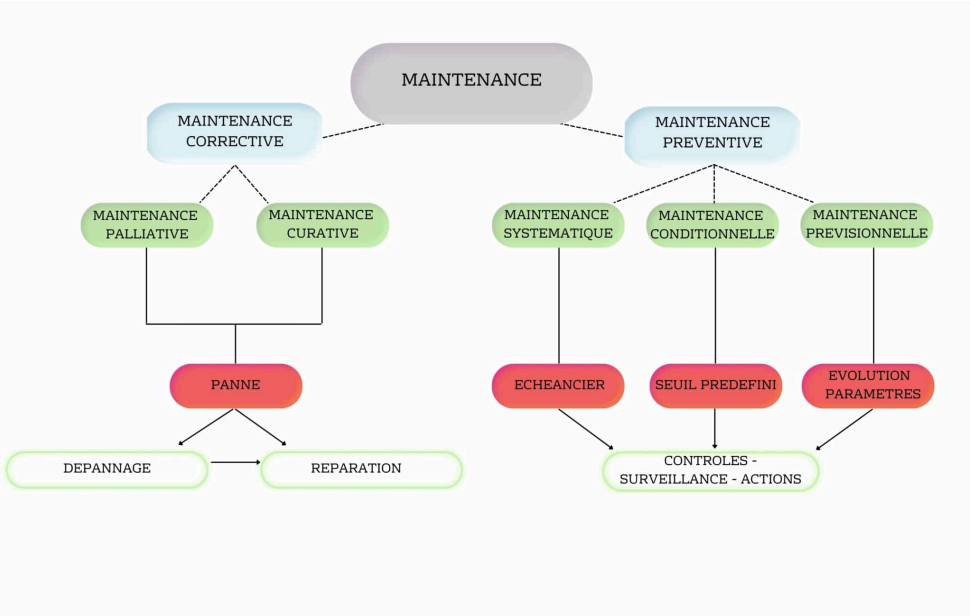
ReNewIT utilise la norme AFNOR X 60-010 pour ses niveaux de maintenance interne. La proposition est de l'étendre à PrintCorp pour avoir des niveaux clairement définis. Ces mesures visent à garantir la disponibilité, la sécurité et la continuité des services informatiques critiques.



B. Typologie de maintenance mise en oeuvre

:
Les types de maintenance se divise en 2 types :

- **Préventive** : se fonde sur l'expression "mieux vaut prévenir que guérir", sur la connaissance des machines, la prise en compte des signes précurseurs et le réalisme économique.
- **Correctif** : se fonde sur la défaillance physique d'un matériel.



1. Maintenance corrective :

La maintenance corrective intervient après la survenue d'une défaillance et vise à remettre un équipement ou un système en état de fonctionnement. Elle se décline en deux formes :

- **la maintenance palliative** : consiste à apporter une solution temporaire afin de maintenir l'activité en attendant une réparation définitive

Dans le cas de PrintCorp, un utilisateur à un ordinateur inapproprié (cassé/dysfonctionnement du clavier/…). Lui prêter un ordinateur en attendant de pouvoir réparer et changer le sien est une maintenance palliative.

- **la maintenance curative** : vise à corriger définitivement la panne.

Par exemple, après diagnostic d'un disque dur défectueux sur un serveur de base de données, l'équipe Infrastructure procède au remplacement du disque avec restauration intégrale des données, assurant la pérennité de la solution.

Chez PrintCorp, ces deux formes de maintenance sont encadrées par des procédures précises et des délais d'intervention définis dans les SLA, afin de limiter l'impact sur la production.

2. Maintenance préventive

La maintenance préventive repose sur le principe d'anticipation des pannes afin de garantir la continuité de service et de réduire les coûts liés aux arrêts non planifiés. Chez PrintCorp, elle se divise en deux catégories principales :

- **Systématique** : Maintenance préventive exécutée à des intervalles de temps préétablis ou selon un nombre défini d'unités d'usage mais sans contrôle préalable de l'état du bien.

Par exemple, les **imprimantes réseau** font l'objet d'un **nettoyage et remplacement des pièces d'usure tous les six mois**, sur la base des statistiques de panne.

- **Conditionnel** : Maintenance préventive basée sur une surveillance du fonctionnement du bien et/ou des paramètres significatifs de ce fonctionnement intégrant les actions qui en découlent.

Ainsi, des **capteurs de température et d'usure** installés dans les **salles serveurs** permettent à l'équipe IT de détecter les signes avant-coureurs d'une défaillance (surchauffe, vibration anormale, etc.) et d'agir avant la panne.

C. Facteur Machine

Chaque matériel a un "facteur machine" dépend de plusieurs critères :

- son niveau de risque **R**
- son importance **I**
- sa charge machine **C**

Plus le facteur machine est haut, plus il est important d'anticiper une action.

Critère \ Valeur	4	3	2	1
Risque **R**	Inacceptable	Répercutions graves sur qualité / délais	Répercutions rattrapables (retouches, retards...)	Risque faible ou Aucun risque
Importance machine **I**	Stratégique	Importante	Banale	Peu importante
Charge machine **C**	Saturée	Forte (> 95%)	Moyenne (80-95%)	Faible (<80%)

On le calcule de la manière suivante : **$Facteur_{machine} = R \times I \times C$**

Il est donc possible de classer les équipements dans plusieurs catégories ainsi que d'adresser une politique de maintenance efficace.

Classe	Type machines	Type de maintenance
A	Critiques	Maintenance conditionnelle
B	Ordinaires	Maintenance préventive
C	Banals	Maintenance curative

D. Etude de cas : Serveur de fichier interne

Le **serveur de fichiers** centralise tous les documents de travail internes de PrintCorp : contrats, bons de commande, procédures techniques, fichiers clients, supports marketing, rapports de production, etc. Il est utilisé par **toutes les directions** (commerciale, IT, juridique, logistique…) et est fortement sollicité en journée. Un arrêt de ce serveur signifie une **interruption immédiate de la productivité** de la majorité des employés.

