KATANE

EFREI B1-CS2 COURS

19 septembre 2025

Qui suis-je ?

Nafissata JEGOU

Présidente de la société KATANE Cybersécurité

nafissata.jegou@katane.fr / +33 6 09 49 68 14

EFREI

BACHELOR - GESTION DE PROJET

Cybersécurité et développement durable

01

Les fondamentaux de la gestion de projet

1.Définitions générales
2.Le cycle de vie du projet: du BUILD au RUN
3. Les phases clés de la gestion de projet
4. Le triangle d'or (coût, délai, qualité)
5. Gouvernance : rôles & responsabilité
Projets :

- Réalisation d'un GANTT
- Réalisation d'un RACI

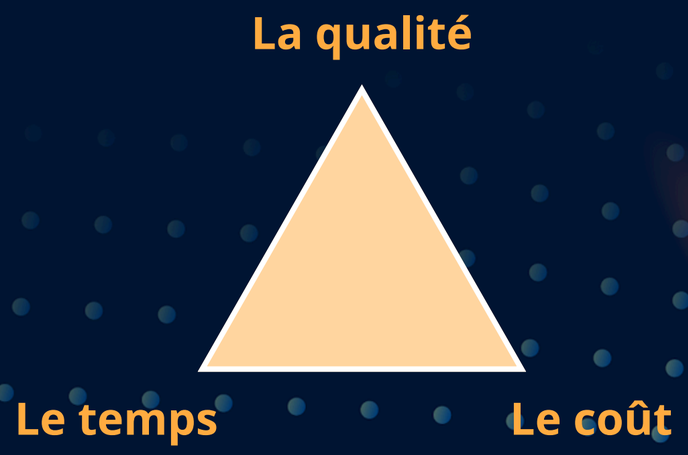
Définition : qu’est-ce qu’un projet ?

Un ensemble d'activités ou d'actions qui sont réalisées pour atteindre un **objectif**

Il se distingue des opérations courantes par plusieurs caractéristiques fondamentales par une **durée de vie limitée** et un **objectif unique** : Il vise à produire un livrable ou un résultat spécifique qui n'existait pas auparavant.

Des contraintes majeures interdépendantes que le projet doit respecter :

Le temps (les délais et les dates limites)
Le coût (le budget et les ressources)
La qualité (les spécifications et les fonctionnalités du livrable)



Dans quel contexte réalisons nous la gestion de projet

Dans toutes les entreprises, par exemple :

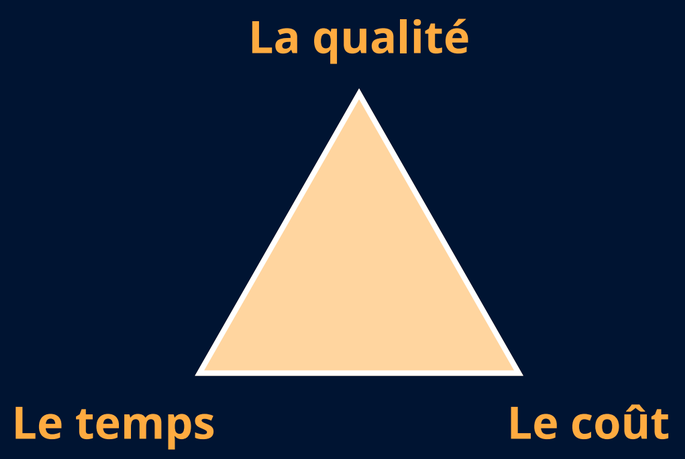
L'IT (technologie de l'information)

Bâtiment (construction)

Marketing (Lancement d'un produit)

Education (Réforme d'un programme scolaire)

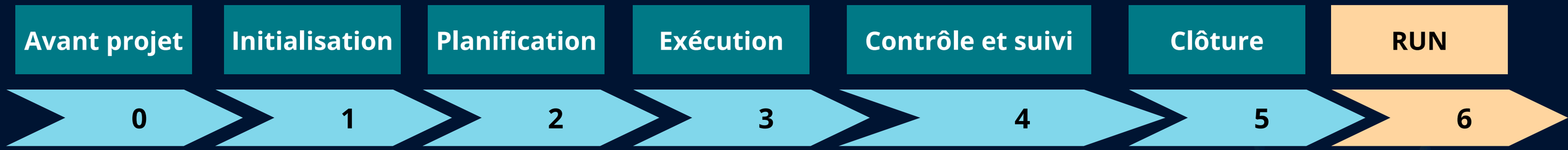
Définition : Triangle d’or



+ Sécurité

+ Durabilité

Phases clés de la gestion de projet



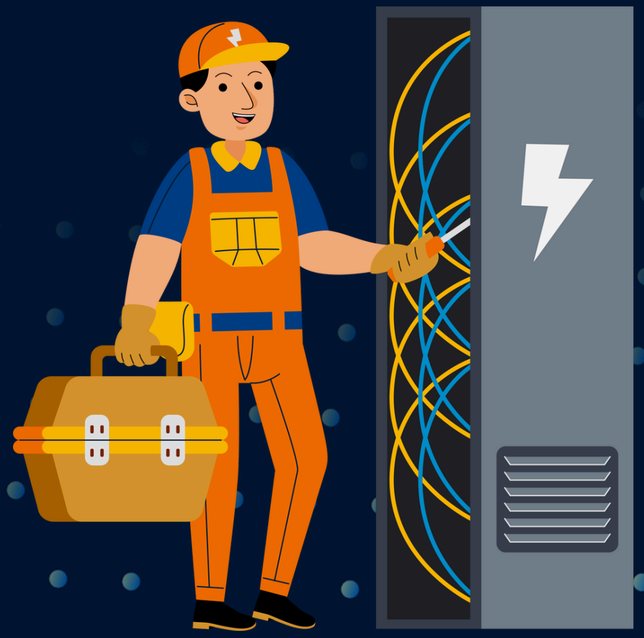
BUILD - RUN

BUILD

Construction et mise en place

RUN

Exploitation & maintenance



BUILD - RUN

Caractéristique	Phase BUILD	Phase RUN
Objectif	Construire et livrer un système.	Maintenir le système en production.
Responsabilité	Équipe de projet (développement).	Équipe d'exploitation (maintenance, support).
Durée	Limitée dans le temps (début et fin).	Continue, tant que le système est utilisé.
Indicateurs clés	Respect du budget, des délais et du périmètre.	Disponibilité (SLA), temps de résolution des incidents.

Rôles et responsabilités

Chef de projet *: Il supervise et pilote l'ensemble des activités du projet, de l'initialisation à la clôture.*

Sponsor du projet *: Acteur clé qui entoure le projet et influence son bon fonctionnement. La validation finale des livrables incombe souvent au sponsor.*

Project Management Office (PMO) *: Dans le cadre par exemple de programme (composition de plusieurs projets), il a pour mission d'apporter un soutien individualisé aux chefs de projet, de coordonner les ressources et d'avoir une vision stratégique du portefeuille de projets.*

Scrum Master *: Dans les méthodologies agiles, il est le chef d'orchestre pour la bonne organisation du projet.*

Product Owner / Responsable Produit *: Également un rôle clé dans les projets agiles. Il est la personne de référence pour les questions liées aux exigences, aux évolutions et à l'allocation des ressources du projet.*

Membres de l'équipe projet ***:*** *Ce sont les ressources humaines (internes ou externes) qui exécutent les tâches nécessaires à la réalisation du projet.*

Parties prenantes *: Cet ensemble inclut toutes les personnes ou groupes qui peuvent influencer le projet ou être affectés par celui-ci, comme la Direction générale, les métiers (marketing, finance), et les partenaires.*

Besoins / exigences / Spécifications

KATANE

Le besoin est le point de départ. C'est le problème qu'on cherche à résoudre ou l'opportunité qu'on veut saisir. Il est principalement exprimé par l'utilisateur final ou le client.

Exemple : J'ai besoin de protéger les données personnelles de mes clients

Une fois le besoin identifié, il faut le transformer en **exigences**. Elles sont une traduction du besoin en critères mesurables, testables et réalisables. Elles précisent "quoi" faire, sans décrire "comment" le faire. Il existe deux types d'exigences : fonctionnelles & non fonctionnelles

Exemple : "Le système doit permettre aux utilisateurs de s'authentifier."

La **spécification** est le document technique qui détaille "comment" les exigences seront satisfaites.

Exemple : "Le système doit utiliser une technique dde chiffrement xxx

Du besoin à l’objectif SMART

Un objectif SMART est une méthode pour définir un objectif de manière claire et précise.

S : Spécifique : L'objectif doit être précis et clairement défini. "Qui est concerné ?", "Qu'est-ce que je veux accomplir ?" et "Où et quand ?"
non-SMART : "Je veux être plus productif” / SMART : "Je veux terminer le rapport financier pour la fin du mois."

M : Mesurable : L'objectif doit être quantifiable. Il faut pouvoir mesurer le succès ou l'échec de l'objectif avec un chiffre ou un indicateur. "Combien ?" ou "À quelle fréquence ?"
non-SMART : "Je veux avoir plus de clients." / SMART : "Je veux acquérir 10 nouveaux clients par mois."

Du besoin à l’objectif SMART

A : Atteignable : L'objectif doit être réaliste et à la portée de la personne ou de l'équipe qui doit l'atteindre. Un objectif trop ambitieux peut démotiver. Il répond à la question : "Est-ce que c'est possible avec les ressources dont je dispose ?"
non-SMART : "Je veux devenir milliardaire en un an." SMART : "Je veux augmenter mon chiffre d'affaires de 15 % au prochain trimestre.”

R : Réaliste : L'objectif doit être pertinent. Il doit s'inscrire dans une stratégie plus large et avoir du sens pour l'entreprise ou la personne. Il répond à la question : "Est-ce que cet objectif est important pour moi ou mon entreprise ?"
non-SMART : "Je vais apprendre le japonais pour un voyage aux États-Unis." SMART : "Je vais passer ma certification en cybersécurité pour évoluer dans mon poste."

T : Temporellement défini : L'objectif doit avoir une date limite. Sans échéance, un objectif risque de ne jamais être atteint. Il répond à la question : "Pour quand ?"
non-SMART : "Je veux être certifié." SMART : "Je veux obtenir ma certification d'ici le 30 novembre."

Exercice : du besoin vague à l'objectif SMART

KATANE

Pour chacun des besoins suivants, travaillez en groupe pour transformer les besoin en un objectif SMART (Spécifique, Mesurable, Atteignable, Réaliste, Temporellement défini).

Besoin A : "Nous devons renforcer la sécurité de notre application web."

Besoin B : "Notre entreprise doit réduire son empreinte environnementale liée à l'informatique."

Besoin C : "Nous devons former nos employés à la cybersécurité."

Besoin D : "Nous devons mieux gérer les mises à jour de sécurité de nos systèmes."

Plannification d’un projet

En résumé, la planification n'est pas une simple formalité, mais un processus rigoureux qui permet de s'assurer que vous avez une feuille de route claire pour atteindre vos objectifs. Sans une bonne planification, même le meilleur projet peut dérailler.

Méthode possible : Diagramme de Gantt : Celui-ci a été inventé par **Henry Gantt en 1910.** C’est une représentation graphique des tâches d’un projet sur une échelle de temps. Il permet de mettre en évidence le chemin critique par lequel vous devez passer pour réaliser vos projets.

Grâce au diagramme de Gantt vous visualisez:

- les différentes étapes du projet
- l’enchaînement des tâches
- le délai de chaque tâche
- les dépendances entre les tâches
- le chevauchement entre les activités

Plannification - exemple diagramme de gantt

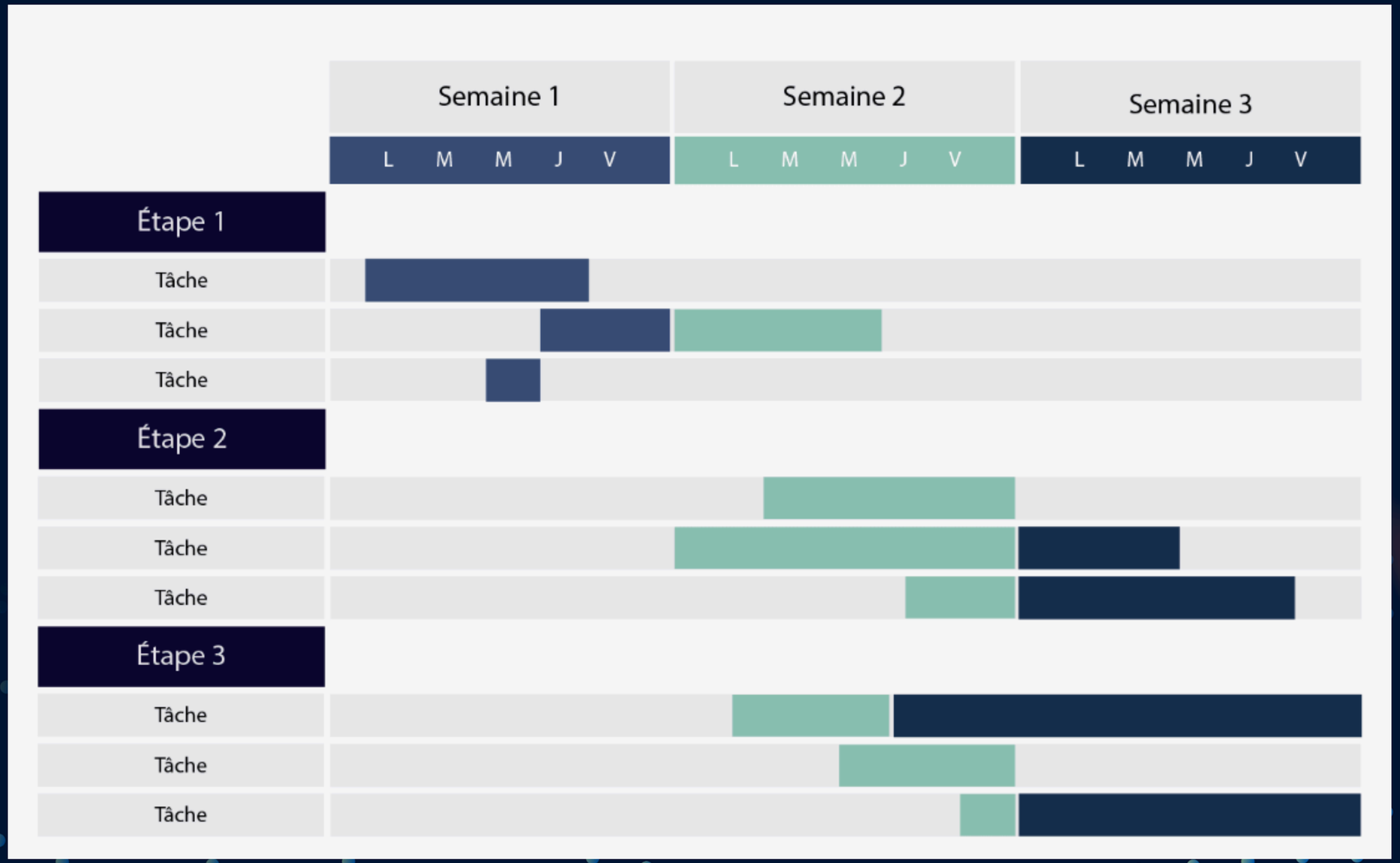


Diagramme de gantt - exercice 1 Lancement d'un Centre d'Opérations de Sécurité (SOC)

Vous êtes chef de projet pour la mise en place d'un Centre d'Opérations de Sécurité (SOC) au sein d'une entreprise de taille moyenne. Ce projet est critique et implique plusieurs équipes. Le projet doit être lancé dans 15 semaines.

Tâches, durées, dépendances et ressources :

Phase 1 : Planification et Conception (Semaines 1-4)

Tâche A : Définir les besoins et les exigences du SOC (Durée : 3 semaines). Ressource : Chef de projet, expert en cybersécurité.
Tâche B : Choisir la solution technologique (SIEM, EDR, etc.) (Durée : 2 semaines). Dépend de la Tâche A. Ressource : Expert en cybersécurité, architecte réseau.

Phase 2 : Infrastructure et Déploiement (Semaines 5-10)

Tâche C : Commander et recevoir le matériel (serveurs, etc.) (Durée : 4 semaines). Dépend de la Tâche B. Ressource : Équipe d'achats.
Tâche D : Installer et configurer les serveurs (Durée : 3 semaines). Dépend de la Tâche C. Ressource : Administrateur système, équipe d'infrastructure.
Tâche E : Déployer et configurer les outils de sécurité (SIEM, EDR) (Durée : 5 semaines). Dépend de la Tâche D. Ressource : Expert en cybersécurité.

