"Si vous n'attaquez pas activement les risques, ils vous attaqueront activement."


Analyse des risques liés aux projets informatiques

Présentation du cours

Introduction générale

Ce cours a pour objectif de familiariser les étudiants L3 IRD avec **les concepts fondamentaux de la gestion des risques appliqués aux projets informatiques**. Dans un monde où la technologie joue un rôle central dans les opérations des entreprises, il est essentiel pour les futurs IT guys de comprendre et de savoir anticiper les risques liés aux projets IT.

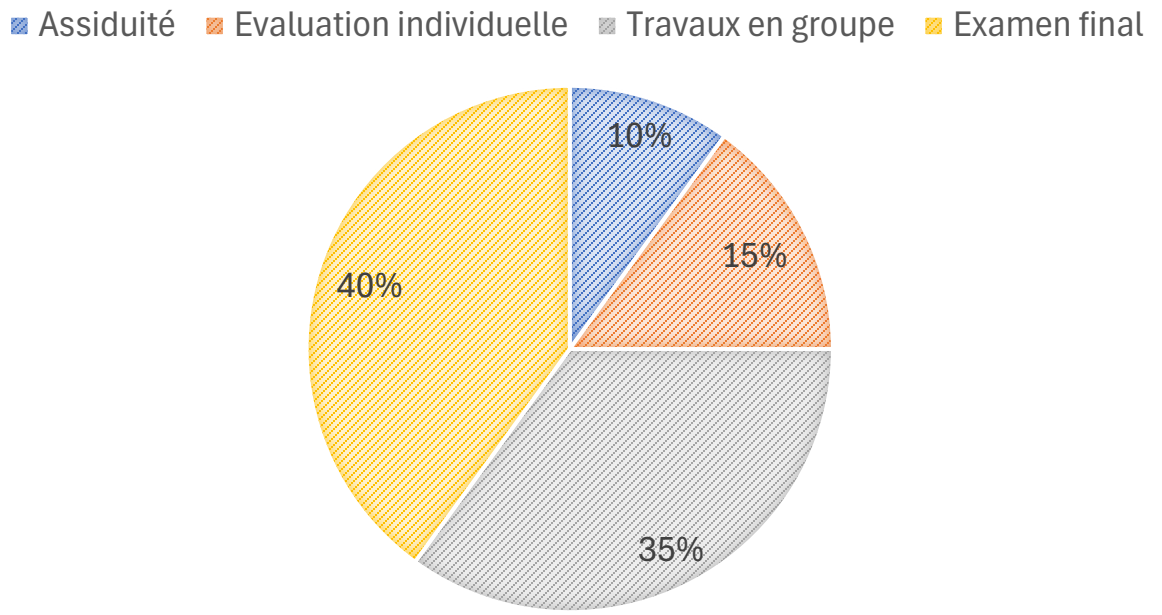
Objectifs Pédagogiques

- Comprendre les types de risques associés aux projets informatiques.
- Apprendre à identifier, évaluer et prioriser les risques.
- Développer des stratégies de gestion des risques.
- Utiliser des outils pour surveiller et contrôler les risques.
- Appliquer des techniques de gestion des risques dans des études de cas réels.

Présentation du cours

1. Introduction à l'analyse des risques
2. Identification des risques
3. Évaluation des risques
4. Stratégies de gestion des risques
5. Surveillance et contrôle des risques
6. Études de cas et applications pratiques

Contenu



Évaluation

Présentons nous maintenant

M. Tsilavina Franco RAKOTOMAHEFA

- Plus de 17 ans dans le domaine de la gestion de projets
- Ayant occupé des postes de responsable au sein d'institutions financière (expériences en expatriation)
- Actuellement je suis Consultant Formateur au sein d'une IMF

À votre tour de vous présenter

- Partagez nous votre nom et votre prénom
- Parlez nous un peu de vous

01

Introduction à l’analyse des risques

Le concept du Risque

Définitions

1. Évènement dont l'apparition n'est pas certaine et dont la manifestation est susceptible d'affecter les objectifs du projet
2. La possibilité qu'un événement ou une action entraîne des conséquences défavorables, compromettant l'atteinte d'un objectif. C'est une combinaison de la probabilité d'un événement et de son impact.

Évènement virtuel	Non identifiable		**IMPREVU**
	Identifiable	Non quantifiable	**ALEA**
	Identifiable	Quantifiable	**RISQUE d'un PROJET**
Évènement déjà réalisé			**PROBLEME**

- **Risque Financier :**
  - Exemple : Une entreprise investit dans une nouvelle technologie. Le risque ici pourrait être la perte de capital si la technologie ne répond pas aux attentes du marché. Ce type de risque est souvent mesuré en termes de volatilité des actifs financiers ou de perte de valeur.
- **Risque Informatique :**
  - Exemple : Une attaque de ransomware peut compromettre la sécurité des données d'une entreprise, entraînant des pertes financières et une atteinte à la réputation. Ici, le risque concerne la sécurité des systèmes d'information et la protection des données.
- **Risque Industriel :**
  - Exemple : Dans une usine, l'utilisation de machines lourdes comporte des risques pour la sécurité des travailleurs. Les pannes de machines ou les accidents peuvent causer des pertes de production ou des blessures graves.

- **Une menace** est tout ce qui a le potentiel de causer un dommage ou une perturbation. Les menaces peuvent être internes (comme un employé mécontent) ou externes (comme un cybercriminel), et peuvent être intentionnelles (attaques délibérées) ou accidentelles (pannes de système, catastrophes naturelles). Par exemple, une menace informatique pourrait être un logiciel malveillant conçu pour voler des informations sensibles.

- **La vulnérabilité** est une faiblesse ou une faille dans un système qui peut être exploitée par une menace pour provoquer un dommage. Les vulnérabilités peuvent être de nature technique (comme une faille de sécurité dans un logiciel) ou organisationnelle (comme une mauvaise gestion des droits d'accès). Une vulnérabilité, en soi, n'entraîne pas nécessairement des dommages, mais elle augmente le risque si une menace exploite cette vulnérabilité.

