STRATÉGIE DE TEST POUR PROGICIEL – UNE APPROCHE DE GESTION DES RISQUES

par Jean-François Desroches

Dans le contexte de l'implantation d'un progiciel, la stratégie de test est l'un des principaux piliers d'une approche d'implantation efficace.

La stratégie de test d'un grand projet peut compter jusqu'à 15 catégories de tests différentes qui peuvent se regrouper en deux grandes classes : tests de solution et tests de certification technique. La page 3 de cet article présente la liste des 15 catégories de tests et leur définition.

La sélection des catégories de tests requises par le contexte d'un projet sera influencée par l'ensemble des risques en présence. On devra davantage tester les portions de la solution qui comportent le plus de complexité et pour lesquelles des défectuosités entraînent les plus grands impacts.

Tout au long de l'exécution de la stratégie de test, les experts en processus d'affaires et les experts en progiciels travaillent conjointement à la préparation des scénarios de tests ainsi qu'à leur exécution. La mise en commun des connaissances des experts en affaires et en progiciels est essentielle, afin d'en arriver à une paramétrisation optimale du progiciel.

Afin de bien contrôler les activités de chacune des catégories et d'en mesurer l'avancement, il est souhaitable d'utiliser des outils spécialisés en gestion de tests. Ces outils permettent de gérer les scénarios de tests, les résultats et le suivi de la résolution des anomalies et de préparer la reddition de comptes.

L'ensemble des catégories de tests sera exécuté dans des environnements informatiques contrôlés par l'équipe de projet. Il est recommandé d'installer un total de huit environnements, et ce, en plus de l'environnement de production.

Il est important de prévoir un niveau de soutien technique adéquat tout au long de l'exécution des tests. Une équipe dédiée d'experts en infrastructure, en systèmes d'exploitation, en bases de données et en progiciels se consacrera au projet. Cette équipe procédera aux installations de l'équipement et des progiciels, en assurera l'administration et la performance, appliquera les rustines nécessaires et se chargera des copies de sûreté ainsi que du rafraîchissement des environnements.

Les scénarios de tests préparés lors d'un projet sont un actif à préserver et à réutiliser lors de projets subséquents de mise à niveau ou d'ajout de fonctionnalités. Les scénarios servent également de base à la documentation des processus d'affaires et au développement du matériel de formation des usagers. Il est possible d'accélérer la préparation des scénarios de tests en ayant recours à une banque de scénarios prédéfinis. Certains éditeurs de progiciels et de firmes en services-conseils possèdent dans leur capital intellectuel des jeux de scénarios de tests qui peuvent être mis à la disposition de leurs clients.

L'investissement dans l'automatisation des tests n'est pas toujours opportun, cette décision sera fortement influencée par la quantité de cycles de tests de régression potentiels, le nombre de mises en service annuelles, ainsi que la nature des tests visés.

Une stratégie de test se doit de contrôler chacune des variables qui sont introduites tout au long des différentes catégories de tests, afin de pouvoir plus facilement isoler, diagnostiquer et résoudre les anomalies détectées. Les principales variables rencontrées sont : l'infrastructure, les progiciels, la paramétrisation, les données ainsi que les interfaces.

