UNIVERSITÉ DE NANTES
FACULTÉ DE PHARMACIE

ANNÉE 2012 **N° 049**

THÈSE

pour le

DIPLÔME D'ÉTAT

DE DOCTEUR EN PHARMACIE

par

Jean-François Rousseaux

Présentée et soutenue publiquement le 5 juillet 2012

La validation des systèmes informatisés dans l'industrie pharmaceutique réglementation, méthodologie et application au laboratoire de contrôle

Président : **M. Alain PINEAU, Professeur de Toxicologie**

Membres du jury : **M. Frédéric DEHAUT, Pharmacien Responsable**

M. Loïs REYMOND, Chargé de mission

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS **5**

LISTE DES ILLUSTRATIONS ET DES ANNEXES **6**

INTRODUCTION **8**

PARTIE 1 : GÉNÉRALITÉS SUR LA QUALITÉ ET SUR LES SYSTÈMES D'INFORMATIONS DANS L'INDUSTRIE **10**

1.1 LE CONCEPT DE VALIDATION 11
1.1.1 Historique 11
1.1.2 Pourquoi valider ? 12

1.2 LES SYSTÈMES D'INFORMATIONS 14
1.2.1 Le système informatique 14
1.2.2 Un système, « informatisé » 16

1.3 LA RÉGLEMENTATION DE L'INDUSTRIE PHARMACEUTIQUE 18
1.3.1 Les organisations réglementaires 18
1.3.2 Les organisations d'origine institutionnelle 20

1.4 LA RÉGLEMENTATION DES SYSTÈMES INFORMATISÉS 23
1.4.1 Les débuts à partir des années 1980 23
1.4.2 Les BPF européennes : l'annexe 11 25
1.4.3 Les BPF européennes : le chapitre 4 29

1.5 CONCLUSION PARTIE 1 30

PARTIE 2 : LA DÉMARCHE DE VALIDATION DES SYSTÈMES INFORMATISÉS **31**

2.1 PRÉ REQUIS : LE SYSTÈME DE GESTION DE LA QUALITÉ 33
2.1.1 Ses objectifs 34
2.1.2 Ses ressources 34
2.1.3 Au cœur du système : une gestion volontaire 35
2.1.4 Les clés de l'amélioration continue 35

2.2 LE CHOIX D'UNE STRATÉGIE DE VALIDATION 36
2.2.1 La politique qualité de l'entreprise comme point de départ 36
2.2.2 La gestion du risque qualité 38
2.2.3 La gestion de projet 49

2.3 MÉTHODOLOGIE DE LA VALIDATION 54
2.3.1 Le cycle de développement d'un système informatisé 54
2.3.2 Définition du besoin et revues de conception 56
2.3.3 Développement et audit du fournisseur 61
2.3.4 Qualification et maintien de l'état validé 63

PARTIE 3 : VALIDATION D'UN SYSTÈME INFORMATISÉ DE LABORATOIRE 72

3.1 CONTEXTE PROFESSIONNEL DE LA MISSION [35] 74

3.2 PLANIFICATION DE LA VALIDATION 75

3.2.1 Évaluation préalable du système 75

3.2.2 Aperçu de la stratégie de validation du laboratoire 78

3.3 LA VALIDATION DU SYSTÈME INFORMATISÉ DE SPECTROPHOTOMÉTRIE 81

3.3.1 Description du système 81

3.3.2 La SBU 82

3.3.3 La SAT 87

3.3.4 Les tests de qualification 87

3.3.1 Maintien de l'état validé 92

3.4 CONCLUSION PARTIE 3 92

CONCLUSION GÉNÉRALE 93

ANNEXES 94

GLOSSAIRE 107

BIBLIOGRAPHIE 111

Je tiens à exprimer mes remerciements,

À Monsieur Frédéric DEHAUT, Pharmacien Responsable à l'Établissement Français du Sang, je vous remercie d'avoir accepté de diriger ma thèse d'exercice. Je souhaite vous exprimer mon profond respect, et toute ma reconnaissance pour vos précieux conseils qui m'ont guidé au cours de ces années.

À Monsieur Alain PINEAU, Professeur de Toxicologie et Doyen de la faculté de Pharmacie de Nantes, pour l'honneur que vous me faites de présider ce jury de thèse.

À Loïs REYMOND, Chargé de mission aux Laboratoires Chiesi, je te remercie vivement cher confrère et ami, d'avoir accepté de juger la qualité de ce travail.

À mes parents et à mon frère Emmanuel,
Pour vos encouragements et votre soutien tout au long de mes études, je vous dédie cette thèse.

À mes amis, Alexis, Pierre, Romain, Pierre-Jean, Claire et Sharon, d'avoir été là durant toutes ces années, à partager les rires, les doutes, le stress et la joie. Pour tous ces meilleurs moments passés et à venir, je vous remercie du fond du cœur.

À Jessica FOREST, Consultante spécialisée à CVO-Europe, pour ton investissement dans le suivi de mon stage professionnel. « Le gamin » te remercie de lui avoir montré la voie !

