

Gouvernance IT et Méthodologies des SI

Un cours de Yann Fornier

Définitions et concepts de base

Qu'est ce que la gouvernance informatique ?

La **gouvernance informatique**, les **normes** et les **standards** forment le socle sur lequel repose la **fiabilité**, la **sécurité** et la **conformité** des systèmes informatiques modernes.



Définitions et concepts de base

Qu'est ce que la gouvernance informatique ?

La **gouvernance informatique** se réfère à l'ensemble des **règles**, des **processus** et des **pratiques** qui guident la manière dont une organisation utilise ses ressources informatiques pour atteindre ses **objectifs stratégiques**. Cela inclut la **prise de décisions**, la **gestion des risques**, la conformité aux **normes** et la **supervision** des opérations informatiques.

Nous étudierons la gouvernance dans le cours 3 "La Gouvernance Informatique"



Définitions et concepts de base

Qu'est ce qu'une norme?

Les **normes** sont des **spécifications techniques** qui définissent les exigences minimales à respecter pour garantir la **qualité**, la **compatibilité** et la **sécurité** des produits, des services ou des systèmes informatiques. Elles sont élaborées par des organismes de normalisation pour standardiser les pratiques et faciliter l'interopérabilité.





Définitions et concepts de base

Il existe 3 grands types de normes “primaires”

Produits

Production du consommateur & Interopérabilité

Services

Seuil minimum de qualité de prestation

Processus

Production & Distribution de services et produits

Il existe également d'autres normes “secondaires”

Formelles

Informelles

Propriétaires

Accessibilité

Compatibilité

Sécurité

etc...

Définitions et concepts de base

Les **standards**, souvent utilisés de manière interchangeable avec le terme "normes", désignent des **critères de référence** acceptés par l'**industrie** ou la **communauté** pour évaluer la **conformité**, la **performance** ou la **sécurité**. Les standards peuvent être internes à une organisation ou définis par des organismes externes.



Principaux organismes de Normalisation

Les organismes de normalisation jouent un rôle central dans le développement et la maintenance des normes et des standards en informatique.





L'ISO : International Organization for Standardization



ISO (Organisation internationale de normalisation) :

L'ISO est une organisation internationale qui élabore des normes mondialement reconnues dans divers domaines, y compris la sécurité de l'information (ISO 27001), la gestion de la qualité (ISO 9001) et d'autres domaines liés à l'informatique.

ISO 27001
Sécurité de l'information

ISO 9001
Gestion de la qualité

ISO 45001
SST

The NIST : National Institute of Standards and Technology

NIST (Institut national des normes et de la technologie) :

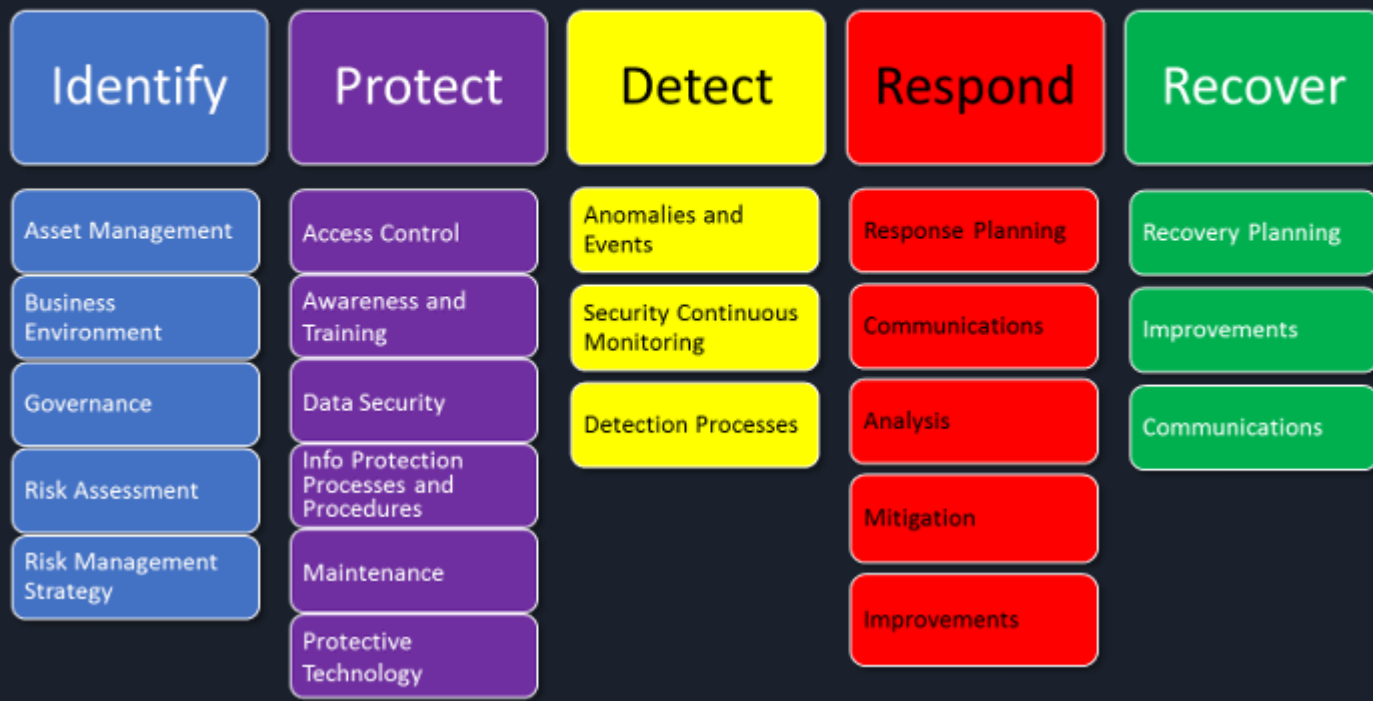
Le NIST est une agence gouvernementale des États-Unis qui développe des normes et des lignes directrices en matière de cybersécurité, de cryptographie et d'autres domaines liés à la technologie.






NIST

NIST Cyber Security Framework





L'ITU : L'International Telecommunication Union



ITU (Union internationale des télécommunications - Secteur de la normalisation des télécommunications) :

L'ITU élabore des normes dans le domaine des télécommunications, y compris les normes relatives aux réseaux de communication et à l'interopérabilité.




L'ANSSI : Agence Nationale de Sécurité des Systèmes d'Information



L'ANSSI (**Agence nationale de la sécurité des systèmes d'information**) est une agence gouvernementale française chargée de la sécurité informatique et de la protection des systèmes d'information sensibles en France.

Fondée en 2009, l'ANSSI opère sous l'autorité du Secrétaire général de la défense et de la sécurité nationale (SGDSN) et du Ministère des Armées.



L'ANSSI : Agence Nationale de Sécurité des Systèmes d'Information



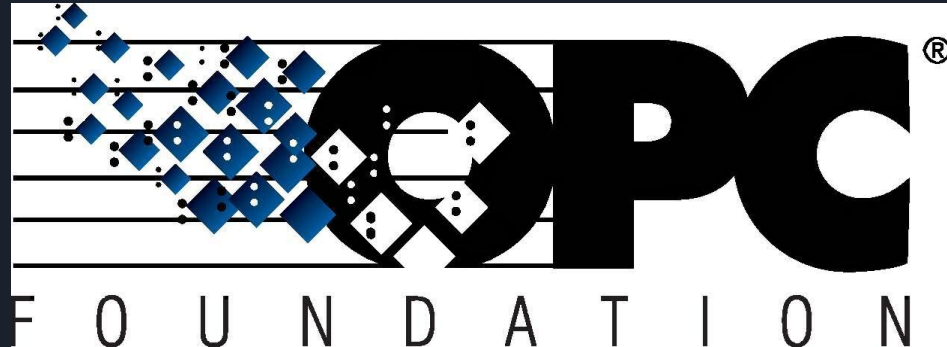
Ses principales missions comprennent la **surveillance** et la **protection des réseaux et systèmes d'information sensibles**, la **prévention des cyberattaques**, la **gestion des incidents de sécurité informatique**, et la promotion de **bonnes pratiques** en matière de **sécurité de l'information** au sein des administrations et des entreprises françaises.



Définitions et concepts de base

Qu'est ce qu'un standard?

Un **standard** est un **référentiel** publié par une **entité privée** autre qu'un organisme de normalisation national ou international ou non approuvé par un de ces organismes pour un usage national ou international. On ne parle de standard qu'à partir du moment où le référentiel a une diffusion large, on parle alors de **standard de facto** (standard de fait).



L'OPC Foundation - USA

Définitions et concepts de base

Qu'est ce qu'un standard?

