Module Qualité pour 3AE

Membres du groupe:

- Charles-Albert Kotto
- Ehian Christian
- François Collu
- Abdelmoutakabir Oumaima
- Franck Mevengue
- Job-Daryl Massande

Sous la supervision de
M. Xavier Van Lindt

ECAM EPMI
GRADUATE SCHOOL OF ENGINEERING

Livrables du TP 1/4

- **Lean :**
  - Muri, Mura, Muda : donner un exemple IT ou Sécurité :
- ***Muri (excès)* :** l'exemple d'une entreprise qui maintient un centre de données surdimensionné par rapport à ses besoins réels en termes de capacité de stockage. Cela peut entraîner une surconsommation d'énergie, des coûts élevés de refroidissement et d'électricité, ainsi que la gestion de ressources inutilisées entraînant des dépenses excessives et une inefficacité opérationnelle. (exemple IT)
- ***Mura (irrégularité)* :** l'approvisionnement en matériel informatique essentiel, comme des disques durs ou des composants de serveur, est soumis à des ruptures fréquentes, cela crée des irrégularités dans la disponibilité des ressources. Les délais de livraison imprévisibles et les ruptures d'approvisionnement peuvent entraîner des retards dans les projets et augmenter les coûts. (exemple IT)
- ***Muda (gaspillage)* :** l'installation manuelle de mises à jour de logiciels sur chaque poste de travail d'une entreprise. Cela représente une activité répétitive qui n'ajoute aucune valeur significative, et qui pourrait être automatisée à l'aide de solutions de gestion de mises à jour pour économiser du temps et des ressources. (exemple IT)

Livrables du TP 1/4

- **Lean :**
  - **DOWNTIME :** donner un exemple IT ou Sécurité de chaque lettre

- ***(D) Default - Défaut (IT) :*** les erreurs de codage.
- ***(O) Overproduction - Surproduction (IT) :*** La création excessive de rapports ou de documents.
- ***(W) Wait - Attente (IT) :*** L'attente de l'approbation pour un changement de configuration.
- ***(N) Not used - Non utilisé (IT) :*** Les ressources informatiques non utilisées, comme les serveurs inactifs.
- ***(T) Transport - Transport (IT)* :** Le déplacement physique de matériel informatique entre les sites.
- ***(I) Inventory - Stock (IT) :*** La surprovision de matériel ou de licences logicielles.
- **(M) Motion - Mouvement (IT) :** Les mouvements inutiles effectués par les employés lors de la réalisation de tâches informatiques.
- ***(E) Extra processing - Processus (Sécurité) :*** La mise en place de processus de sécurité excessifs.

Livrables du TP 1/4

- **Gestion des Services IT (ITSM) :**
  - les 8 Points de JP Kotter :
    - Description et exemple IT ou Sécurité (fil directeur) en décrivant chaque point

- ***1. Créer un sentiment d'urgence* :** Il s'agit de sensibiliser les acteurs à l'importance de la sécurité informatique ou du changement à mettre en place. Créez un sentiment d'urgence en montrant les risques et les conséquences d'une inaction. **Exemple Sécurité :** Mettre en évidence les résultats d'une évaluation de la cybersécurité montrant des vulnérabilités majeures, ou les impacts potentiels d'une violation de données sur la réputation de l'entreprise.
- **2. Former une 'Coalition' Puissante :** Constituez une équipe de leadership influente pour piloter la transformation. Cette équipe ne se limite pas aux personnes ayant des postes hiérarchiques élevés, mais inclut celles ayant une légitimité pour le changement. **Exemple Sécurité :** Impliquez des experts en cybersécurité, des responsables de la conformité et des cadres supérieurs dans une équipe de sécurité pour diriger les initiatives de sécurité.
- **3. Créer une Vision de l'État Futur :** Définissez clairement la vision de la sécurité informatique ou de la transformation. Basez-vous sur des valeurs pour donner un sens à la démarche et utilisez des outils pour décrire la transition d'un état à un autre. **Exemple Sécurité :** Décrivez la vision d'un environnement informatique hautement sécurisé où les données sont protégées, les menaces sont anticipées, et la conformité est maintenue.