LISTE DES ABRÉVIATIONS

API	Automate Programmable Industriel (*Programmable Logic Controller – PLC*)
AQ	Assurance Qualité (*Quality Assurance – QA*)
BPC	Bonnes Pratiques Cliniques (*Good Clinical Practice – GCP*)
BPD	Bonnes Pratiques de Distribution (*Good Distribution Practice – GDP*)
BPF	Bonnes Pratiques de Fabrication (*Good Manufacturing Practice – GMP*)
BPI	Bonnes Pratiques d'Ingénierie (*Good Engineering Practice – GEP*)
BPIT	Bonnes Pratiques Informatiques (*Good IT Practice – GITP*)
BPL	Bonnes Pratiques de Laboratoire (*Good Laboratory Practice – GLP*)
CAPA	*Corrective Actions and Preventive Actions*
COTS	*Commercially available Off-The-Shelf* (logiciel standard du commerce)
cGMP	*current Good Manufacturing Practice*
ERP	*Enterprise Resource Planning* (Progiciel de Gestion Intégrée – PGI)
FAT	Tests d'Acceptation Fournisseur (*Factory Acceptance Testing*)
FDA	*Food and Drug Administration*
FS	Spécifications Fonctionnelles (*Functional Specification*)
GAMP	*Good Automated Manufacturing Practice*
GTC	Gestion Technique Centralisée (*Building Management System – BMS*)
GxP	Bonnes Pratiques (forme générique, où x correspond à : Clinique Distribution Laboratoire ou Fabrication)
HAT	Tests d'acceptation matérielle (*Hardware Acceptance Testing*)
HDS	Spécifications techniques du matériel (*Hardware Design Specification*)
ISPE	*International Society for Pharmaceutical Engineering*
IS/IT	Service Informatique (*Information Solution / Information Technology*)
LIMS	Système de gestion des informations de laboratoire (*Laboratory Information Management System*)
MES	*Manufacturing Execution System*
MRP II	*Manufacturing Resource Planning*
PDA	*Parenteral Drug Association*
PDV	Plan Directeur de Validation (*Validation Master Plan – VMP*)
PICS	*Pharmaceutical Inspection Co-operation Scheme*
PV	Plan de Validation
QC	Qualification de Conception (*Design Qualification – DQ*)
QI	Qualification d'Installation
QO	Qualification Opérationnelle
QP	Qualification de Performance
RV	Rapport de Validation
SAT	Tests d'Acceptation sur Site (*Site Acceptance Testing*)
SBU	Spécification du Besoin Utilisateur (*User Requirement Specification – URS*)
SCADA	*Supervision, Control, and Data Acquisition*
SDS	Spécifications de conception logicielle (*Software Design Specification*)
SLA	Charte de service (*Service Level Agreement*)
SMQ	Système de gestion de la qualité (*Quality Management System*)
SNCC	Système Numérique de Contrôle-Commande (*Digital Control System – DCS*)
SOP	Procédure opérationnelle normalisée (*Standard Operating Procedure*)

LISTE DES ILLUSTRATIONS ET DES ANNEXES

LISTE DES FIGURES

Figure 1 : Schématisation des composants d'un système informatisé dans son environnement opérationnel 17
Figure 2 : les principes d'un Système de Gestion de la Qualité Pharmaceutique 33
Figure 3 : Schéma du processus général de gestion du risque 39
Figure 4 : Méthode d'évaluation et de classification des risques des GAMP 44
Figure 5 : Schématisation des paramètres critiques d'un projet 50
Figure 6 : Exemple de mode d'organisation avec facilitateur 51
Figure 7 : Exemple de mode d'organisation avec coordinateur 52
Figure 8 : Exemple de mode d'organisation matriciel 53
Figure 9 : Application du modèle en V au cycle de vie d'un système informatisé 55
Figure 10 : Enchaînement des étapes de qualification 64
Figure 11 : Schématisation du déroulement classique des phases de qualification 65
Figure 12 : Extrait du support de formation - Chargé de Qualification / Validation 77
Figure 13 : résumé des étapes de la validation du système informatisé de spectrophotométrie avec les acteurs et les documents attendus 80
Figure 14 : Le système informatique : PC de laboratoire avec son spectrophotomètre 81
Figure 15 : SBU 2.0 – Les trois types de profil utilisateur définis par l'utilisateur 82
Figure 16 : SBU 2.0 – Les paramètres critiques du logiciel Spectra Manager CFR® 82
Figure 17 : SBU 2.0 – Spectrophotomètre V-630 (extraits) 83
Figure 18 : SBU 2.0 – Documentation 84
Figure 19 : SBU 2.0 – Partie logicielle ; les enregistrements électroniques 84
Figure 20 : SBU 2.0 – Partie logicielle ; les données d'entrée (extrait) 85
Figure 21 : SBU 2.0 – Partie logicielle ; les données en sortie (extrait) 85
Figure 22 : SBU 2.0 – Partie logicielle ; les niveaux d'accès (extraits) 86
Figure 23 : SBU 2.0 – Partie logicielle ; l'audit trail (extrait) 86
Figure 24 : PQ – Liste des fiches de tests de qualification d'installation (extrait) 87
Figure 25 : PQ – FPG : les prérequis généraux à la qualification opérationnelle (extrait) . 88
Figure 26 : PQ – FVD : la vérification documentaire 89
Figure 27 : PQ – FQO03 : gestion des comptes utilisateurs, annexe de traçabilité 90
Figure 28 : Rapport – FQO04 : test de déconnexion automatique 91
Figure 29 : Rapport – FQO10 : vérification de l'audit trail (extrait) 91
Figure 30 : PQ – Liste des fiches de tests de qualification de performance 92

LISTE DES TABLEAUX

Tableau I : Les principaux faits historiques de la réglementation des systèmes informatisés dans le monde 23
Tableau II : Exemples d'analyse des scénarios à risque 43
Tableau III : Exemples d'exigences de spécification utilisateur (URS) 57
Tableau IV : Exemples d'exigences de spécifications fonctionnelles (FS) 59
Tableau V : Matrice de choix de la qualification après évaluation des risques 75
Tableau VI : les relations entre l'évaluation de criticité / complexité des systèmes informatisés et les étapes de validation 76

