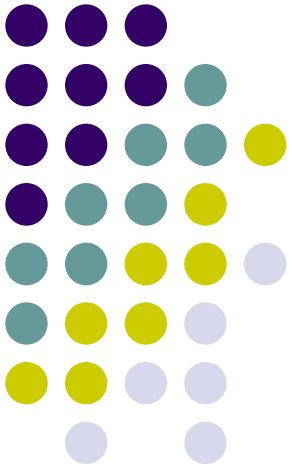
Les Projets et les Risques

EBIOS en gestion des risques

JL Allard
CISM, CIS
MISIS scri



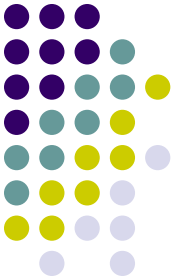
MISIS

Agenda

- Les risques dans la gestion des projets
- EBIOS dans ce ‘jeu’

Ou les suites d’une formation à EBIOS auprès d’un auditeur.

L’auditeur et les projets



- Ce qu’il recherche
  - Qualité du ‘produit’
  - Risques projet
  - Suivi projet
  - Early Life Support (ITIL)

- Base: CobiT 4.1

Idée de départ

- Analyser les processus CobiT
  - PO8 – Assurance de la Qualité
  - PO9 – Gestion des risques
    - Changement de focale (TIC ➔ Projet)
  - PO10 – Gestion des projets
- Etude
  - Attentes et possibilités selon le niveau de Maturité de la Capacité
- 1re Approche
- Apport d'EBIOS
- Concertation interne et 2e approche

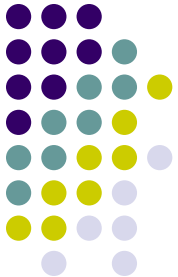
CobiT

- Intéressant mais vite complexe
  - (voir exemple)
- Points clé
  - Cible de la gestion des risques
  - Audience
  - Livrables

Exemple: PO10

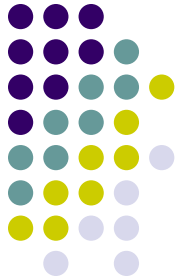
Assess and Manage all Project Risks						
	Demande	**Initiation**	**Planning**	**Exécution**	**Clôture**	**Maintenance & opérations**
Objectif d'audit	*s'assurer que les risques relatifs à l'objet de la demande sont correctement définis, que les objectifs 'qualité' que le projet afin de couvrir ces risques sont définis .*	*s'assurer que les risques relatifs au projet sont correctement identifiés et pris en compte, qu'un programme de réponse est défini.*	*s'assurer que les risques 'qualité' et 'projet' sont correctement pris en compte et que les ressources nécessaires à leur couverture sont identifiés et budgétisés*	*s'assurer d'une mise en œuvre correcte des actions de traitement des risques et de réponse aux évènements*	*s'assurer que les risques relatifs à une clôture imparfaite sont pris en compte et que les mesures sont définies pour y faire face*	*s'assurer que le client dispose d'une documentation et des moyens indispensalbes à une réponse appropriée aux risques 'opération' de la solution*
PO9.1 - Risk Mgt Framework		(inclus dans le plan de travail) Il existe une politique de gestion de tous les risques et un méthode unique à employer dans le cadre des projets	Il existe un plan de gestion des risques et de réaction aux évènements est publié (commun)	idem	idem	la documentation nécessaire au client pour une réaction adéquate aux risques 'opératoires' à été jointe à la solution livrée. La formation nécessaire à été ndonnée.
PO9.2 - Context establishment	Défini dans le cadre de l'objet de la demande de projet	Défini dans le cadre du projet et de sa charge pour le département	na	na	na	na
PO9.3 - Event identification	- Niveau de besoin en qualité de l'objet de la demande - Scénarii d'atteinte aux besoins de l'objet de la demande	- Niveau de besoin de contrôle du projet - Scénarri définis pour chaque phase du projet sur les informations, les activités et les ressources	na	Détection et transmission des incidents et problèmes relatifs au projet tant au point de vue 'qualité' de la solution que gestion des ressources. Corrections au plan de traitement suite aux leçons apprises.	liste des évènements rendant la clôture imparfaite	liste des évènements opératoires pouvant amener une non atteinte des objectifs de la solution
PO9.4 - Risk assessment	Liste hiérérchisée de risques de non-atteinte des objectifs du projet (vision 'objet de la demande' par le 'client')	Liste hiérarchisée des risques 'projet'	na	Evaluation des impacts et classification de l'évènement	classification des évènements	evaluation et classification des évènements
PO9.5 - Risk response	Objectifs de traitement des risques	Objectifs et programme de traitement des risques	prise en compte des ressources de traitement des risques projet dans le plan	Activation des mesures prévues dans le programme de réaction aux évènements	réponse à apporter pour ramener le projet dans les limites du contrôle de gestion	support (2e ligne) au client dans la résolution des évènements
PO9.6 - Action plan monitoring & maintenance	na	na	identification des points et indicateurs de contrôle des risques projet	mise à jour du répertoire des réactions selon l'expérience. Mise à jour du mode de réaction. Mise à jour du mode de dtermination des réactions.	intégration de l'expérience dans le répertoire des réponses et du mode de détermination de la réponse appropriée	intégration des 'lessons learned' dans le support au client