Critère	Valeur	Justification
Risque (R)	3	Perte d'accès aux documents critiques et arrêt du travail dans plusieurs services.
Importance (I)	4	Ressource transversale pour tous les départements.
Charge machine (C)	3	Charge soutenue (> 90%) pendant les heures de bureau.

Facteur machine = R × I × C = 3 × 4 × 3 = 36
Ce score le classe parmi les **équipements critiques de classe A**, nécessitant une **maintenance conditionnelle renforcée**.

Solutions de maintenance à mettre en place

- Surveillance conditionnelle via outils de monitoring (ZABBIX)
- Alerte sur seuil critique
- Redondance matérielle
- Plan de maintenance systématique trimestrielle
- Sauvegarde locale et cloud hybride
- Tests mensuels de restauration
- Audit annuel de la structure de fichiers et archivage automatique

Indicateurs de performance associés

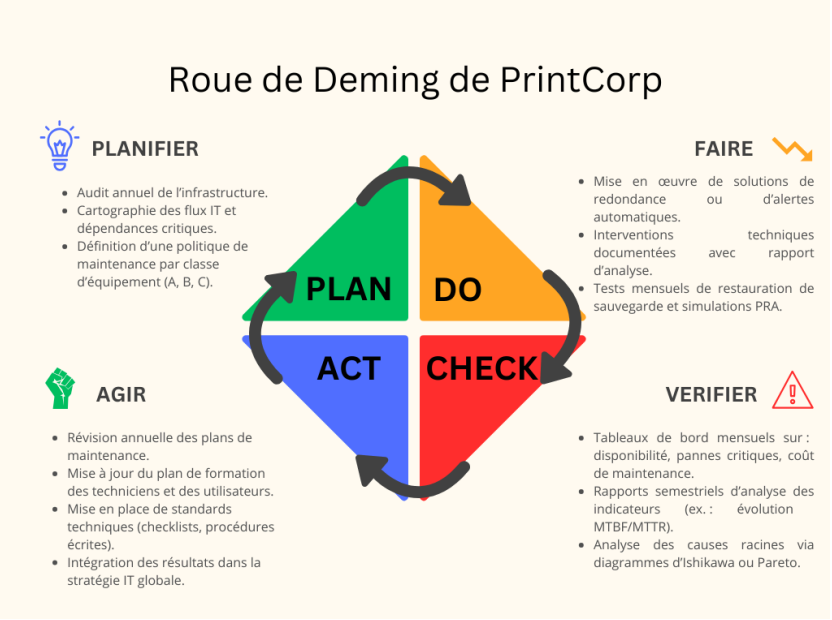
- **MTBF cible** : > 1500 heures (prévenir les pannes disques ou surcharge)
- **MTTR cible** : < 2 heures (intervention rapide avec pièces de rechange disponibles)
- **Taux de disponibilité visé** : > 99,5 % (moins de 2 jours d'arrêt par an)

E. Amélioration continue

Pour l'amélioration continue de PrintCorp, on va utiliser le principe de la roue de Deming (page 63).

La roue de Deming ou PDCA est utilisée pour optimiser les processus. Il repose sur quatre étapes : **Planifier** les objectifs et les actions, **Réaliser** les tâches prévues, **Vérifier** les résultats obtenus, puis **Agir** pour corriger ou améliorer. Ce modèle itératif permet de structurer les actions correctives et préventives dans une logique de progression constante. Il est largement utilisé en gestion de la qualité, maintenance et management opérationnel.

Pour le cas de PrintCorp, on peut définir la roue suivante :



VIII. Veille Technologique

Lors de la conception jusqu'à l'écriture du projet PrintCorp, je m'assurai de maintenir mes informations à jours. En effet, j'effectue une veille technologique quotidiennement. J'ai à ma disposition un ensemble de sites spécialisés sur l'informatique et chacun avec sa spécialité. Je vous transmet cette documentation :

IT

- **ZDNet** (https://www.zdnet.fr/) – Actualité technologique et analyses.
- **Silicon.fr** (https://www.silicon.fr/) – Tendances IT et cybersécurité.
- **01net** (https://www.01net.com/) – Actualités générales sur le numérique.
- **LeMagIT** (https://www.lemagit.fr/) – Articles techniques pour pros IT.
- **Journal du Net (JDN)** (https://www.journaldunet.com/) – Transformation numérique et innovations.

Cybersécurité & Réseaux

- **CERT-FR (ANSSI)** (https://www.cert.ssi.gouv.fr/) – Alertes de sécurité officielles.
- **Krebs on Security** (https://krebsonsecurity.com/) – Blog reconnu en cybersécurité.
- **Bleeping Computer** (https://www.bleepingcomputer.com/) – Vulnérabilités et malwares.
- **The Hacker News** (https://thehackernews.com/) – Actualités cyber.
- **Security Week** (https://www.securityweek.com/) – Tendances et incidents de sécurité.

Communautés & veille collaborative

- **Reddit** (https://www.reddit.com/r/netsec/, https://www.reddit.com/r/sysadmin/) – Forums spécialisés.
- **Stack Overflow / Stack Exchange** (https://stackoverflow.com/) – Échanges techniques.
- **GitHub Trending** (https://github.com/trending) – Suivi des projets open source populaires.
- **Medium (section Tech & Security)** (https://medium.com/) – Articles de spécialistes.