LISTE DES ANNEXES

Annexe 1 : les BPF Européennes - Annexe 11 - Version 1992 95
Annexe 2 : les BPF Européennes - Annexe 11 - Version 2011 97
Annexe 3 : Formulaire d'évaluation de la criticité et de la complexité des systèmes 101
Annexe 4 : Liste des fiches de tests de qualification opérationnelle 103
Annexe 5 : Fiche d'anomalie n°1 105
Annexe 6 : Fiche de tests de qualification de performance : documents d'exploitation ... 106

INTRODUCTION

C’est à partir des années 1970, avec l’arrivée du microprocesseur sur le marché que l’outil informatique s’est développé à très grande échelle. La production et la distribution massive de cette nouvelle technologie ont permis aux entreprises de progresser dans tous les secteurs industriels. D’une année sur l’autre, l’accroissement constant de cette nouvelle puissance de calcul n’a cessé de repousser les limites de l’automatisation des procédés industriels. L’informatique a révolutionné notre quotidien et celui des grandes organisations, au point d’être aujourd’hui indispensable à n’importe quelle opération. Pour les industries réglementées, auxquelles appartiennent les établissements pharmaceutiques, se pose la question de la maîtrise de cet outil si habituel : permet-il vraiment d’assurer la qualité des médicaments produits ?

Parallèlement à cette informatisation progressive des industries, de nombreuses organisations compétentes dans le domaine de l’assurance de la qualité sont apparues au cours de ces dernières années. De nombreux guides, référentiels et standards applicables au secteur de la santé furent publiés dans le but de garantir la sécurité du médicament donc du patient. C’est pourquoi aujourd’hui tout établissement pharmaceutique est tenu de respecter un certain nombre de Bonnes Pratiques, permettant d’assurer la qualité des médicaments. Le champ d'application ne se limite pas à la seule fabrication des médicaments mais est aussi valable en recherche et développement, pour les essais cliniques, pour la distribution et pour tout ce qui impacte sur la sécurité du patient et sur la qualité du médicament.

Les technologies industrielles et les exigences réglementaires évolueront toujours ensemble, comme les deux faces d’une même pièce, ainsi le développement perpétuel de l’informatique associé à sa banalisation dans le paysage industriel a placé la validation des systèmes informatisés au cœur des préoccupations industrielles et réglementaires.

En janvier 2011, la réglementation européenne concernant les systèmes informatisés dans l'industrie pharmaceutique a évolué. Ayant eu l'opportunité de réaliser la validation d'un système informatisé de laboratoire durant mon stage professionnel, cette thèse est pour moi l'occasion de rassembler mes connaissances et d'apporter, à la hauteur de mes compétences, pour mes actuels et futurs confrères Pharmaciens, un regard neuf sur la validation de ces systèmes.

Nous commencerons l'exercice par une présentation générale des concepts de validation et de système d'information. Après avoir retracé l'historique de la réglementation des systèmes informatisés, nous examinerons les nouvelles dispositions introduites en 2011.

Dans une deuxième partie, nous aborderons en détail l'organisation adoptée par les établissements pharmaceutiques pour définir leur stratégie de validation, et nous présenterons la méthodologie adaptée à ce type de projet.

Enfin, nous illustrerons notre analyse réglementaire et méthodologique de la validation des systèmes informatisés par l'étude d'une application pratique. La démarche de validation proposée est issue d'une unité de recherche et de développement pharmaceutique du groupe Sanofi Pasteur.

- PREMIÈRE PARTIE -
GÉNÉRALITÉS SUR LA QUALITÉ ET SUR LES SYSTÈMES D'INFORMATIONS DANS L'INDUSTRIE

1.1 LE CONCEPT DE VALIDATION

1.1.1 Historique

C'est dans les années 1970 que le terme de validation a été proposé pour la première fois, par Ted BYERS et Bud LOFTUS, deux représentants de la *Food and Drug Administration* (FDA), afin d'améliorer la qualité des produits pharmaceutiques. Lors de la révision des *current Good Manufacturing Practice*[1] (cGMP) en 1978, le terme s'appliquait uniquement au procédé de stérilisation. Les premières activités de validation ont donc concerné les processus de production de médicaments dédiés à l'usage parentéral, puis se sont rapidement étendues au contrôle de l'environnement, à la désinfection des équipements et à la production d'eau purifiée. À partir du début des années 1980, la FDA a porté son attention sur la validation de procédés non stérilisants. [1]

En 1987, un guide de la FDA dédié à la validation des procédés définit la validation comme étant « l'établissement de la preuve documentée fournissant avec un haut degré d'assurance qu'un processus spécifique est capable de produire invariablement à un certain niveau de qualité, un produit conforme à ses spécifications préétablies » [2]. Cette exigence a englobé les systèmes informatisés utilisés dans l'industrie du médicament et des dispositifs médicaux, au fur et à mesure qu'ils s'imposaient comme outils indispensables à toute opération de développement et de production. Aujourd'hui, la définition de la validation prend donc en compte l'environnement opérationnel du système.

Ainsi, nous définissons la validation comme l'établissement de la **preuve documentée** démontrant avec une **forte assurance** qu'un système va **fonctionner invariablement** selon les **exigences préétablies** dans **l'environnement opérationnel prévu**.