Collaboration Domain Specific Information Models

The OPC Foundation closely cooperates with organizations and associations from various branches. Specific information models of other standardization organizations are mapped onto OPC UA and thus become portable.



Etude de cas

Fonctionnement d'un organisme de normalisation

Par groupes, vous allez sélectionner un organisme et produire un document explicatif de leur fonctionnement et donner votre ressenti quant au fonctionnement de ce dernier.

La longueur du document est libre.





Les normes de Sécurité de l'Information

La sécurité de l'information est une préoccupation majeure en informatique. Les normes de sécurité définissent les bonnes pratiques pour protéger les données sensibles et les systèmes contre les menaces. Cette section se penche sur quelques-unes des normes les plus importantes.

La norme ISO 27001:2022 (date la plus récente)

L'ISO 27001 est une norme internationale pour la gestion de la sécurité de l'information. Elle établit un cadre pour l'identification des risques, la mise en place de contrôles de sécurité et la gestion continue de la sécurité.



<https://www.iso.org/fr/standard/27001>



Triade CID (CIA en anglais)

Confidentialité
Confidentiality

Intégrité de l'Information
Integrity

Disponibilité des données
Availability

Confidentialité : Seules les bonnes personnes ont accès aux informations détenues par l'organisation.

Intégrité de l'Information : Les données utilisées par l'organisation dans le cadre de ses activités ou celles dont elle assure la sécurité pour d'autres sont stockées de manière fiable et ne sont ni effacées, ni endommagées.

Disponibilité des données : L'organisation et ses clients ont accès aux informations à tout moment afin de répondre aux objectifs opérationnels et aux attentes des clients.



La norme ITIL

(Information Technology Infrastructure Library)

ITIL est un ensemble de bonnes pratiques pour la gestion des services informatiques. Il propose un cadre pour la planification, la mise en œuvre et la gestion des services informatiques afin d'optimiser la valeur pour l'entreprise.



Release de l'ITIL V4 (28 février 2019)



La norme ISO 9001

L'ISO 9001 est une norme de gestion de la qualité qui peut s'appliquer aux services informatiques. Elle met l'accent sur la satisfaction du client, l'amélioration continue et la gestion efficace des processus.






La norme PCI DSS

(Payment Card Industry Data Security Standard)

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) définit les exigences de sécurité pour les organisations qui traitent des paiements par carte. Elle vise à protéger les données des titulaires de cartes de crédit.





Etude de cas

Mise en conformité

Mise en conformité ISO 27001 pour une entreprise de Services Financiers.

Une entreprise de services financiers opère dans un environnement hautement réglementé et gère des informations sensibles telles que les données personnelles des clients et les informations financières. Cette dernière souhaite renforcer sa sécurité de l'information et garantir la conformité avec la norme ISO 27001.

La suite dans le Github !

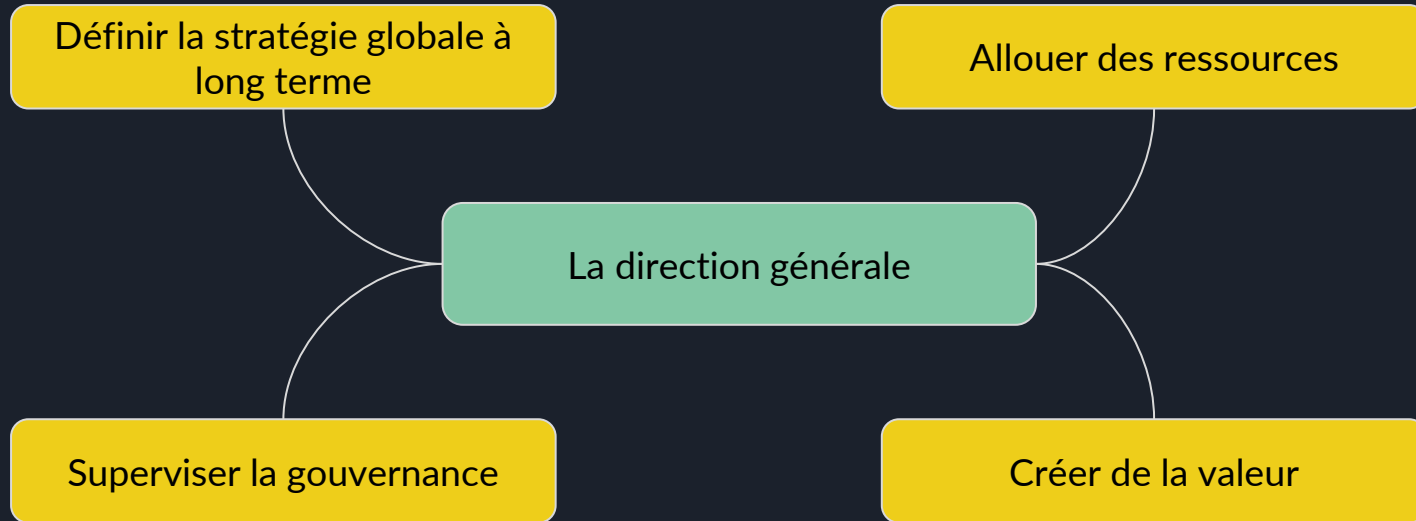


Rôles et responsabilités dans la gestion des systèmes d'informations

La gestion des systèmes d'informations implique la collaboration de différents acteurs au sein de l'organisation. Voici les principaux acteurs et leurs fonctions :