IX. Annexes

Audit de PrintCorp (par PrintCorp)

Site	Nombre de serveurs	Nombre de PC	Routeurs	Points d'accès Wi-Fi	Téléphonie	Observations
Paris (Siège)	4	90	1	8	Téléphonie analogique	- Serveurs pour ERP, CRM, et Active Directory. - Routeur unique avec des limites de performances. - Téléphonie analogique non centralisée.
New York	3	60	1	6	Téléphonie analogique	- Serveur pour gestion locale et cache des applications métiers. - Wi-Fi basique sans segmentation. - Téléphonie analogique locale.
Berlin	2	50	1	5	Téléphonie analogique	- Serveurs pour gestion logistique et production européenne. - Téléphonie analogique sans interconnexion avec les autres sites.
Singapour	2	30	1	4	Téléphonie analogique	- Serveurs pour données régionales et réplication. - Wi-Fi basique. - Téléphonie analogique locale.
Montréal	10	20	1	3	Téléphonie analogique	- Serveurs principaux pour le data center global. - Téléphonie analogique locale utilisée pour les besoins techniques.

Comparatif NinjaOne

Fonctionnalité	NinjaOne	ConnectWise Automate	Kaseya	Atera
Interface utilisateur	Intuitive et moderne	Robuste, mais peut être complexe	Traditionnelle, en évolution	Moderne et personnalisable
Automatisation	Forte	Forte	Forte	Forte
Intégrations	Nombreuses	Nombreuses	Nombreuses	Nombreuses
Flexibilité	Très élevée	Élevée	Élevée	Élevée
Support client	Réactif	Bon	Variable selon les plans	Bon
Gestion mobile	Oui	Oui	Oui	Oui
Sécurité	Bonne	Bonne	Bonne	Bonne
Mise à jour	Régulière	Régulière	Régulière	Régulière

Problèmes et limites détaillés

- Serveurs physiques vieillissants :
  - Tous les sites utilisent des serveurs sous Windows Server 2012, qui présentent des limites en termes de performances et de support.
  - o Pas de virtualisation ni d'infrastructure centralisée pour la gestion des applications métiers.

- Systèmes de sauvegarde manuels :
  - Les sauvegardes sont effectuées sur des disques durs externes, avec une fréquence irrégulière et un risque élevé de perte de données.

- Réseau non sécurisé :
  - Chaque site utilise un simple routeur pour gérer la connexion Internet, sans segmentation ni protection avancée (ex : pare-feu).

- Routeurs non sécurisés :
  - Chaque site utilise un routeur basique fourni par le fournisseur d'accès Internet.
  - Aucun VLAN ni segmentation réseau pour séparer les services critiques.

- Absence d'un système de supervision :
  - Les serveurs et équipements réseau ne sont pas surveillés en temps réel.
  - Les journaux d'accès et les anomalies ne sont pas analysés.

- Accès aux fichiers non sécurisé :
  - Les employés accèdent aux fichiers via des partages réseaux ouverts, sans gestion fine des permissions.

- Pas de solution centralisée :
  - Les données critiques sont stockées localement sur des disques durs externes ou sur les PC des utilisateurs.

- Pas de politique de sécurité :
  - Les mots de passe sont souvent faibles ou partagés entre plusieurs utilisateurs.
  - Aucune méthode d'authentification forte (ex : MFA).

Environnement de travail obsolète et non homogène :

- ~50% des PC utilisent une version obsolète de Windows (7 et 8).
- Il y a quelques machines qui tournent sous Linux mais ne présentent aucune homogénéité entre elles.
- Trop de postes ont des performances limitées. Processeurs dépassés, manque de ram (4 à 8 Go) ainsi que des disques durs classiques.

Téléphonie et collaboration :

- Pas de système de téléphonie VoIP.
- Les échanges collaboratifs sont faits via des outils basiques ou personnels, souvent non adaptés (ex : emails non sécurisés).

Détail des expériences utilisateurs des utilisateurs sur l'ensemble des sites

1. **Employés du siège à Paris (Direction, Finance, IT, R&D)**

📌 Problèmes rencontrés :

- Temps de réponse très lent des serveurs vieillissants, affectant l'accès aux fichiers et aux applications métiers.
- Accès aux fichiers chaotique : partage réseau mal sécurisé, documents parfois corrompus ou introuvables.
- Problèmes de connexion VPN lorsqu'ils travaillent à distance.
- Pas de supervision IT proactive → les problèmes ne sont détectés qu'une fois critiques.

🖥️ Expérience utilisateur

- Un directeur financier tente d'accéder aux rapports de vente sur un ERP vieillissant, mais l'application met plusieurs minutes à charger. Il abandonne et demande un export manuel à l'IT.
- Un ingénieur R&D veut partager des fichiers volumineux, mais le réseau saturé ralentit tout. Il envoie finalement les fichiers via un service tiers (risque de fuite de données).
- Un administrateur IT passe ses journées à éteindre des incendies : disques saturés, utilisateurs bloqués, demandes urgentes de récupération de fichiers perdus.

2. **Équipe commerciale (New York & Singapour)**

📌 Problèmes rencontrés :

- Système de CRM non centralisé, synchronisation lente entre les sites.
- Mauvaise connexion aux serveurs, entraînant des interruptions de service en rendez-vous client.
- Difficulté d'accès aux ressources techniques en déplacement (absence de solutions cloud efficaces).

🛒 Expérience utilisateur :

- Un commercial à New York en réunion avec un client ne peut pas afficher les catalogues produits car le serveur interne ne répond pas. Il doit utiliser un ancien PDF stocké sur son PC.
- Un manager commercial à Singapour demande une analyse des ventes, mais il faut plusieurs jours pour recevoir un rapport car l'extraction des données est manuelle et lente.

3. **Équipe logistique et production (Berlin)**

📌 Problèmes rencontrés :

- Système de gestion des stocks vieillissant, entraînant des erreurs d'inventaire.
- Machines industrielles mal intégrées au SI, nécessitant des opérations manuelles chronophages.
- Aucune visibilité en temps réel sur la chaîne logistique, entraînant des retards de production.