[1] Les Bonnes Pratiques de Fabrication américaines

1.1.2 Pourquoi valider ?

La validation des procédés, des systèmes et des méthodes apporte bien des avantages aux industriels, en augmentant la connaissance et la fiabilité de leurs outils de travail. L'objectif le plus important est de protéger la santé humaine ; non seulement celle des patients consommateurs du produit thérapeutique fabriqué, mais aussi le personnel de l'établissement de santé utilisant des systèmes parfois dangereux. Bien souvent par le passé, l'introduction de nouvelles technologies s'est faite au détriment de la sécurité des usagers. Car le risque potentiel lié à l'utilisation de systèmes informatisés dans les établissements de santé n'a pas toujours été bien évalué. La prise de conscience sur la nécessité de valider les systèmes informatisés s'est faite en réponse à la survenue d'accidents majeurs les impliquant directement.

L'accident du Therac-25 en 1985 en est un très bon exemple [3]. Therac-25 était le nom d'un système informatique de radiothérapie basé sur l'accélération des électrons. Développée conjointement par l'*Atomic Energy of Canada Limited* (AECL) et l'entreprise française CGR MeV, il s'agissait d'une évolution des modèles Therac-6 et Therac-20. Entre 1985 et 1987, le Therac-25 a été impliqué dans 6 accidents connus, incluant 3 décès directement attribuables à des surdoses de radiation. La cause directe du dysfonctionnement était d'ordre informatique. Plusieurs problèmes importants ont été identifiés, parmi lesquels :

- L'AECL ne disposait pas d'un organisme indépendant pour l'évaluation du code source et avait négligé certaines étapes liées au test du logiciel.
- La documentation du système n'expliquait pas de manière adéquate les codes indiquant des erreurs.
- La machine ne possédait pas de dispositif physique pour bloquer le flux d'électrons en mode « haute énergie » en cas de mauvaise utilisation. La sécurité, à ce niveau, reposait ainsi uniquement sur le logiciel.
- Les ingénieurs avaient réutilisé des morceaux de code provenant des modèles précédent, or ces modèles possédaient des sécurités physiques et n'étaient donc pas autant vulnérables aux erreurs logicielles.

Si une véritable stratégie de validation avait été conduite en amont, l'accident n'aurait pas eu lieu. La première édition des BPF européennes est sortie quatre ans après cet épisode tragique.

Les BPF stipulent que le Pharmacien Responsable de tout établissement pharmaceutique à en charge de s'assurer que tout système informatisé aidant à la réalisation d'un acte pharmaceutique réglementé a fait l'objet d'une validation documentée, afin que cet acte soit sécurisé. En effet ces systèmes produisent, traitent et stockent des informations pouvant avoir un impact critique sur la qualité du médicament tout au long de son cycle de vie (fabrication, distribution, essais cliniques, etc.).

L'industrie pharmaceutique a pour vocation à participer à l'amélioration du niveau de santé publique. Or dans un système capitaliste, l'objectif principal de toute entreprise reste de générer du profit. La découverte, la mise en place et l'exploitation efficace des innovations technologiques sont au cœur de la compétitivité des entreprises. C'est pourquoi la validation des systèmes informatisés trouve aussi des justifications technico-économiques :

- bien comprendre le fonctionnement du système avant son exploitation,
- optimiser son rendement, ses performances,
- identifier ses faiblesses et prendre les mesures correctives nécessaires,
- faciliter l'adhésion et l'appropriation du système par ses futurs utilisateurs.

En pratique, cela peut se traduire par une baisse du taux de non-conformités en production, par la diminution du nombre de rappels de lots, et bien évidemment par la satisfaction des autorités réglementaires.

1.2 LES SYSTÈMES D'INFORMATIONS

L'informatique est la science du traitement de l'information. On utilise traditionnellement les termes de systèmes d'information ou technologies de l'information qui sont les traductions de l'anglais *information technology* (IT). Ces expressions présentent l'intérêt de bien différencier l'informatique proprement dite, d'activités qui y sont souvent rattachées comme la programmation ou la bureautique [4]. Il est primordial de bien définir tous les éléments qui composent un système informatisé. Nous commencerons par le système informatique.

1.2.1 Le système informatique

La complexité des systèmes varie selon leur taille, leur fonction et leur place dans l'organisation de l'entreprise. Néanmoins, la technologie informatique se caractérise toujours par la combinaison d'une partie matérielle (*hardware*) et d'une partie logicielle (*software)*. On entend par matériel « l'ensemble des éléments physiques employés pour le traitement de l'information (dispositifs d'entrées-sorties, organes de liaison, mémoires, circuits de traitement) » [5], par opposition au logiciel qui est « l'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données » [6]. Pour faire fonctionner un système informatique, deux types de logiciels sont nécessaires.

1.2.1.1 *Les logiciels systèmes*

Ils sont conçus pour piloter la partie matérielle afin de fournir les ressources nécessaires au fonctionnement des logiciels applicatifs. On retrouve dans cette catégorie les *drivers*, *firmware* et un ensemble d'outils et de services constituant le système d'exploitation [7]. Il est important de comprendre qu'un système d'exploitation (tel que Windows®) n'est pas qu'une simple interface graphique destinée à faciliter l'utilisation des applicatifs. C'est en premier lieu le centre de gestion de la compatibilité des équipements, dont il faudra maîtriser la configuration.