Le concept du Risque

Exemple concrets

- **Secteur Financier :** La crise financière de 2008 est un exemple de risques systémiques où la mauvaise évaluation des risques de crédit a conduit à une crise mondiale.
- **Secteur Informatique :** La fuite massive de données de Facebook en 2018, où des millions de comptes ont été exposés, a montré les risques de gestion insuffisante de la sécurité des données.
- **Secteur Industriel :** L'accident de la centrale nucléaire de Fukushima en 2011 a illustré les risques d'ignorance ou de sous-estimation des risques naturels dans la gestion des infrastructures critiques.

Importance de l'Analyse de Risques

Pourquoi Analyser les Risques ?

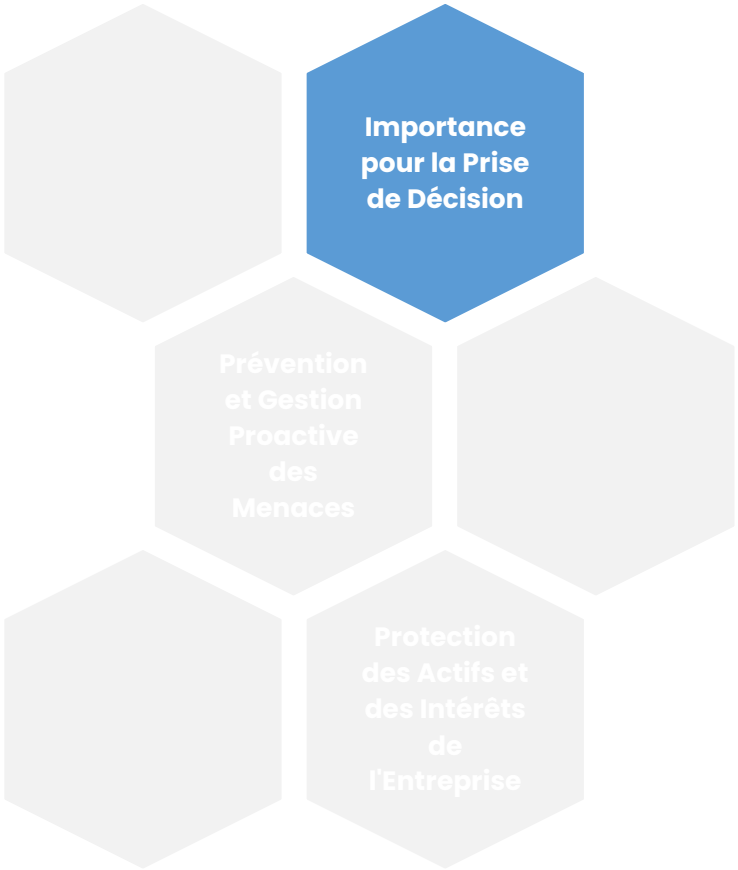
Importance pour la Prise de Décision

Prévention et Gestion Proactive des Menaces

Protection des Actifs et des Intérêts de l'Entreprise

Importance de l'Analyse de Risques

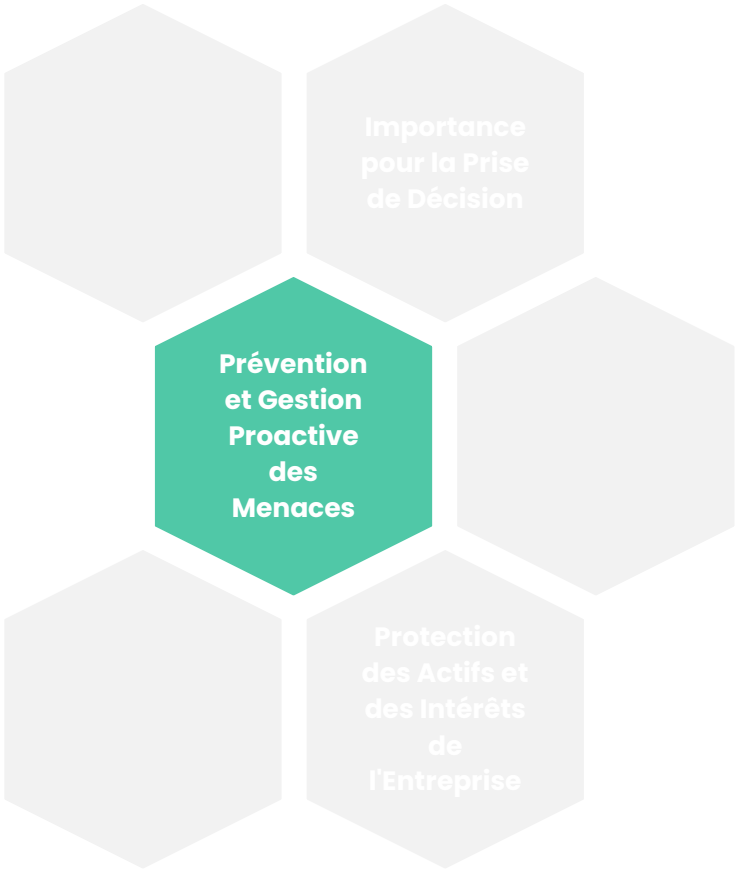
Pourquoi Analyser les Risques ?



1. **Rôle de l'analyse de risques :**
   - L'analyse de risques aide les décideurs à comprendre les incertitudes qui entourent un projet ou une stratégie. En identifiant les risques, les gestionnaires peuvent prendre des décisions plus éclairées qui tiennent compte des éventualités possibles.
   - **Exemple :** Lorsqu'une entreprise envisage de pénétrer un nouveau marché, l'analyse des risques peut révéler des obstacles potentiels tels que des régulations locales strictes, des différences culturelles, ou des concurrents déjà bien établis.
2. **Méthodes courantes utilisées :**
   - **Cartographie des risques :** Utilisation de matrices pour évaluer la probabilité et l'impact de différents risques, aidant à prioriser les actions.
   - **Scénarios hypothétiques :** Création de scénarios basés sur des risques potentiels pour évaluer les impacts sur la prise de décision.