1re Approche



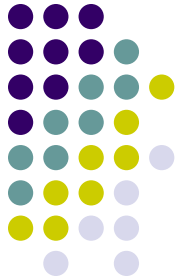
- **Demande**
  - s'assurer que les risques relatifs à l'objet de la demande sont correctement définis, que les objectifs 'qualité' que le projet afin de couvrir ces risques sont définis.
- **Initiation**
  - s'assurer que les risques relatifs au projet sont correctement identifiés et pris en compte, qu'un programme de réponse est défini.
- **Planning**
  - s'assurer que les risques 'qualité' et 'projet' sont correctement pris en compte et que les ressources nécessaires à leur couverture sont identifiés et budgétisés
- **Exécution**
  - s'assurer d'une mise en œuvre correcte des actions de traitement des risques et de réponse aux évènements
- **Clôture**
  - s'assurer que les risques relatifs à une clôture imparfaite sont pris en compte et que les mesures sont définies pour y faire face
- **Maintenance et opérations**
  - s'assurer que le client dispose d'une documentation et des moyens indispensables à une réponse appropriée aux risques 'opération' de la solution

Apport d'EBIOS



- Démarche commune
  - ISO 27005 ➔ EBIOS
- Méthode commune?
  - Objets différents
  - Objectifs différents
  - Cycles de vie différents
  - Nature différente des risques
    - Éléments menaçants/dangers
    - Vulnérabilités
    - Dommages

Apport d'EBIOS



- Techniques communes?
  - EBIOS
    - Contextes différents
    - Besoins de sécurité différents
    - Estimation des risques
    - Appréciation des risques et sélection de l'objectif de traitement
    - Sélection des 'mesures'
  - Les techniques conviennent

Apport d'EBIOS

- Outils communs?
  - Options et Objectifs
  - Couverture
  - 'Efficacité'

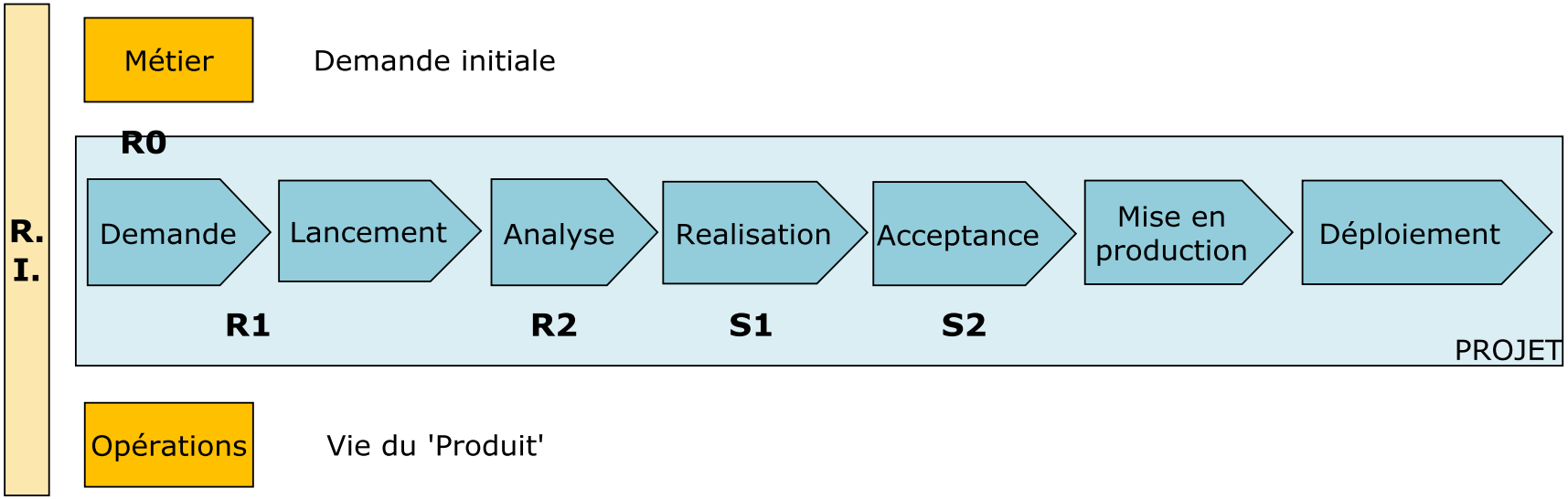
  sauf (guides 4 et 5)
  - Menaces/dangers et dommages
    - 'produit': risques opérationnels
    - 'projet': risques 'management'
    - 'information': EBIOS
  - Vulnérabilités et Mesures
    - Spécifiques