1.2.1.2 *Les logiciels applicatifs*

Ce sont les plus courants et les plus connus. « Aussi appelés applications informatiques, leurs automatismes permettent d'assister l'utilisateur dans une activité spécifique » [8]. Le développement de logiciels applicatifs « personnalisés » peut être réalisé en interne, ou sous-traité à un développeur spécialisé. Mais la plupart du temps, des logiciels couvrant les principaux besoins des entreprises existent déjà sur le marché. Ce type de logiciel est souvent désigné par l'appellation « COTS » pour *Commercially available Off-The-Shelf* (logiciel disponible sur le marché). Ces logiciels doivent généralement faire l'objet d'une configuration appropriée pour satisfaire les exigences de l'utilisateur ; c'est pourquoi on parle parfois de progiciel. Bien sûr, il en va de la responsabilité de l'entreprise de vérifier que ces logiciels sont développés selon un système de gestion de la qualité adéquat et qu'ils subissent une validation avec succès.

Nous aborderons en détail la classification des logiciels dans la deuxième partie. Néanmoins, on peut dès à présent noter que dans un établissement pharmaceutique, on trouvera :

- des progiciels non configurés, représentant la très grande majorité des logiciels couramment utilisés dans les domaines non réglementés [9]. Exemples : Microsoft Office®, logiciels d'acquisition de données, de modélisation, de statistiques…
- des progiciels configurés, fonctionnant selon des paramètres définis et verrouillés. Exemple : un système informatique de gestion de laboratoire (LIMS) ou un progiciel de gestion intégré (ERP), qui facilite le fonctionnement de l'entreprise en intégrant tous les services de celle-ci (SAP®, Oracle®)
- des logiciels personnalisés que l'on ne retrouvera pas sur le marché, développés sur mesure (en interne ou en sous-traitance) pour répondre à un besoin spécifique et inédit.

En résumé le **système informatique** est un ensemble d'éléments en interaction comprenant des **matériels** informatiques (unités centrales, écrans, imprimantes, câblages…) et des **logiciels** (applications, base de données, feuilles Excel®…). La complexité du système informatique (notamment de la partie logicielle) aura un impact très important sur la stratégie de validation.

1.2.2 Un système, « informatisé »

Pour bien comprendre le concept, il faut revenir à la définition d'un « système ». On entend par système « un ensemble d'éléments humains et matériels en interdépendance les uns les autres, et qui interagissent à l'intérieur de frontières, ouvertes ou non à un environnement défini. Les éléments matériels sont composés de sous-ensembles de technologies variées : mécanique, électrique, électronique, informatique, réseaux de communication, etc. » [33]. Donc *a priori*, un système informatisé est simplement un système possédant au moins un sous-ensemble informatique.

Depuis 1995, la FDA définit dans son glossaire les systèmes informatisés de la façon suivante :

« **Système informatisé**. Comprend les matériels, les logiciels, les équipements périphériques, le personnel et la documentation ; par exemple, les manuels et les procédures opérationnelles normalisées » [10].

Dans les BPF européennes, la définition est restée plus limitée :

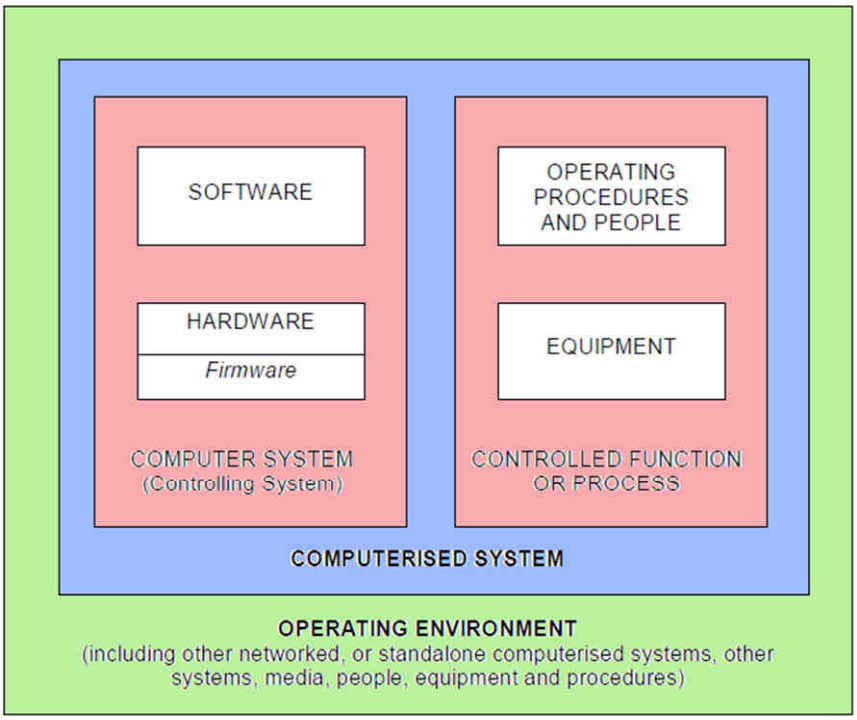
« Un système informatisé est l'association de matériels et de logiciels qui remplissent ensemble certaines fonctionnalités » [11].

Stricto sensu, il ne s'agit que de traiter les matériels et les logiciels. Mais en réalité, les processus opérationnels qu'ils supportent sont réglementés par les autres chapitres correspondants (ex. : la Production par le chapitre 5).

Enfin, le guide du PICS[2] intitulé « La validation des systèmes informatisés dans les environnements GxP[3] » est une référence internationale en la matière, et en donne une définition complète, illustrée par la figure suivante.

[2] *Pharmaceutical Inspection Cooperation Scheme*, sera traité au paragraphe § 1.3.2.1.
[3] Forme anglaise pour les Bonnes Pratiques de Fabrication, de Laboratoire, de Distribution et Clinique.