🏭 Expérience utilisateur :

- Un responsable logistique voit une rupture de stock sur un composant essentiel, mais le système ne l'a pas alerté à temps. La production est stoppée.
- Un technicien doit entrer manuellement les données de production, car les machines ne sont pas connectées au système. Cela crée des erreurs et ralentit les opérations.

4. **Équipe support technique & IT (Montréal)**

📌 Problèmes rencontrés :

- Absence d’outils de monitoring centralisés → difficile de diagnostiquer les pannes à distance.
- Téléphonie analogique obsolète, empêchant une bonne coordination entre les sites.
- Sauvegardes manuelles irrégulières, risque élevé de perte de données.

🛠️ Expérience utilisateur :

- Un technicien support reçoit des plaintes d’utilisateurs dont les fichiers ont disparu. Il doit fouiller des disques externes pour tenter une récupération.
- Un responsable IT voit qu’un serveur critique est saturé, mais ne peut pas agir rapidement faute de supervision automatique.

Détail du matériel de PrintCorp

Postes utilisateurs :

- **110 postes HP:**
  - **90 laptops HP Compaq 6910q (4Go RAM):** Leur faible capacité RAM et leur système d'exploitation obsolète limitent considérablement leurs performances et leur compatibilité avec les logiciels récents.
  - **20 postes fixes HP EliteDesk 800 G1 (i3, 8Go RAM):** ces postes fixes souffrent également d'une capacité de stockage limitée et d'une absence de ports USB 3.0
- **60 laptops Lenovo ThinkPad X270:** Ces laptops sont équipés de systèmes d'exploitation obsolètes (Windows 7 ou 8). Leur configuration est insuffisante pour des applications plus exigeantes.
- **80 laptops DELL Latitude 7480 (16Go RAM):** Ces laptops offrent de bonnes performances grâce à leur processeur de dernière génération et à leur capacité RAM élevée. Ils sont équipés de ports USB 3.0 et d'un SSD, ce qui accélère considérablement les temps de chargement et de réponse.

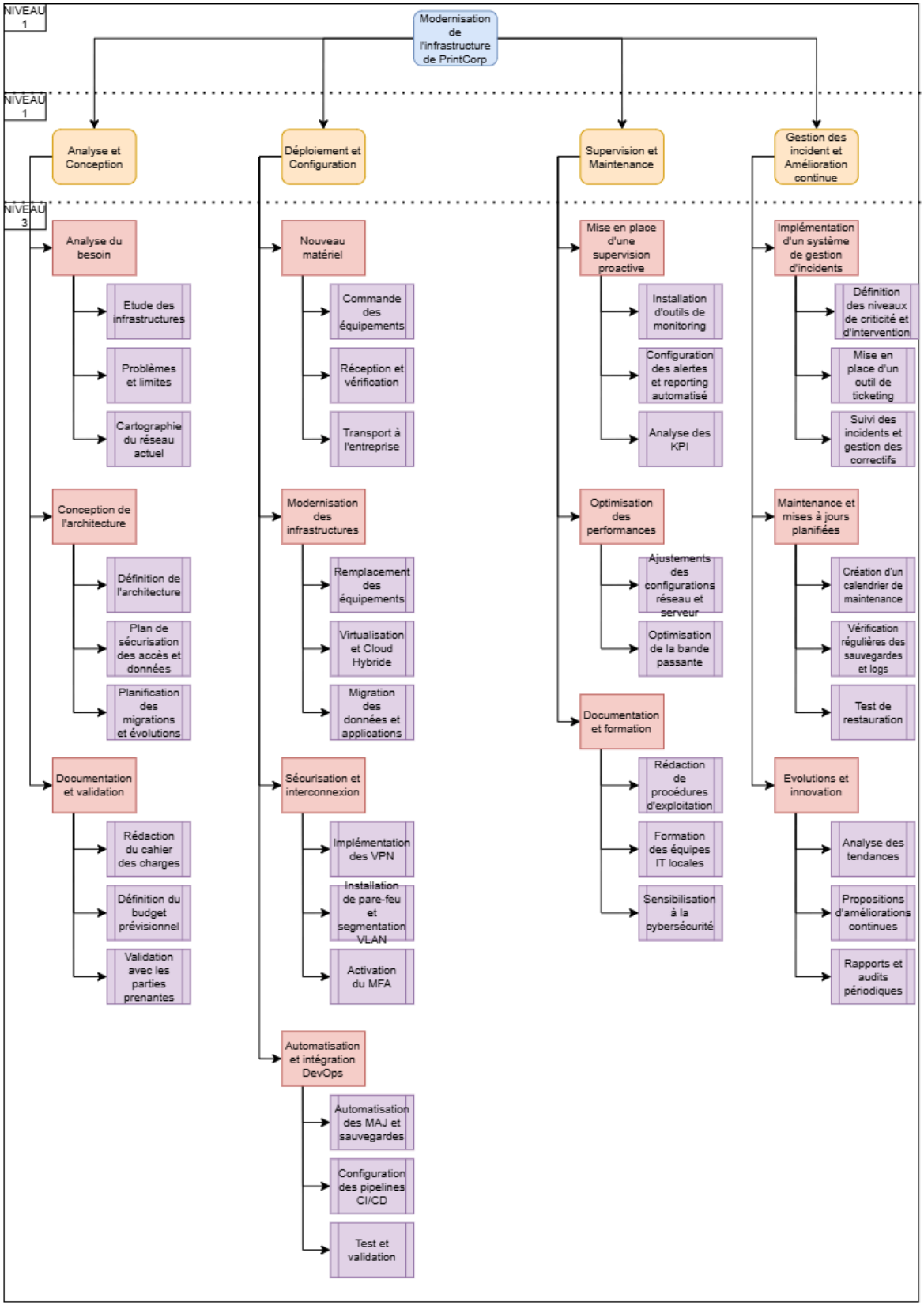
Pour le matériel réseau, on retrouve :