Livrables du TP 1/4

- **Gestion des Services IT (ITSM) :**
  - les 8 Points de JP Kotter :
    - Description et exemple IT ou Sécurité (fil directeur) en décrivant chaque point

- **4. Communiquer la Vision :** Communiquez la vision de la sécurité ou du changement de manière dynamique et constante. Insistez sur l'urgence du changement à chaque occasion. **Exemple Sécurité :** Communiquez régulièrement sur les objectifs de sécurité, les mises à jour de politique et les incidents de sécurité afin de maintenir la sensibilisation.
- **5. Inciter à l'Action et Abaisser les Obstacles :** Impliquez les collaborateurs dans la sécurité informatique ou le changement. Aidez-les à surmonter les obstacles qui pourraient entraver leur participation.**Exemple Sécurité :** Encouragez les employés à signaler les problèmes de sécurité, à suivre les procédures de sécurité et à participer à des programmes de sensibilisation.
- **6. Générer des Victoires à Court Terme :** Établissez des jalons intermédiaires pour maintenir l'engagement et la motivation de l'équipe. Célébrez les petites victoires en cours de route. **Exemple Sécurité :** Définissez des objectifs de sécurité à court terme, tels que l'amélioration des scores de conformité ou la réduction des incidents de sécurité, et célébrez les réalisations.

Livrables du TP 1/4

- **Gestion des Services IT (ITSM) :**
  - les 8 Points de JP Kotter :
    - Description et exemple IT ou Sécurité (fil directeur) en décrivant chaque point

- **7. Consolider les Succès pour Plus de Changement :** Un succès initial ne suffit pas. Assurez-vous de généraliser les pratiques de sécurité ou de changement à l'ensemble de l'organisation. Identifiez et surmontez les obstacles persistants.**Exemple Sécurité :** Étendez les meilleures pratiques de sécurité à l'ensemble de l'entreprise, en mettant en œuvre des politiques et des procédures de sécurité cohérentes dans tous les services.
- **8. Ancrer les Nouvelles Approches dans la Culture d'Entreprise** : Intégrez les nouvelles pratiques de sécurité ou de changement dans la culture organisationnelle. Mettez à jour les documents opérationnels pour refléter les nouvelles normes.**Exemple Sécurité :** Intégrez les protocoles de sécurité dans les processus opérationnels, mettez à jour les politiques de sécurité et assurez-vous que la sécurité est une composante clé de la culture d'entreprise.

Livrables du TP 1/4

- La roue de Deming : PDCA
  - Description et exemple IT ou Sécurité (fil directeur) en décrivant chaque point

- **1. Plan (Préparation et Planification) :** Dans cette étape, l'organisation identifie les objectifs de qualité, définit les processus nécessaires pour les atteindre, et planifie les ressources nécessaires. C'est le stade de la préparation. **Exemple IT :** Une entreprise de développement logiciel décide de mettre en place une nouvelle politique de gestion des incidents pour améliorer la réactivité face aux problèmes. Dans la phase "Plan", elle identifie les objectifs de réduction des temps de résolution, définit les procédures pour signaler et suivre les incidents, et planifie la formation du personnel sur ces nouvelles procédures.

- 2. **Do (Développement, Réalisation et Mise en Œuvre) :** Dans cette étape, les plans élaborés précédemment sont mis en œuvre. Les processus sont exécutés conformément à la planification. C'est le stade de la réalisation. **Exemple Sécurité** : Une entreprise de sécurité informatique décide de déployer une nouvelle technologie de détection d'intrusion sur son réseau. Dans la phase "Do", elle installe la nouvelle technologie sur l'ensemble du réseau, configure les alertes, et met en place des procédures de gestion des alertes en cas de détection d'activité suspecte.

Livrables du TP 1/4

- La roue de Deming : PDCA
  - Description et exemple IT ou Sécurité (fil directeur) en décrivant chaque point

- **3. Check (Contrôle et Vérification) :** Dans cette étape, les résultats et les performances sont surveillés pour s'assurer qu'ils correspondent aux objectifs définis dans la phase "Plan". Les données sont collectées, analysées, et comparées aux normes de qualité. C'est le stade du contrôle.
  Exemple IT : Dans le cadre de la gestion des incidents, l'entreprise vérifie régulièrement les métriques liées au temps de résolution, au taux de réouverture d'incidents, et à la satisfaction des utilisateurs par rapport au nouveau processus. Les données sont collectées et analysées pour évaluer la performance.

- **4. Act (Action, Ajustement et Réaction) :** Sur la base des résultats de la phase "Check", des mesures correctives sont prises pour améliorer la qualité et l'efficacité des processus. C'est le stade de l'action et de l'amélioration.
  Exemple Sécurité : Si les analyses révèlent que la nouvelle technologie de détection d'intrusion n'a pas atteint les objectifs de détection souhaités, l'entreprise prend des mesures correctives, telles que la révision de la configuration, la mise à jour de la technologie, ou la formation supplémentaire du personnel.