Figure 1 : Schématisation des composants d'un système informatisé dans son environnement opérationnel



Sources in Good Practices for Computerised Systems in Regulated « GXP » Environments (PICS)

Il est donc clairement établi qu'un **système informatisé** est un système informatique dont l'utilisation est intégrée à l'environnement opérationnel (les autres systèmes, le personnel, les équipements, le système documentaire, etc.). On comprend que si les futurs utilisateurs du système ne sont pas impliqués dans son élaboration puis dans sa validation, le système aura peu de chance de fonctionner correctement. Il en va de même concernant l'élaboration des procédures (documents de travail) et la qualification des équipements liés.

L'environnement opérationnel s'étend aux locaux, équipements, documentation de travail et personnels chargés de la maintenance informatique de l'entreprise (service IS/IT). La plateforme réseau de l'entreprise doit permettre d'assurer la bonne exploitation, la sécurité et la fiabilité du nouveau système informatisé. Sa validation est réalisée en amont et est indépendante des nouveaux systèmes à implémenter.

1.3 LA RÉGLEMENTATION DE L'INDUSTRIE PHARMACEUTIQUE

1.3.1 Les organisations réglementaires

Durant le 20ème siècle, les principaux pays développés, inquiets de la sécurité d'utilisation des médicaments et autres produits de santé, ont répondu par la création d'une autorité nationale dédiée à la sécurité et au contrôle des médicaments.

Entre les années 1960 et 1985, chaque pays fonctionnait selon ses propres règles de fabrication, d'essai thérapeutique ou de distribution et ce, que le médicament soit destiné au marché national ou non. À partir de 1985, les nations ont peu à peu compris que la mondialisation des échanges rendait nécessaire l'internationalisation des réglementations. Depuis nous assistons à ce mouvement qui se heurte encore à quelques difficultés liées aux différences culturelles et au manque d'harmonisation (que les conférences d'harmonisation de l'ICH[4] tendent de gommer).

En attendant l'harmonisation complète des réglementations à l'internationale, tout établissement doit appliquer la réglementation en vigueur dans le pays destinataire du médicament fabriqué. Les réglementations édictées par les organisations présentées ci-dessous sont les plus importantes à prendre en compte pour un établissement pharmaceutique français.

1.3.1.1 *La FDA*

Aux États-Unis d'Amérique, la *Food and Drug Administration* est l'agence du ministère de la Santé responsable de la protection des consommateurs de produits alimentaires et médicamenteux. Ses origines remontent au « Bureau des brevets » autour de 1848. Avant, il n'existait aucune loi fédérale, ni réglementation protégeant les consommateurs des substances pouvant présenter des risques, dans les médicaments ou les aliments. L'activité était à l'époque entièrement dédiée à l'analyse chimique des produits agricoles. C'est à partir de l'année 1930 que l'organisme hérita de son nom actuel, pour assurer les fonctions de réglementation des aliments puis des médicaments. [13]

[4] Conférence Internationale pour l'Harmonisation

En 1962, le Congrès des États-Unis a chargé la FDA de s'assurer que tous les médicaments produits le soient conformément à des « Bonnes Pratiques de Fabrication » [37]. Depuis, les « *current Good Manufacturing Practices* » (cGMP) désignent la version la plus actuelle des BPF américaines, la plus en phase avec l'évolution des technologies et des standards de qualité. Les cGMP sont généralement considérées comme le standard de qualité le plus avancé dans le monde.

1.3.1.2 *L'AFSSAPS ou ANSM*

L'Agence Française de Sécurité Sanitaire des Produits de Santé est un établissement public français, dont la mission principale est d'évaluer les risques sanitaires présentés par les médicaments et plus généralement tous les produits de santé destinés à l'homme. Crée en 1998 sur les bases de l'ancienne Agence du médicament, « elle est remplacée par l'Agence Nationale de Sécurité du Médicament (ANSM) suite à l'adoption d'un projet de loi visant à réformer le contrôle des médicaments. » [14]

L'ANSM édite le référentiel français des Bonnes Pratiques de Fabrication (BPF), référentiel qualité opposable lors de ses inspections. Les deux premières éditions des BPF datent respectivement de 1978 et de 1985, et leur contenu était intégralement d'origine française. C'est à partir de la troisième édition, en 1992, que la mise à jour du texte **intégrera les dispositions du référentiel européen**. La dernière édition des BPF françaises à été révisée en 2011. L'ANSM est membre de la PICS.

1.3.1.3 *La Commission européenne*

Instituée en 1957, la Commission européenne est l'une des principales institutions de l'Union européenne. Elle est composée d'un commissaire par État membre. Sa principale fonction est de « proposer et de mettre en œuvre les politiques communautaires, garant de l'intérêt général de l'Union européenne » [15]. C'est pourquoi elle vote les Directives européennes et édite en conséquence les **BPF européennes**. La Commission agit indépendamment des gouvernements des États membres.

L'ensemble de la législation de l'Union européenne applicable au secteur pharmaceutique est compilé en une série de textes (une dizaine de volumes indépendants). Parmi ces textes figurent une majorité de lignes directrices. Le volume 4 « Lignes

directrices des Bonnes Pratiques de Fabrication pour les médicaments à usage humain ou vétérinaire » consacre un long chapitre aux systèmes informatisés.