Commutateur TP-LINK JetStream T1600G-28TS
- Géré
- 24 x 10/100/1000
- 4 x SFP Gigabit combiné

Serveur DELL PowerEdge T310
- Xeon Quad Core X3460 2.8Ghz
- 8Go
- 146Go SAS

Synology DiskStation DS1515 5 To
- Boitier 5 baies
- HHD 5 X 1 TO
- Interface disque : SATA II

Tableau WBS


NIVEAU 1
Modernisation de l'infrastructure de PrintCorp
NIVEAU 1
Analyse et Conception
Déploiement et Configuration
Supervision et Maintenance
Gestion des incident et Amélioration continue
NIVEAU 3
Analyse du besoin
Etude des infrastructures
Problèmes et limites
Cartographie du réseau actuel
Conception de l'architecture
Définition de l'architecture
Plan de sécurisation des accès et données
Planification des migrations et évolutions
Documentation et validation
Rédaction du cahier des charges
Définition du budget prévisionnel
Validation avec les parties prenantes
Nouveau matériel
Commande des équipements
Réception et vérification
Transport à l'entreprise
Modernisation des infrastructures
Remplacement des équipements
Virtualisation et Cloud Hybride
Migration des données et applications
Sécurisation et interconnexion
Implémentation des VPN
installation de pare-feu et segmentation VLAN
Activation du MFA
Automatisation et intégration DevOps
Automatisation des MAJ et sauvegardes
Configuration des pipelines CI/CD
Test et validation
Mise en place d'une supervision proactive
Installation d'outils de monitoring
Configuration des alertes et reporting automatisé
Analyse des KPI
Optimisation des performances
Ajustements des configurations réseau et serveur
Optimisation de la bande passante
Documentation et formation
Rédaction de procédures d'exploitation
Formation des équipes IT locales
Sensibilisation à la cybersécurité
Implémentation d'un système de gestion d'incidents
Définition des niveaux de criticité et d'intervention
Mise en place d'un outil de ticketing
Suivi des incidents et gestion des correctifs
Maintenance et mises à jours planifiées
Création d'un calendrier de maintenance
Vérification régulières des sauvegardes et logs
Test de restauration
Evolutions et innovation
Analyse des tendances
Propositions d'améliorations continues
Rapports et audits périodiques

Matrice RACI

Tâches WBS	Direction Générale	DAF & Admin	IT (CTO & Équipes)	Opérations (PMO)	Commercial	R&D & Innovation	Logistique & Achats
1. Analyse et Conception	A	C	R	C	C	C	I
1.1. Analyse des besoins	A	C	R	C	C	C	I
1.2. Conception de l'architecture	A	C	R	C	I	C	I
1.3. Documentation et validation	A	C	R	C	I	I	I
2. Déploiement et Configuration	I	C	R	C	I	C	I
2.1. Nouveau matériel	A	C	R	I	C	I	A
2.2. Modernisation des infrastructures	I	C	R	C	I	C	I
2.3. Sécurisation et interconnexion	I	C	R	C	I	C	I

2.4. Automatisation et intégration DevOps	I	C	R	C	I	C	I
3. Supervision et Maintenance	I	C	R	C	I	C	I
3.1. Supervision proactive	I	C	R	C	I	C	I
3.2. Optimisation des performances	I	C	R	C	I	C	I
3.3. Documentation et formation	I	C	R	C	I	I	I
4. Gestion des Incidents & Amélioration Continue	I	C	R	C	I	C	I
4.1. Gestion des incidents	I	C	R	C	I	I	I
4.2. Maintenance et mises à jour	I	C	R	C	I	I	I
4.3. Évolutions et innovation	I	C	R	C	I	R	I

Méthodologie PRINCE2

1. Démarrage du Projet (Starting Up a Project - SU)

Objectif : Valider la faisabilité et cadrer le projet.

WBS ciblé : Analyse du besoin / Documentation et validation

Activités clés :

- **Analyse du contexte PrintCorp :**
  - Diagnostic de l'infrastructure vieillissante.
  - Identification des besoins en virtualisation et en sécurité.
- **Identification des parties prenantes :**
  - Direction IT PrintCorp (décideurs techniques).
  - Direction Générale PrintCorp (validation budgétaire).
  - Employés utilisateurs (impact direct).
  - Direction ReNewIt (planification et exécution).
- **Validation du Business Case :**
  - Évaluer le retour sur investissement (ROI) des solutions IT proposées.
  - Chiffrage des économies réalisées (réduction coûts maintenance, amélioration productivité).
- **Nomination des rôles clés chez ReNewIt :**
  - **Chef de projet global :** Supervise la mise en œuvre.
  - **Responsable technique :** Définit l'architecture et les choix technologiques.
  - **Responsable sécurité :** Gère l'intégration des mesures de cybersécurité.
  - **Consultants infrastructure :** Experts techniques sur les migrations et la virtualisation.
- **Préparation du Plan de Projet Initial (Project Brief).**

Livrables :
✅ **Étude de faisabilité**
✅ **Business Case** validé par PrintCorp
✅ **Équipe projet nommée**
✅ **Plan de phase d'initiation**

---

2. Initialisation du Projet (Initiating a Project - IP)

Objectif : Définir précisément la gouvernance et les étapes clés.