Importance de l'Analyse de Risques

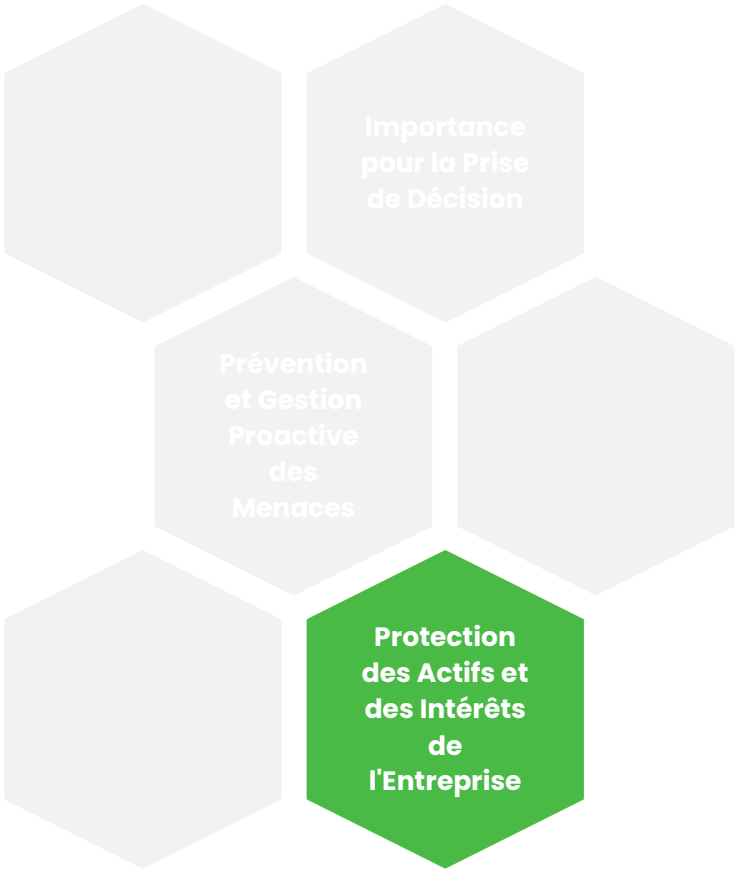
Pourquoi Analyser les Risques ?



1. **Pourquoi être proactif :**
   - Attendre que les risques se manifestent peut entraîner des pertes majeures. Une approche proactive permet de prendre des mesures préventives pour atténuer ou éviter les impacts négatifs.
   - **Exemple :** Dans le domaine de la cybersécurité, les entreprises qui investissent dans la prévention des cyberattaques (par exemple, à travers la formation des employés ou la mise en place de pare-feu robustes) évitent souvent des coûts énormes liés aux violations de données.
2. **Outils de gestion proactive :**
   - **Audit de sécurité :** Réaliser des audits réguliers pour identifier les failles potentielles avant qu'elles ne soient exploitées.
   - **Plans de continuité des activités :** Développement de stratégies pour maintenir les opérations en cas d'événements perturbateurs (catastrophes naturelles, pannes technologiques).

Importance de l'Analyse de Risques

Pourquoi Analyser les Risques ?



1. **Importance de la protection des actifs :**
   - Les actifs tangibles (infrastructures, équipements) et intangibles (données, propriété intellectuelle) sont essentiels à la survie et au succès d'une entreprise. L'analyse de risques identifie les menaces potentielles pour ces actifs et propose des stratégies pour les protéger.
   - **Exemple :** Une entreprise pharmaceutique peut protéger ses brevets contre le vol ou la contrefaçon en évaluant les risques associés aux partenariats internationaux ou à la gestion des données.
2. **Stratégies de protection :**
   - **Assurance :** Souscrire à des polices d'assurance adaptées pour couvrir les pertes potentielles liées aux risques identifiés.
   - **Cryptage des données :** Utilisation de technologies avancées pour protéger les informations sensibles contre les cyberattaques.

Importance de l'Analyse de Risques

Avantages d’analyser les Risques

Importance de l'Analyse de Risques

Avantages d’analyser les Risques

1. **Comment l'analyse de risques réduit les pertes :**
   - En anticipant les risques, les entreprises peuvent mettre en place des mesures préventives qui réduisent la probabilité d'occurrence ou atténuent les effets négatifs.
   - **Exemple :** Dans l'industrie alimentaire, l'analyse des risques sanitaires permet d'éviter des rappels de produits coûteux en détectant les problèmes avant qu'ils ne deviennent critiques.
2. **Étapes clés :**
   - **Identification :** Déterminer les risques potentiels à travers des audits et des analyses.
   - **Évaluation :** Quantifier la probabilité et l'impact des risques pour prioriser les mesures de réduction.

Importance de l'Analyse de Risques

Avantages d’analyser les Risques

1. **Qu'est-ce que la résilience organisationnelle ?**
   - La capacité d'une organisation à résister aux chocs externes et à se rétablir rapidement. L'analyse de risques joue un rôle clé en identifiant les vulnérabilités et en préparant l'entreprise à faire face aux crises.
   - **Exemple :** Une entreprise manufacturière qui a des plans de continuité robustes peut reprendre rapidement ses opérations après une catastrophe naturelle.
2. **Stratégies de renforcement :**
   - **Diversification des fournisseurs :** Pour éviter la dépendance excessive à un seul fournisseur.
   - **Simulation de crises :** Exercice régulier pour tester la réactivité de l'organisation face à différents scénarios de risques.