La première édition des BPF européennes a été publiée en 1989. Cette première édition était en fait une copie exacte du guide de la PIC. En réponse à la directive européenne 91/356/CEE, une seconde édition a vu le jour en 1992, incluant 12 annexes. Par la suite, le texte a subi de nombreuses modifications jusqu'à devenir la version de janvier 2011 actuellement en vigueur. [16]

1.3.2 Les organisations d'origine institutionnelle

1.3.2.1 *Le PICS [17] [18]*

Le *Pharmaceutical Inspection Cooperation Scheme* (PICS) est un système de coopération en matière d'inspection des produits pharmaceutiques. Son origine réside dans la Convention pour l'Inspection Pharmaceutique (PIC) fondée en octobre 1970 dans le cadre de l'Association européenne de Libre Échange (AELE) dont le siège est situé à Genève. À l'époque, dix pays se sont associés pour créer cette Convention. Il s'agissait là d'un traité international entre États dont les principaux buts étaient :

- l'harmonisation des règles concernant les Bonnes Pratiques de Fabrication,
- la mise en place de systèmes d'inspection harmonisés,
- la reconnaissance mutuelle des rapports d'inspection,
- la formation des inspecteurs.

Le PICS est doté d'un système documentaire étoffé devant être utilisé par les autorités compétentes qui le composent. Il est important de savoir que le PICS **n'émet que des recommandations** (à la différence de la Commission européenne) et il appartient à ses membres de les intégrer dans leur propre législation.

Le PICS assure la formation des inspecteurs à l'aide de séminaires, de cercles d'experts et d'inspections conjointes. Le but est d'assurer l'interprétation des BPF ainsi que de définir les besoins en terme d'harmonisation ou de formation. Des ateliers sont ainsi menés en collaboration avec des associations de professionnels de l'industrie pharmaceutique.

Aujourd'hui, le PICS est une association de 40 autorités compétentes, dont l'Agence Française fait partie. Ses relations extérieures sont bien développées : l'EMA participe au Comité des officiels, et des échanges formels existent avec la Commission européenne. Le PICS a aussi conclu un accord de coopération avec le Département européen pour la Qualité des Médicaments (EDQM). Des relations étroites existent aussi depuis très longtemps avec deux départements de l'Organisation Mondiale de la Santé (OMS). Dans tous ces cas, il s'agit de bâtir des synergies, dans les domaines de compétence du PICS, afin d'éviter la redondance des actions et les déperditions de ressources.

1.3.2.2 *L'OMS*

L'Organisation Mondiale de la Santé, fondée en 1948, est une institution spécialisée de l'Organisation des Nations Unies pour la santé publique. Selon sa constitution, l'OMS a pour objectif d'amener tous les peuples du monde au niveau de santé le plus élevé possible. Membre partenaire du PICS, elle édite son propre guide des Bonnes Pratiques de Fabrication et d'Inspection pour le compte des pays en voie de développement. [19]

1.3.2.3 *Le Forum GAMP [20] [21]*

En 1991 au Royaume-Uni, un groupe d'experts le *Computer System forum* a été fondé par des professionnels de l'industrie, pour répondre au besoin de ces industries d'améliorer leur compréhension des exigences des autorités réglementaires en Europe. À présent connu sous le nom de Forum GAMP[5], ce groupe est désormais un comité technique de l'*International Society for Pharmaceutical Engineering* (ISPE).

Une des priorités du Forum GAMP a été d'établir un guide à l'usage des **fournisseurs de systèmes automatisés** à destination de **l'industrie pharmaceutique**. Ce guide prenait en compte les exigences des autorités réglementaires tant européennes qu'américaines et utilisait les standards internationalement reconnus. Cette première ébauche fût mise à disposition des fournisseurs en 1994. Les versions suivantes ont vu l'intégration d'une nouvelle partie à l'usage **des utilisateurs** de ces systèmes automatisés et informatisés. Au fur et à mesure de ses mises à jour, le guide des GAMP est rapidement

[5] « *Good Automated Manufacturing Practice* » ; les Bonnes Pratiques de Fabrication Automatisée

devenu la référence internationale pour traiter des questions de **validation** des systèmes informatisés et automatisés, car il permet de réconcilier les deux protagonistes essentiels (l'industriel et le fournisseur) autour de celle-ci. Depuis mars 2008, c'est la version 5 du guide qui est en vigueur.

1.3.2.4 *L'ICH [22]*

L'ICH est la « Conférence Internationale pour l'Harmonisation des exigences techniques pour l'enregistrement des produits pharmaceutiques à usage humain ». Elle fût fondée en 1989 en vue d'harmoniser le contrôle des médicaments entre l'Union européenne, les États-Unis et le Japon. Son objectif principal est de réduire le coût global de la recherche pharmaceutique dans le monde en évitant la duplication de travaux, comme la préparation des dossiers et des études, et ainsi accélérer la mise à disposition des médicaments innovants. Cette conférence, qui se tient deux fois par an, est organisée alternativement en Europe, au Japon et aux États-Unis.

1.4 LA RÉGLEMENTATION DES SYSTÈMES INFORMATISÉS

1.4.1 Les débuts à partir des années 1980

La prise de conscience des risques liés à l'utilisation des systèmes informatisés dans les activités règlementées a été progressive. L'explication réside dans l'inégale distribution de la technologie de l'information dans les industries, au départ très coûteuse et donc moins rentable. C'est aux États-Unis que les premières réflexions sur le sujet ont été menées. Le tableau suivant reprend les principaux faits historiques de la réglementation de ces systèmes.