Livrables du TP 1/4

- La cascade : Vision -> Objectifs -> KPI -> Métriques -> Mesures

1. **Vision :** La vision représente une image globale des aspirations et des objectifs à long terme de l'entreprise en matière de technologie ou de sécurité. Exemple IT : La vision pourrait être de devenir un leader en matière de solutions cloud sécurisées pour les clients.

2. **Mission :** La mission précise la raison d'être de l'organisation, décrivant son rôle et son engagement envers ses clients ou la sécurité de l'entreprise. Exemple Sécurité* : La mission pourrait être de protéger les actifs numériques de l'entreprise et de garantir la confidentialité des données sensibles.

3. **Buts :** Les buts définissent les objectifs généraux à atteindre pour soutenir la vision et la mission. Exemple IT : Un but pourrait être d'optimiser les coûts informatiques tout en améliorant la qualité des services.

4. **Objectifs :** Les objectifs spécifient les résultats mesurables à court terme qui contribueront à atteindre les buts. Exemple Sécurité : Un objectif pourrait être de réduire de 20% le nombre d'incidents de sécurité liés aux logiciels malveillants au cours de l'année.

Livrables du TP 1/4

- La cascade : Vision -> Objectifs -> KPI -> Métriques -> Mesures

5. **CSF (Critical Success Factors)** : Les facteurs de succès critiques identifient les éléments clés qui doivent être en place pour atteindre les objectifs. Exemple IT : L'adoption réussie d'une nouvelle technologie cloud est un CSF pour réaliser des économies de coûts.

6. **KPI (Key Performance Indicators) :** Les indicateurs clés de performance mesurent la réussite par rapport aux objectifs. Exemple Sécurité : Un KPI pourrait être le taux de détection des incidents de sécurité, mesuré mensuellement.

7. **Métriques** : Les métriques détaillent la façon dont les KPI sont mesurés, y compris les méthodes de collecte de données. Exemple IT : La métrique peut préciser que le taux d'adoption d'une nouvelle technologie est mesuré par le nombre d'utilisateurs actifs.

8. **Mesures** : Les mesures sont les données réelles recueillies pour évaluer les performances par rapport aux métriques. Exemple Sécurité : Les mesures peuvent inclure le nombre total d'incidents de sécurité détectés et le temps moyen de réponse pour y faire face.

Livrables du TP 1/4

- Fournir 10 KPI’s classiques d’un SLA pour Gestion des Incidents, Changements, Demandes :

- 1. **Temps de résolution des incidents (Incident Resolution Time):** Mesure le temps nécessaire pour résoudre un incident depuis son signalement jusqu'à la résolution complète.

Formule : Temps de résolution = Date de clôture de l'incident - Date de création de l'incident.

- **2. Taux de résolution au premier contact (First Contact Resolution Rate) :** Indique la proportion d'incidents résolus lors du premier contact avec le support.

Formule : Nombre d'incidents résolus lors du premier contact / Nombre total d'incidents.

- **3. Respect des délais des changements (Change Timeliness):** Mesure si les changements sont réalisés dans les délais prévus.

Formule : Nombre de changements réalisés dans les délais / Nombre total de changements.

- **4. Taux de rejets de changements (Change Rejection Rate):** Évalue le pourcentage de changements rejetés lors de l'examen.

Formule : Nombre de changements rejetés / Nombre total de changements soumis.

- **5. Temps de traitement des demandes (Request Processing Time) :** Mesure le temps nécessaire pour traiter une demande depuis sa réception jusqu'à sa réalisation.

Formule : Temps de traitement = Date de réalisation de la demande - Date de réception de la demande.

Livrables du TP 1/4

- Fournir 10 KPI’s classiques d’un SLA pour Gestion des Incidents, Changements, Demandes :

- **6. Taux de satisfaction des demandeurs (Requester Satisfaction Rate) :** Évalue la satisfaction des demandeurs par rapport aux services rendus.

Formule : Nombre de demandeurs satisfaits / Nombre total de demandeurs.

- **7. Taux d'incidents récurrents (Recurrent Incident Rate) :** Mesure la fréquence à laquelle un même incident se reproduit.

Formule : Nombre d'incidents récurrents / Nombre total d'incidents.

- **8. Taux de réussite des changements (Change Success Rate) :** Indique la proportion de changements réussis par rapport au nombre total de changements.