Importance de l'Analyse de Risques

Avantages d’analyser les Risques

1. **Priorisation des ressources :**
   - En identifiant et en classant les risques, l'analyse de risques permet aux entreprises de concentrer leurs ressources (financières, humaines) sur les zones les plus critiques.
   - **Exemple :** Une entreprise de technologie pourrait décider d'investir davantage dans la sécurité informatique après avoir identifié une vulnérabilité majeure.
2. **Outils utilisés :**
   - **Budgétisation basée sur les risques :** Allocation des fonds en fonction de l'importance des risques identifiés.
   - **Matrice d'impact :** Visualisation des risques pour déterminer les priorités.

Importance de l'Analyse de Risques

Analyse d'une entreprise ayant utilisé l'analyse de risques pour éviter un échec majeur :

1. **Présentation du cas :**
   - **Entreprise :** Toyota lors de la crise de rappel de véhicules en 2009-2010.
   - **Contexte :** Toyota a rappelé des millions de véhicules en raison de défauts potentiels. Grâce à une analyse de risques proactive, l'entreprise a pu identifier les défauts avant qu'ils ne causent des dommages irréparables à sa réputation.
   - **Stratégies employées :** Toyota a mis en place des procédures de contrôle de qualité plus strictes, et a amélioré sa communication de crise pour gérer l'impact sur sa réputation.
2. **Résultats :**
   - Bien que la crise ait eu un impact temporaire sur les ventes et la réputation de Toyota, l'approche proactive de gestion des risques a permis à l'entreprise de se rétablir rapidement et de renforcer la confiance des consommateurs.

Importance de l'Analyse de Risques

Processus d’Analyse de Risques

- Un processus continu qui s'adapte aux évolutions du projet.
- Il permet de minimiser les incertitudes, de prendre des décisions éclairées et de s'assurer que les risques ne compromettent pas la réalisation des objectifs du projet.
- Une approche proactive de la gestion des risques contribue à la réussite des projets et à la réduction des impacts négatifs potentiels

Processus d'Analyse de Risques

Identifier les risques

- Lister tous les risques encourus

Évaluer les risques

- Mesurer les impacts des risques

Répondre aux risques

- Définir le plan d'actions

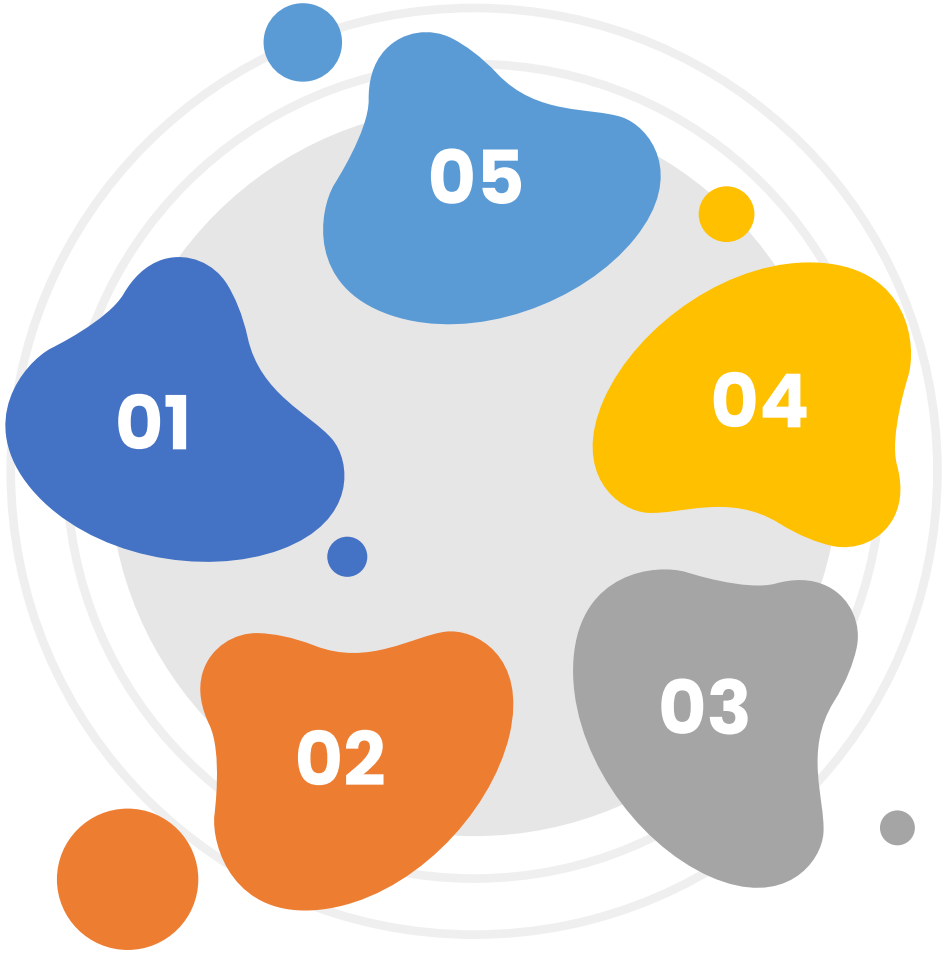
Maîtriser les risques

- Appliquer le plan d'actions et le mettre à jour dans le cas échéant

Types de risques

Risques financiers

Risques opérationnels



Risques stratégiques

Risques de conformité

Cyber – risques

Risques financiers

1. **Définition :**
   - Les risques financiers concernent la possibilité de pertes monétaires pour une entreprise, dus à des facteurs économiques, tels que les fluctuations des marchés financiers, les variations des taux de change, les taux d'intérêt, ou le risque de crédit.
2. **Exemples :**
   - **Fluctuations des Marchés :** Une entreprise investissant en bourse peut subir des pertes si les marchés chutent brusquement.
   - **Risque de Taux d'Intérêt :** Les entreprises ayant des emprunts peuvent être affectées par une augmentation des taux d'intérêt, augmentant le coût du service de la dette.
3. **Illustration :**
   - **Cas de la crise financière de 2008 :** Plusieurs entreprises ont fait faillite en raison de la chute des marchés financiers, causée par le défaut de paiement des prêts hypothécaires subprimes.