OUI

2e Approche

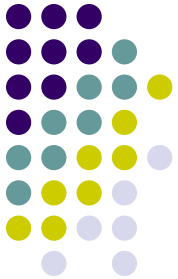
- Tient compte d'une 'maturité' à
  - [1] pour les 'clients' [administration]
    - En gestion des risques
    - En préparation de projets
  - [2] pour les département [Service TIC]
    - En gestion des risques
    - En mise en œuvre de projets
  - Pour l'auditeur
    - [3] en gestion des risques et de la qualité
    - [5] en audit et gestion de projet.

Le projet et les risques



R0 – Risque Fonctionnel
R1 – Risque Projet
R2 – Risque Exploitation
S1 – Suivi 1
S2 – Suivi 2

Questionnaire



- Basé sur 7 critères
  - Efficacité: répond aux attentes + performance
  - Efficience: rendement moyens et ressources
  - Confidentialité
  - Intégrité
  - Disponibilité
  - Conformité + éthique
  - Fiabilité: information ‘correcte et à jour’

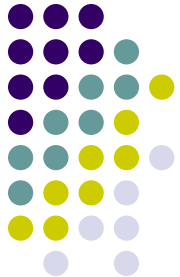
Vocabulaire ‘simple’ et applicable

Avant - R0 - Demande:

- Risques Fonctionnels
  - Produit actuel
  - Nouveau produit
  - Risques d'un produit ne répondant pas 'exactement' au Cahier des Charges
- Pas toujours du ressort du gestionnaire de projet
- Demande Claire? Testable? Stable?

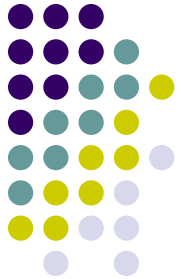
- Questionnaire
  - + responsabilités

Projet - R1 - Initiation:



- Risques projet
  - Délai, Budget, Ressources
- *Questionnaire*
  - *Conformité*
    - *Projet conforme aux règlements?*
    - *Cadre légal connu?*
    - *Périmètre précis?*
    - *Autorisations?*
  - *Efficacité*
    - *Liste et description des livrables?*
    - *Implication des 'parties prenantes'?*
    - *Méthode de gestion de projets respectée?*
    - *Moyens à disposition?*
  - *Efficience*
    - *Organisation?*
    - *Compétence?*
    - *Ressources?*
    - *Formation utilisateurs prévue?*

Après - R2 – Risques d'Exploitation



- Couvre la vie du livrable
- Répond au besoin d' « *Early Life Support* » recommandé par ITIL
  - Mode d'emploi + formation
  - réponse aux incidents, réponse aux problèmes
- Questionnaire 'hybride'
  - Risque informationnel/opérationnel
  - Cible
    - Livrable
    - Informations
    - Objectifs métier

Le risque informationnel…

… et si l'information (à chaque étape) n'était pas

- Fiable
- Autorisé
- Accessible
- Utile

Qualité

Besoin de Sécurité

En supplément

Intégré aux questionnaires

Questionnaires

- Simplifiés à l'extrême
  - Oui/non - 0, 1, 2 ou 3
  - Risque
    - pas menace, vulnérabilité, impact
    - Selon la 'perception'
- Traitement du risque
  - ce que l'on veut contrer
  - Stratégie : ce que l'on veut faire

Catégories de mesures

Stratégies possibles	En agissant sur	
Je veux	Probabilité	Impact
Supprimer le risque	**Prévention**: sur les causes	**Protection**: sur els effets
Accepter le risque	**Suivre** les menaces	
Réduire le risque	**Transfert**: sous-traitance	**Transfert**: assurances
		Partage: fournisseur, mirroring
	Duplication: back-ups, pièces de rechange	
	Prévention: certaines causes	**Protection**: certains effets

Conclusion

- Audit des projets
  - Phases
    - Démarrage
    - Suivi
    - Livraison (+ recette/homologation)
  - Objets
    - Solution
    - Ressources
    - Information
  - *Même combat*, même approche, même méthode, mêmes techniques
  - Outils adaptés

Conclusion générale

- EBIOS pour toute gestion de risques?
- OUI !
- Comme pour ITIL, il faut

Adopter
&
Adapter

www.misis.be