Phase 3 : Intégration et Tests (Semaines 11-13)

Tâche F : Intégrer les outils de sécurité avec l'infrastructure existante (Durée : 2 semaines). Dépend de la Tâche E. Ressource : Expert en cybersécurité, administrateur système.
Tâche G : Former l'équipe du SOC aux nouveaux outils (Durée : 3 semaines). Dépend de la Tâche E. Ressource : Expert en cybersécurité, équipe de formation. Note : Cette tâche peut se faire en parallèle avec la Tâche F.

Phase 4 : Validation et Go-Live (Semaines 14-15)

Tâche H : Réaliser les tests de validation finaux (Durée : 2 semaines). Dépend de la Tâche F. Ressource : Auditeur externe, expert en cybersécurité.
Tâche I : Lancement officiel du SOC (Go-Live) (Durée : 1 semaine). Dépend de la Tâche H. Ressource : Chef de projet.

Diagramme de gantt - exercice 2 Lancement du projet Projet "Data Center Vert"

Vous êtes chef de projet pour la transformation d'un centre de données (data center) classique en un "data center vert"qui réduit sa consommation d'énergie et son impact environnemental. Le projet est ambitieux et doit être réalisé en 12 semaines.

Tâches, durées, dépendances et ressources :

Phase 1 : Audit et Planification (Semaines 1-3)
Tâche A : Réaliser un audit énergétique et de l'infrastructure existante (Durée : 3 semaines). Ressource : Chef de projet, auditeur externe.
Tâche B : Définir la nouvelle architecture "verte" (virtualisation, consolidation des serveurs) (Durée : 2 semaines). Dépend de la Tâche A. Ressource : Architecte système.
Phase 2 : Déploiement et Configuration (Semaines 4-8)
Tâche C : Commander le nouveau matériel (serveurs basse consommation, systèmes de refroidissement) (Durée : 4 semaines). Dépend de la Tâche B. Ressource : Équipe d'achats.
Tâche D : Consolider les serveurs physiques en machines virtuelles (Durée : 5 semaines). Dépend de la Tâche B.Ressource : Administrateur système, équipe d'infrastructure.
Tâche E : Déployer les systèmes de refroidissement optimisés (Durée : 3 semaines). Dépend de la Tâche C.Ressource : Équipe d'infrastructure.
Phase 3 : Migration et Tests (Semaines 9-11)
Tâche F : Migrer les données vers la nouvelle infrastructure (Durée : 2 semaines). Dépend des Tâches D et E.Ressource : Administrateur système.
Tâche G : Réaliser des tests de performance et de consommation énergétique (Durée : 3 semaines). Dépend de la Tâche F. Ressource : Auditeur externe.
Phase 4 : Documentation et Démantèlement (Semaine 12)
Tâche H : Rédiger la documentation du projet (Durée : 1 semaine). Dépend de la Tâche G. Ressource : Chef de projet.
Tâche I : Démanteler et recycler l'ancien matériel (Durée : 1 semaine). Dépend de la Tâche G. Ressource :Équipe d'infrastructure. Note : Cette tâche peut se faire en parallèle avec la Tâche H.

MATRICE RACI

Une matrice RACI est un outil de gestion de projet qui permet de clarifier les rôles et les responsabilités de chaque partie prenante pour chaque tâche ou livrable d'un projet. Son nom est un acronyme des quatre rôles qu'elle définit :

- **R (Responsible) :** La personne ou le groupe **qui réalise** l'exécution d'une tâche. C'est elle qui fait le travail. Il peut y avoir plusieurs Responsible par tâche.
- **A (Accountable) :** La personne redevable ou **responsable** final. C'est elle qui est l'unique responsable de l'approbation du travail et qui doit rendre des comptes. Elle s'assure que la tâche est achevée correctement. Il ne doit y avoir qu'un seul Accountable par tâche.
- **C (Consulted) :** Les personnes qu'il faut **consulter** avant que le travail soit finalisé et approuvé. Elles apportent leur expertise ou leur avis.
- **I (Informed) :** Les personnes qu'il faut **informer** de l'avancement ou de la complétion d'une tâche. Elles n'apportent pas de contribution directe au travail, mais ont besoin d'être tenues au courant. La communication est unidirectionnell

MATRICE RACI - Exemple

Exemple 1 : Matrice RACI pour un Plan de Réponse aux Incidents (Cybersécurité)

Vous êtes chef de projet pour la mise en place d'un plan de réponse aux incidents de sécurité. L'objectif est de définir clairement qui fait quoi en cas de cyberattaque.

Tâches du projet :

1. Détection de l'incident : Identification d'une alerte par le SIEM (outil de gestion des événements et d'informations de sécurité).
2. Analyse de l'incident : Évaluer l'étendue de l'attaque et la gravité de la menace.
3. Contention de l'incident : Isoler les systèmes affectés pour empêcher l'attaque de se propager.
4. Notification : Informer la direction et les parties prenantes externes (autorités, clients si nécessaire).
5. Réduction : Réduire la menace des systèmes affectés.
6. Récupération : Restaurer les systèmes et les données à un état opérationnel.
7. Leçons apprises : Analyser les événements pour améliorer les procédures.

Rôles :

- **RSSI (Responsable de la Sécurité des Systèmes d'Information)**
- **Équipe SOC (Centre d'Opérations de Sécurité)**
- **Direction (CEO, CTO)**
- **Équipe informatique (Service IT)**
- **Service juridique**

MATRICE RACI - Exemple

Tâches	RSSI (Accountable)	Équipe SOC (Responsable)	Direction (Informée)	Équipe IT (Consultée/Responsable)	Service Juridique (Consulté/Informé)
1. Détection de l'incident	A	R	I	C	
2. Analyse de l'incident	A	R	I	C	
3. Contention de l'incident	A	R	I	R	
4. Notification	A	R	R		C
5. Éradication	A	R	I	R	
6. Récupération	A	C	I	R	
7. Leçons apprises	A	R	C	C	I

MATRICE RACI - Exemple

Exercice 2 : Matrice RACI pour la Mise en place d'une politique Green IT

Vous êtes chargé de la mise en œuvre d'une politique de réduction de la consommation énergétique du parc informatique de votre entreprise.

Tâches du projet :

1. Audit des équipements : Mesurer la consommation actuelle des ordinateurs, imprimantes et serveurs.
2. Rédaction de la charte Green IT : Définir les règles (extinction des écrans, achat d'équipements certifiés, etc.).
3. Achat de nouveaux équipements : Commander des ordinateurs portables et des imprimantes moins énergivores.
4. Sensibilisation des employés : Lancer une campagne de communication pour encourager les bonnes pratiques.
5. Démantèlement et recyclage : Organiser la collecte et le recyclage des anciens équipements.
6. Mesure de l'impact : Calculer la réduction de la consommation électrique après six mois.

Rôles :

- **Chef de projet Green IT**
- **Direction générale**
- **Service des achats**
- **Service IT**
- **Service de communication**
- **Employés**

Consigne :

Créez une matrice RACI avec les tâches et les rôles.
Attribuez les rôles R, A, C et I pour chaque tâche.
Analysez les interactions : Par exemple, pourquoi le service des achats est-il R pour une tâche et C pour une autre ? Quel est le rôle des employés dans ce projet, et comment se traduit-il dans la matrice ?

02

Intégrer la cybersécurité dans les projets

Rappel : Quels sont 3 les critères fondamentaux de la Sécurité des Systèmes d’information ?

Rappel des principes Cybersécurité / SSI

KATANE

« La SSI est l'ensemble des moyens **techniques**, **organisationnels**, **juridiques**, **humains** nécessaires à la mise en place d'actions visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du SI » ***ANSSI***

"Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la **disponibilité**, **l'intégrité** ou la **confidentialité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La **cybersécurité** fait appel à des techniques de **sécurité des systèmes d'information** et s'appuie sur la lutte contre la **cybercriminalité** et sur la mise en place d'une **cyberdéfense**." **ANSSI**

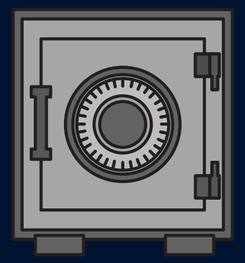
Rappel des principes Cybersécurité / SSI

Caractéristique	Cybersécurité	SSI (Sécurité des Systèmes d'Information)
Champ d'action	Protection contre les menaces malveillantes dans l'espace cyber.	Protection contre tous les risques (malveillants et accidentels) pesant sur les systèmes d'information.
Objectif principal	Défendre contre les cybercriminels et les attaques.	Assurer la confidentialité, l'intégrité et la disponibilité des systèmes et des données.
Exemple de risque	Un ransomware qui chiffre des données.	Un incendie dans un centre de données ou une panne de serveur.

Rappel : Qu’est-ce qu’un risque ?

Risque : la vraissemblance qu’une menace exploite une vulnérabilité entrainant des conséquences

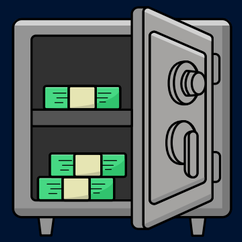
Rappel : Qu’est-ce qu’un risque ?



Bien support : Coffre fort
Information sensible : Liste de criminels à l’intérieur du coffre

Vulnérabilité : Laisser la clé du coffre sur votre bureau

Menace : Une personne prend la clé et tente d’ouvrir le coffre



Impact : La personne récupère la liste de criminels et créer de gros ennuis

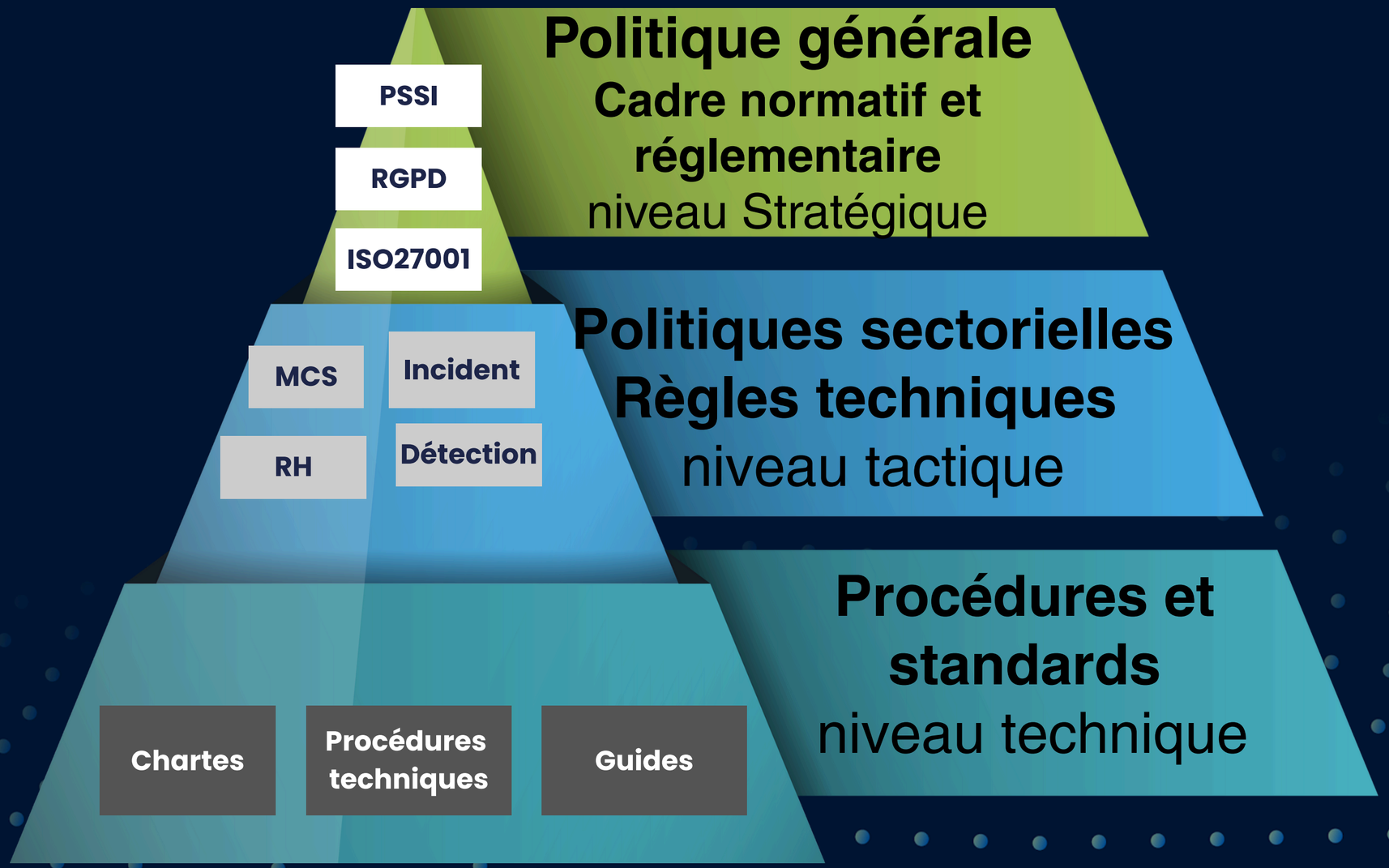
Contre mesures

Prendre les clés sur soi

Risque résiduel

Subir un vol à l’arraché

Socle de sécurité d'un entreprise

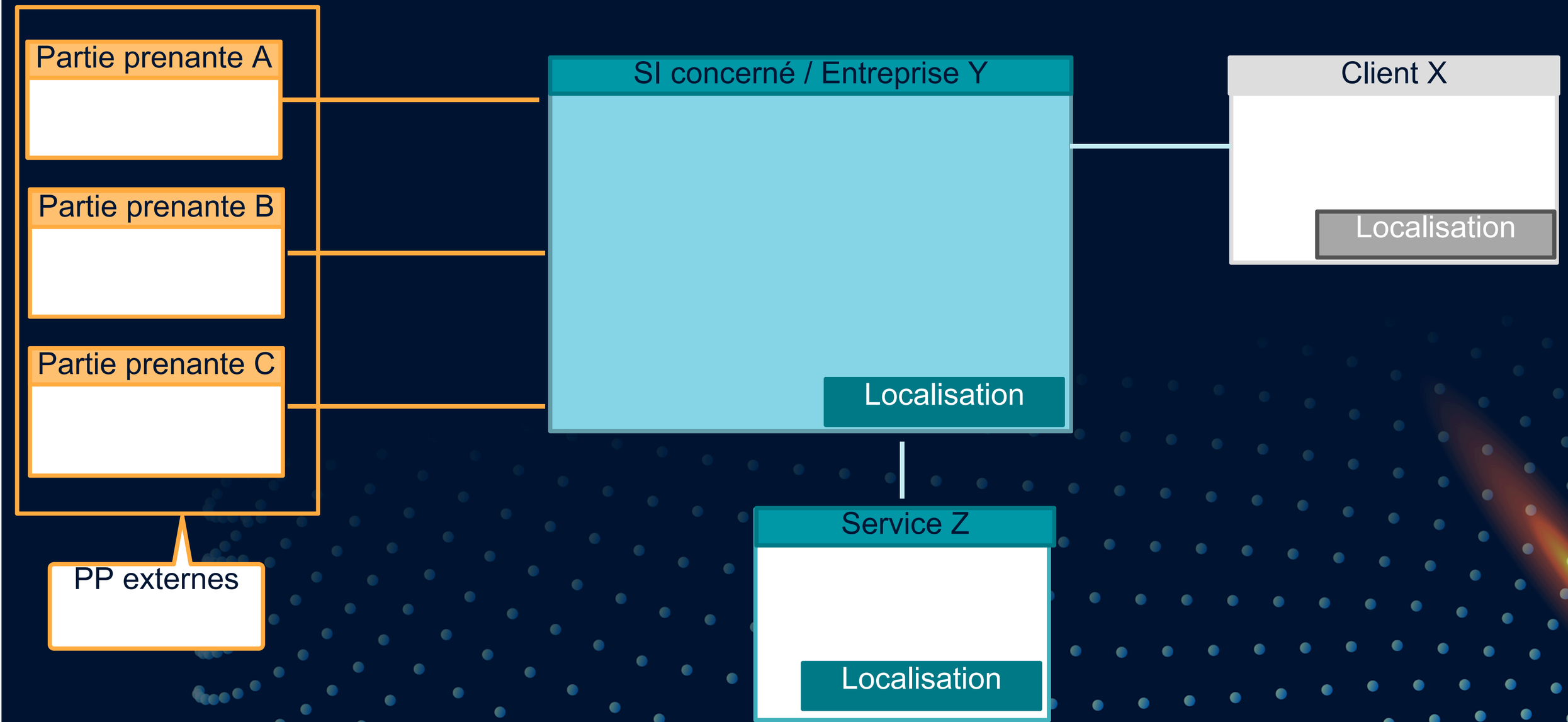


Politiques de sécurité / Procédures

L'ISO 27001 impose une vision en couches :