Risques opérationnels

1. **Définition :**
   - Les risques opérationnels sont liés aux défaillances internes d'une organisation, y compris les erreurs humaines, les dysfonctionnements techniques, les interruptions des processus, et les défauts de contrôle.
2. **Exemples :**
   - **Erreurs Humaines :** Une erreur de saisie dans un système de gestion des commandes peut entraîner des livraisons incorrectes ou retardées.
   - **Dysfonctionnements Techniques :** Une panne du serveur central peut paralyser les opérations de l'entreprise pendant des heures.
3. **Illustration :**
   - **Cas de British Airways en 2017 :** Une panne informatique majeure a causé l'annulation de centaines de vols, entraînant des pertes financières et une atteinte à la réputation.

Risques stratégiques

1. **Définition :**
   - Les risques stratégiques sont liés aux décisions à long terme d'une organisation, telles que les expansions sur de nouveaux marchés, les acquisitions, ou les lancements de nouveaux produits. Ces risques peuvent impacter la position concurrentielle de l'entreprise.
2. **Exemples :**
   - **Expansion sur de Nouveaux Marchés :** Une entreprise qui s'aventure dans un marché étranger sans bien comprendre la culture locale peut échouer.
   - **Lancement de Nouveaux Produits :** Le lancement d'un produit qui ne répond pas aux attentes des consommateurs peut entraîner des pertes financières et nuire à la marque.
3. **Illustration :**
   - **Cas de Nokia :** La décision stratégique de Nokia de ne pas adopter rapidement Android a contribué à sa perte de parts de marché face à ses concurrents.

Risques de conformité

1. **Définition :**
   - Les risques de conformité surviennent lorsqu'une organisation ne respecte pas les lois, les règlements, ou les normes éthiques. Cela peut entraîner des amendes, des sanctions légales, et des dommages à la réputation.
2. **Exemples :**
   - **Non-conformité aux Régulations Financières :** Une banque qui ne respecte pas les régulations anti-blanchiment risque des amendes sévères.
   - **Violation des Normes de Sécurité :** Une entreprise qui ne respecte pas les normes de sécurité du travail peut faire face à des poursuites judiciaires après un accident.
3. **Illustration :**
   - **Cas de Volkswagen :** Le scandale des émissions truquées a entraîné des amendes de plusieurs milliards de dollars pour non-conformité aux régulations environnementales.

Cyber – Risques

- **Définition :**
  - Les cyber-risques concernent les menaces qui pèsent sur les systèmes informatiques et les données d'une organisation, y compris les cyberattaques, les violations de données, et les pannes de systèmes.
- **Exemples :**
  - **Cyberattaques :** Les ransomwares peuvent paralyser les opérations d'une entreprise en chiffrant ses données et en demandant une rançon pour les débloquer.
  - **Violation de Données :** La fuite de données personnelles peut entraîner des pertes financières et nuire à la réputation.
- **Illustration :**
  - **Cas de l'attaque de WannaCry en 2017 :** Ce ransomware a affecté des milliers d'ordinateurs dans le monde, causant des perturbations majeures dans divers secteurs, y compris les services de santé.

Type de risques

- **Applications**
  - Déterminer le type de risques
  - Évaluer les implications et les conséquences possibles

✓ Un investisseur ayant perdu de l'argent suite à l'effondrement des actions.

✓ Une chaîne de production arrêtée en raison d'une panne d'équipement.

✓ Une entreprise pharmaceutique qui investit massivement dans un médicament qui échoue lors des essais cliniques.

✓ Une entreprise énergétique sanctionnée pour non-respect des normes environnementales.

✓ Une entreprise de commerce en ligne victime d'un vol de données clients.

Type de risques

- **Applications**
  - Déterminer le type de risques
  - Évaluer les implications et les conséquences possibles

✓ **Risques Financiers :** Un investisseur ayant perdu de l'argent suite à l'effondrement des actions.

✓ **Risques Opérationnels :** Une chaîne de production arrêtée en raison d'une panne d'équipement.

✓ **Risques Stratégiques :** Une entreprise pharmaceutique qui investit massivement dans un médicament qui échoue lors des essais cliniques.

✓ **Risques de Conformité :** Une entreprise énergétique sanctionnée pour non-respect des normes environnementales.

✓ **Cyber-Risques :** Une entreprise de commerce en ligne victime d'un vol de données clients.

Type de risques

- **Applications**
  - Déterminer le type de risques
  - Évaluer les implications et les conséquences possibles

Impact à Court Terme : Coûts immédiats tels que des amendes, des pertes de revenus, ou des coûts de réparation.
Impact à Long Terme : Conséquences durables telles que la perte de clients, une réputation ternie, ou une baisse des parts de marché.