Formule : Nombre de changements réussis / Nombre total de changements.

- **9. Temps moyen de résolution des demandes (Average Request Resolution Time) :** Calcule le temps moyen nécessaire pour résoudre toutes les demandes.

Formule : Somme des temps de résolution de toutes les demandes / Nombre total de demandes.

- **10. Taux de conformité aux SLA (SLA Compliance Rate)** : Mesure le pourcentage d'incidents, de changements et de demandes qui respectent les SLA définis.

Formule : Nombre de cas conformes aux SLA / Nombre total de cas gérés.

Livrables du TP 2/4

- **La dette technique :**
  - 5 exemples et leur explication (Pourquoi) en IT ou Sécurité

- **1. Utilisation d'actifs obsolètes (HW, SW, OS) :** L'utilisation continue d'actifs matériels ou logiciels obsolètes peut entraîner des vulnérabilités de sécurité et une inefficacité opérationnelle.

- Pourquoi : Les mises à jour et les remplacements nécessaires peuvent être coûteux et perturber les opérations, incitant les organisations à retarder la mise à niveau.

- **2. Absence de contrats de maintenance :** Les actifs informatiques sans contrats de maintenance risquent de ne pas être pris en charge en cas de problème, ce qui peut entraîner des temps d'arrêt prolongés.

- Pourquoi : Éviter les coûts des contrats de maintenance peut sembler rentable à court terme, mais expose l'organisation à des risques importants.

Livrables du TP 2/4

- **La dette technique :**
  - 5 exemples et leur explication (Pourquoi) en IT ou Sécurité

- **3. Actifs non patchés ou mis à jour :** L'omission des mises à jour de sécurité expose les systèmes à des failles de sécurité connues.

- Pourquoi : Les mises à jour peuvent nécessiter du temps et des tests, ce qui entraîne parfois des retards.

- **4. Solutions de contournements/patches sans solution définitive :** L'utilisation de correctifs temporaires (patches) sans résoudre les problèmes sous-jacents peut entraîner une accumulation de dette technique.

- Pourquoi : Les correctifs temporaires sont parfois utilisés pour gagner du temps, mais sans résoudre le problème fondamental, ce qui aggrave la dette.

- **5. Non-conformité aux meilleures pratiques de sécurité :** L'ignorance des meilleures pratiques de sécurité ou des recommandations de conformité peut entraîner des vulnérabilités et des failles de sécurité.

- Pourquoi : Les contraintes budgétaires, le manque de sensibilisation à la sécurité ou la négligence peuvent conduire à une non-conformité aux normes de sécurité.

Livrables du TP 2/4

- **DevOps :**
  - TDD : exemple IT ou Sécurité
  - BDD : exemple IT ou Sécurité

- **TDD (Test-Driven Development)** : Dans le cadre de la sécurité, TDD peut être appliqué pour s'assurer que des tests de sécurité sont écrits avant même le développement d'une nouvelle fonctionnalité. Par exemple, avant d'ajouter une nouvelle fonctionnalité à une application, l'équipe de développement peut d'abord élaborer des tests de sécurité pour s'assurer qu'elle est exempte de vulnérabilités connues.
- **BDD (Behavior-Driven Development)** : Dans le contexte de la sécurité, BDD pourrait être utilisé pour définir des spécifications de comportement de sécurité pour les nouvelles fonctionnalités. Par exemple, les spécifications de sécurité pour une nouvelle fonctionnalité pourraient inclure des critères sur la confidentialité des données ou la protection contre les attaques spécifiques.

Livrables du TP 2/4

- **DevOps :**
  - Canary Testing : exemple IT ou Sécurité

- **Exemple IT** : Lors d'une mise à jour logicielle, une entreprise peut déployer la nouvelle version sur un petit groupe d'utilisateurs (canaris) avant de la déployer sur l'ensemble de la base d'utilisateurs. Cela permet de détecter et de corriger rapidement les problèmes potentiels sans affecter l'ensemble de l'infrastructure IT.

Livrables du TP 2/4

- **DevOps :**
  - Blue/Green testing : exemple IT ou Sécurité

- **Exemple IT** : Lors d'une mise à jour logicielle, un environnement "Blue" (en production) est actuellement utilisé, tandis que l'environnement "Green" (nouvelle version) est préparé en parallèle. Une fois que le test en environnement "Green" est réussi, le basculement entre les deux environnements peut se faire rapidement pour minimiser les interruptions de service.