Politique de Sécurité du SI (PSSI) : Quoi et Pourquoi ? (**Niveau stratégique)**
Politiques Sectorielles : Comment ? **(Niveau tactique)**
Procédures : Avec quelles actions concrètes ? **(Niveau opérationnel)**

Périmètre d'analyse sur une entreprise



Périmètre d'impact sur une entreprise

Prestataire/fournisseur	Entreprise	Client
L'ensemble des parties prenantes externes à l'entreprise La chaîne d'approvisionnement, entreprises qui gèrent la maintenance d'équipements, l'externalisation de certains services, la fourniture de matériel, de logiciel, etc..	L'impact peut concerner : • L'ensemble des systèmes d'information • Un système d'information spécifique • Un service spécifique • Un groupe d'utilisateur spécifique • Uniquement les administrateurs du SI • …	L'impact peut s'étendre jusqu'aux clients de l'entreprise

biens supports

Physique (locaux)	Matériel IT	Logiciel
Concerne le bâtiment, les accès physiques (porte électroniques), les systèmes de surveillance et détection (caméras, détecteurs, alarmes), les systèmes de sécurité (incendies,..), les systèmes de chauffage ou refroidissement, les systèmes électriques	L'ensemble des équipements physiques, -en datacenter (équipements réseaux, serveurs de stockage, les baies, etc..) -dans les bureaux (PC, imprimantes, disques durs, etc..), -Les endpoints (portables, tablettes, etc..)	L'ensemble des logiciels utlisé par une entreprise.

biens supports

BIEN SUPPORT	EXEMPLES (LISTE NON EXHAUSTIVE)
SYSTÈMES INFORMATIQUES ET DE TÉLÉPHONIE	
MATÉRIELS[1]	
TERMINAL UTILISATEUR	Ordinateur fixe, ordinateur portable, tablette, téléphone mobile.
PÉRIPHÉRIQUE	Imprimante, scanner, clavier, souris, caméra, microphone, objet connecté.
TÉLÉPHONE	Téléphone fixe ou mobile analogique ou IP.
ÉQUIPEMENT DE STOCKAGE	Clé USB, disque dur, CD-ROM, carte mémoire.
SERVEUR	*Mainframe*, serveur lame, serveur *rack*.
MOYEN D'ADMINISTRATION	Poste d'administration, serveur outils d'administration, bastion.
ÉQUIPEMENT RÉSEAU	Commutateur, routeur, passerelles d'entrée depuis l'extérieur, borne WI-FI.
ÉQUIPEMENT DE SÉCURITÉ	Pare-feu, sonde (IDS/IPS), passerelle VPN.
ÉQUIPEMENT INDUSTRIEL	Automate programmable industriel, capteur, actionneur, système SCADA, système instrumenté de sécurité.
LOGICIELS	
SERVICE D'INFRASTRUCTURE	Service d'annuaire, service de gestion d'adresse IP (DHCP), service de nom de domaine (DNS), contrôleur de domaine, serveur d'impression.
APPLICATION/SERVICE APPLICATIF	Serveur web, service web, serveur d'application, serveur de courrier électronique, serveur de bases de données, progiciels (RH, relation client, ERP).
INTERGICIEL (*MIDDLEWARE*)	*Entreprise Application Integration* (EAI), *Extract-Transform-Load* (ETL), *Open DataBase Connectivity* (ODBC).
SYSTÈME D'EXPLOITATION, HYPERVISEUR	Windows, Linux, MacOS, Xen.
MICROGICIEL (*FIRMWARE*)	*Basic Input Output System* (BIOS), *Unified Extensible Firmware Interface* (UEFI), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur.
LOGICIEL DE SÉCURITÉ	Outil de gestion d'évènements *Security Information and Event Management* (SIEM).
RÉSEAUX/CANAUX INFORMATIQUES ET DE TÉLÉPHONIE	
RÉSEAU/CANAL INFORMATIQUE	Câble réseau, fibre optique, liaison radio (Wi-Fi, Bluetooth, etc.).
RÉSEAU/CANAL TÉLÉPHONIQUE	Ligne téléphonique.
ORGANISATIONS	
PERSONNE	Employé, stagiaire, prestataire, personnel d'entretien.
SUPPORT PAPIER	Document manuscrit ou imprimé.
ÉCHANGE VERBAL	Réunion, échange informel.
ÉLÉMENT D'INGÉNIERIE SOCIALE	Information partagée sur les réseaux sociaux.
LOCAUX ET INSTALLATIONS PHYSIQUES	
SITE/BÂTIMENT/SALLE	Siège social, usine, site de stockage, bâtiment industriel, salle de réunion, salle serveur.
SYSTÈME DE SÉCURITÉ PHYSIQUE	Système d'accès par badge, système de détection d'intrusion, système de vidéo-protection.
SYSTÈME DE SÛRETÉ DE FONCTIONNEMENT	Climatisation, sécurité incendie, alimentation électrique.

Catégorisation d'impact

impact opérationnel
impact humain ;
impact financiers;
mpact juridiques;
impact sur l'image;

IMPACT	EXEMPLES (LISTE NON EXHAUSTIVE)
IMPACTS SUR LES MISSIONS ET SERVICE DE L'ORGANISATION	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA RÉALISATION DES MISSIONS ET SERVICES	Incapacité à fournir un service, dégradation de performances opérationnelles, retards, impacts sur la production ou la distribution de biens ou de services, impossibilité de mettre en œuvre un processus clé.
IMPACTS HUMAINS, MATÉRIELS OU ENVIRONNEMENTAUX	
IMPACTS SUR LA SÉCURITÉ OU SUR LA SANTÉ DES PERSONNES CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'INTÉGRITÉ PHYSIQUE DE PERSONNES	Accident du travail, maladie professionnelle, perte de vies humaines, mise en danger, crise ou alerte sanitaire.
IMPACTS MATÉRIELS DÉGÂTS MATÉRIELS OU DESTRUCTION DE BIENS SUPPORTS	Destruction de locaux ou d'installations, endommagement de moyens de production, usure prématurée de matériels.
IMPACTS SUR L'ENVIRONNEMENT CONSÉQUENCES ÉCOLOGIQUES À COURT OU LONG TERME, DIRECTES OU INDIRECTES	Contamination radiologique ou chimique des nappes phréatiques ou des sols, rejet de polluants dans l'atmosphère.
IMPACTS SUR LA GOUVERNANCE	
IMPACTS SUR LA CAPACITÉ DE DÉVELOPPEMENT OU DE DÉCISION CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA LIBERTÉ DE DÉCIDER, DE DIRIGER, DE METTRE EN ŒUVRE LA STRATÉGIE DE DÉVELOPPEMENT	Perte de souveraineté, perte ou limitation de l'indépendance de jugement ou de décision, limitation des marges de négociation, perte de capacité d'influence, prise de contrôle de l'organisation, changement contraint de stratégie, perte de fournisseurs ou de sous-traitants clés.
IMPACTS SUR LE LIEN SOCIAL INTERNE CONSÉQUENCES DIRECTES OU INDIRECTES SUR LA QUALITÉ DES LIENS SOCIAUX AU SEIN DE L'ORGANISATION	Perte de confiance des employés dans la pérennité de l'organisation, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, perte de sens des valeurs communes.
IMPACTS SUR LE PATRIMOINE INTELLECTUEL OU CULTUREL CONSÉQUENCES DIRECTES OU INDIRECTES SUR LES CONNAISSANCES NON-EXPLICITES ACCUMULÉES PAR L'ORGANISATION, SUR LE SAVOIR-FAIRE, SUR LES CAPACITÉS D'INNOVATION, SUR LES RÉFÉRENCES CULTURELLES COMMUNES	Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés.
IMPACTS FINANCIERS	
CONSÉQUENCES PÉCUNIAIRES, DIRECTES OU INDIRECTES	Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées.
IMPACTS JURIDIQUES	
CONSÉQUENCES SUITE À UNE NON-CONFORMITÉ LÉGALE, RÉGLEMENTAIRE, NORMATIVE OU CONTRACTUELLE	Procès, amende, condamnation d'un dirigeant, amendement de contrat.
IMPACTS SUR L'IMAGE ET LA CONFIANCE	
CONSÉQUENCES DIRECTES OU INDIRECTES SUR L'IMAGE DE L'ORGANISATION, LA NOTORIÉTÉ, LA CONFIANCE DES CLIENTS	Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte de notoriété, perte de confiance d'usagers.

Exemples de menaces/impacts

Exemples Causes / Périmètres concernés	Prestataires / fournisseurs	Datacenter	DSI entrepise et/ou collaborateurs hors DSI
Changement climatique (canicules, tsunamis, inondations, tempêtes etc..)	-Perturbation des transports d'approvisionnement de matériels -Perturbation de la fourniture de service	-Surchauffe des équipements -Destruction/Panne des équipements -Perte des sauvegardes - dysfonctionnement des systèmes de détection d'intrusion, du système de vidéosurveillance, etc.)	-Réduction de la disponibilité du personnel -Augmentation stresse/anxiété -Perturbation de l'activité dû à des coupures d'électricité --dysfonctionnement des gestions des accès -dysfonctionnement des portes à serrure magnétiques, -Dégradation de la vigilance des mesures d'hygiènes cyber
Risques sanitaires, maladies, prolifération d'animaux « nuisibles »	-Réduction de la disponibilité du personnel	-Introduction d'animaux « nuisibles» exemple rongeur de câble	-Réduction de la disponibilité du personnel -Propagation de cluster de maladie dans l'entreprise
Risques géopolitiques induits	Contraintes politiques dans l'usage de certains moyens de transport	-Contraintes d'hébergement de données dans de nouvelles zones géographiques	Augmentation du risque de cyberattaque lié à l'installité politique

Exemple d’échelle de gravité d’un impact

NIVEAU DE L’ÉCHELLE	DÉFINITION
G5 – CATASTROPHIQUE	**Conséquences sectorielles ou régaliennes au-delà de l’organisation.** Écosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables. Et/ou : difficulté pour l’État, voire incapacité, d’assurer une fonction régalienne ou une de ses missions d’importance vitale. Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d’infrastructures essentielles, etc.).
G4 – CRITIQUE	**Conséquences désastreuses pour l’organisation avec d’éventuels impacts sur l’écosystème.** Incapacité pour l’organisation d’assurer la totalité ou une partie de son activité, avec d’éventuels impacts graves sur la sécurité des personnes et des biens. L’organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d’activité ou étatiques dans lesquels elle opère seront susceptibles d’être légèrement impactés, sans conséquences durables.
G3 – GRAVE	**Conséquences importantes pour l’organisation.** Forte dégradation des performances de l’activité, avec d’éventuels impacts significatifs sur la sécurité des personnes et des biens. L’organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.
G2 – SIGNIFICATIVE	**Conséquences significatives mais limitées pour l’organisation.** Dégradation des performances de l’activité sans impact sur la sécurité des personnes et des biens. L’organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 – MINEURE	**Conséquences négligeables pour l’organisation.** Aucun impact opérationnel ni sur les performances de l’activité ni sur la sécurité des personnes et des biens. L’organisation surmontera la situation sans trop de difficultés (consommation des marges).

KATANE

Calculer la vraissemblance

Exemple d'échelle

ÉCHELLE DE PROBABILITÉ DE SUCCÈS D'UNE ACTION ÉLÉMENTAIRE	
NIVEAU DE L'ÉCHELLE	DESCRIPTION
4 – QUASI-CERTAINE	Probabilité de succès quasi-certaine > 90%
3 – TRÈS ÉLEVÉE	Probabilité de succès très élevée > 60%
2 – SIGNIFICATIVE	Probabilité de succès significative > 20%
1 – FAIBLE	Probabilité de succès faible < 20%
0 – TRÈS FAIBLE	Probabilité de succès très faible < 3%

Classification d’un risque

Gravité	Vraissemblance			
	Mineur	Significatif	Fort	Maximale
Mineur				
Significatif				
Elevé				
Critique				

-Risque faible
-Risque acceptable
-Risque inacceptable
-Risque intolérable

Projet étape 1/3 - Cadre et Analyse du Risque

Par groupe de 5 :

- **Identifier un rapporteur**
- **Choisir un sujet**

En respectant les étapes d'un projet, dans la phase de réalisation ;

- **Identifier un périmètre d'analyse**

(Décrire le Système d'Information (SI) de l'entreprise (schéma simple ou liste d'entités/applications clés) et définir clairement les actifs (biens supports et informations) inclus dans l'analyse).

- **Identifier deux menaces environnementales majeures pesant sur la sécurité du système d'information.**
- **Identifier chaque menaces choisies, identifier plusieurs vulnérabilités présent sur le système d'information avec leur bien support.**

(Ex vulnérabilités: "Pas de redondance géographique", "Locaux serveurs au sous-sol", "Dépendance à un unique fournisseur d'énergie").
(Ex bien support: Serveur d'applications, Base de données clients, Routeur central)

- **Identifier pour chaque vulnérabilité un impact potentiel et son critère SSI** (Disponibilité, Intégrité, Confidentialité)
- **Catégoriser les impacts** (image, opérationnel, juridique, humain, financier)
- **Evaluer la gravité pour chaque impact** (la justification est plus importante que la mesure)
- **Evaluer la vraissemblance pour chaque impact** (la justification est plus importante que la mesure)

- **Déterminer le niveau de risque** (Gravité/Vraissemblance)

Projet étape 1/3 - Cadre et Analyse du Risque

KATANE

Sujet A

Entreprise de reconditionnement de téléphone, tablette, PC

Activité principale basée à Cannes

Entre 50 & 100 salariés internes

Prestataires (logistique)

Sujet B

Centrale nucléaire

Activité principale basée dans le finistère

6 000 salariés sur site

Prestataires (logistique)

Sujet C

Hôpital

Activité principale basée à Mayotte

Entre 20 & 80 salariés internes

Prestataires (logistique)

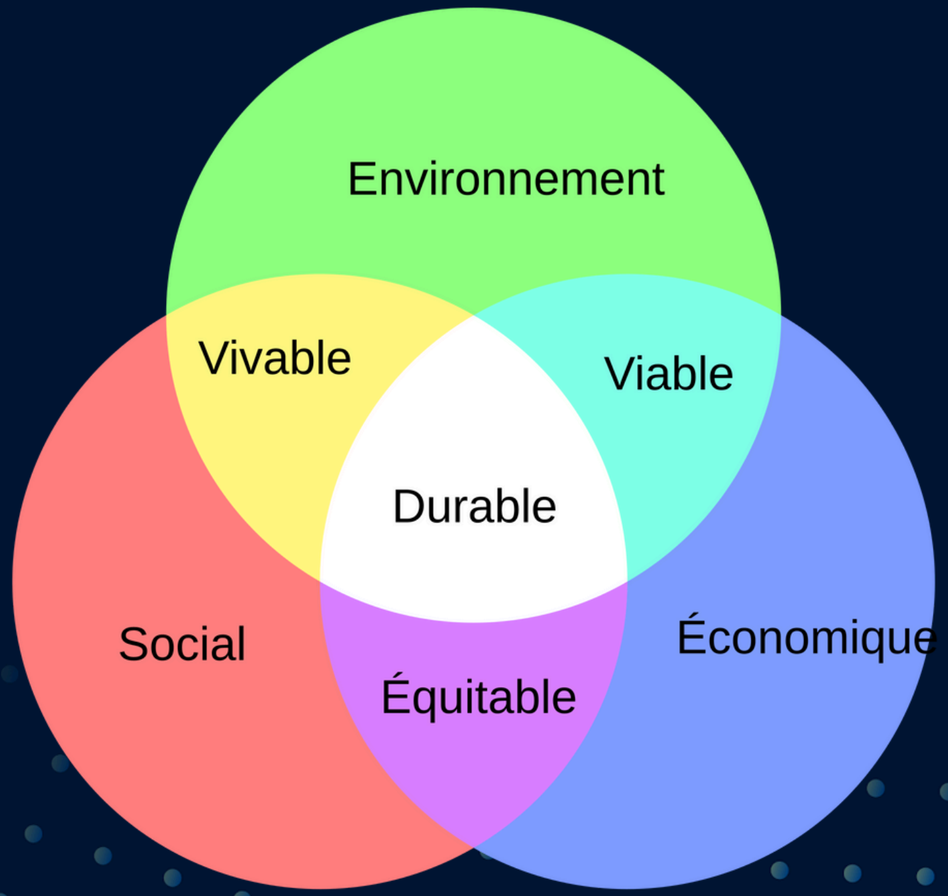
03

Green IT et RSE dans les projets

1.Définitions & Enjeux du GreenIT
2. Distinction cruciale : Green for IT vousIT for Green
3. Eco conception
4. Optimisation de la consommation énergétique des centres de données