02

Identification des risques

Rappel du Module 1

Processus d'Analyse de Risques

Identifier les risques

- Lister tous les risques encourus

Évaluer les risques

- Mesurer les impacts des risques

Répondre aux risques

- Définir le plan d'actions

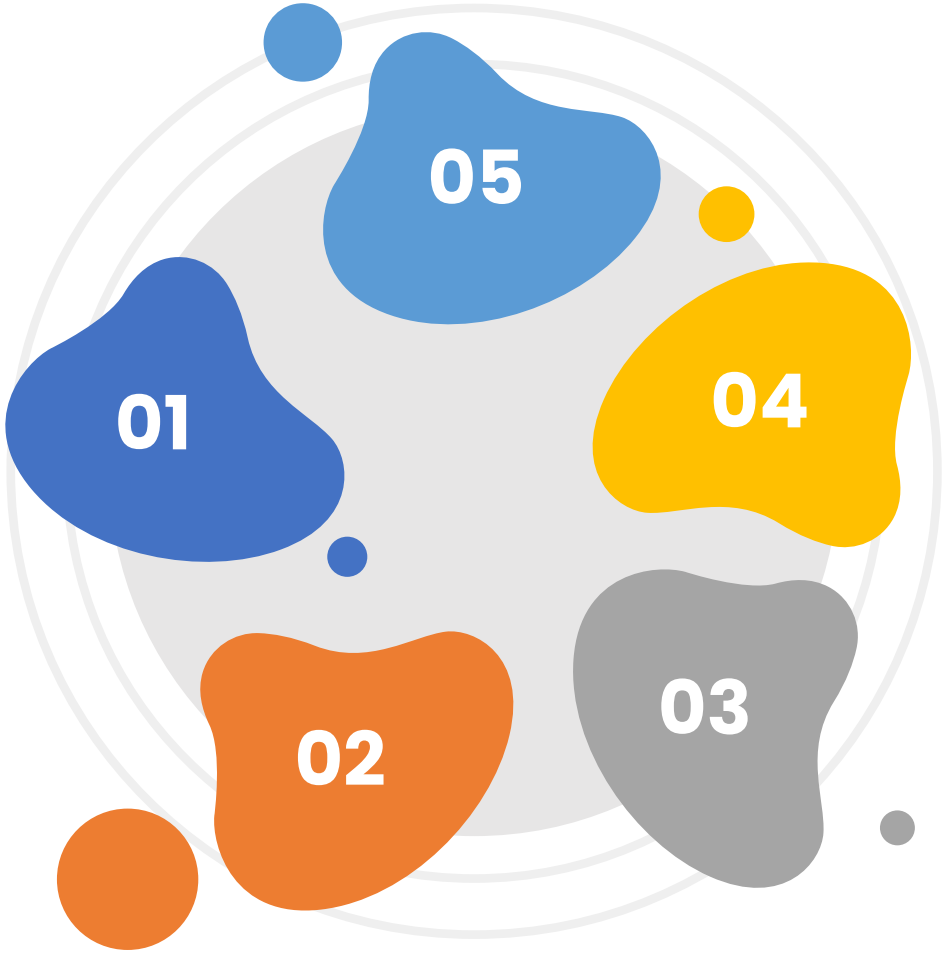
Maîtriser les risques

- Appliquer le plan d'actions et le mettre à jour dans le cas échéant

Types de risques

Risques financiers

Risques opérationnels



Risques stratégiques

Risques de conformité

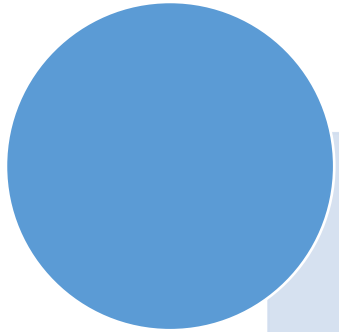
Cyber – risques

Introduction à l'Identification des Risques

- L'identification des risques consiste à **détecter** et à **décrire tous les risques susceptibles d'affecter le projet**. Ce processus est essentiel pour anticiper les problèmes potentiels avant qu'ils ne surviennent.

- **Importance** :

> Une identification précoce des risques permet de planifier des réponses adéquates et de minimiser l'impact des risques sur le projet.



Savoir identifier les risques pertinents dans un projet informatique.

Comprendre et appliquer différentes techniques d'identification des risques.

Documenter correctement les risques pour un suivi efficace.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

1. Brainstorming

Description : Le brainstorming est une technique collective où les membres de l'équipe sont encouragés à exprimer spontanément leurs idées sur les risques potentiels du projet. Cette méthode permet de générer rapidement un grand nombre d'idées sans se soucier de leur faisabilité immédiate.

Processus :

- **Préparation :** Définir le cadre et les objectifs de la session de brainstorming.
- **Session :** Les participants expriment librement leurs idées. Il est important de créer un environnement où toutes les contributions sont respectées, sans jugement.
- **Analyse :** Les idées sont classées et évaluées pour déterminer leur pertinence et leur impact potentiel.

Avantages :

- Encourage la participation de toute l'équipe.
- Permet de découvrir des risques auxquels on n'aurait pas pensé individuellement.

Limitations :

- Peut-être moins efficace si certains membres de l'équipe ne participent pas activement.
- Le processus peut générer un grand nombre de risques peu pertinents ou trop génériques.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

2. Analyse SWOT

Description : L'analyse SWOT (Strengths, Weaknesses, Opportunities, Threats) est une méthode structurée qui évalue les forces, faiblesses, opportunités et menaces liées à un projet. Chaque élément de la matrice SWOT peut révéler des risques potentiels.

Processus :

- **Forces et Faiblesses :** Évaluer les aspects internes du projet qui peuvent soit constituer un atout (forces) ou un point faible (faiblesses).
- **Opportunités et Menaces :** Examiner les facteurs externes qui peuvent offrir des avantages (opportunités) ou poser des défis (menaces).
- **Identification des Risques :** Relier les faiblesses et les menaces pour identifier les risques spécifiques.

Avantages :

- Fournit une vue d'ensemble complète du projet.
- Facilite la reconnaissance des risques internes et externes.

Limitations :

- Peut-être trop général et ne pas fournir une identification exhaustive des risques.
- Nécessite une analyse approfondie pour être vraiment utile.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

3. Interviews et Questionnaires

Description : Les interviews et les questionnaires sont utilisés pour recueillir des informations directement auprès des parties prenantes, des experts et des membres de l'équipe sur les risques qu'ils perçoivent.

Processus :

- **Interviews :** Conduire des entretiens individuels ou en groupe pour obtenir des informations qualitatives détaillées sur les risques.
- **Questionnaires :** Distribuer des questionnaires structurés pour recueillir des données sur les risques perçus à un plus grand nombre de personnes.
- **Analyse :** Les réponses sont compilées et analysées pour identifier les tendances et les risques majeurs.

Avantages :

- Permet d'obtenir des insights détaillés et spécifiques sur les risques.
- Les questionnaires peuvent être distribués à un large public pour recueillir une diversité d'opinions.