WBS ciblé : Conception de l'architecture

Activités clés :

- **Élaboration du Plan de Projet détaillé :**
  - Séquencement des tâches de migration et virtualisation.
  - Définition des jalons clés (installation serveurs, test réseau, formation utilisateurs).
- **Plan de gestion des risques :**

    - Risque : Panne lors de la migration → Solution : Plan de rollback avec infrastructure temporaire.
    - Risque : Résistance au changement des employés → Solution : Communication et formation progressive.
- **Définition des critères de qualité :**
    - Serveurs virtualisés fonctionnels avec un SLA de 99,9 %.
    - Réseau sécurisé avec firewall et authentification forte.
    - Performance améliorée avec un temps de réponse < 50 ms.
- **Organisation de la communication interne/externe :**
    - Réunions hebdomadaires avec PrintCorp pour reporting.
    - Documentation technique et guides utilisateurs.
    - Sessions de formation sur les nouveaux outils.

Livrables :
✅ **Project Initiation Document (PID)**
✅ **Plan de gestion des risques**
✅ **Plan de gestion de la qualité**
✅ **Stratégie de communication interne/externe**

---

3. Diriger un Projet (Directing a Project - DP)

Objectif : Assurer un pilotage efficace par la direction de ReNewIt et PrintCorp.

WBS ciblé : Documentation et validation

Activités clés :

- **Suivi stratégique des jalons avec la Direction PrintCorp :**
    - Validation des infrastructures réseau et serveurs avant migration.
    - Feu vert pour le déploiement progressif.
- **Gestion des décisions stratégiques :**
    - Ajustements budgétaires si nécessaire.
    - Choix entre solutions cloud public ou hybride en fonction des tests initiaux.
- **Communication avec les équipes opérationnelles :**
    - Transmission des priorités aux équipes terrain (techniciens, ingénieurs).
    - Ajustements sur la roadmap en cas d'imprévus.

Livrables :
✅ **Rapports d'avancement à la direction**
✅ **Feu vert pour les étapes critiques du projet**

---

4. Contrôle d'une Séquence (Controlling a Stage - CS)

Objectif : Suivre et ajuster le déploiement.

WBS ciblé : Nouveau matériel / Modernisation des infrastructures / Sécurisation et interconnexion

Activités clés :

- **Phase 1 : Modernisation infrastructure locale**
  - Installation des serveurs physiques et virtualisation (VMware/Hyper-V).
  - Déploiement des firewalls et segmentation réseau.
  - Migration des premiers services internes (ex : messagerie).
- **Phase 2 : Migration Cloud progressive**
  - Transfert des applications vers le cloud hybride.
  - Tests de connectivité et performances.
  - Sécurisation des accès distants.
- **Phase 3 : Formation et adoption**
  - Sessions de formation des employés.
  - Mise en place de la documentation utilisateur.
  - Suivi des KPI de satisfaction.

Livrables :
✅ **Environnements IT modernisés**
✅ **Tests de performance et sécurité validés**
✅ **Formation des utilisateurs**

---

5. Gestion de la Livraison des Produits (Managing Product Delivery - MP)

Objectif : Assurer une transition fluide vers la nouvelle infrastructure.

WBS ciblé : Mise en place d'une supervision proactive / Optimisation des performances Documentation et formation / Implémentation d'un système de gestion d'incidents

Activités clés :

- **Validation des performances :** Tests de charge et sécurité.
- **Documentation technique :** Guide d'exploitation pour les équipes IT de PrintCorp.
- **Support post-déploiement :** Assistance pendant les premières semaines.

Livrables :
✅ **Nouveaux systèmes opérationnels**
✅ **Documentation et guides livrés**
✅ **Assistance technique en place**

---

6. Gestion des Limites de Séquence (Managing a Stage Boundary - SB)

Objectif : Évaluer chaque phase et ajuster le projet.

WBS ciblé : Évolutions et innovation

Activités clés :

- **Révision des performances après chaque phase.**
- **Correction des problèmes remontés par les utilisateurs.**

- **Validation des prochaines étapes avant de continuer.**

Livrables :
✅ **Rapports d'évaluation**
✅ **Mise en place des ajustements nécessaires**

---

7. Clôture du Projet (Closing a Project - CP)

Objectif : Assurer un passage de relais efficace.

Activités clés :

- **Évaluation des bénéfices atteints :**
  - Sécurité améliorée, systèmes modernisés, réduction des incidents IT.
- **Retour d'expérience (RETEX) :**
  - Ce qui a fonctionné, ce qui peut être amélioré.
- **Handover vers les équipes internes de PrintCorp :**
  - Dernière formation.
  - Remise de la documentation finale.

Livrables :
✅ **Rapport final du projet**
✅ **Évaluation de la satisfaction utilisateur**
✅ **Clôture contractuelle avec PrintCorp**

Détail du risque de MONTRÉAL

Etude de cas : La salle Serveur de MONTRÉAL

Définition des risques

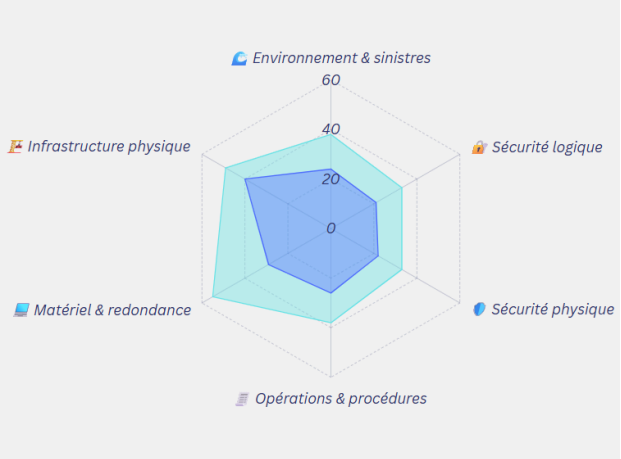
Définition des catégories du ticket pour ce risque :

- Infrastructure physique: Risques liés au bâtiment, à l'alimentation, au refroidissement, etc.
- Sécurité physique: Accès non autorisé, surveillance, intrusion…
- Sécurité logique: Contrôle d'accès, supports amovibles, PRA/PCA, etc.
- Matériel & redondance: Pannes, obsolescence, redondance, support…
- Environnement & sinistres: Incendie, inondation, séisme, nuisibles…
- Opérations & procédures: Documentation, erreurs humaines, maintenance, conformité…

Nous allons décrire l'ensemble des risques possible assigner à la salle serveur de Montréal ainsi que sa catégorie, son impact, sa probabilité et sa criticité (voir annexe)

Mise en place du plan de prévention pour chaque risque (voir annexe)

Voici le même diagramme pour comparer l'avant/après le plan de prévention en fonction de leurs criticités.