Projet

Développement durable



Urgence climatique

L'**urgence climatique** signifie que la situation actuelle du changement climatique est devenue **critique** et constitue une menace globale à laquelle est confrontée la planète, affectant l'ensemble des droits de l'Homme et mettant en **péril l'existence de l'humanité**. Elle nécessite ainsi la mise à en place de mesures urgentes pour « atténuer » cette menace

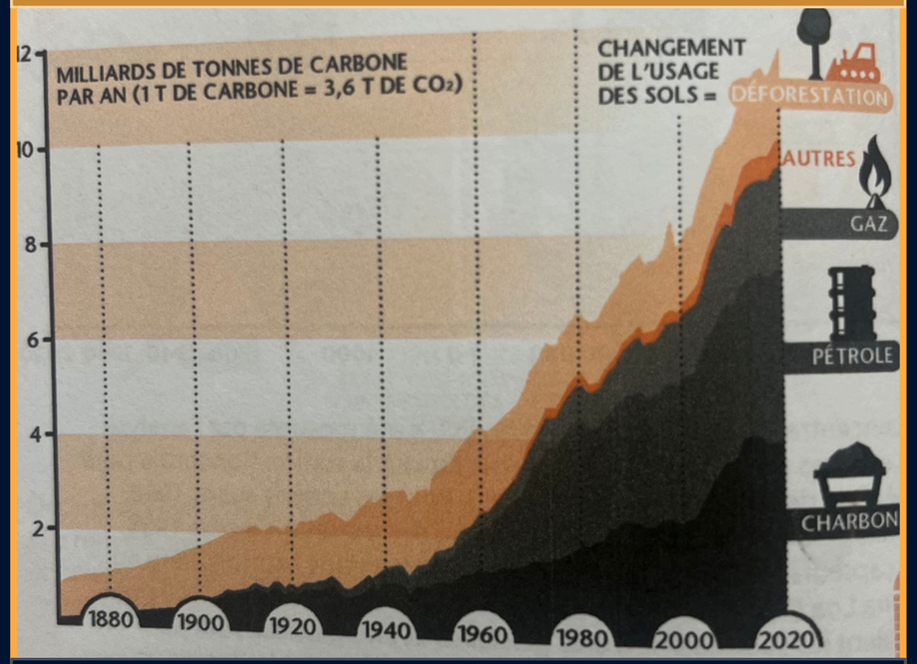
En 2019, le Parlement européen **déclare l'urgence climatique** avec pour actions concrètes :

- La Commission doit veiller à ce que toutes ses propositions soient alignées sur l'objectif de 1,5°C en termes de réchauffement climatique
- L'UE prévoit de réduire ses émissions de 55% d'ici 2030 pour atteindre la neutralité carbone d'ici 2050
- Appel à la réduction des émissions mondiales issues des transports aérien et maritime

La résolution déclarant l'urgence climatique et environnementale a été adoptée par 429 voix pour, 225 voix contre et 19 abstentions.

Causes du réchauffement climatique

Origine et évolution
des émissions annuelles de CO2



Les émissions de CO2 anthropiques sont passées d'environ 2 milliards de tonnes de carbone par an en1920 à près de 12 milliards de tonnes en 2020. Cette multiplication par six provient pour l'essentiel de la combustion du charbon, du pétrole et du gaz fossile

Source : Le GIEC URGENCE CLIMAT 2023
Source : Chapitre 5, rapport complet Groupe 1 du GIEC

Production d'énergie

La production d'électricité et de chaleur par la combustion de combustibles fossiles

Fabrication de produits

Combustion de combustibles fossiles pour produire l'énergie nécessaire à la fabrication de produits tels que le ciment, le fer, l'acier, les composants électroniques, les matières plastiques, les vêtements et d'autres biens.

Abattage de forêts

Une fois coupés, les arbres libèrent le carbone qu'ils ont stocké. Chaque année, environ 12 millions d'hectares de forêt sont détruits

Utilisation de moyens de transport

Les voitures, les camions, les navires et les avions sont pour la plupart alimentés par des combustibles fossiles.

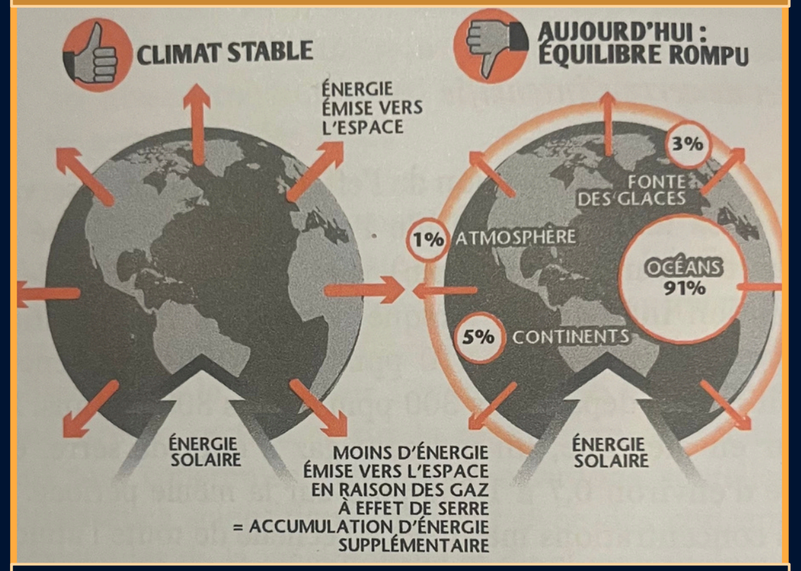
Surconsommation

Le logement dans lequel on vit, l'énergie que l'on consomme, le mode de déplacement que l'on utilise, ce que l'on mange et la quantité de déchets que l'on met au rebut sont autant d'éléments qui contribuent aux émissions de gaz à effet de serre. Il en va de même des biens que l'on consomme, tels que les vêtements, les appareils électroniques et les matières plastiques

KATANE

Causes du réchauffement climatique

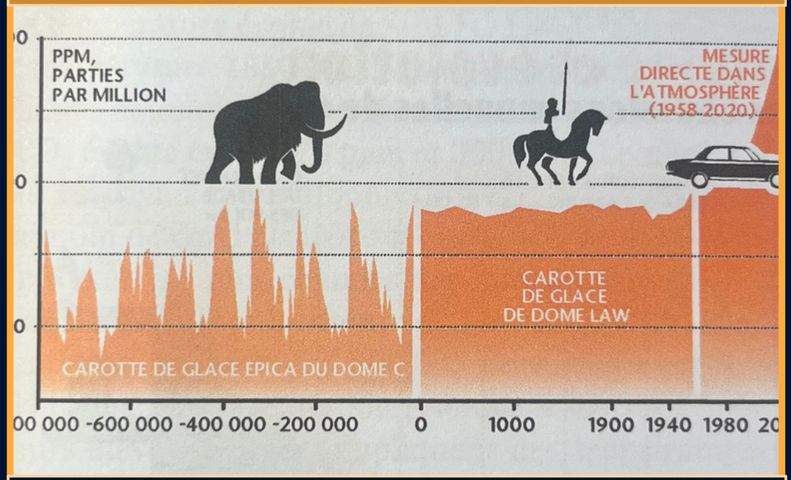
Le déséquilibre énergétique de la Terre



Depuis au moins 1970, l'équilibre énergétique de la planète est rompu. Elle renvoie moins d'énergie vers l'Espace qu'elle en reçoit du Soleil en raison de l'intensification de l'effet de serre. Plus de 90% de cette énergie supplémentaire a été stockée dans les océans

Source : Le GIEC URGENCE CLIMAT 2023
Source : Chapitre 5, rapport complet Groupe 1 du GIEC

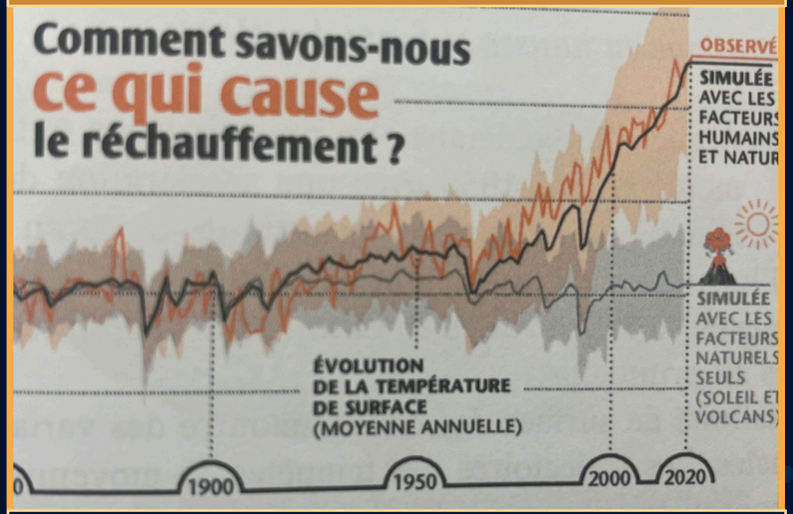
L'évolution de la concentration atmosphérique en CO2



La concentration atmosphérique en CO2 a été mesurée par l'analyse des carottes de glace forées en Antarctique à la station Concordia pour la période de 800 000 ans avant l'an 0. La concentration en CO2 était stable depuis un peu plus de 10 000 ans. Elle s'élève fortement en avril 2022 en raison de nos émissions de GES d'origine humaine.

Source : Le GIEC URGENCE CLIMAT 2023
Source : Chapitre 5, rapport complet Groupe 1 du GIEC

Cause naturelle vous Cause humaine



Les simulations climatiques sur ordinateurs ne parviennent pas à retrouver le réchauffement observé lorsqu'elles ne tiennent pas compte de l'augmentation de la teneur en GES.

Source : Le GIEC URGENCE CLIMAT 2023
Source : Chapitre 5, rapport complet Groupe 1 du GIEC

Conséquences du réchauffement climatique

Augmentation des sécheresses

Le changement climatique influe sur la disponibilité de l'eau, qui devient plus rare dans un plus grand nombre de régions.

Réchauffement et montée des océans

Les océans absorbent la majeure partie de la chaleur liée au réchauffement de la planète

Températures plus élevées

La hausse des températures entraîne une augmentation des maladies liées à la chaleur et rend le travail en plein air plus difficile. Les incendies de forêt se déclenchent plus facilement et se propagent plus rapidement dans des conditions plus chaudes.

Tempêtes plus violentes

Du fait de la hausse des températures, une plus grande quantité d'humidité s'évapore, ce qui aggrave les précipitations extrêmes et les inondations et provoque des tempêtes plus dévastatrices

Accroissement des risques sanitaires

Pollution atmosphérique, maladies, phénomènes météorologiques extrêmes, déplacements forcés, pressions sur la santé mentale, aggravation de la faim et de la malnutrition

Pauvreté et déplacements de populations

Au cours de la dernière décennie (2010-2019), en raison de phénomènes météorologiques, environ 23,1 millions de personnes ont été déplacées en moyenne chaque année et bien davantage encore se sont retrouvées exposées à un risque de pauvreté.

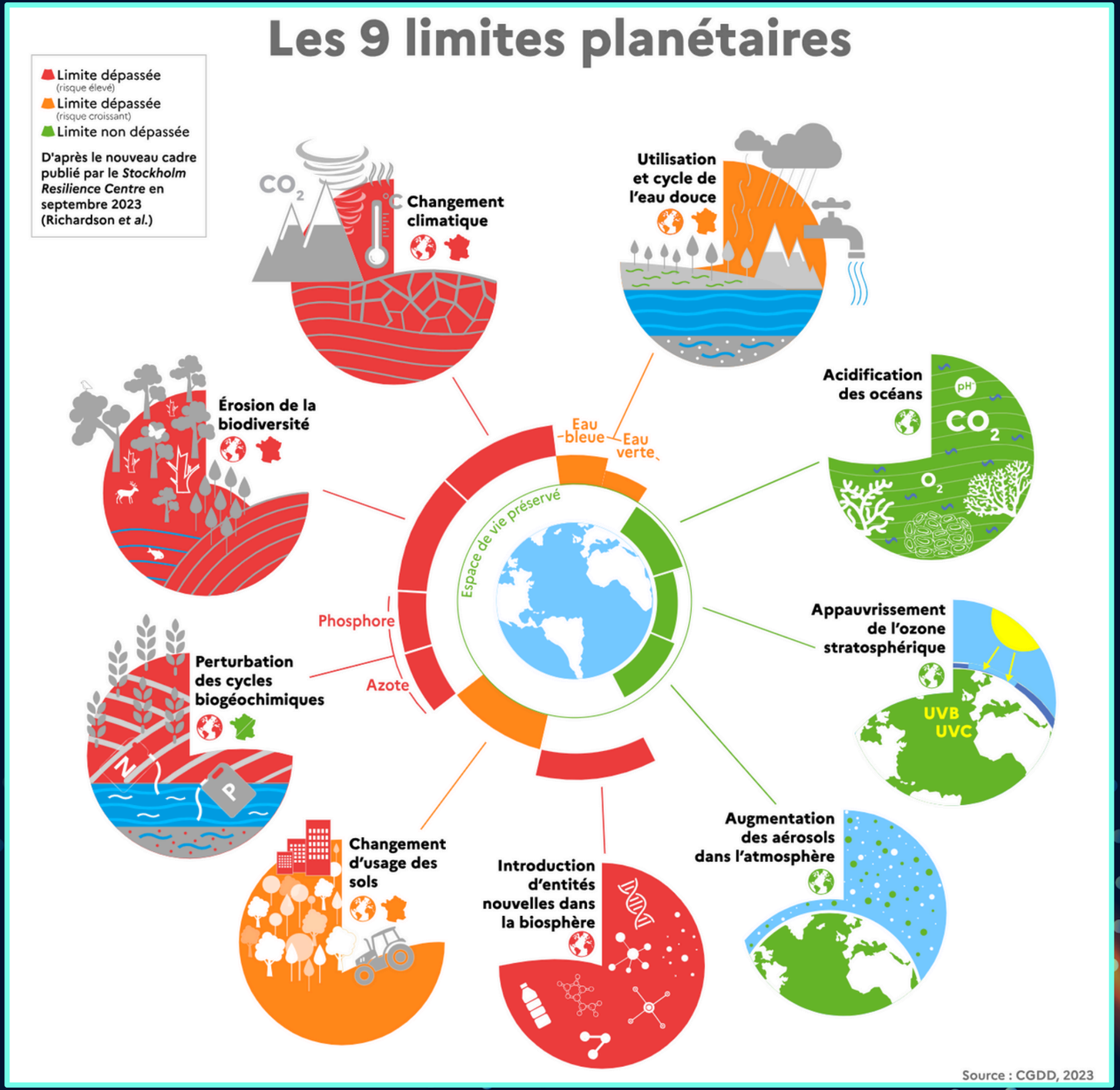
KATANE

Les limites planétaires

Les limites planétaires définissent les paramètres selon lesquels la Terre peut fonctionner de manière stable et durable.

En septembre 2023, seules les trois dernières limites n'avaient pas été franchies.

Avec six limites franchies sur neuf, la planète se trouve aujourd'hui bien au-delà de l'espace de fonctionnement sûr pour l'humanité.



Frise chronologique

KATANE

1824 — **FOURIER** Joseph
Concept l'effet de serre

1860 — **TYNDALL** John
CO2 comme gaz à effet de serre

1896 — **SVANTE** Arrhenius
Impact des émissions anthropiques de gaz à effet de serre sur le système climatique

1968 — Famines au Sahel et en Ethiopie liées à la sécheresse (+1M de morts)

1972 — **Conférence de Stockholm Création du PNUE**

1979 — **Conférence mondiale sur le climat à Genève**

1988 — **Création GIEC**

1990 — **Premier rapport d'évaluation du GIEC**

1992 — **Conférence de RIO Conférence des Nations unies sur l'environnement et le développement**

1992 — **Signature de la CCNUCC** Convention cadre des Nations unies sur les changements climatiques

2015 — **Accord de Paris adopté à la COP21**

2020 — Epidemie COVID 19

2021 — **SYUKURO** Manabe
Prix Nobel de physique, "pour la modélisation physique du climat.. »

2021 — **Retour des E-U dans l'accord de Paris**

2021 — **loi européenne sur le climat"**

2022 — **6ième extinction de masse** entre 7,5% et 13% des espèces animales auraient disparu depuis l'an 1500, au lieu des 0,04% estimées

2023 — Été 2023, le plus chaud jamais enregistré sur Terre

2023 — **Le Parlement européen reconnaît l'écocide**

2023 — **Sixième rapport d'évaluation du GIEC**

Qu’est-ce que le GIEC ?