Limitations :

- Les interviews peuvent être chronophages et nécessitent des compétences en communication.
- Les questionnaires doivent être bien conçus pour éviter des réponses trop vagues ou biaisées.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

4. Check-lists

Description : Les check-lists sont des listes prédéfinies de risques potentiels basées sur l'expérience des projets antérieurs. Elles servent de guide pour s'assurer que les risques courants ne sont pas omis.

Processus :

- **Création de la Check-list :** Basée sur des projets similaires antérieurs, une liste de risques potentiels est élaborée.
- **Utilisation :** À chaque phase du projet, la check-list est parcourue pour identifier tout risque applicable.
- **Mise à jour :** Les check-lists doivent être mises à jour régulièrement pour inclure de nouveaux risques découverts au fil du temps.

Avantages :

- Facile à utiliser et à intégrer dans le processus de gestion des risques.
- Garantit qu'aucun risque important n'est oublié.

Limitations :

- Peut limiter la créativité et conduire à une dépendance excessive à l'égard de la liste.
- Les risques spécifiques à un projet particulier peuvent ne pas être couverts.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

5. Diagramme de Cause à Effet (Ishikawa)

Description : Le diagramme de cause à effet, également connu sous le nom de diagramme d'Ishikawa ou diagramme en arête de poisson, est un outil visuel qui permet de déterminer les causes profondes des risques en les classant par catégories (équipements, processus, personnes, etc.).

Processus :

- **Identification du Problème :** Définir le problème ou l'effet à analyser.
- **Catégorisation :** Déterminer les principales catégories sous lesquelles les causes potentielles seront classées (par exemple, méthode, main-d'œuvre, matériel, environnement).
- **Brainstorming :** Identifier les causes potentielles sous chaque catégorie.
- **Analyse :** Examiner les causes identifiées pour déterminer lesquelles sont les plus susceptibles de générer des risques.

Avantages :

- Aide à identifier les causes profondes des problèmes potentiels.
- Encourage une réflexion structurée et exhaustive sur les sources de risques.

Limitations :

- Peut devenir complexe pour les projets de grande envergure avec de nombreuses variables.
- Nécessite une bonne connaissance du projet pour être efficace.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

6. Techniques de Groupes Nominales

Description : La technique de groupe nominal (TGN) est une méthode structurée pour générer et hiérarchiser les risques. Elle combine le brainstorming individuel avec une discussion de groupe et un vote pour déterminer les risques les plus critiques.

Processus :

- **Phase 1 :** Chaque membre du groupe liste les risques potentiels individuellement.
- **Phase 2 :** Les risques sont ensuite partagés avec le groupe et discutés collectivement.
- **Phase 3 :** Un vote est effectué pour classer les risques selon leur importance ou leur probabilité.

Avantages :

- Combine les avantages du brainstorming avec une structure pour une meilleure prise de décision.
- Encourage la participation de tous les membres et évite la domination par une seule personne.

Limitations :

- Peut être plus long que d'autres méthodes.
- Nécessite un bon modérateur pour assurer le respect du processus.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

7. Analyse des Causes Racines (RCA)

Description : L'analyse des causes racines est une méthode approfondie pour identifier la cause principale d'un problème ou d'un risque. Elle est souvent utilisée après la survenance d'un incident pour comprendre ce qui s'est passé et comment prévenir sa récurrence.

Processus :

- **Identification du Problème :** Déterminer le problème ou le risque à analyser.
- **Collecte des Données :** Recueillir toutes les informations pertinentes sur l'incident ou le risque.
- **Analyse :** Utiliser des techniques comme les 5 Pourquoi ou le diagramme de cause à effet pour identifier la cause racine.
- **Recommandations :** Proposer des actions correctives pour éviter que le problème ne se reproduise.

Avantages :

- Permet de comprendre profondément les causes d'un problème, ce qui peut aider à prévenir des risques similaires à l'avenir.
- Peut être utilisée pour améliorer continuellement les processus de gestion des risques.

Limitations :

- Peut être complexe et nécessiter une analyse détaillée qui prend du temps.
- Nécessite une expertise pour bien interpréter les résultats et identifier la véritable cause racine.

Méthodes d'Identification des Risques

Les méthodes d'identification des risques sont essentielles pour **découvrir les risques potentiels dans un projet**. Voici un aperçu détaillé des principales méthodes utilisées pour identifier les risques dans les projets informatiques, ainsi que leurs avantages et limitations.

Ces méthodes offrent une variété d'approches pour identifier les risques dans un projet informatique. Leur utilisation dépendra de la nature du projet, des ressources disponibles et du stade du projet. En combinant plusieurs de ces méthodes, les gestionnaires de projet peuvent obtenir une vue d'ensemble complète des risques potentiels et se préparer efficacement à les gérer.

Consignes d'applications

1. Reprenez vos projets
2. Dressez la Fiche synthétique Projet
   - Nom du projet
   - Objectifs(s) du projet
   - Etapes et phasage
   - Ressources
3. Identifiez **tous** les risques de votre projet

Processus d'Analyse de Risques

Identifier les risques

- Lister tous les risques encourus

Évaluer les risques

- Mesurer les impacts des risques

Répondre aux risques

- Définir le plan d'actions

Maîtriser les risques

- Appliquer le plan d'actions et le mettre à jour dans le cas échéant

Identification des risques sur les projets informatiques

INITIALISATION	PLANIFICATION	CONCEPTION	EXECUTION	CLOTURE
Définir les objectifs généraux, les parties prenantes, et l'envergure du projet.	Détail des étapes du projet, identification des ressources, des délais et des coûts.	Définir en détail les spécifications techniques et fonctionnelles du projet.	Mise en œuvre des travaux, développement du projet, tests et ajustements.	Finalisation et livraison du projet, évaluation des résultats, et retour d'expérience.