On peut clairement voir la différence de criticités. Certaines catégories ont perdu la moitié de valeurs.

Focus : Panne de Courant

Catégorie : Infrastructure physique
Responsable : Responsable Infrastructure & Maintenance – Direction Technique (**Lucas Bernard** / Service Infrastructure & Cloud)

Descriptif du risque :

Le site de Montréal héberge une salle serveur critique pour le fonctionnement de l'entreprise. En cas de panne d'alimentation électrique, l'ensemble des équipements informatiques (serveurs, stockage, réseaux) serait instantanément arrêté, provoquant une interruption de service totale. Cela inclut l'accès aux données, aux applications, et aux ressources réseau.

Causes possibles du risque :

- Incident sur le réseau électrique public (tempête, surcharge, panne locale)
- Travaux de voirie ou d'électricité dans la zone
- Dysfonctionnement du tableau électrique interne
- Mauvais entretien de l'installation électrique

Impacts estimés :

- **Coût :** Élevé – perte d'exploitation, interventions d'urgence, matériel endommagé
- **Délai :** Rétablissement du service pouvant prendre de quelques heures à plusieurs jours selon la gravité
- **Valeur ajoutée :** Forte atteinte à la disponibilité des services, avec conséquences sur la productivité et la relation client

Probabilité estimée :

- **Avant plan de prévention :** 4/5 – Risque jugé fréquent dans la région en raison de conditions météorologiques saisonnières
- **Impact :** 5/5 – Tous les services IT seraient indisponibles sans alimentation
- **Criticité : 20 / Critique** 🔴

Actions de surveillance :

- Contrôle régulier des équipements électriques (tableaux, disjoncteurs, onduleurs)
- Supervision de la tension réseau via des sondes SNMP et alertes automatiques
- Revue semestrielle des rapports d'incidents électriques
- Test de bascule en mode secours (alimentation de secours) deux fois par an

Actions préventives :

- Installation d'un **onduleur (UPS)** double conversion dimensionné pour l'ensemble des équipements critiques
- Mise en place d'un **groupe électrogène** avec démarrage automatique et autonomie suffisante (>8h)
- Intégration du risque dans le **PRA (Plan de Reprise d'Activité)** avec priorité haute
- Maintenance préventive du système d'alimentation : tests, changements de batteries UPS tous les 3 ans

Actions correctives et de contournement :

- En cas de coupure prolongée : activation du groupe électrogène via démarrage automatique
- Bascule des services critiques vers un site secondaire si la coupure dépasse la durée prévue (dans le cadre du PRA)
- Notification immédiate aux équipes techniques et à la Direction
- Redémarrage contrôlé des serveurs et équipements réseau après stabilisation

Nouvelle évaluation du risque après mise en place des solutions :

- **Nouvelle probabilité :** 2/5 (moins probable grâce aux protections)
- **Impact :** 5/5 (impact toujours maximal si le risque survient)
- **Nouvelle criticité : 10 / Moderé**🟡

#	Risque	Catégorie	Impact (I)	Probabilité (P)	Criticité (I×P)	Niveau
1	Incendie	🌊 **Environnement & sinistres**	5	2	10	Élevé 🔶
2	Inondation	🌊 **Environnement & sinistres**	5	3	15	Élevé 🔶
3	Surchauffe (clim défaillante)	🏗️ **Infrastructure physique**	4	5	20	**Critique** 🔴
4	Coupure électrique	🏗️ **Infrastructure physique**	5	4	20	**Critique** 🔴
5	Variation de tension	🏗️ **Infrastructure physique**	3	3	9	Modéré 🟡
6	Poussières et particules	🌊 **Environnement & sinistres**	2	3	6	Modéré 🟡
7	Infestation nuisible	🌊 **Environnement & sinistres**	2	2	4	Faible 🟢
8	Séisme (léger)	🌊 **Environnement & sinistres**	3	1	3	Faible 🟢
9	Intrusion ou vandalisme	🛡️ **Sécurité physique**	4	3	12	Élevé 🔶
10	Défaillance matérielle	💻 **Matériel & redondance**	4	4	16	Critique 🔴
11	Panne de sauvegarde	💻 **Matériel & redondance**	5	3	15	Élevé 🔶
12	Absence de redondance	💻 **Matériel & redondance**	4	3	12	Élevé 🔶

13	Obsolescence matériel	💻 **Matériel & redondance**	3	4	12	Élevé 🔶
14	Erreur humaine	🗒️ **Opérations & procédures**	3	3	9	Modéré 🟡
15	Personnel non qualifié	🗒️ **Opérations & procédures**	4	2	8	Modéré 🟡
16	Accès non maîtrisé	🛡️ **Sécurité physique**	5	3	15	Élevé 🔶
17	Absence de PRA/PCA	🔐 **Sécurité logique**	5	3	15	Élevé 🔶
18	Doc. obsolète/inexistante	🗒️ **Opérations & procédures**	3	3	9	Modéré 🟡
19	Maintenance non planifiée	🗒️ **Opérations & procédures**	3	4	12	Élevé 🔶
20	Non-conformité réglementaire	🔐 **Sécurité logique**	3	2	6	Modéré 🟡
21	Pas de vidéosurveillance	🛡️ **Sécurité physique**	2	3	6	Modéré 🟡
22	Supports amovibles non filtrés	🔐 **Sécurité logique**	4	3	12	Élevé 🔶