KATANE

GIEC

GIEC :
GROUPEMENT d’EXPERTS INTERGOUVERNEMENTAL SUR L’ÉVOLUTION DU CLIMAT

IPCC
INTERGOVERNEMENTAL PANEL ON CLIMATE CHANGE

Dates clés

1988 Date de création du GIEC

1990 Création du premier rapport du GIEC

2021-2023 I 6ième rapport du GIEC

Le GIEC a pour objectif d’identifier les causes, les conséquences de la menace du changement climatique puis d’émettre des recommandations à destination de l’ensemble des acteurs : gouvernements comme citoyens, dirigeants d’entreprises comme travailleurs ou consommateurs, jeunes et moins jeunes.

Qu’est-ce que le GIEC ?

Le GIEC se divise en 3 groupes

Physique et climat

Groupe 1

Analyse de risque du changement climatique pour les sociétés et écosystèmes

Groupe 2

Moyen d’atténuation de la menace

Groupe 3

Constats / Préconisations

Accord de Paris

Contenir d'ici à 2100 le réchauffement climatique bien en dessous de 2 °C par rapport aux niveaux préindustriels

Limiter la hausse des températures à 1,5 °C. L'accord est entré en vigueur le 4 novembre 2016.

C'est le premier accord mondial et juridiquement contraignant sur le climat.

AR6 6ième rapport d'évaluation du GIEC

En 2019, la concentration de CO2 dans l'atmosphère est à un taux qui n'avait pas été atteint depuis 2 millions d'années.

Le niveau de réchauffement global de 1,5 °C par rapport à l'ère préindustrielle sera atteint en 2030.

Les politiques actuellement en place conduiraient vers un réchauffement global de 3,2 °C d'ici à la fin du siècle (valeur médiane).

Les stratégies d'atténuation basées sur la demande en trois options : **"Éviter – Changer – Améliorer".**

2015 — 2023

Matériel vs Usage

Matériel	Usage
Représente les équipements physiques, les supports, tels qu'un PC, un clavier, un support USB, un commutateur ou une diode.	Représente la manière d'utiliser un équipement physique ou un logiciel

Green IT

« Démarche d’amélioration continue qui vise à réduire l’empreinte économique, écologique et sociale d’un produit ou d’un service, grâce au numérique ».

GreenIT.fr

Le Green IT constitue le volet écologique du numérique responsable, une approche qui s’intéresse simultanément aux impacts écologiques et sociaux du numérique.

Empreinte écologique

L'empreinte écologique est une méthode de calcul permettant de mesurer l'impact de l'Homme sur son environnement.

Elle consiste à estimer la quantité de terre et d'eau nécessaire à la fois à la consommation et à l'absorption des déchets produits par un individu, une ville, une population…

Ou plus concrètement, quelle taille devrait avoir une île pour répondre à ses besoins durablement si un être humain y vivait en autarcie, sans épuiser les ressources naturelles ni perturber l'écosystème.

Sobriété numérique

Changement d'usage en profondeur des outils digitaux permettant, d'une part, de modérer les consommations numériques au strict nécessaire, et d'autre part, de tenter d'éliminer les productions et usages superflus.

BPI france

Sobriété numérique - dynamique des 5R

Refuser : refuser de remplacer un équipement fonctionnel
Réduire : réduire l'usage des équipements, les volumes de données..
Réparer : pour prolonger la durée de vie
Réutiliser : politique de réemploi, seconde vie
Recycler

Couverture fonctionnelle :
Près de 50% des fonctionnalités développées ne sont presque jamais utilisées, et sur les 50% restant, seules 20% le sont régulièrement.
(rapport « Exceeding value »

Exemple d'Excel en entreprise

Exemple de bonnes résolutions de sobriété numérique

KATANE

Favoriser des équipements reconditionnés

Mise en place d’une politique de seconde main

Gérer la fin de vie de son matériel informatique

Adopter le cloud, mais veiller à l’effet rebond

Favoriser les applications et les fournisseurs éthiques pour le Green IT

Participer à des initiatives de durabilité numérique et mesure l’impact environnemental de mon SI

Quelques chiffres

À l'échelle mondiale, en 2017
la fabrication et l'usage des outils du numérique ont consommé 3000 TWh d'énergie (soit 2,7 % du total de la consommation)

et émis 1800 Mt CO2e de gaz à effet de serre (GES) (soit 3,4 % du total des émissions) (source : The Shift project).

Si le numérique était un pays, il serait le 2e plus gros consommateur d'énergie au monde et le 4e plus gros émetteur de GES (chiffres pour l'année 2017, sources : Enerdata, Global carbon atlas et The Shift project

TOP 5 des plus gros consommateurs d'énergie (en TWh, toutes sources d'énergie confondues)	TOP 5 des plus gros émetteurs de gaz à effet de serre (en Mt CO2e)
1. Chine : 3050	1. Chine : 9850
2. **Numérique : 3000**	2. USA : 5270
3. USA : 2180	3. Inde : 2470
4. Inde : 900	4. **Numérique : 1800**
5. Russie : 770	5. Russie : 1700

Quelques chiffres

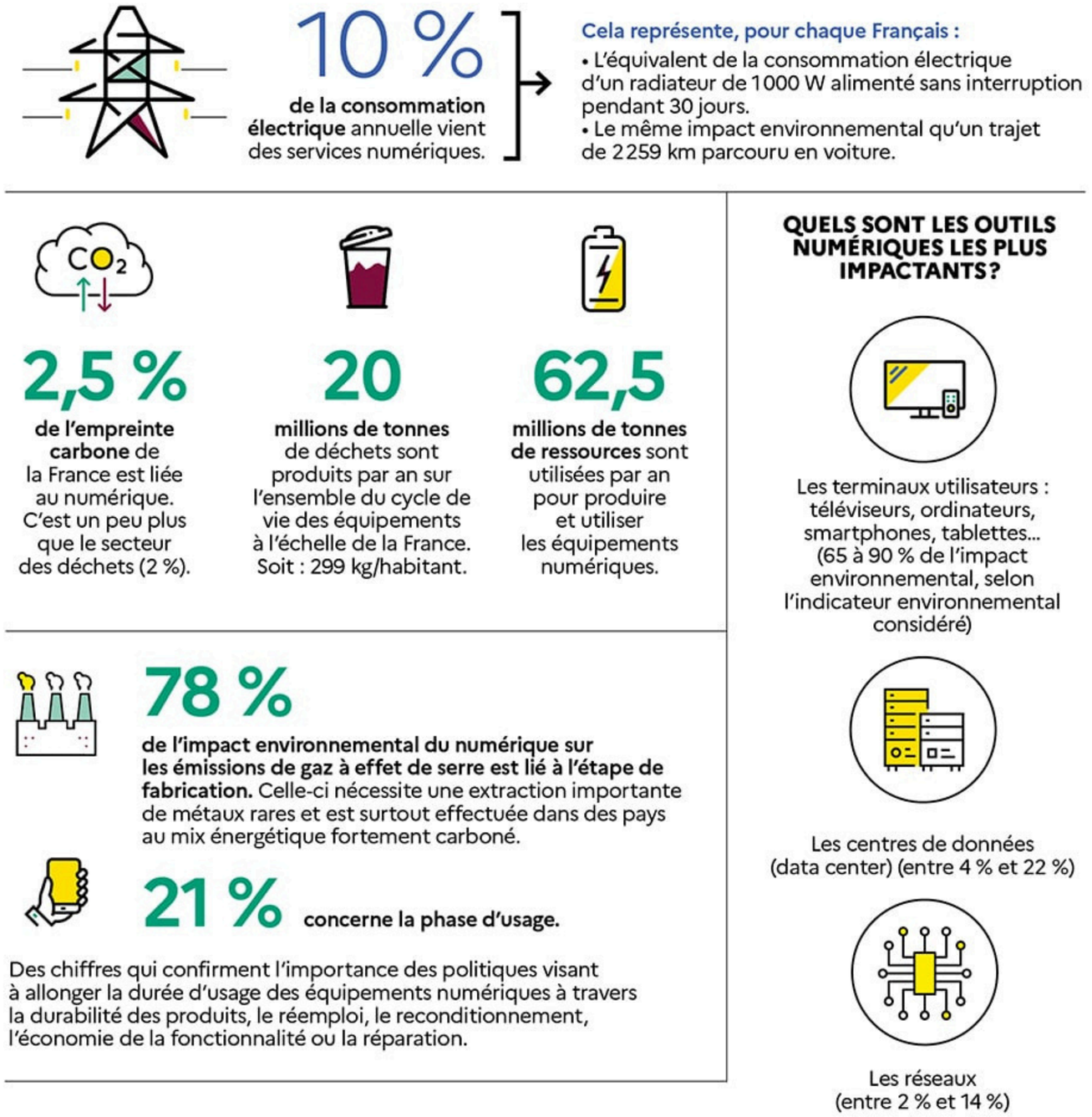
10% de la consommation électrique annuelle vient des services numériques.

Cela représente, pour chaque Français :
– L'équivalent de la consommation électrique d'un radiateur de 1 000W alimenté sans interruption pendant 30 jours.

62,5 millions de tonnes de ressources sont utilisées par an pour produire et utiliser les équipements numériques.

KATANE

Source : ADEME
Date : 2022



Deux facteurs principaux

La multiplication des équipements et problématiques d'obsolescence : dans les pays occidentaux, on comptait par exemple un équipement (ordinateur personnel) pour plusieurs personnes dans les années 1980, un par personne dans les années 1990 et 2000 et plusieurs par personne à partir des années 2010 (ordinateurs, smartphone, tablettes, objets connectés, etc.).

L'explosion du volume de données échangées : la croissance du nombre d'utilisateurs d'internet, du nombre d'équipements par utilisateur et des débits (grâce notamment à la fibre optique et aux technologies mobiles 4G et 5G) entraîne une croissance exponentielle du volume de données échangées. L'équipementier Cisco prévoit une croissance de 25 % par an en moyenne sur la période 2016-2021 (source : The Shift project).

Obsolescence des équipements

Obsolescence technique

Obsolescence logicielle

Obsolescence psychologique

Conséquences du numérique sur l'environnement

Au-delà de la consommation d'énergie et des émissions de gaz à effet de serre, le processus de fabrication et l'usage des outils du numérique mobilisent d'importantes quantités de **métaux**, d'**eau** et de **produits chimiques**. Ils rejettent également de grandes quantités de **polluants** dans l'air, l'eau et les sols

Les outils du numérique reposent sur une grande diversité de matériaux : métaux, plastiques, verre, céramique, etc. Une étude d'Orange labs montre par exemple qu'un smartphone comprend en moyenne une trentaine de métaux différents, notamment du cuivre, de l'étain, du cobalt, du lithium, des métaux précieux (or, argent, platine) et des "terres rares".

Eco-conception

KATANE

Démarche qui consiste à concervoir, reconcevoir et optimiser un service numérique en mesurant ses impacts environnementaux, dans le but de les miniser. Cette réflexion porte particulièrement sur le périmètre fonctionnel du service ainsi que sur son implémentation technique

GreenIT

L’écoconception des services numériques

D’après le livre blanc L’écoconception des services numériques,

“Un service numérique répond à un besoin spécifique, il a une ou plusieurs fonctionnalités et des utilisateurs. Il est considéré comme l’association :

- d’équipements permettant de stocker, manipuler, afficher des octets (serveurs, terminaux utilisateurs, box ADSL, etc.) ;
- d’infrastructures qui hébergent et relient les équipements (réseaux opérateurs et centres de données notamment) ;
- de plusieurs logiciels empilés les uns sur les autres, qui s’exécutent au-dessus des équipements ;
- d’autres services numériques tiers éventuels.”

Motivation pour une entreprise

KATANE

Financière

- réduire le coût de conception du SI
- réduire le coût de fonctionnement du SI

Stratégique

- améliorer l'expérience utilisateur et la qualité du service rendu
- élargir le public cible du service, notamment lorsqu'elle est couplée à une démarche d'accessibilité numérique ;
- expérimenter des modèles d'affaires plus vertueux pour l'environnement, tels que l'économie circulaire et l'économie de la fonctionnalité
- renforcer les relations entre l'entreprise et ses fournisseurs par un échange accru d'informations et le développement de nouveaux produits
- renforcer la mobilisation des salariés grâce à une démarche porteuse de sens

Ethique

- contribuer à l'effort généra de résolution des problèmes écologiques

Analyse du Cycle de vie (ACV)

l'**Analyse en cycle de vie** (ACV). Celle-ci consiste à mesurer l'ensemble des effets quantifiables d'un produit ou d'un service sur notre environnement naturel durant les différentes phases de son cycle de vie (du début de sa fabrication à sa fin de vie) (source : ADEME). Par exemple, le cycle de vie d'un smartphone comporte les phases suivantes :

- Extraction des matières premières et raffinage
- Fabrication et assemblage des composants
- Distribution du produit fini
- Utilisation
- Fin de vie

Parties prenantes concernées

La démarche d'éco-conception est un sujet transversal qui touche différents métiers au sein de l'entreprise

Les salariés de l'entreprise en charge de :

- la conception des matériels et logiciels,
- du développement de ceux-ci,
- et des achats,

mais également :

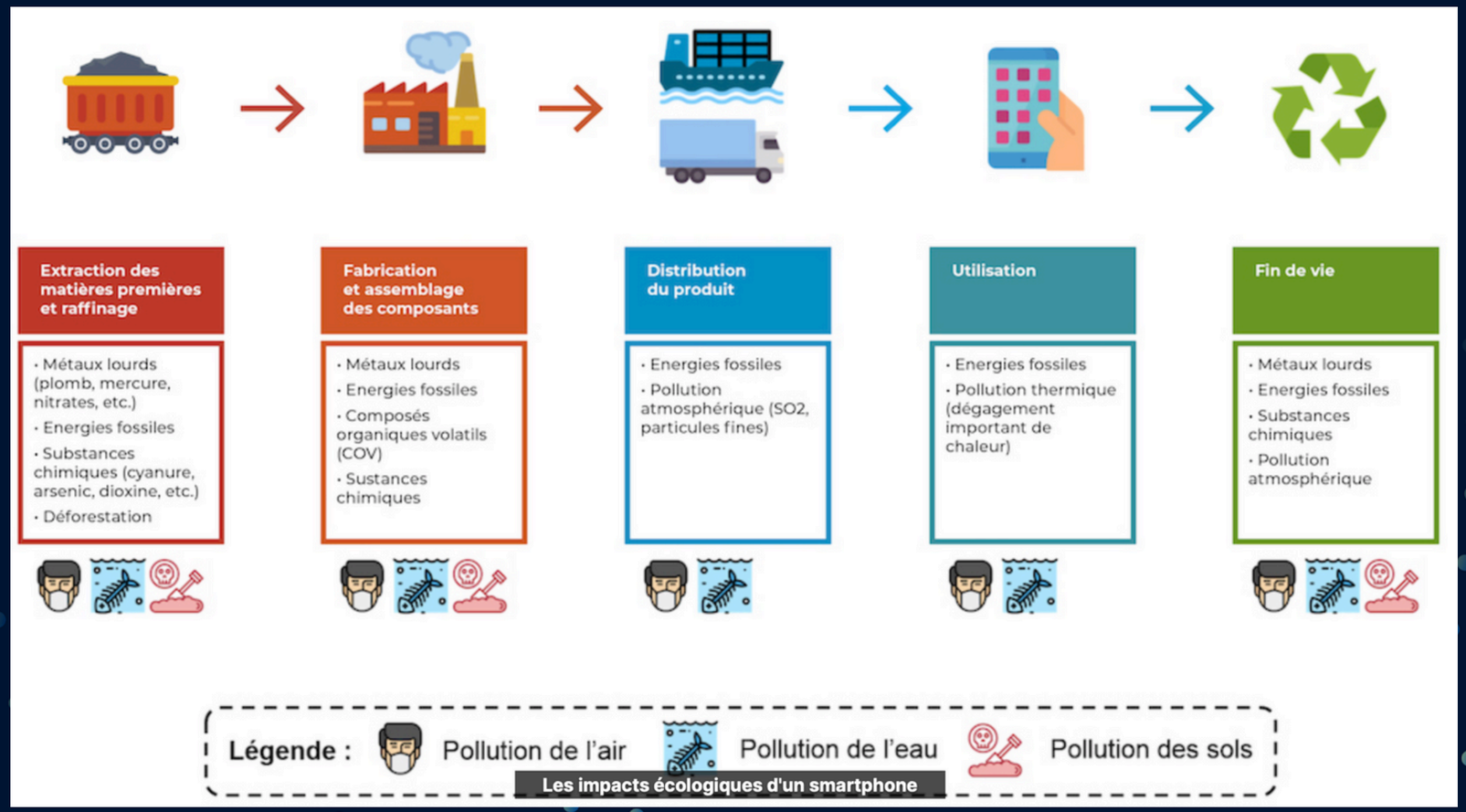
- les utilisateurs finaux (services métier, fonctions support, aussi appelés "clients internes" par les DSI),
- et les salariés en charge de la gestion des déchets.