Livrables du TP 2/4

- **DevOps :**
  - Feature Toggle : exemple IT ou Sécurité

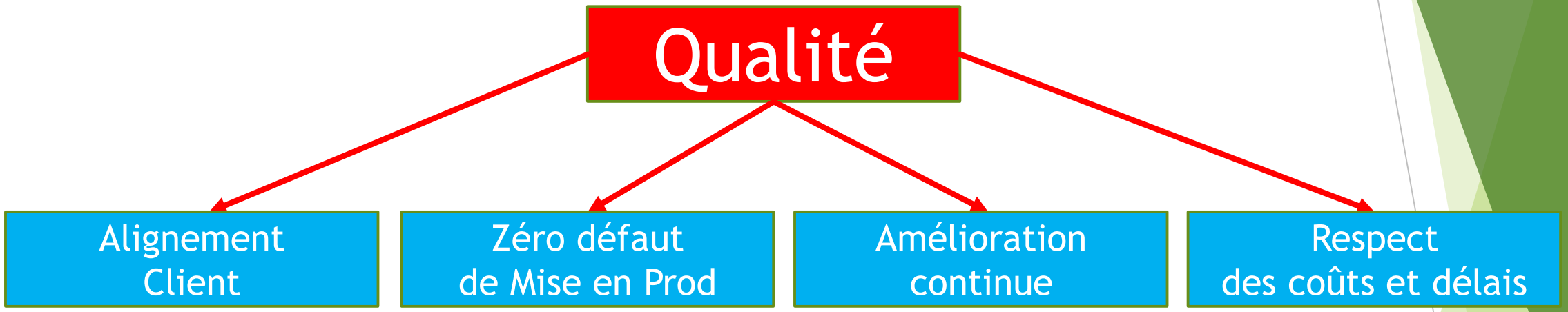
- **Exemple IT** : Une équipe de développement peut utiliser un "Feature Toggle" pour activer ou désactiver une nouvelle fonctionnalité dans une application, permettant ainsi de la tester avec un groupe d'utilisateurs restreint avant de la déployer largement.

Livrables du TP 2/4

- **DevOps :**
  - A/B testing : exemple IT ou Sécurité

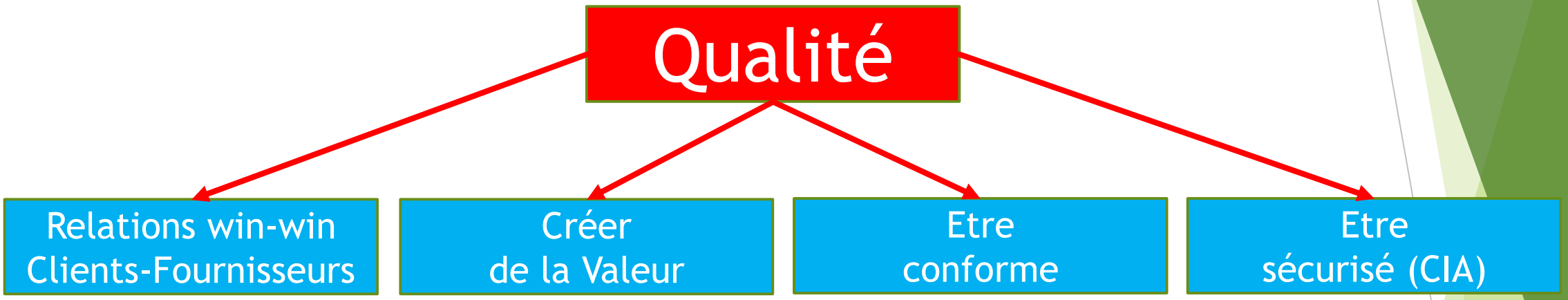
- **Exemple Sécurité - A/B Testing :** Dans le domaine de la sécurité, une équipe utilise l'A/B testing pour évaluer l'efficacité de deux méthodes de sécurité différentes. Par exemple, deux méthodes d'authentification peuvent être testées sur deux groupes d'utilisateurs différents. L'équipe peut ainsi mesurer laquelle offre une meilleure sécurité en fonction des résultats des tests.

Livrables du TP 3/4



_ KPI _ BDD	_ TDD _ Canary Testing _ Blue/Green Deployment	_ PDCA _ Feature Toggle _ Les 8 points de JP Kotter	_ KPI _ PDCA

Livrables du TP 4/4



_ KPI _ BDD	_ Business Case _ KPI	_ A/B Testing _ Blue/Green Deployment _ KPI	_ Blue/Green Deployment _ Feature Toggle

FIN