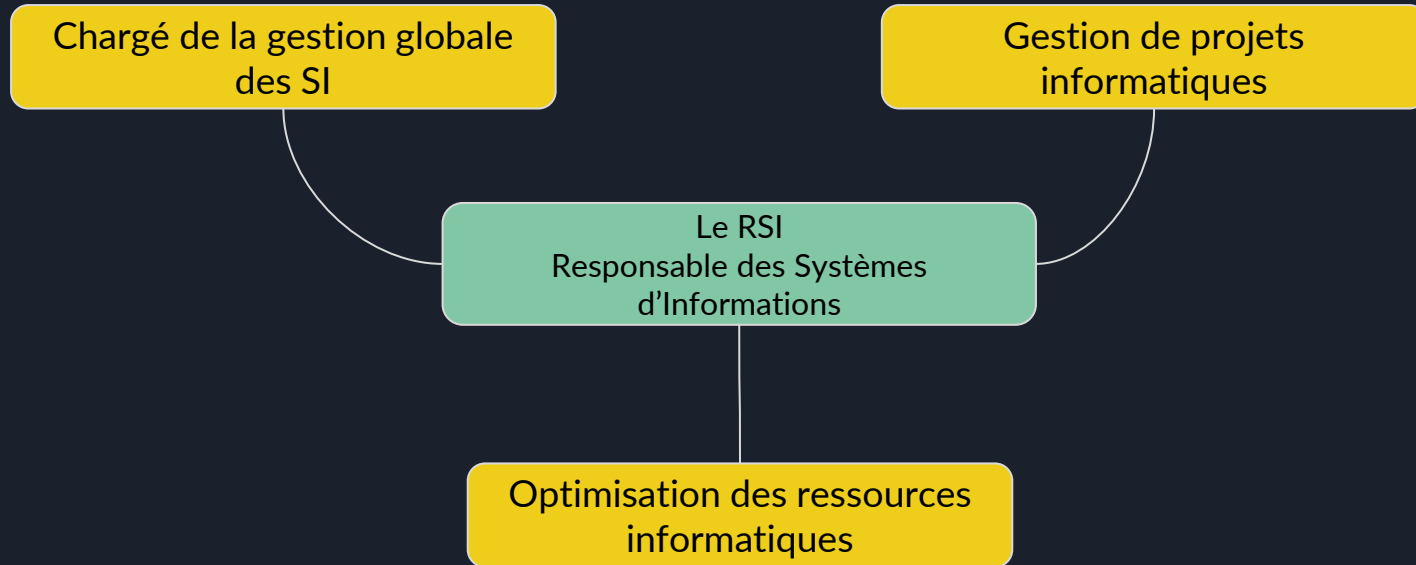


Rôles et responsabilités des SI



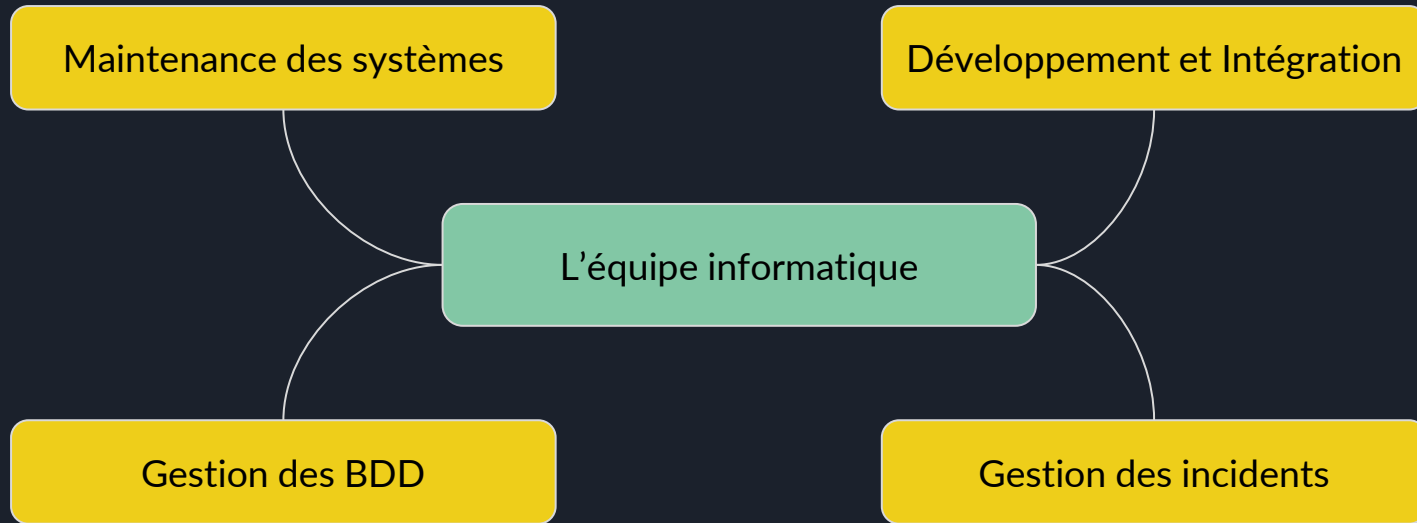


Rôles et responsabilités des SI



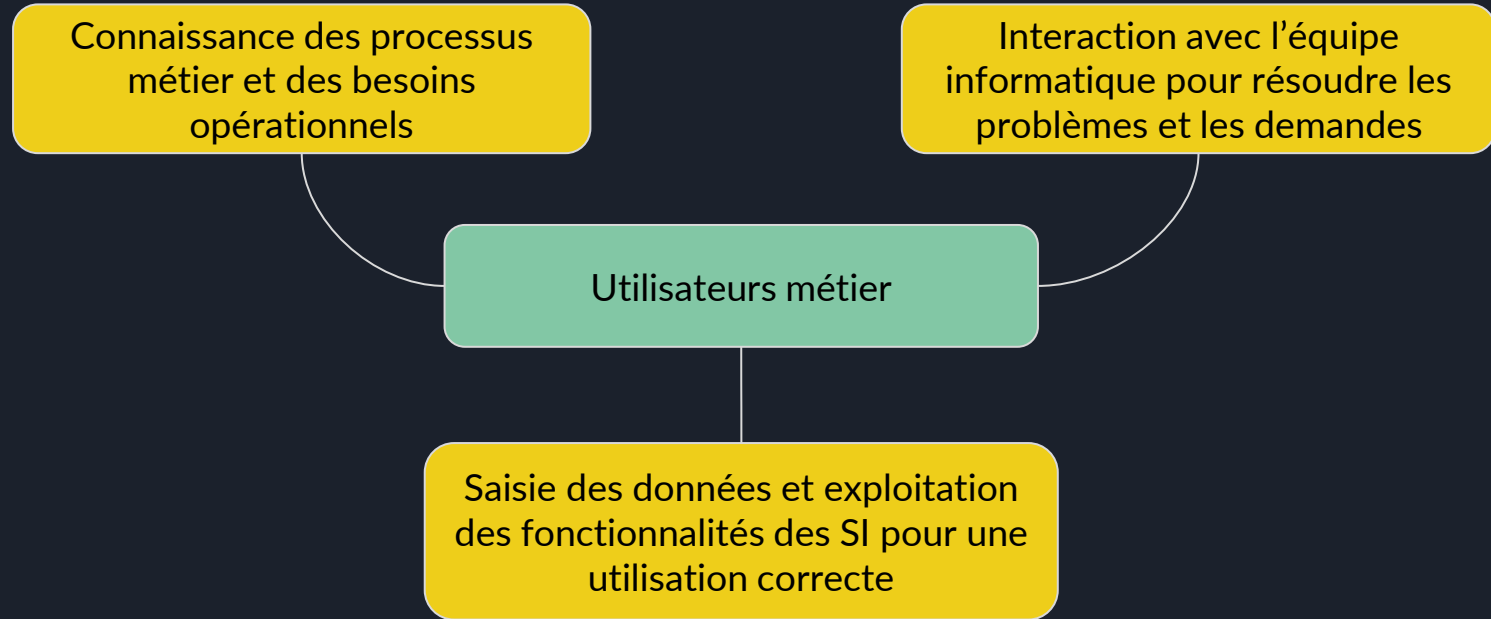


Rôles et responsabilités des SI



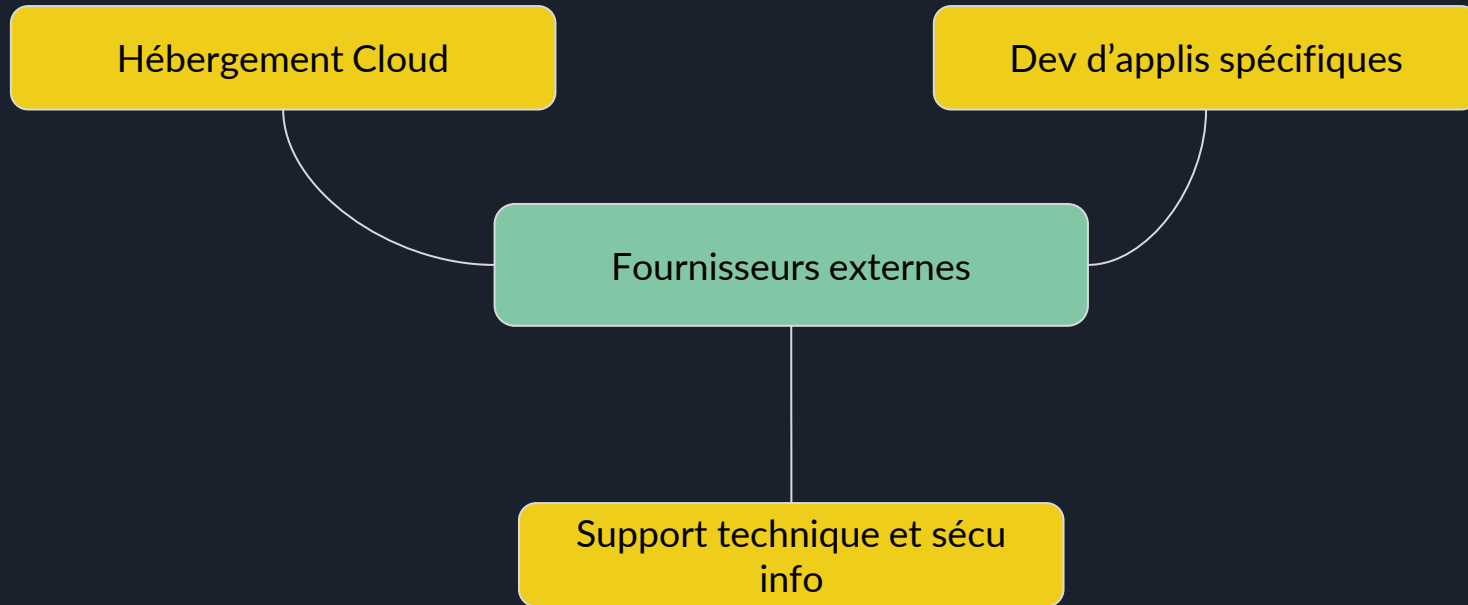


Rôles et responsabilités des SI





Rôles et responsabilités des SI






Management : Alignement sur la stratégie d'entreprise

Les systèmes d'informations doivent être alignés sur la stratégie globale de l'entreprise pour maximiser leurs valeurs.

Identification des
objectifs stratégiques
de l'entreprise

Intégration des SI dans
les processus métiers

Communication/Collab
oration avec les parties
prenantes




Management : Alignement sur la stratégie d'entreprise

Identification des objectifs stratégiques de l'entreprise

Identifier les objectifs stratégiques afin de trouver comment les systèmes d'information peuvent les soutenir (Processus, Méthodes, Outils)

Déterminer les investissements nécessaires pour tendre vers les objectifs visés.




Management : Alignement sur la stratégie d'entreprise

Intégration des SI dans les processus métiers

Intégrer les SI dans les processus métiers pour les accompagner et faciliter leur travail.

Rationaliser les processus de travail et éviter les pertes de temps et la qualité des données.