Et les **parties prenantes externes** tels que :

- Les fournisseurs
- Fabricants
- Prestataires
- Clients

Cycle de vie d’un produit

Pour les smartphones, ordinateurs fixes et portables, les deux premières étapes sont celles où les impacts sont les plus importants.



Source de l'image : Eric Drezet

Transfert d'impact

On parle de transfert d'impact lorsque la réduction d'un impact écologique entraîne l'accroissement d'un autre impact. Le plus souvent, ce transfert se fait entre deux étapes du cycle de vie. Par exemple, améliorer l'isolation d'un réfrigérateur diminuera sa consommation d'énergie à l'usage, mais augmentera la quantité de matériaux utilisés et l'énergie nécessaire pour extraire ces matériaux.

Raisonner en cycle de vie permet ici de voir si l'effet net est positif ou négatif.

Quantifier l’impact écologique - unité fonctionnelle

Unité fonctionnelle : c’est un niveau de performance attendu pour un usage déterminé.
Elle sert de base de calcul pour chiffrer les impacts écologiques à la modélisation et permet de comparer différents produits sur une même base.

Par exemple, pour effectuer l’ACV d’une lampe, l’unité fonctionnelle pourra être « éclairer avec une luminosité de 60 W pendant 1 000 h ». Pour celle d’un webmail, cela pourra être « envoyer un e-mail pesant 500 ko à 10 personnes ».

Mettre en oeuvre une démarche d'éco-conception

KATANE

Phase A : structuration du projet

Étape 1 : Initier

Étape 2 : Porter

Étape 3 : Mobiliser

Phase B : identification des impacts

Étape 4 : Évaluer

Étape 5 : Analyser

Phase C : réduction des impacts

Étape 6 : Imaginer

Étape 7 : Réaliser

Phase D : partage des résultats (reporting)

Étape 8 : Vérifier

Étape 9 : Communiquer

Mini-projet - À partir des résultats de l'ACV, identifiez 3 pistes d'amélioration permettant de réduire l'impact écologique du service numérique.

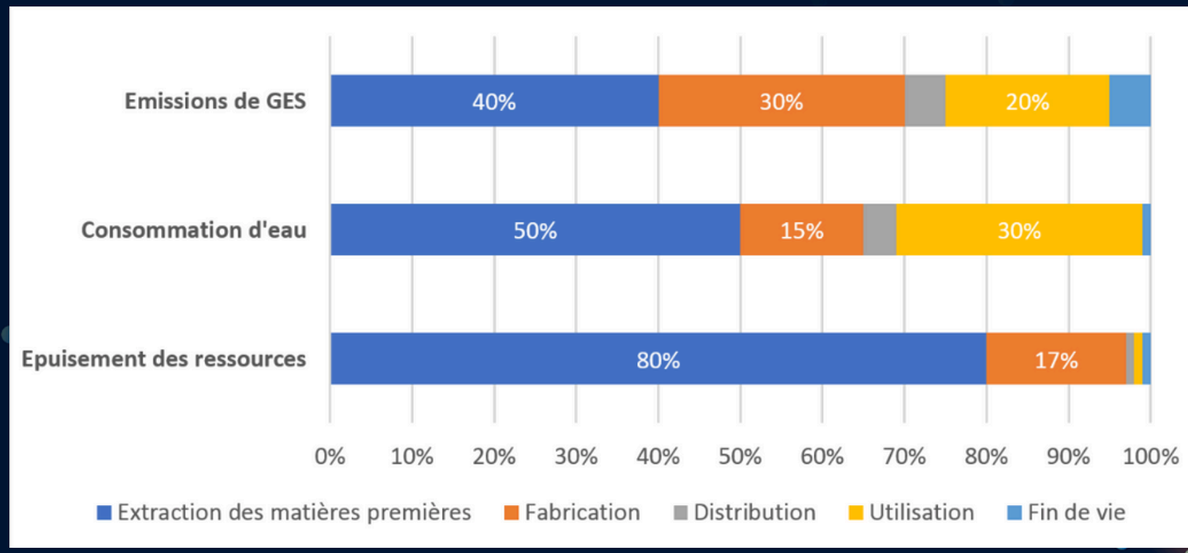
Sujet prototype de chaussette connectée

Unité fonctionnelle : afficher et évaluer l'état de santé des pieds et chevilles du coureur durant 250 heures d'utilisation du produit (dont 200 heures en entraînement, soit une année à un rythme de 3 sessions d'une heure par semaine).
Composition du service numérique : chaussette, capteur, smartphone, application mobile, réseau, data center.
Impacts étudiés : épuisement des ressources, consommation d'eau et émissions de GES.
40 % des émissions de GES de la chaussette connectée sont liées à l'extraction des matières premières.

Éléments d'explication des impacts

- La chaussette est en coton cultivé en agriculture conventionnelle (usage important d'eau et de pesticides).
- La chaussette est équipée de 10 capteurs qui couvrent l'intégralité de celle-ci.
- Les capteurs sont allumés en permanence. Ils se rechargent en partie en récupérant l'énergie de la foulée du coureur.
- L'application mobile affiche les informations sous forme de graphiques dynamiques actualisés toutes les 5 secondes.

Répartition des impacts



Eco-conception - Focus sites web

- Dans une architecture web client-serveur, les impacts écologiques proviennent en priorité des terminaux, puis du réseau et des data centers.

- 3 leviers permettent d'alléger l'empreinte écologique d'un site web :
  la frugalité fonctionnelle, l'optimisation du contenant, l'optimisation du contenu.

- Il est possible de travailler sur un site web existant, un site en cours de refonte ou sur un projet de site.

- La démarche à suivre part de l'existant et consiste à mettre en place une série d'actions pour réduire l'empreinte écologique du site web, puis à évaluer le gain réalisé (par rapport à la situation initiale).

Eco-conception - exemple

Exemples d'optimisation du contenant : **Facebook et Linkedin** (source : Frédéric Bordage)

Pour la refonte de son réseau social, Facebook a travaillé sur l'optimisation du code serveur pour diminuer les ressources nécessaires à son interprétation. Il a développé le programme « HipHop for PHP » qui permet de compiler du code PHP en C++. Ceci a permis de diviser par 2 le nombre de serveurs nécessaires au fonctionnement du réseau social pour un nombre donné d'utilisateurs.

Pour la création de son site web mobile, LinkedIn a travaillé sur le même sujet que Facebook. Il a été décidé de travailler en Node.js plutôt qu'avec un proxy synchrone en Ruby on Rails. Ceci a permis de diviser le nombre de serveurs nécessaires par 8 pour un nombre donné d'utilisateurs.

Eco-conception - focus sites web - 115 bonnes pratiques

https://collectif.greenit.fr/ecoconception-web/115-bonnes-pratiques-eco-conception_web.html

KATANE

Extract non exhaustif

Specification	Conception	Utilisation	Production	Utilisation	Support, maintenance, fin de vie
Ne pas retenir les fonctionnalités non essentielles	Optimiser le parcours utilisateur	Limiter le nombre de CSS	Réduire au nécessaire les logs des serveurs	Optimiser et générer les médias avant importation sur un CMS	Eviter les redirections
Quantifier précisément le besoin	Respecter le principe de navigation rapide dans l'historique	Limiter le nombre de requêtes HTTP	Définir une politique d'expiration et suppression des données	Éviter la lecture et le chargement automatique des vidéos et des sons	Avoir une stratégie de fin de vie des contenus
Supprimer les fonctionnalités non utilisées	Mettre en cache les données calculées souvent utilisées	Optimiser les requêtes aux bases de données	Stocker les données dans le cloud	Limiter la taille des emails envoyés	Mettre en place un plan de fin de vie du site

- **Site internet que vous avez développé vous même**
- **Choisissez un site tel que : le CNES, ArianeGroup, EFREI, Bugatti**
- **Testez son impact et étudier les recommandations sur : https://www.ecoindex.fr**

Green IT / IT for Green

KATANE

Distinguez Green IT et IT for Green

Parfois utilisés de manière interchangeable, ces deux termes ne recouvrent pas la même réalité. Le Green IT s'intéresse aux impacts écologiques du numérique en lui-même, alors que l'approche IT for Green (ou Green by IT) désigne une application du numérique à visée écologique (par exemple : un logiciel de reporting environnemental ou une technologie comme les smart grids). Cette dernière s'intéresse donc à la manière dont est appliqué le numérique.

Le lien entre ces deux approches n'est pas automatique :

Ce n'est pas parce qu'un matériel ou un logiciel a un impact écologique réduit qu'il a forcément un intérêt écologique (par exemple : un smartphone reconditionné peut tout à fait servir à réserver des billets d'avion pour un pays lointain).

Inversement, ce n'est pas parce qu'un matériel ou un logiciel est à visée écologique qu'il a forcément un faible impact écologique (par exemple : un supercalculateur servant à modéliser le changement climatique a un fort impact écologique).

Néanmoins, ces deux approches restent complémentaires. Leur utilisation conjuguée est d'ailleurs l'une des meilleures manières de rendre le numérique compatible avec la transition écologique.

Frise chronologique des référentiels

KATANE

2009
Règlement EMAS

2013
Règlement Européen n° 801/2013 à propos de la consommation d'électricité

2015
Obsolescence
la loi n° 2015-992 du 17 août 2015 **relative à la transition énergétique pour la croissance verte**

2020
Loi AGEC
Transformer l'économie linéaire, « produire, consommer, jeter », en une économie .circulaire

2021
Loi REEN
Réduction de l'Empreinte Environnemental e du Numérique

2022
Haut Comité pour le Numérique Écoresponsable (HCNE)
Création

04

Projets d’audit Cyber/RSE

Processus d’audit

KATANE

Initiation de l’audit	Audit	Conclusion / Clôture
Etablir la convention d’audit (Contexte de l’entreprise, Type d’audit, Périmètre, Acteurs, Référentiels applicables, critères d’évaluation, reprise de l’expression du besoin)	Réalisation de l’audit : • via l’interview des acteurs du projet • via l’exécution du plan de test et la récupération de preuves	Présentation et explication des résultats Transmission du rapport Proposition de recommendations
Définir le programme d’audit Préparer les plans de test	- Evaluation et contextualisation des non-conformités et potentielles vulnérabilités - Etablissement de l’analyse d’écart entre l’existent et le référentiel.	
Planifier une réunion d’ouverture : - Présenter la démarche avec les objectifs • Collecter les informations • Préparer l’audit		

Exemple d'outil/référentiel pour réaliser un audit d'éco-conception

https://www.arcep.fr/uploads/tx_gspublication/referentiel_general_ecoconception_des_services_numeriques_version_2024.pdf

Le PDF sera téléchargé dans le groupe sur Teams

KATANE

5.8 Le service numérique a-t-il une stratégie d'archivage et de suppression, automatique ou manuelle, des contenus obsolètes ou périmés ?

Niveau de difficulté :

Niveau de priorité :

Cible : N/A si le service ne gère pas de contenu

Métiers concernés : Architecte Logiciel, *Data Scientist*, Responsable de la sécurité informatique, Responsable Juridique

OBJECTIF

Alléger les bases de données et les serveurs physiques de données non utiles.

MISE EN ŒUVRE

Définir une stratégie d'archivage et de suppression des contenus obsolètes, périmés, dépassés ou inutiles à conserver dans le service numérique. Cette stratégie peut être automatique en définissant une date d'expiration et un processus d'archivage et/ou de purge automatique.

De façon complémentaire à des mécanismes d'archivage automatique, prévoir également des mécanismes de suppression manuelle pour les contenus spécifiques qui nécessitent une évaluation humaine.

Cette stratégie est obligatoire pour le sous-ensemble des données personnelles collectées par les services, qui impose de définir et communiquer une durée de conservation des données personnelles (art. 13-2 du RGPD).

MOYEN DE TEST OU DE CONTRÔLE

Pour valider ce critère, vérifier l'existence d'une stratégie d'archivage et de suppression clairement définie, l'existence de mécanismes automatiques et de processus manuels pour les contenus dont le traitement requiert une intervention humaine. Le suivi de cette stratégie pourra être réalisé en évaluant régulièrement le taux d'occupation des bases de données et des serveurs physiques.

Réaliser un audit RSE en fonction du RGE SN

L'audit RSE, contrairement à une simple vérification technique, doit couvrir l'intégralité du cycle de vie du service numérique. Le RGE-SN structure ses critères selon 9 axes qui correspondent **aux phases de conception** et aux domaines de responsabilité au sein de l'entreprise :

Axe du RGE-SN	Phase du Cycle de Vie	Métiers Principalement Concernés
Axe 1 & 2	**Stratégie & Spécifications**	Direction, Chef de Produit, PO, MOA, RSE.
Axe 3, 4 & 5	**Conception & Contenu**	UX/UI Designers, Ergonome, Rédacteurs, Chef de Projet.
Axe 6, 7 & 8	**Développement & Infrastructure**	Développeurs (Frontend/Backend), Architecte, DevOps, DSI.
Axe 9	**Algorithmie (IA/ML)**	Data Scientists, Architecte Logiciel.

KATANE

Réaliser un audit RSE en fonction du RGE SN - approche par le risque ou approche par la preuve ?

Approche par la preuve : L'auditeur ne se contente pas de cocher des cases ; il vérifie les preuves (documentations, tests de performance, code, stratégie d'entreprise) qui attestent du respect des critères.

Approche par le risque : L'auditeur se base sur les évènements redoutés et sur les scénarios de risques pour les éprouvés (approche particulièrement applicable à la cybersécurité)

KATANE

Système de priorisation et de scoring

KATANE

RSE : Pour éviter l'effet "usine à gaz" et se concentrer sur l'impact, le RGE-SN pondère les critères, tous les critères n'ont pas la même importance :

- **Critères Prioritaires (x 1,5)** : C'est le cœur de l'écoconception. Leur non-respect est la plus grande source de dette environnementale. (Exemple : L'utilité du service ou l'adaptabilité aux vieux terminaux.)
- **Critères Recommandés (x 1,25)** : Bonnes pratiques à adopter pour optimiser. (Exemple : La compression avancée des images.)
- **Critères Modérés (x 1,0)** : Critères de base ou moins impactants.

Concept du Score d'Avancement : À la fin de l'audit, un score est calculé, reflétant la maturité RSE. L'objectif n'est pas d'atteindre 100% du jour au lendemain, mais d'établir une feuille de route basée sur les critères prioritaires non validés.

Cybersécurité : la priorisation des vulnérabilités lors d'un audit est réalisé grâce à la criticité (vraissemblance x gravité).
La priorisation des recommandations est réalisée grâce au coût, à la complexité de mise en oeure et à son impact.

Système de priorisation et de scoring - comparatif RSE / Cybersécurité

KATANE

Audit de Sécurité	Audit RSE (RGE-SN)
Axe d'audit	**Domaine d'impact**
Vulnérabilité critique	*Critère Prioritaire (x1.5)*
Risque de perte de données / indisponibilité	*Risque de forte empreinte carbone / obsolescence forcée*
Le « Patch »	**Le « Correctif Éco »**
*Le non-respect est une **faille de sécurité***	*Le non-respect est une **dette environnementale***

Zoom sur les critères prioritaires étude de cas

KATANE

Etude de cas 1- Utilité et Simplicité (Axe 1 & 5)

Critère 1.1 (Prioritaire) : S'assurer que le service a fait l'objet d'une évaluation favorable en termes d'utilité et de fonctionnalités.

Implication RSE : Si le service n'est pas utile, toutes les ressources utilisées pour le développer, l'héberger et le faire utiliser sont du gaspillage.

Impact Cyber : Un service surchargé de fonctionnalités inutiles ("feature bloat") augmente la surface d'attaque. Plus il y a de code, plus il y a de risques de bugs, et potentiellement de failles de sécurité.

Critère 1.1 (Prioritaire) : S'assurer que le service a fait l'objet d'une évaluation favorable en termes d'utilité et de fonctionnalités.

Implication RSE : Les dark patterns (conception manipulatrice qui pousse l'utilisateur à faire une action coûteuse ou rester en ligne) obligent à une consommation énergétique non souhaitée.

Impact Cyber : Les dark patterns sont une forme d'ingénierie sociale au niveau de l'interface, rompant la confiance et la transparence – des piliers de la sécurité et de la résilience.

KATANE

Etude de cas 2 - L'Obsolescence Logicielle et Matérielle (Axe 2)

Critère 2.2 (Prioritaire) : S'assurer que le service est utilisable sur des terminaux anciens.

Implication RSE : Si le service n'est pas utile, toutes les ressources utilisées pour le développer, l'héberger et le faire utiliser sont du gaspillage.

Impact Cyber : Un service surchargé de fonctionnalités inutiles ("feature bloat") augmente la surface d'attaque. Plus il y a de code, plus il y a de risques de bugs, et potentiellement de failles de sécurité.