Identification des risques sur les projets informatiques

Phase du projet	Méthodes d'identification des risques
Initialisation	Analyse SWOT, Interviews et Questionnaires, Check-lists
Planification	Brainstorming, Check-lists, Techniques de Groupes Nominales, Analyse des Causes Racines (RCA)
Conception	Diagramme de Cause à Effet (Ishikawa), Analyse des Causes Racines (RCA), Check-lists
Exécution	Check-lists, Diagramme de Cause à Effet (Ishikawa), Analyse des Causes Racines (RCA), Brainstorming
Clôture	Brainstorming, Analyse des Causes Racines (RCA), Interviews et Questionnaires, Check-lists

03

Évaluation des risques

Introduction à l'évaluation des Risques

Définition

- L'évaluation des risques est le processus qui consiste à analyser la gravité des risques identifiés afin de déterminer leur impact potentiel sur les objectifs du projet.

Importance de l'évaluation des risques

- Prioriser les risques pour allouer des ressources de manière efficace.
- Aider à la prise de décision en matière de gestion des risques.
- Faciliter la communication sur les risques avec les parties prenantes.

Les deux dimensions de l'évaluation des risques

- Probabilité d'occurrence : La chance que le risque se produise.
- Impact : Les conséquences si le risque se réalise (financières, temporelles, qualitatives).

Introduction à l’évaluation des Risques

L'évaluation des risques est itérative :

initialement lors de la planification, puis régulièrement pendant toute la durée du projet.

Evaluer les risques

- Mesurer les impacts des risques en terme de:
  - Probabilité de survenance
  - Niveau de gravité

Probabilité>

Quelle est la probabilité que le risque survienne?

Gravité>

Quel sera l'impact du risque s'il survient?

Evaluer les risques

Criticité = Probabilité x Gravité

Pour classer les risques de manière plus objective, on peut attribuer une note à chaque risque.

- La note de probabilité va de 1 à 5, la note de 1 correspondant aux risques très improbables.
- La note de gravité va de 1 à 4, la note de 1 correspondant aux risques insignifiants.

On peut aussi utiliser un barême qui donne plus de poids aux risques dont le niveau de gravité est important.

Par exemple :

- Risques insignifiants : 1
- Risques marginaux : 2
- Risques critiques : 5
- Risques catastrophiques : 8

Evaluer les risques

		GRAVITE			
		Insignifiant	Marginal	Critique	Catastrophique
PROBABILITE DE SURVENANCE	Très Probable	A gérer	Inacceptable	Inacceptable	Inacceptable
	Probable	A gérer	A gérer	A gérer	Inacceptable
	Possible	Négligeable	Négligeable	A gérer	A gérer
	Peu Probable	Négligeable	Négligeable	Négligeable	Négligeable
	Très Improbable	Négligeable	Négligeable	Négligeable	Négligeable

Evaluer les risques

A gérer

Le risque pour lequel on prévoit des mesures :
- préventives, qui sont mises en place avant le projet.
- curatives, qui seront mises en place en cas d'occurrence effective du problème en cours de projet.

Inacceptable

Le niveau de risque le plus élevé.
Il est appelé inacceptable, parce qu'en l'état, il met en danger la bonne réalisation du projet.
Dans ce cas :
- Soit on repense le projet de manière à déplacer ces risques vers des risques à traiter ou négligeables.
- Soit on arrête le projet.

Négligeable

On ne prévoit pas de mesure spécifique pour ce type de risque. On considère :
- que son impact est insignifiant sur la réussite du projet.
- ou que sa probabilité est trop faible pour qu'on s'en inquiète.

Annexes

Le concept du Risque

Quelles sont les différences entre un risque perçu et un risque réel au niveau des entreprises sur le domaine des projets informatiques ? Comment les organisations peuvent-elles mieux gérer ces différences ?

Risque Perçu et **Risque Réel** sont deux concepts essentiels mais distincts dans la gestion des risques, notamment dans le cadre des projets informatiques.

1. Risque Perçu

Le **risque perçu** est la manière dont les parties prenantes d'une organisation *croient* qu'un risque pourrait affecter un projet. Cette perception peut être influencée par l'expérience personnelle, les biais cognitifs, la culture d'entreprise, ou même la couverture médiatique des incidents similaires. Le risque perçu peut être soit exagéré, soit sous-estimé par rapport à la réalité.

Exemple : Une entreprise pourrait percevoir un risque élevé de cyberattaque simplement parce qu'elle a lu un article sur une attaque récente dans le secteur, même si ses systèmes sont correctement sécurisés.

2. Risque Réel

Le **risque réel** représente la *véritable probabilité* et *impact potentiel* d'un risque sur un projet, basé sur des données factuelles, des analyses statistiques, et une évaluation rigoureuse. Le risque réel est généralement déterminé à travers des méthodes d'analyse quantitative et qualitative, incluant l'identification des vulnérabilités, l'évaluation des menaces, et la probabilité de leur occurrence.

Exemple : En réalité, si l'infrastructure informatique est robuste et que les systèmes de sécurité sont à jour, le risque réel de cyberattaque peut être beaucoup plus faible que ce que l'entreprise perçoit.

Le concept du Risque

Comment peut-on quantifier des risques dans un domaine où les données sont limitées ?

Bien que la quantification des risques dans un domaine avec des données limitées soit complexe, l'utilisation combinée d'approches qualitatives, de scénarios, d'analogies, de méthodes bayésiennes, et de l'analyse de sensibilité peut offrir des estimations précieuses. Il est également essentiel d'intégrer continuellement de nouvelles informations pour affiner ces estimations. Les organisations doivent être prêtes à adapter leur évaluation des risques à mesure que de nouvelles données deviennent disponibles.

Le concept du Risque

Pensez-vous que certaines organisations sont plus tolérantes au risque que d'autres ? Pourquoi ?

Oui, certaines organisations sont plus tolérantes au risque que d'autres, et cette tolérance varie en fonction de plusieurs facteurs, notamment la culture organisationnelle, le secteur d'activité, la taille de l'entreprise, et sa stratégie globale.