Management : Alignement sur la stratégie d'entreprise

Communication/Collaboration avec les parties prenantes

Identifier plus rapidement les exigences des SI pour le besoin opérationnel

S'assurer que les SI respectent la conformité aux normes et réglementations.



Alignement stratégique dans la gouvernance des SI

Comprendre les besoins de l'entreprise

La compréhension claire des objectifs et des besoins de l'entreprise permet de bien définir sa roadmap et sa stratégie.

Définitions des contributions

La réalisation des objectifs de l'entreprise passe par une gouvernance et des contributions clairement définies

Cohérence avec les priorités

Pour garantir l'alignement stratégique, les investissements technologiques doivent être cohérents avec les priorités de l'entreprise.



Gestion des risques des SI

Identification des
risques

L'identification des
risques liés aux SI est
le premier pas pour
une gestion efficace
des SI

Evaluation des risques

L'évaluation des
risques informatiques
permet de
déterminer leur
gravité et de
prioriser les actions
de gestion des
risques

Gestion des risques

Vise à réduire les
vulnérabilités des SI
et à garantir la
continuité des
opérations. Elle inclut
également des
mécanismes de
contrôle et de
surveillance pour
détecter et prévenir
les risques potentiels



Sécurité des systèmes d'information

Protection des données

Gestion des risques

Sécurité des réseaux

Gestion des incidents de
sécurité



L'auditeur : Audit et évaluation des systèmes d'information

Identifier les forces et les faiblesses des SI

Evaluer la performance des systèmes d'information

Vérifier la conformité

Proposer des améliorations et des solutions

DCG 8

Oona Hudin-Hengoa
Nathalie Le Gallo
Sylvie Vidalenc

Systeme d'information de gestion

2^e édition

Manuel

Savoirs et compétences

Conforme
au programme

- Cours complet
- Sujet type d'examen corrigé
- 80 exercices progressifs et 35 cas
- Méthodologie et conseils

Méthodologies de gestion des systèmes d'informations

La gestion des systèmes d'information (SI) nécessite l'utilisation de méthodologies spécifiques pour planifier, organiser, mettre en œuvre, contrôler et améliorer les activités liées aux SI. Les méthodologies de gestion des SI fournissent un cadre structuré pour assurer une gestion efficace, sécurisée et alignée sur les objectifs de l'entreprise. Voici quelques-unes des méthodologies couramment utilisées :

1. Méthodologies de gestion des systèmes d'informations

ITIL

COBIT

PMBOK

Agile Scrum

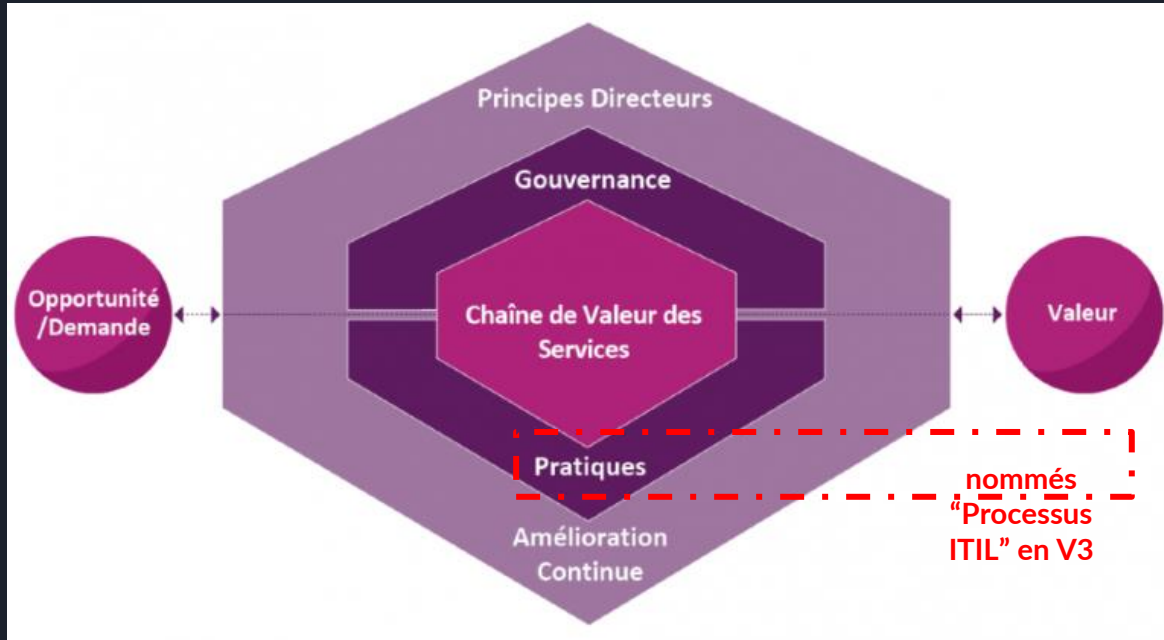
Six Sigma

Lean IT

DevOps

ITIL SVS (*Système de Valeur de Services*)

L'ITIL SVS montre comment différents composants d'une entreprise peuvent créer de la valeur à travers leurs services informatiques.





La norme COBIT

La norme COBIT (Control Objectives for Information and Related Technologies) est un cadre de gouvernance et de gestion des technologies de l'information (TI) qui fournit des directives et des meilleures pratiques pour aider les organisations à atteindre leurs objectifs stratégiques en utilisant efficacement et en toute sécurité les systèmes informatiques.





La norme COBIT

COBIT a été développé par l'ISACA (Information Systems Audit and Control Association) et est largement utilisé dans le monde entier.

Ses principaux éléments comprennent un modèle de processus, des objectifs de contrôle, des principes fondamentaux et un ensemble de bonnes pratiques pour la gouvernance des TI.

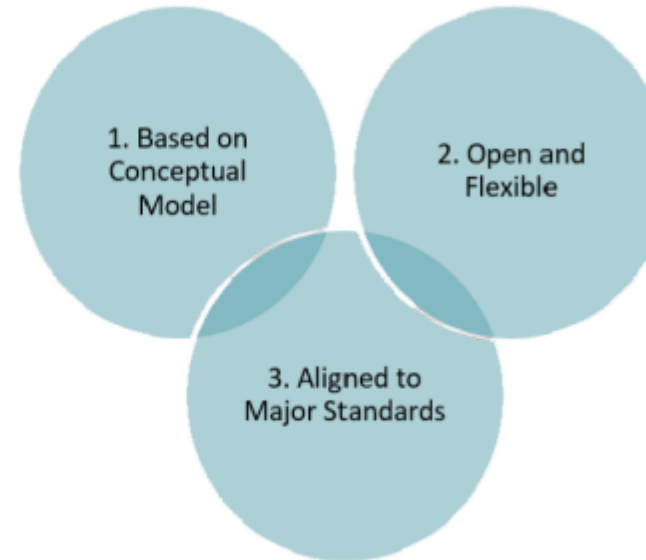


COBIT®

PRINCIPLES Governance System



PRINCIPLES Governance Framework





Objectif de la norme COBIT

COBIT vise à améliorer la gestion des TI, à assurer la conformité aux réglementations, à gérer les risques informatiques et à mesurer la performance des processus informatiques, le tout dans le but d'aligner les TI sur les objectifs métier de l'organisation.

Fondamentaux de COBIT 4.1 et COBIT 5

1.c. PMBOK (Project Management Body of Knowledge)

PMBOK est un guide de bonnes pratiques en gestion de projet développé par le Project Management Institute (PMI). Bien qu'il ne soit pas spécifique aux SI, il est souvent utilisé pour la gestion de projets informatiques.