KATANE

Etude de cas 3 - L'Hébergement et la Frugalité (Axe 8 & 9)

Critère 8.1 (Prioritaire) : S'assurer que l'hébergeur a mis en place une démarche de réduction de son empreinte environnementale.

Implication RSE : L'énergie consommée par les centres de données. Le choix d'un hébergeur qui utilise de l'énergie décarbonée est fondamental.

Impact Cyber (Risque Tiers) : C'est l'exemple parfait du risque de la chaîne d'approvisionnement Un hébergeur qui ne gère pas son impact RSE est souvent un acteur qui pourrait négliger d'autres domaines (comme la sécurité physique ou logique de ses data centers).

KATANE

Etude de cas 4 - La Chaîne d'Approvisionnement

Le maillon faible dans la sécurité comme dans le RSE est souvent le tiers (fournisseur, sous-traitant).

Le Cas RSE (Critère 2.8 / 8.1)

Si votre service utilise un fournisseur de carte ou d'hébergement dont la politique RSE est inexistante (mauvaise performance énergétique), vous héritez de leur empreinte carbone.

Le Cas Cyber (ISO 27001 - A.15)

Si ce même fournisseur a des politiques de sécurité faibles, vous héritez de leur risque de fuite de données ou d'indisponibilité.

Question de Réflexion : Comment la réduction du volume de données stockées (objectif RSE) contribue-t-elle directement à la réduction du risque de fuite de données (objectif Cyber) ?

Projet étape 2/3 - analyse des impacts environnementaux sur un système d'information

En gardant les mêmes groupes & mêmes sujets
Proposer des actions de remédiation pour chacun des risques

Lister les éléments permettant de construire un PCA et PRA

Définition du PCA (Plan de Continuité d'Activité)

Le Plan de Continuité d'Activité (PCA) est une procédure préventive conçue pour mettre en œuvre l'ensemble des mesures nécessaires en cas de défaillance du système d'information afin de rester opérationnel après un événement imprévu. Ce plan permet une continuité de l'activité en cas de panne ou d'incident, grâce à une anticipation du risque et de ses conséquences.

Définition du PRA (Plan de Reprise d'Activité)

Le Plan de Reprise d'Activité (PRA) est une procédure curative visant à réparer les dégâts causés par un sinistre informatique. C'est un processus de reprise rapide d'activité portant notamment sur la restauration des données. Il intervient ainsi après une interruption.

Définition : cybersecurite-management.fr

05

Gestion de projet & éthique

Responsabilité & éthique

Ethique des vertus - Aristote

Les trois traditions éthiques classiques

1. Éthique des vertus (Aristote)

Question centrale : comment bien vivre ? Ethôs

- **Être vertueux, c'est aligner intention et action dans la quête du Bien.**
- **En cybersécurité : un RSSI vertueux doit avoir à la fois l'intention de protéger et la pratique effective (sécuriser vraiment les données, pas seulement en apparence).**

KATANE

Ethique des vertus - Aristote

L'Intégrité du Chef de Projet et la Sécurité du SI (Phronesis et Qualité)

=> Est-ce que l'intégrité et les vertus du PM sont des facteurs critiques de succès, au même titre que la maîtrise des outils (Gantt, matrices de risques).

=> Appliquer la Phronesis : Utiliser le concept de Phronesis (Prudence/Sagesse Pratique) pour analyser les décisions prises lors de la phase d'analyse des risques.

=> Est-ce que l’excès ou le manque de Courage ou d'Honnêteté peut conduire à sous-estimer un risque critique, compromettant ainsi la sécurité de l'entreprise.

Responsabilité & éthique

Ethique déontologique - KANT

Éthique déontologique (Kant)

deon = devoir / *logos* = raison

- Fondée sur le devoir et l’universalité.
- Agir moralement = agir selon un principe valable pour tous, indépendamment des conséquences.
- En cybersécurité : appliquer une règle stricte (ex. mot de passe complexe) non par commodité, mais par devoir universel de protection.

KATANE

Ethique déontologique - Kant

Formule	Principe	Application en Gestion de Projet et Cyber
1. La Loi Universelle	"Agis uniquement d'après la maxime qui fait que tu peux vouloir en même temps qu'elle devienne une loi universelle."	**Le Test du Mensonge :** Si je mens sur l'état d'avancement pour respecter le délai (ma *maxime*), est-ce que je peux vouloir que *tout* PM mente sur l'état de son projet ? Non, car si le mensonge était universel, la confiance dans les rapports PM s'effondrerait, rendant la GP impossible. Donc, mentir est immoral.
2. L'Humanité comme Fin	"Agis de telle sorte que tu traites l'humanité, aussi bien dans ta personne que dans la personne de tout autre, toujours en même temps comme une fin, et jamais simplement comme un moyen."	**Le Respect des Parties Prenantes :** Utiliser les données des clients ou la sécurité des employés **uniquement** comme un moyen d'atteindre l'objectif de profit (la fin du projet) est immoral. La sécurité des données (Confidentialité) et la santé des employés (Disponibilité) sont des fins en soi.

KATANE

Ethique des vertus - Kant

Objectif : Rédiger un rapport justifiant le maintien ou l'abandon d'une action de sécurité critique en utilisant uniquement le cadre éthique kantien.

Dilemme : Choisir une action de réduction de risque nécessaire pour la conformité (ex: Implémentation de l'authentification multi-facteurs, Redondance géographique de la BDD, Mise à jour coûteuse d'un SI obsolète).

La Contrainte du Succès : Déterminer que cette action critique ferait dépasser de 15% le budget OU de 2 mois le délai de livraison.

La Pression : Le sponsor (fictif) exige de maintenir la date/le budget et propose un "contournement temporaire" non-conforme, mais jugé "suffisamment bon" pour le lancement.

Action Proposée	Maxime de l'Action	Test d'Universalisation
Contournement Temporaire	"Je me décharge de mon devoir critique de sécurité quand il y a des contraintes de budget/délai, en faisant semblant d'être conforme."	Si tous les PM le font, la conformité devient une farce, les SI ne sont plus sécurisés, et les lois (RGPD) perdent leur force. **Contradiction.**
Exiger la Conformité Totale	"J'accomplis mon devoir de sécurité (protection de l'actif critique) même si cela met en péril les objectifs secondaires (budget/délai)."	Si tous les PM le font, la sécurité des systèmes est garantie. **Pas de Contradiction.**

Responsabilité & éthique

Ethique conséquentialiste - Hans Jonas

Éthique conséquentialiste / utilitariste (Mill, Hans Jonas)

- **C’est la conséquence qui détermine la valeur morale.**
- **Une action est juste si elle maximise le bien-être ou réduit les dommages.**
- **En cybersécurité :**
  - **divulguer rapidement une faille pour protéger un maximum d’utilisateurs,**
  - **ou au contraire différer la divulgation pour éviter une exploitation massive.**
- **Peu importe l’intention, seule la conséquence finale compte.**

Projet étape 1/3 - Cadre et Analyse du Risque

Par groupe de 5 :

- **Identifier un rapporteur**
- **Choisir un sujet**

En respectant les étapes d'un projet, dans la phase de réalisation ;

- **Identifier un périmètre d'analyse**

(Décrire le Système d'Information (SI) de l'entreprise (schéma simple ou liste d'entités/applications clés) et définir clairement les actifs (biens supports et informations) inclus dans l'analyse).

- **Identifier deux menaces environnementales majeures pesant sur la sécurité du système d'information.**
- **Identifier chaque menaces choisies, identifier plusieurs vulnérabilités présent sur le système d'information avec leur bien support.**

(Ex vulnérabilités: "Pas de redondance géographique", "Locaux serveurs au sous-sol", "Dépendance à un unique fournisseur d'énergie").
(Ex bien support: Serveur d'applications, Base de données clients, Routeur central)

- **Identifier pour chaque vulnérabilité un impact potentiel et son critère SSI** (Disponibilité, Intégrité, Confidentialité)
- **Catégoriser les impacts** (image, opérationnel, juridique, humain, financier)
- **Evaluer la gravité pour chaque impact** (la justification est plus importante que la mesure)
- **Evaluer la vraissemblance pour chaque impact** (la justification est plus importante que la mesure)

- **Déterminer le niveau de risque** (Gravité/Vraissemblance)

Projet étape 2/3 - analyse des impacts environnementaux sur un système d'information

En gardant les mêmes groupes & mêmes sujets
Proposer des actions de remédiation pour chacun des risques

Lister les éléments permettant de construire un PCA et PRA

Définition du PCA (Plan de Continuité d'Activité)

Le Plan de Continuité d'Activité (PCA) est une procédure préventive conçue pour mettre en œuvre l'ensemble des mesures nécessaires en cas de défaillance du système d'information afin de rester opérationnel après un événement imprévu. Ce plan permet une continuité de l'activité en cas de panne ou d'incident, grâce à une anticipation du risque et de ses conséquences.

Définition du PRA (Plan de Reprise d'Activité)

Le Plan de Reprise d'Activité (PRA) est une procédure curative visant à réparer les dégâts causés par un sinistre informatique. C'est un processus de reprise rapide d'activité portant notamment sur la restauration des données. Il intervient ainsi après une interruption.

Définition : cybersecurite-management.fr

Projet étape 3/3 - analyse des impacts environnementaux sur un système d'information

En gardant les mêmes groupes & mêmes sujets :

=> Intégrer les principes éthiques pour chaque proposition d'actions de remédiation au sein de votre PCA/PRA et justifiez vos choix. #éthique_vertus#éthique_universaliste#éthique_conséquentialiste

=> Réalisation un plan de sensibilisation contextualisé avec votre sujet en intégrant les principes éthiques évoqués en cours

Définition : cybersecurite-management.fr

Responsabilité & éthique

Ethique conséquentialiste - Hans Jonas

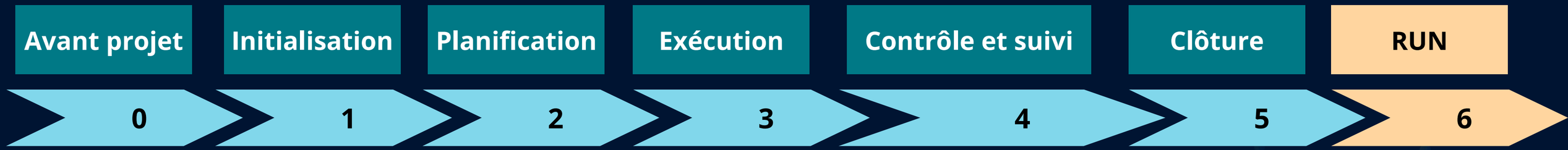
Éthique conséquentialiste / utilitariste (Mill, Hans Jonas)

- **C’est la conséquence qui détermine la valeur morale.**
- **Une action est juste si elle maximise le bien-être ou réduit les dommages.**
- **En cybersécurité :**
  - **divulguer rapidement une faille pour protéger un maximum d’utilisateurs,**
  - **ou au contraire différer la divulgation pour éviter une exploitation massive.**
- **Peu importe l’intention, seule la conséquence finale compte.**