Plan de prévention de MONTRÉAL

Environnement & sinistres							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
1	Incendie	5	2	10	Détection & extinction automatique	1	5
2	Inondation	5	3	15	Détection fuite + évacuation	2	10
3	Séisme (léger)	3	1	3	Infrastructure aux normes	1	3
6	Poussière	2	3	6	Nettoyage + filtration	2	4
7	Infestation	2	2	4	Traitement préventif	1	2
Environnement & sinistres		17	11	38		7	24

Sécurité logique							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
22	Supports amovibles non filtrés	4	3	12	GPO, restriction ports USB	2	8
17	Absence de PRA/PCA	5	3	15	PRA testé et répliqué à distance	2	10
20	Non-conformité réglementaire	3	2	6	Conformité RGPD/ISO	1	3
Sécurité logique		12	8	33		5	21

Sécurité physique							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
9	Intrusion ou vandalisme	4	3	12	Contrôle d'accès + vidéosurveillance	2	8
16	Accès non maîtrisé	5	3	15	Contrôle d'accès + vidéosurveillance	2	10
21	Absence de vidéosurveillance	2	3	6	Mise en place caméras IP	2	4
Sécurité physique		11	9	33		6	22

Opérations & procédures							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
11	Panne de sauvegarde	5	3	15	PRA + supervision	2	10
18	Documentation obsolète	3	3	9	Mise à jour régulière	2	6
14	Erreur humaine	3	3	9	Procédures + formation	2	6
15	Personnel non qualifié	4	2	8	Formations certifiantes	1	4
Opérations & procédures		15	11	41		7	26

Matériel & redondance							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
10	Défaillance matérielle	4	4	16	Renouvellement tous les 3 ans	3	12
13	Obsolescence matériel	3	4	12	Inventaire + remplacement planifié	3	9
12	Absence de redondance	4	3	12	Redondance matérielle	2	8
Matériel & redondance		11	11	40		8	29

Infrastructure physique							
#	Risque	Impact	Proba.	Crit.	Plan de prévention	N. Proba	N. Crit.
4	Coupure électrique	5	4	20	Onduleur + groupe électrogène	2	10
5	Variation de tension	3	3	9	Équipements régulés + onduleurs	2	6
19	Maintenance non planifiée	3	4	12	Planning + GMAO	3	9
8	Séisme (léger)	3	1	3	Infrastructure renforcée	1	3
3	Surchauffe	4	5	20	Clim redondée + alerte température	3	12
Infrastructure physique		18	17	64		11	40

Script sauvegarde

```
# === CONFIGURATION ===
$SourcePath = "C:\Users\Public\Documents\Critiques"       # Dossier à sauvegarder
$BackupRoot = "\\serveur-sauvegarde\Sauvegardes\"         # Destination réseau ou locale
$Date = Get-Date -Format "yyyy-MM-dd_HH-mm"
$BackupPath = Join-Path $BackupRoot "Sauvegarde_$Date"

# === CRÉATION DU DOSSIER DE SAUVEGARDE ===
if (!(Test-Path -Path $BackupPath)) {
    New-Item -ItemType Directory -Path $BackupPath -Force | Out-Null
}

# === COPIE DES FICHIERS ===
try {
    Robocopy $SourcePath $BackupPath /E /Z /R:3 /W:5 /NP /LOG:"$BackupPath\log.txt"
    Write-Host "Sauvegarde terminée avec succès à : $BackupPath"
} catch {
    Write-Error "Une erreur est survenue lors de la sauvegarde : $_"
}
```

Roue de Deming

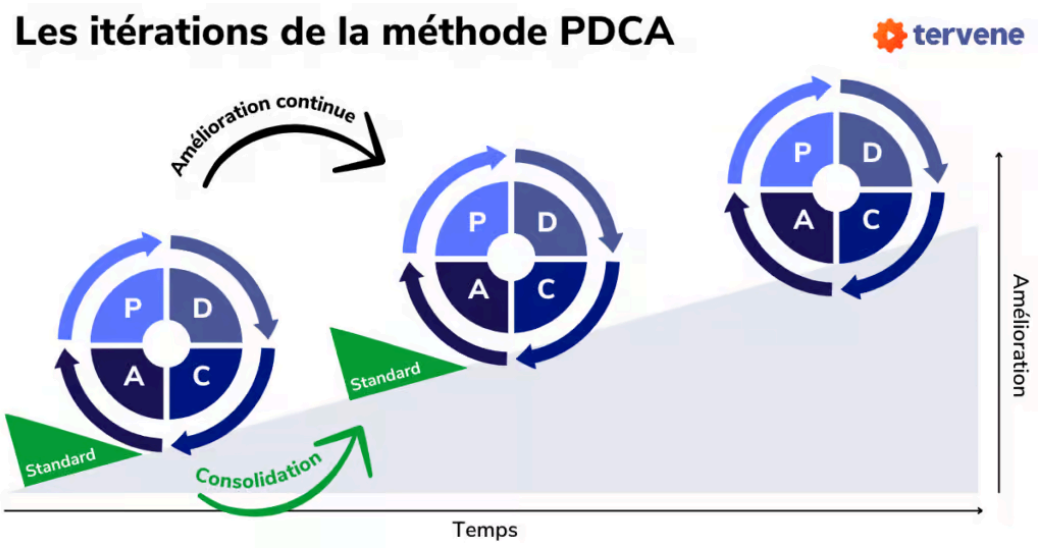


Diagramme de Gantt