Définition des objectifs

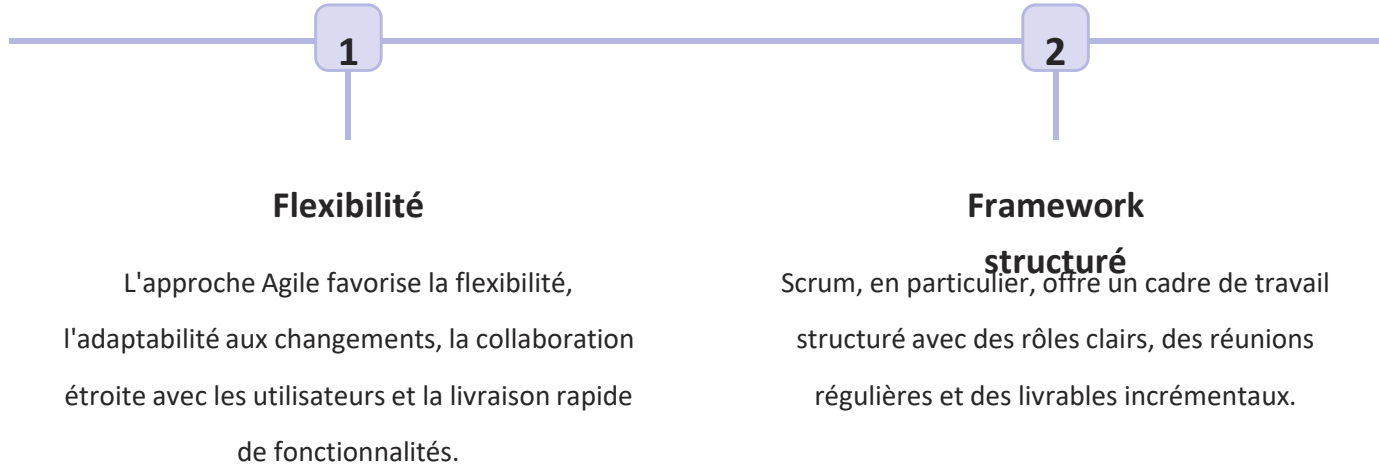
PMBOK fournit un cadre pour la gestion des projets, y compris la définition des objectifs, la planification, l'exécution, le contrôle et la clôture du projet.

Gestion des risques

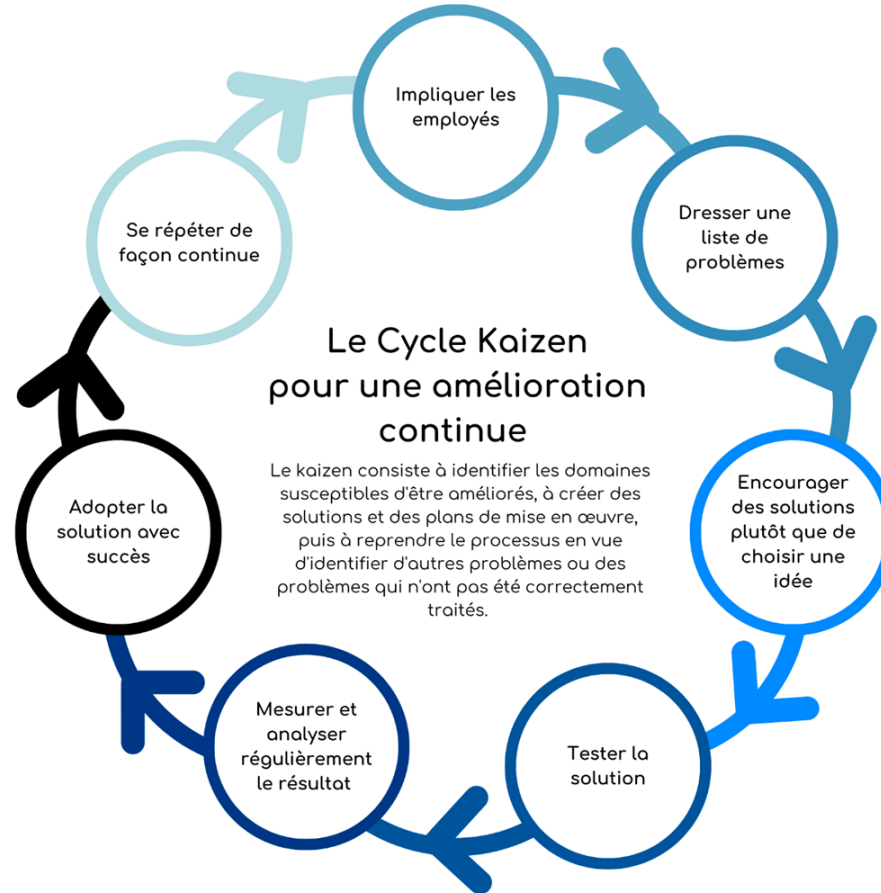
Il couvre les domaines tels que la gestion de la portée, la gestion des risques, la gestion des coûts, la gestion des délais, la gestion de la qualité, etc.

1.d. Agile et Scrum

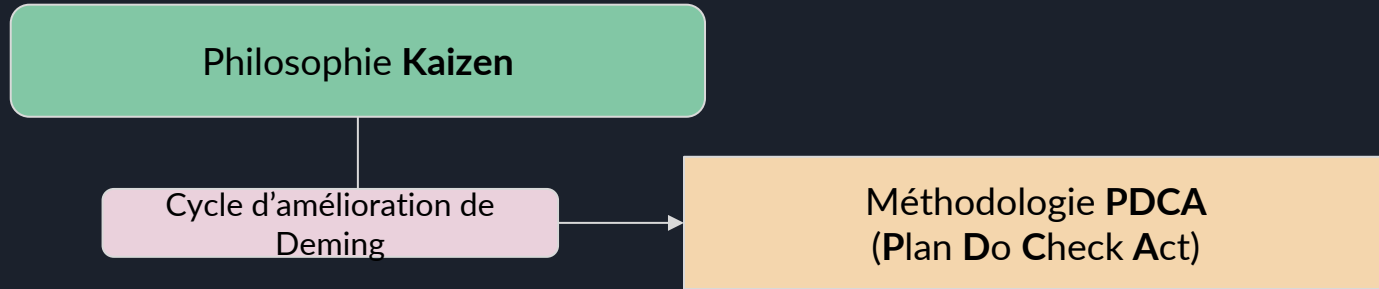
Les méthodologies agiles, notamment le framework Scrum, sont de plus en plus utilisées dans la gestion des projets SI. Elles se concentrent sur une approche itérative et collaborative, où les équipes travaillent en sprints courts pour fournir des résultats concrets de manière incrémentale.



La Philosophie Kaizen

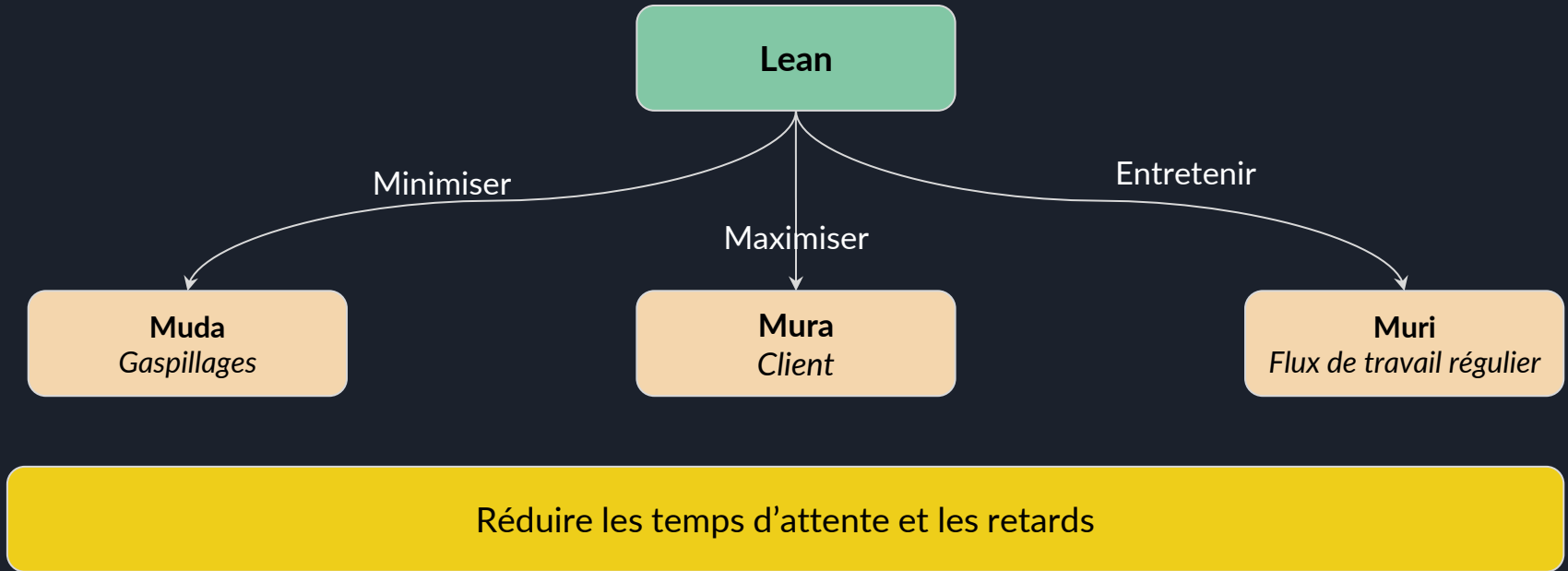


La philosophie Kaizen



P	Définir les objectifs et les processus à améliorer
D	Mettre en oeuvre les changements
C	Phase de contrôle de la réalisation des actions et des effets. Mesurer les résultats
A	Phase de mise à jour du standard si le résultat est atteint et définition des nouveaux objectifs