06

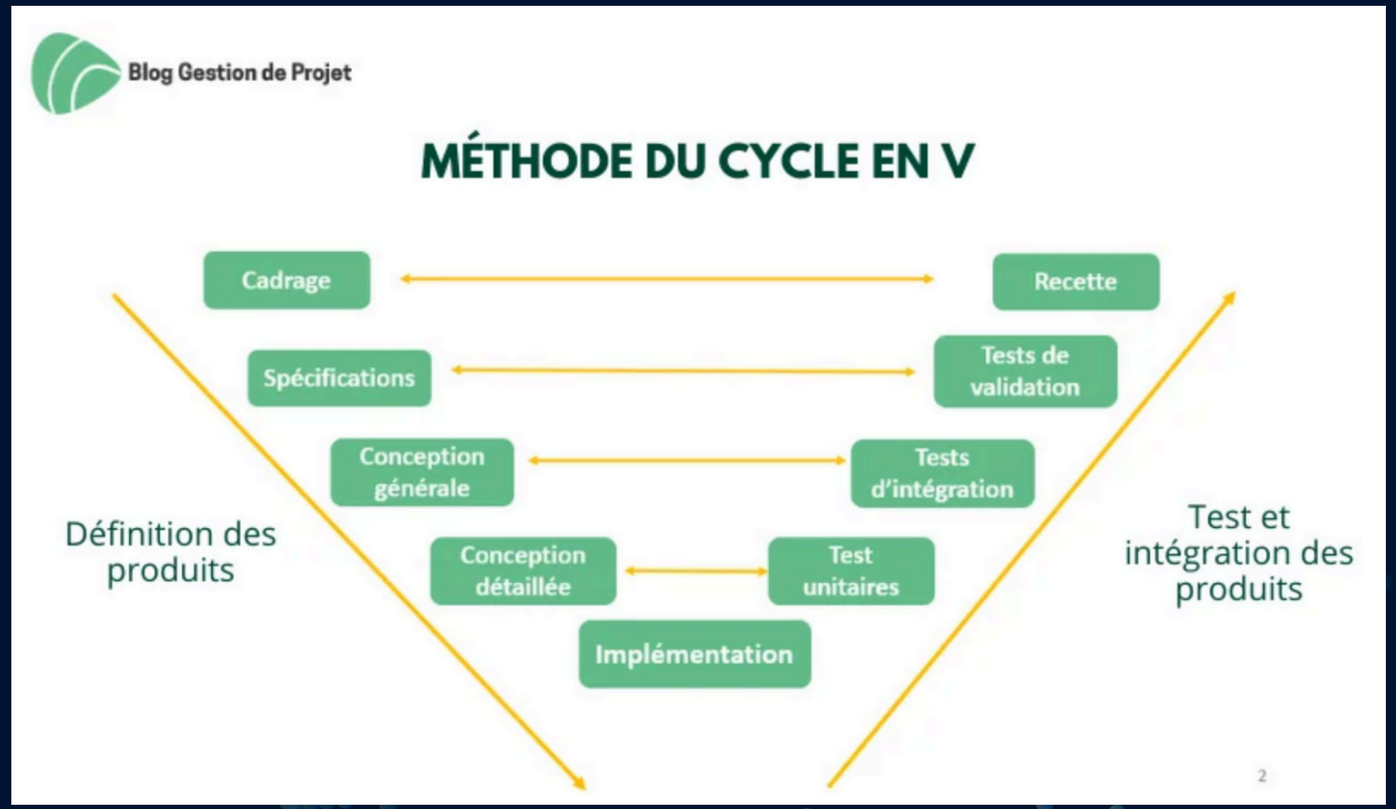
Rappel
Gestion de projet
AGILE

Phases clés de la gestion de projet



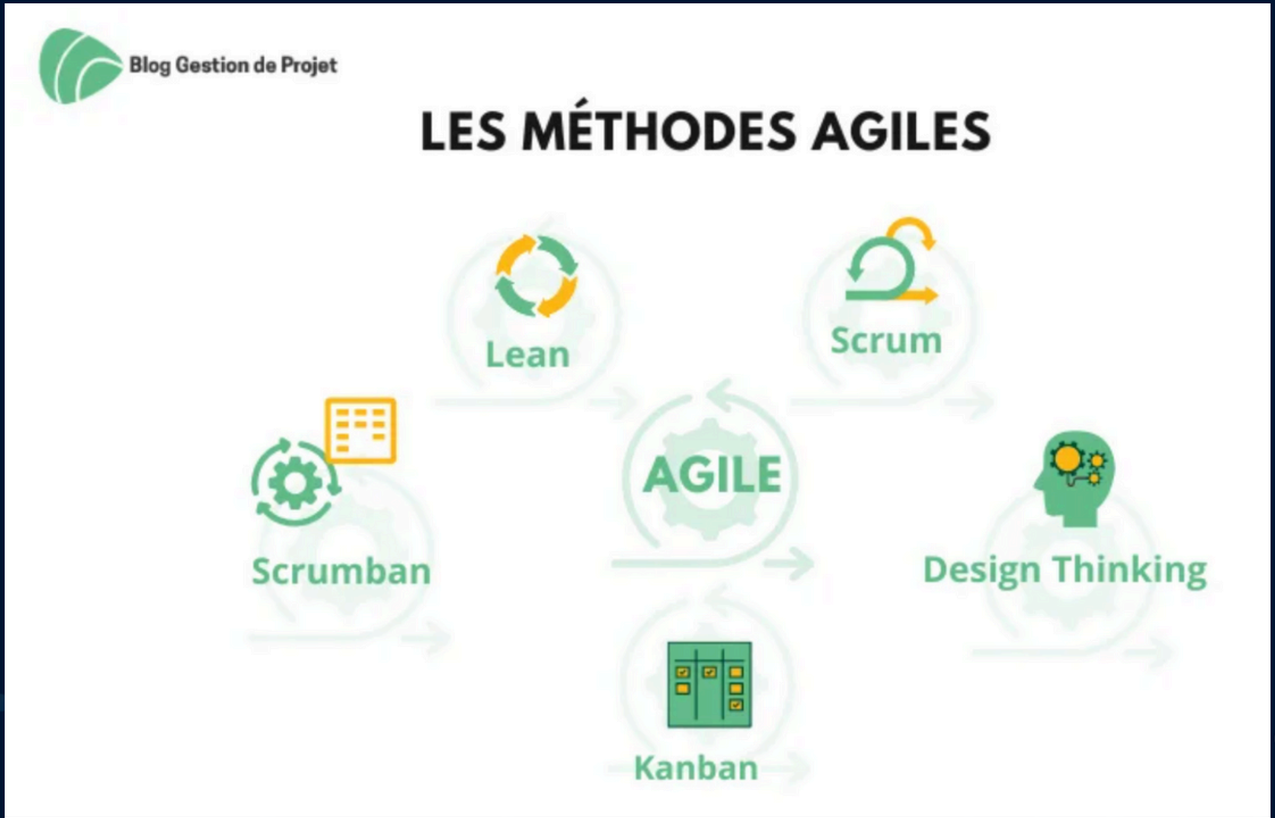
Gestion de projet classique

Cycle en V



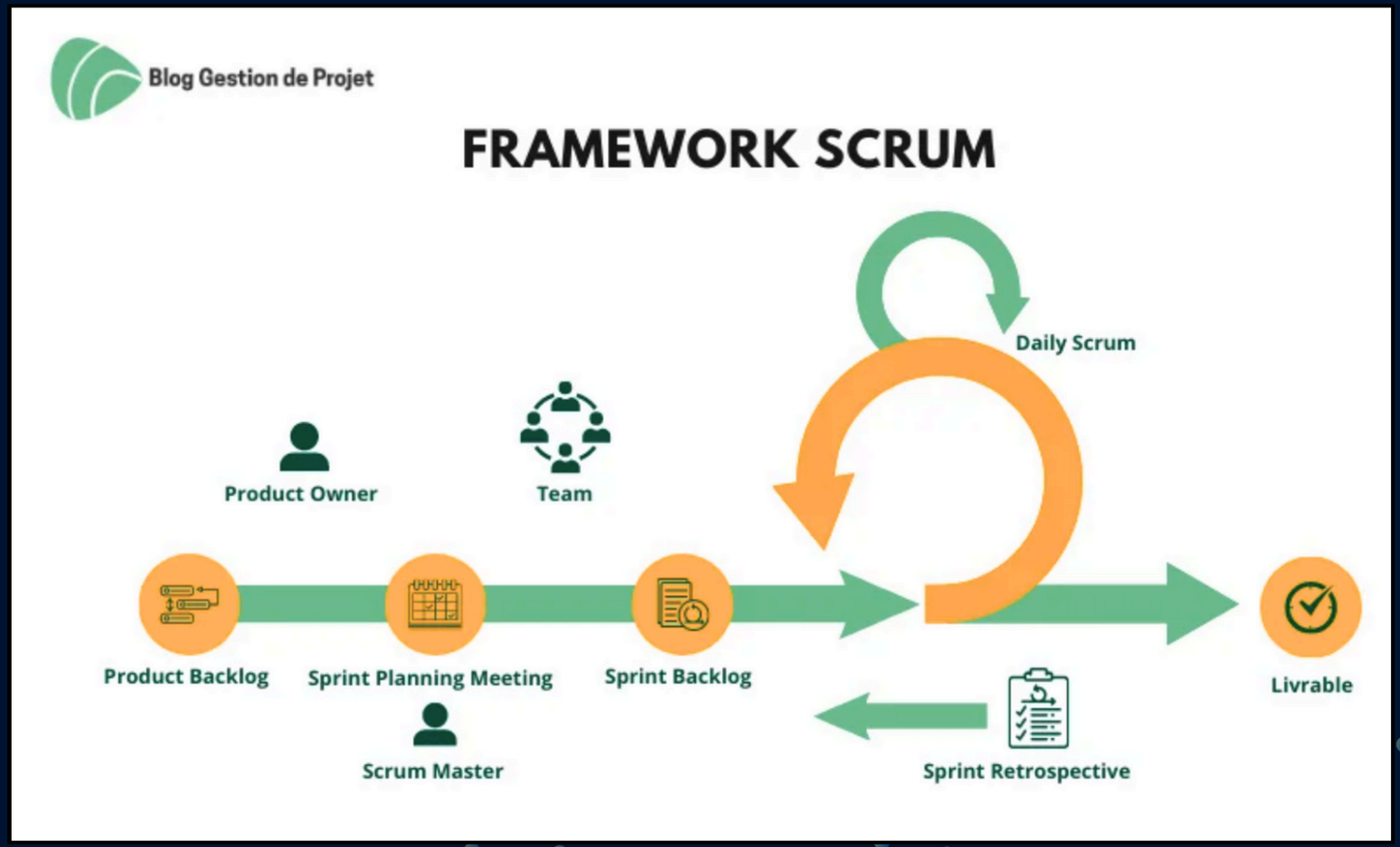
- **Un flux descendant :** qui détaille le produit depuis le cadrage jusqu'à son implémentation en passant par le recueil des expressions et les spécifications
- **Et un flux ascendant :** qui vérifie la qualité du produit à chacune des phases du projet en partant de l'implémentation pour remonter jusqu'au cadrage

Gestion de projet Agile - Types de modèle



Gestion de projet Agile - Types de modèle

SCRUM



La spécificité de Scrum se trouve dans la façon dont elle fonctionne en utilisant :

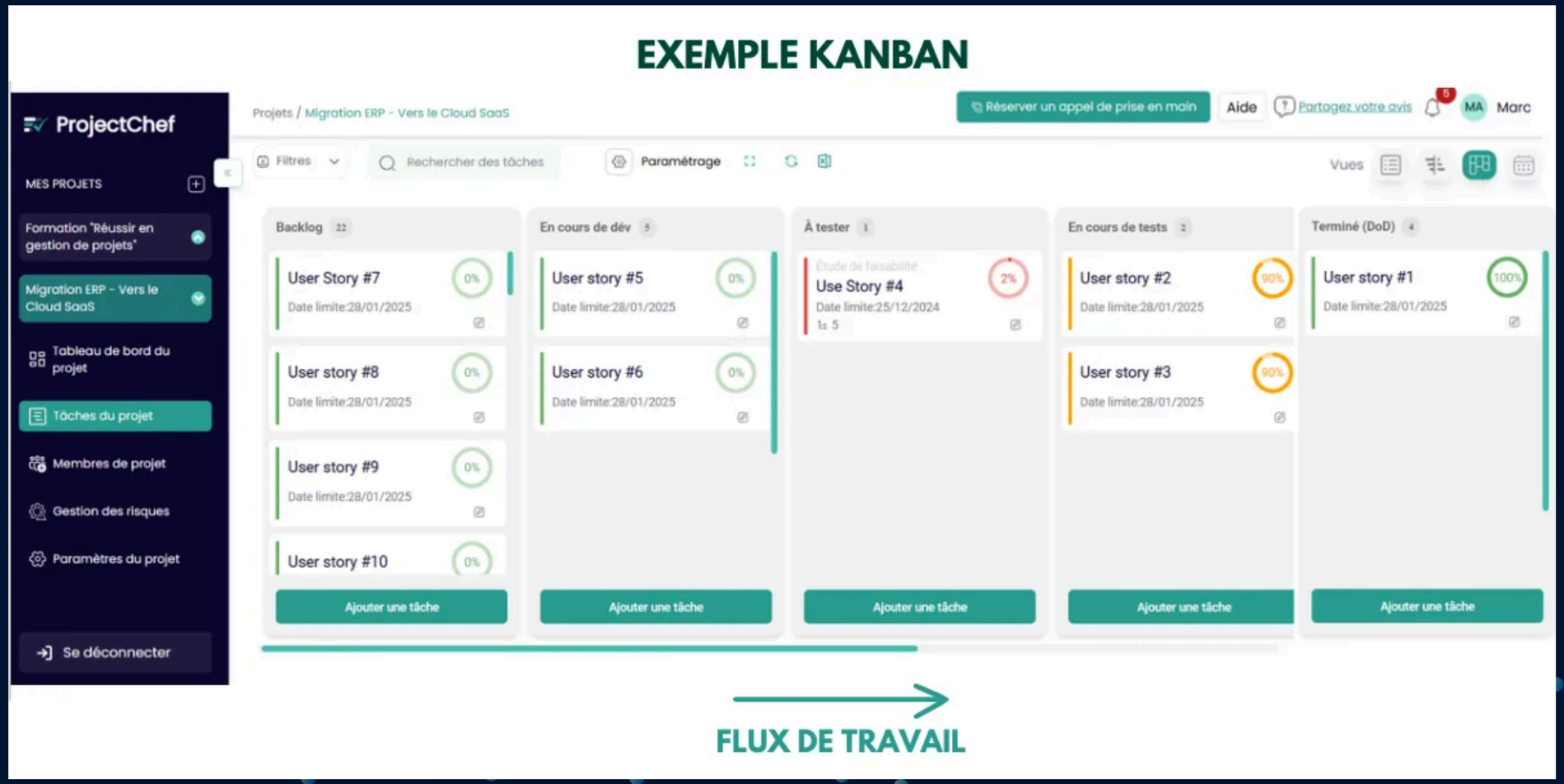
Des rôles : Product Owner, Scrum master, Scrum team,

Des événements : les Sprints à durée bien définie, les Daly Scrum de 15 min par jour, le Sprint Planning meeting, la Sprint review et la Sprint retrospective

Des artefacts : Product backlog, sprint backlog, livrables

Gestion de projet Agile - Types de modèle

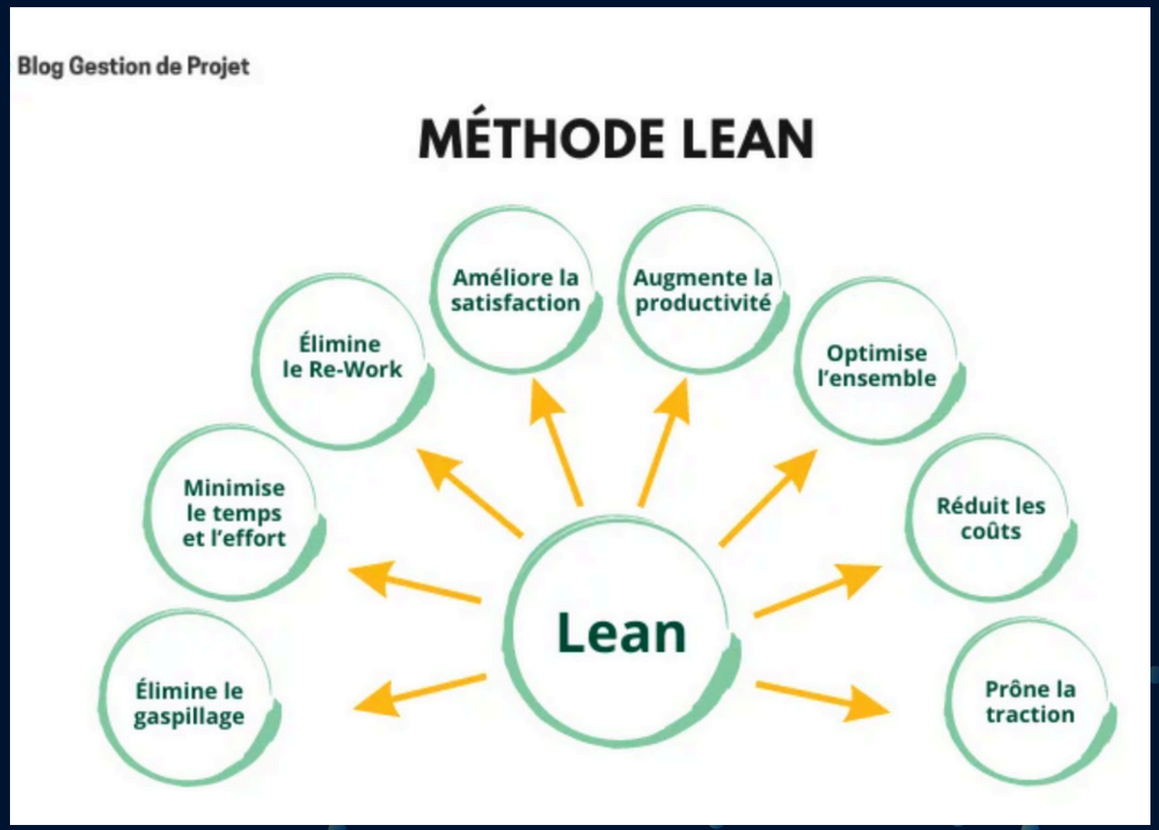
KABAN



1. Visualiser le travail
2. Limiter le travail en cours
3. S'améliorer en continu

Gestion de projet Agile - Types de modèle

LEAN



- **Muda (gaspillage) :** lorsque vous utilisez des ressources sans que ces dernières n'apportent de valeur ajoutée au client
- **Mura (irrégularité)** : lorsque l'avancement plus prononcé d'une partie déséquilibre toutes les autres parties. Cela conduit à une inefficacité des processus et de l'équipe (gaspillage !).
- **Muri (surcharge)** : lorsqu'il y a trop de pression sur les ressources. Cela conduit à des inefficacités - tant au niveau des machines que des personnes

Gestion de projet Agile - Types de modèle

Scrum VS Kanban

Rôles

Des rôles définis pour chaque membre de l'équipe

Les responsabilités de chacun sont flexibles

Engagements

L'équipe s'engage sur la livraison d'un nombre de fonctionnalités en début de sprint

Pas d'engagement sur un nombre. Les équipes réalisent leurs tâches une à une

Cadences

Les tâches doivent être achevées dans un certain laps de temps (sprint)

Pas de restriction de temps. Le but est d'atteindre un écoulement des tâches en continu

Itérations

Une fois le sprint démarré, il ne peut être modifié que dans certaines conditions

Possibilité d'ajouter des tâches dans le tableau si besoin

Equipes

Le backlog d'un sprint n'appartient qu'à une équipe produit

Un tableau Kanban peut être partagé par plusieurs équipes produit

Panomarama des outils phares

Le marché des outils de gestion de projet est dynamique et propose des solutions adaptées à chaque besoin.

Jira : Largement utilisé par les développeurs, il est spécifiquement conçu pour les projets agiles, notamment Scrum, avec des fonctionnalités de suivi des bugs et de rapports de sprint.

Monday.com : Reconnu pour sa flexibilité et son interface intuitive, il permet d'automatiser les tâches et de s'intégrer avec des outils comme Slack ou Microsoft Teams.

Asana : Apprécié pour sa simplicité et ses fonctionnalités d'IA qui aident à prioriser les tâches. Il est particulièrement adapté pour la gestion des équipes à distance.

Wrike : Orienté vers les grandes entreprises, Wrike offre des fonctionnalités avancées de gestion de flux de travail complexes et un accent sur la sécurité des données.

ClickUp : Se positionne comme un outil tout-en-un, centralisant la gestion des tâches, les documents et les discussions.

Outils avec IA intégrée

Outil	Fonctionnalités clés	Fonctions IA intégrées	Points forts	Cas d'usage idéal
Monday.com	Flexibilité, automatisation avancée, intégrations	Automatisation de tâches répétitives	Hautement personnalisable, interface intuitive	Projets complexes qui nécessitent flexibilité et workflows automatisés
Asana	Gestion des tâches, calendriers, tableaux Kanban	Priorisation des tâches, création et attribution automatiques, résumés de projets	Facile à utiliser pour les équipes à distance, excellent pour le suivi des tâches	Gestion de tâches et collaboration d'équipe, simple à complexe
Jira	Suivi des bugs, tableaux Scrum, feuilles de route	Rapports agiles, automatisation du processus	Spécifiquement conçu pour les développeurs, grande flexibilité de l'interface	Projets de développement logiciel et de suivi des incidents
Wrike	Flux d'informations en temps réel, diagramme de Gantt	Non mentionné dans les sources	Fonctions avancées de flux de travail et de reporting, sécurité des données	Grandes entreprises avec des processus complexes et des besoins de reporting détaillés
ClickUp	Tout-en-un (tâches, documents, discussions)	Génération de résumés, mise à jour automatique, réponses instantanées, génération de tâches	Grande personnalisation, couvre tous les besoins d'une équipe	Équipes et entreprises qui recherchent une solution tout-en-un centralisée
PSOhub AI	Suivi du temps, facturation, gestion de contrats	Suivi du temps par IA, analyse prédictive, facturation intelligente	Assistant de gestion de projet, prévisions précises	Équipes qui facturent à l'heure et qui ont besoin de prévisions de trésorerie précises