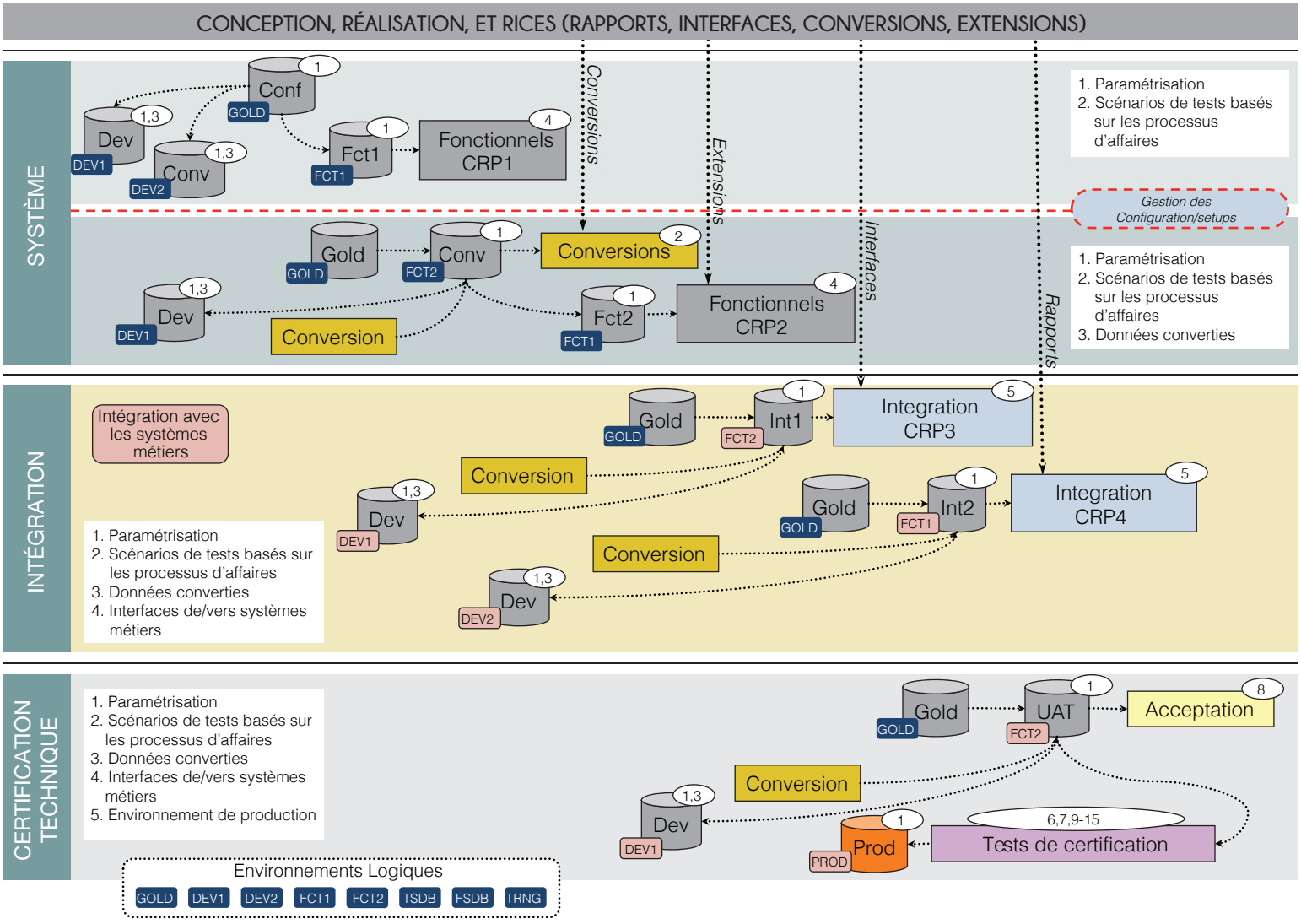
Les changements à la configuration et à la paramétrisation du progiciel doivent être gérés par un groupe central indépendant des équipes de tests afin que les modifications aux configurations soient faites d'une façon contrôlée et qu'elles soient répliquées de façon uniforme et concertée dans tous les environnements. Le contrôle des configurations permet de documenter les différences entre les environnements de tests afin de minimiser les situations pour lesquelles on n'arrive pas à expliquer pourquoi un progiciel se comporte différemment d'un environnement à un autre.

Un diagramme représentant la stratégie discutée dans cet article se trouve en page 2.

***Jean-François Desroches** est directeur de programme chez PlanAxion Solutions. On peut le joindre à jean-francois.desroches@planaxion.com.*

PLANATION

STRATÉGIE DE TEST POUR PROGICIEL – UNE APPROCHE DE GESTION DES RISQUES



TESTS DE SOLUTION		
N°	Nom	Description
1	Environnement	Valider que l'environnement est fonctionnel avant de donner accès à l'équipe de projet, exécuté par les experts Oracle, « tests de fumée ».
2	Conversion de données	Valider que le processus de conversion de données a fonctionné correctement et que les données n'ont pas été altérées de façon inattendue.
3	Unitaires	Confirme que les programmes développés par l'équipe sont fidèles aux spécifications.
4	Fonctionnels	Valider que les applications répondent aux besoins d'affaires. Définition de la paramétrisation.
5	Intégration	S'assurer que les intégrations avec les systèmes métiers fonctionnent correctement. Ajustements à la paramétrisation.
8	Acceptation	Acceptation affaires du nouveau système.

TESTS DE CERTIFICATION TECHNIQUE		
N°	Nom	Description
6	Performance	Validation des temps de réponse du système.
7	Postes de travail	S'assurer que les postes de travail et les imprimantes fonctionnent bien avec le nouveau système.
9	Redondance	Confirmer le comportement des différentes composantes du système lorsque des pannes d'équipement se produisent. Valider les mesures de redondance en place.
10	Mise en production	S'assurer que le plan de mise en production est complet et exact. Récolter des statistiques sur le processus de mise en production.
11	*Dry Run*	Confirmer que le nouveau système et les données converties fonctionnent normalement dans l'environnement de production.
12	*Sanity*	Validation affaires que l'environnement de production est prêt pour les usagers. Ce test est très court et très ciblé.
13	Relève	Confirmer que le plan de relève en cas de catastrophe fonctionne. Selon le plan de relève en place, peut requérir un site secondaire.
14	Plan de retour en arrière *Fallback*	Tester le retour aux systèmes patrimoniaux advenant que la mise en production ne fonctionne pas.
15	Sécurité et intrusion	Validation de la résistance du système aux attaques de sécurité et aux intrusions.