Le Lean Management



Six Sigma

Six Sigma

DMAIC

Définir

Mesurer

Analyser

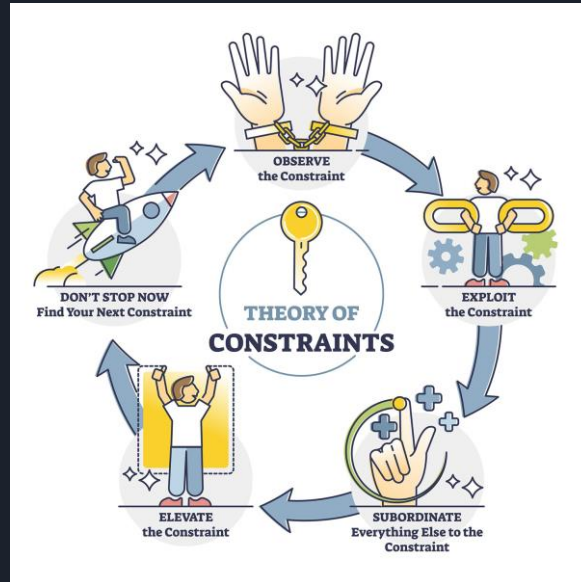
Améliorer
Improve

Contrôler



Théorie des contraintes (TOC)

Cette approche identifie les goulots d'étranglement (contraintes) dans les processus et se concentre sur leur optimisation pour améliorer les performances globales du système.

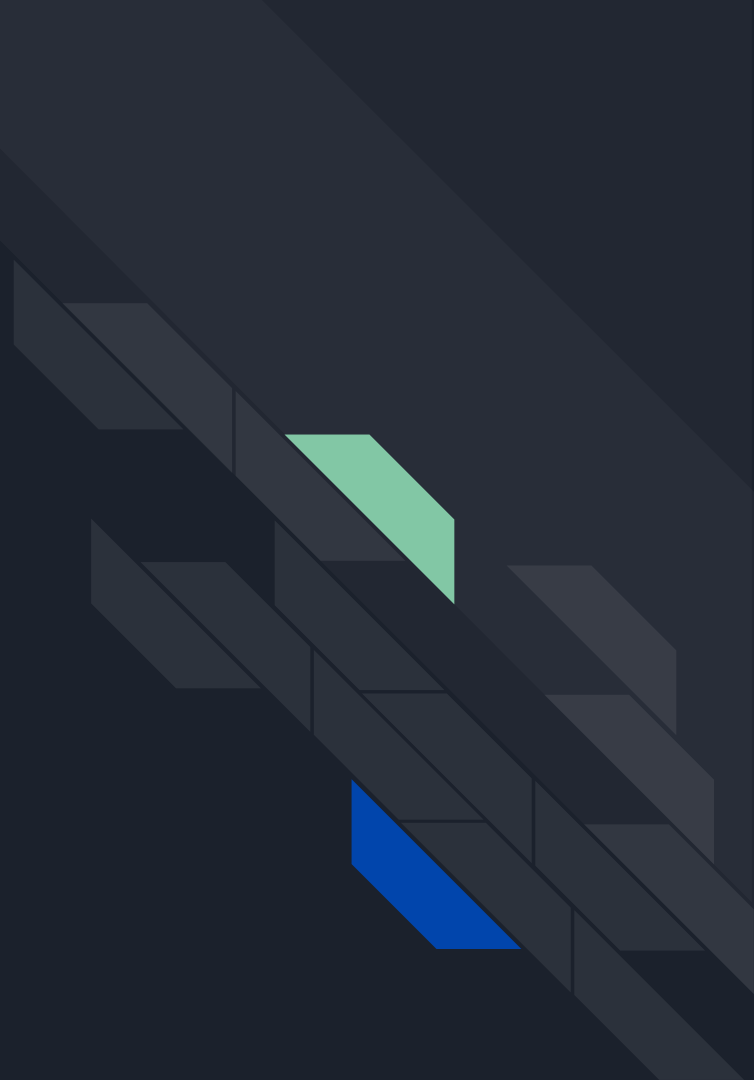


La méthode des 5S

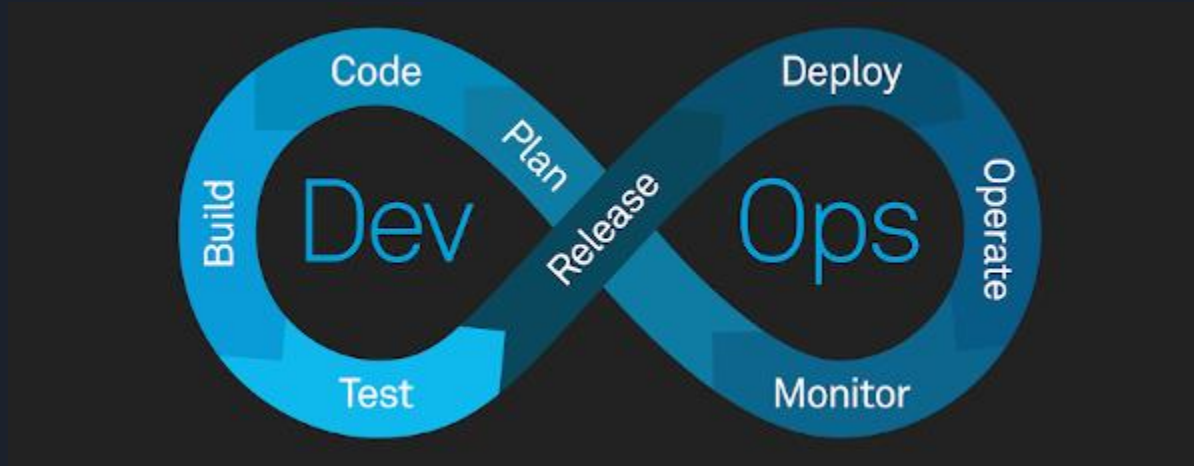
Une méthode de gestion visuelle qui vise à organiser l'espace de travail de manière efficace en se concentrant sur cinq principes : trier, ranger, nettoyer, standardiser et respecter.



Fondements du DevOps



Définition et historique du DevOps



<https://devopssec.fr/article/introduction-au-devops#begin-article-section>



Définition et historique du DevOps

Le mouvement DevOps a émergé au début des années 2000 en réponse aux défis croissants posés par le développement logiciel et les opérations informatiques isolées. Les silos organisationnels traditionnels entre les équipes de développement et d'exploitation ont souvent conduit à des retards, des erreurs et des inefficacités dans le processus de livraison logicielle.

En 2003, Google embauche Ben Treynor (aujourd'hui Vice Président Ingénierie Google) en SRE (Site Reliability Engineering). Les SRE sont les premiers praticiens du DevOps d'aujourd'hui.



Définition et historique du DevOps

Combinant développement (Dev) et opérations (Ops), DevOps est l'union des personnes, des processus et des technologies destinés à fournir continuellement de la valeur aux clients.”

Microsoft

DevOps n'est ni un outil ni une technologie. Il s'agit plutôt d'une idéologie dans laquelle deux parties essentielles d'une entreprise : l'équipe de développement logiciel et l'équipe des opérations informatiques travaillent en étroite collaboration et partagent les progrès. DevOps garantit une bonne communication entre ces équipes, ce qui permet en outre à l'organisation de livrer le produit final en un minimum de temps et avec un minimum de problèmes.

Définition et historique du DevOps

L'idée de fusionner les aspects du développement et des opérations pour favoriser une approche plus collaborative a gagné en popularité grâce à des praticiens et des leaders de l'industrie. En 2009, Patrick Debois et Andrew Clay Shafer ont organisé la première conférence "DevOpsDays" à Ghent, en Belgique, marquant ainsi un jalon important dans la formalisation du mouvement DevOps.



Patrick Debois



Andrew Clay Shafer

Un schéma classique en entreprise



Applicative

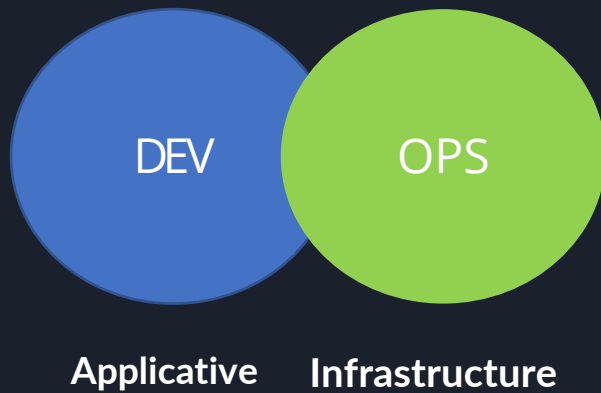


Infrastructure

Mur de la confusion



Le DevOps





Comment le DevOps aide les organisations ?

Le DevOps offre plusieurs avantages aux organisations en favorisant une approche collaborative entre les équipes de développement et d'exploitation, ainsi qu'en intégrant des pratiques et des outils visant à automatiser et optimiser le cycle de vie du développement logiciel.



Présentation des principaux concepts : collaboration, automatisation, intégration continue..

Livraison rapide et continue

Amélioration de la qualité

Collaboration renforcée

Automatisation des
processus

Réduction des coûts

Agilité et adaptabilité

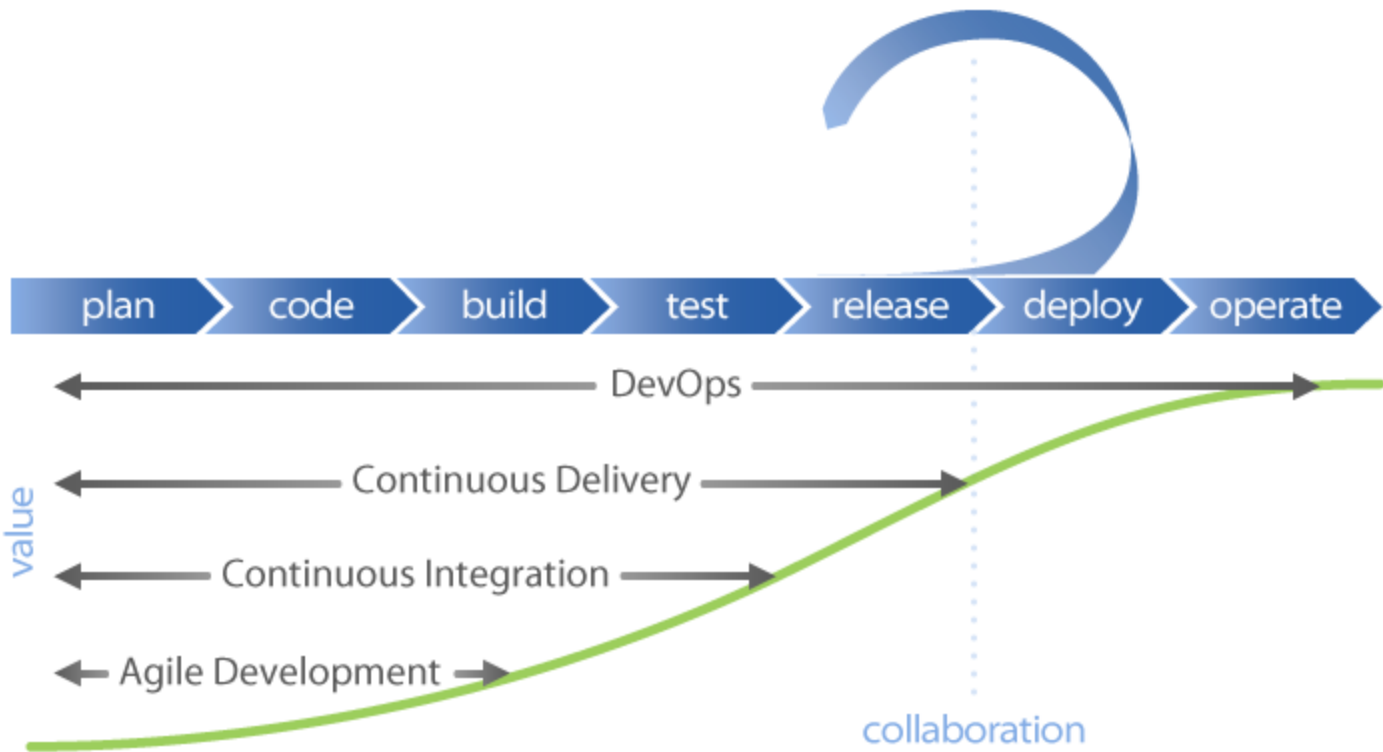
Surveillance et rétroaction
continues



Présentation des principaux concepts :

Livraison rapide et continue

Le DevOps vise à accélérer le processus de livraison logicielle en automatisant les tâches répétitives, en optimisant les workflows, et en intégrant des pratiques de déploiement continu. Cela permet aux organisations de fournir des fonctionnalités plus rapidement et de manière plus régulière.





Présentation des principaux concepts :

L'amélioration de la qualité

L'intégration continue, les tests automatisés et la surveillance constante contribuent à une meilleure qualité du code et à la détection précoce des erreurs. Cela réduit les risques d'incidents en production et améliore la stabilité des applications.



Présentation des principaux concepts :

La collaboration renforcée

Le DevOps encourage la collaboration étroite entre les équipes de développement, d'exploitation et d'autres parties prenantes. En favorisant la communication et le partage des responsabilités, le DevOps brise les silos organisationnels et contribue à une culture de travail plus collaborative.



Présentation des principaux concepts :

L'automatisation des
processus

L'automatisation des tâches manuelles, telles que le déploiement, les tests, et la gestion de l'infrastructure, permet de gagner du temps et de réduire les erreurs humaines. L'automatisation est au cœur du DevOps pour assurer une efficacité opérationnelle accrue.



Présentation des principaux concepts :

La réduction des coûts

En accélérant le cycle de vie du développement logiciel et en automatisant les processus, le DevOps contribue à une utilisation plus efficiente des ressources, ce qui peut se traduire par une réduction des coûts opérationnels.



Présentation des principaux concepts :

L'agilité et l'adaptabilité

Le DevOps permet aux organisations de s'adapter plus rapidement aux changements du marché et aux exigences des clients. La flexibilité accrue dans le développement et le déploiement facilite l'ajustement rapide des fonctionnalités en réponse aux besoins évolutifs.

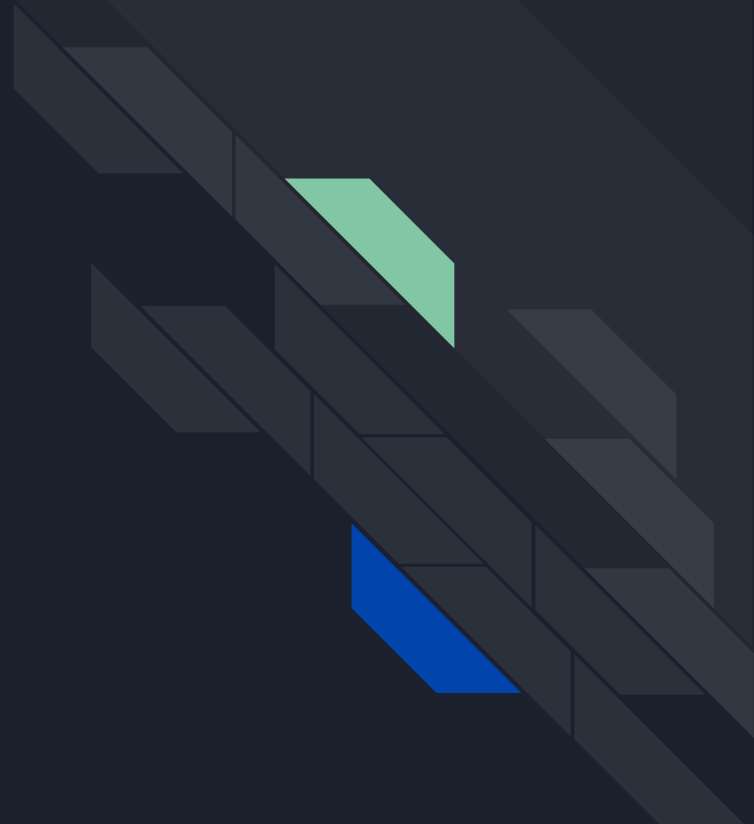


Présentation des principaux concepts :

La Surveillance et la
rétroaction continue

Les pratiques DevOps incluent la surveillance constante des performances et des opérations en production, ainsi que la collecte continue de données et de retours d'expérience. Cela permet aux équipes d'identifier rapidement les problèmes, de les résoudre et de faire de l'itération en continu pour améliorer la performance et la satisfaction client.

Les avantages du DevOps





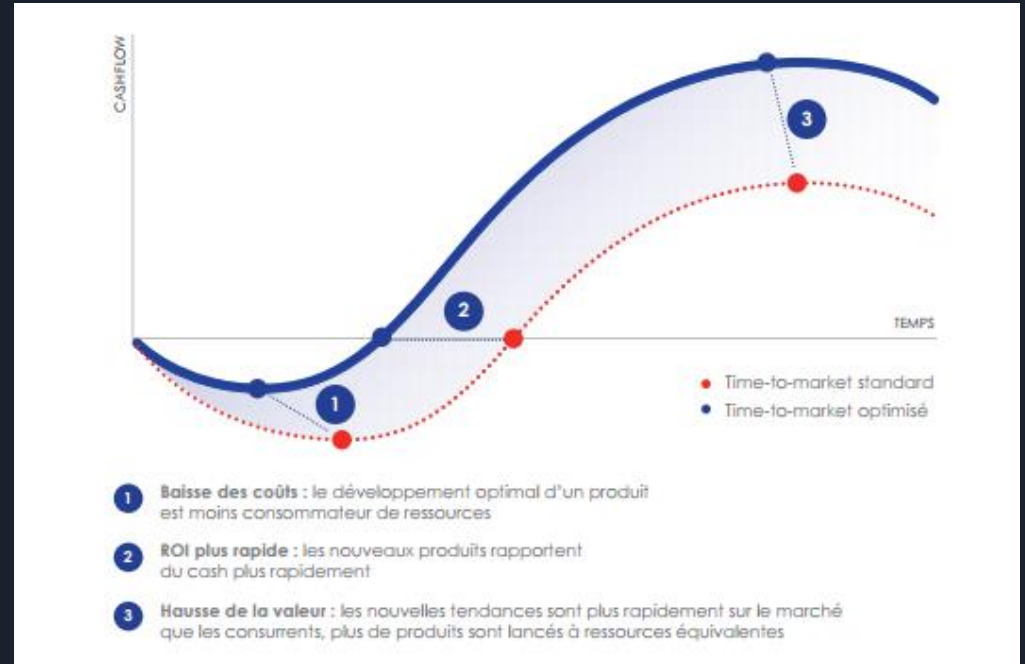
La collaboration

Les principales problématiques des entreprises étaient sur le manque de collaboration entre les équipes de Dev et les équipes Opérationnelles (Ops). L'avantage du DevOps réside dans la collaboration entre ces deux équipes en repensant intégralement l'environnement où ces différentes équipes travaillent afin de créer davantage de valeur pour l'entreprise.

La vitesse

Le DevOps d'aujourd'hui permet d'accélérer la fréquence et la vitesse à laquelle les entreprises peuvent introduire de nouveaux produits afin d'obtenir un avantage concurrentiel.

Cette réduction de temps est liée à ce que l'on appelle le TTM (Time-To-Market)





L'Agilité pour la satisfaction client

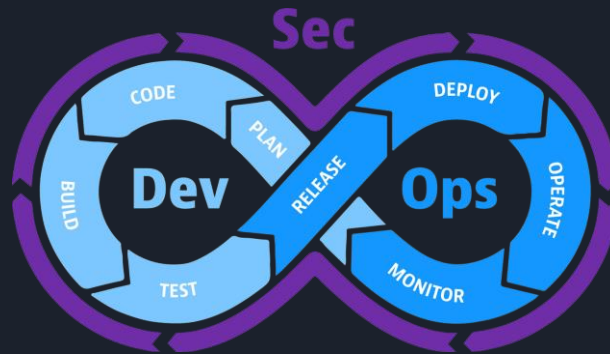
Les exigences des clients modernes sont intenses et demandent une très forte réactivité quant au développement de nouvelles fonctionnalités. Les pratiques DevOps permettent une meilleure flexibilité et aide également les équipes à comprendre comment les clients se servent de leurs produits.

En général les clients détestent attendre les produits d'une entreprise. Plus il y a d'attente plus les effets néfastes s'intensifient. Avec un rythme de livraison plus rapide, la satisfaction client augmente plus rapidement.

La sécurité

Le DevOps permet dans sa version optimisée d'intégrer la sécurité des produits livrés. On parle alors de DevSecOps.

Le DevSecOps étend les principaux composants de développement et d'exploitation du DevOps et y introduit une couche de sécurité en tant que composant distinct dans le pipeline CI/CD. l'essence du DevSecOps est que la majorité des équipes (pas seulement les équipes de sécurité) sont responsables de la sécurité de l'application. Il aide à réduire les coûts et avec lui les équipes sont en mesure de suivre et de détecter les problèmes de sécurité dans les premiers stades de développement.





Ce que n'est pas le DevOps

Une équipe distincte

Un Outil

Une simple combinaison
d'équipes Dev et Ops

Une stratégie universelle

Uniquement
l'automatisation



Conclusion

Le DevOps permet d'améliorer la collaboration entre toutes les parties prenantes de la planification à la livraison et l'automatisation du processus de livraison afin de :

- Améliorer la fréquence de déploiement
- Accélérer la mise sur le marché
- Réduire le taux d'échec des nouvelles livraisons
- Raccourcir le délai entre les correctifs
- Améliorer le temps moyen de récupération
- S'adapter aux changements des besoins client avec l'agilité
- Posséder un avantage concurrentiel
- Satisfaire les clients
- Accroître l'innovation
- Améliorer la sécurité

2. Méthodologies Combinées

Il est également possible d'adapter et de combiner différentes méthodologies en fonction des exigences spécifiques de l'organisation.



Adaptabilité

Adaptez votre méthode aux besoins de votre organisation.



Gestion des Risques

Pensez à la sécurité de votre organisation



Objectif Performances

Améliorez les performances de votre organisation pour atteindre vos objectifs.

Exemple : Gestion des Services Informatiques

Les méthodologies de gestion des SI fournissent un cadre structuré pour assurer une gestion efficace, sécurisée et alignée sur les objectifs de l'entreprise.

Qualité de service

ITIL et COBIT se concentrent sur la qualité de services informatiques.

Gouvernance

COBIT fournit des lignes directrices pour le contrôle et la gouvernance des SI.

Gestion de projet informatique

PMBOK établit les processus pour la gestion des projets informatiques.

Flexibilité et Adaptabilité

Agile et Scrum offrent des approches flexibles et adaptatives pour la gestion des projets SI.

Amélioration des performances

Six Sigma vise à réduire la variation et les défauts pour améliorer les performances et atteindre des niveaux de qualité élevés.





4. Adaptation de la Méthodologie

Il est possible de combiner ou d'adapter les méthodologies de gestion de SI selon les besoins de l'organisation.

Combinaison de Méthodologies

- ITIL et COBIT pour la gestion de la qualité et la gouvernance des SI.
- Agile et Scrum pour la flexibilité et l'adaptabilité.
- Six Sigma pour l'amélioration des performances.

Adaptation des Méthodologies

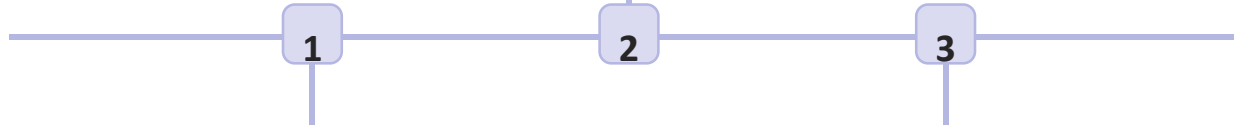
- Choisir les processus les plus pertinents pour l'organisation.
- Personnaliser les rôles, les tâches et les responsabilités.
- Adapter les modèles et les outils utilisés.

5. Conclusion

Les méthodologies de gestion des SI offrent des approches structurées pour la gestion des projets, des processus et des services informatiques. Elles aident les organisations à atteindre leurs objectifs stratégiques, à assurer une qualité de services et à améliorer leur efficacité et leur performance.

Adapter la Méthodologie

Il est possible de combiner ou d'adapter les méthodologies de gestion des SI selon les besoins de l'organisation.



Choisir la Méthodologie Adéquate

Le choix de la méthodologie dépend des besoins spécifiques de l'organisation, de la nature des projets SI, de la culture de l'entreprise et des objectifs stratégiques.

S'améliorer Continuellement

Il est important de mesurer et d'améliorer en continu la performance des SI.

6. Étude de cas : La Gestion des Services Informatiques chez Acciona

L'entreprise Acciona cherche à mettre en place une méthodologie pour améliorer la qualité de ses services informatiques et réduire les coûts. En utilisant cette méthodologie, Acciona a pu identifier les processus critiques, améliorer la gestion des incidents et des problèmes, et améliorer la satisfaction des clients.

1 Objectifs

Avec pour objectif l'amélioration de la qualité des services informatiques, la réduction des coûts et l'amélioration de la satisfaction des clients. Choisissez une méthodologie citée précédemment et faites-en la présentation face au comité de gouvernance des SI.

2 Approche

Implémenter la méthodologie choisie, identifier les processus critiques, améliorer la gestion des incidents et des problèmes.

3 Résultats

Donnez les résultats attendus avec l'application de votre méthodologie.