Tableau I : Les principaux faits historiques de la réglementation des systèmes informatisés dans le monde

Date	Événement
1983	la FDA publie un guide pour l'inspection des systèmes informatisés utilisés dans un processus pharmaceutique, aussi appelé le « livre bleu ». Il rassemblait l'ensemble des dispositions présentes dans les cGMP applicables à la technologie de l'information [23].
1978 1985	Première édition des BPF Françaises en 1978, seconde édition en 1985. Il existe déjà une Ligne Directrice (n°5) abordant la question des systèmes informatisés.
1992	la validation des systèmes informatisés fait l'objet d'une **annexe spécifique** (n°**11**) des **BPF européennes**. À partir de cette date, la validation des systèmes informatisés est obligatoire dans l'Union européenne.
1994	la première édition du guide des GAMP est publiée.
1997	la FDA publie le célèbre article du code fédéral « 21CFR Part 11 » qui spécifie comment doivent être gérées les données électroniques, ainsi que les signatures électroniques [24]. Par la suite, un guide d'aide à son application a été publié, en 2003.
1999	Le monde entier redoute le *bug* présumé de « l'an 2000 ». Le passage informatique à l'an 2000 a suscité de sérieuses inquiétudes à cause d'un problème portant sur le format des dates dans les mémoires des ordinateurs. Dans de nombreux programmes et bases de données, il manquait le chiffre « 19 » correspondant au siècle. Donc le passage de 1999 à 2000 (en réalité de « 99 » à « 00 ») devait produire de nombreux dysfonctionnements dans le traitement des informations.
2002	La FDA publie un guide sur les principes généraux de la validation logicielle.
2004	De la même façon que le « livre bleu » américain de 1983, le PICS a publié cette année-là le guide des « Bonnes Pratiques d'Utilisation des Systèmes Informatisés dans les environnements GxP ». Ce document aide les inspecteurs des autorités internationales membres. La version en vigueur date de 2007.
2005	L'ICH publie le guide **Q9** sur **la Gestion des Risques**, qui sera internationalement adopté par les autorités réglementaires en 2006 et inséré dans leurs BPF.
2008	Publication de la dernière version en date du guide des **GAMP**

Janv. 2011	Mise à jour de **l'annexe 11 des BPF européennes** sur les systèmes informatisés, et du chapitre 4 sur la documentation, actualisé pour intégrer la gestion électronique des documents.
Juin 2011	**Entrée en application** de la nouvelle version des BPF européennes.

Le guide des BPF européennes (et son annexe relative aux systèmes informatisés) est donc notre référentiel depuis 1992, prenant l'ascendant sur notre référentiel français. Toutefois à la fin du 20ème siècle, les systèmes informatisés ont fait l'objet d'un niveau d'attention plus volatile que les systèmes traditionnels. Les attentes des inspecteurs sur le terrain lors des inspections réglementaires étaient variables. Ces systèmes n'étaient pas très bien maîtrisés, car les risques potentiels engendrés par leur utilisation étaient encore mal connus. « Les mises en demeure réglementaires ont été peu fréquentes. » [25]

L'inquiétude mondiale autour du phénomène de « l'an 2000 »[6] ne manqua pas de faire l'objet de surenchérissement en termes d'attentes. Le début du 21ème siècle a connu une période de stabilisation et de maturation. Puis l'utilisation des systèmes informatisés s'est généralisée, mettant en œuvre des systèmes toujours plus complexes et augmentant la méconnaissance des risques. En fait, les « vrais » risques ne sont plus là où ils étaient.

C'est pourquoi vingt ans après sa première publication, l'annexe 11 des BPF européennes vient d'être mise à jour. Largement réorganisé et partiellement réécrit, le document finalisé a été publié le 12 janvier 2011 pour une mise en application au 30 juin 2011. Sa traduction dans les BPF françaises n'a pas encore été réalisée. De plus, quelques ajouts ont été apportés au chapitre 4 des BPF concernant la gestion de la documentation, pour alignement avec la nouvelle annexe 11.

[6] Cette erreur a nécessité de revoir en profondeur l'architecture des systèmes d'information, et des systèmes entiers furent remplacés par anticipation. Finalement, aucun problème critique ne s'est produit, mais des sommes considérables chiffrées en centaines de milliards de dollars dans le monde ont dû être dépensées pour prévenir tout incident [26].
N.B. Il est intéressant de remarquer que ce « bogue de l'an 2000 » n'en ait pas vraiment un : c'est en réalité la conséquence d'une erreur de conception ! Cet événement historique illustre parfaitement bien l'extrême importance de la phase de conception des projets et des systèmes.

1.4.2 Les BPF européennes : l'annexe 11

1.4.2.1 *Aperçu*

La nouvelle version de l'annexe 11 adopte une approche basée sur **la gestion des risques**, méthode qui s'est généralisée dans les établissements pharmaceutiques depuis l'intégration du guide **ICH Q9** dans les BPF en 2006. La nouvelle structure du document est découpée en un principe suivi de trois rubriques : les « généralités », la « phase projet », et la « phase opérationnelle ». La comparaison des deux versions[7] permet de mettre en évidence les évolutions réglementaires.

1.4.2.2 *Principe*

Le principe général de l'annexe 11 reste le même, à savoir que « lorsqu'un système informatisé remplace une opération manuelle, il ne faut pas que la qualité du produit ou l'assurance de la qualité en soit affectée » [11]. Alors qu'avant les systèmes informatisés étaient souvent mis en place pour améliorer ou remplacer une opération manuelle, aujourd'hui leur utilisation est anticipée à chaque lancement d'un nouveau projet industriel. C'est pourquoi la version de 2011 souligne ensuite qu'« il ne devrait y avoir aucune augmentation du risque global de défaillance du processus ».

1.4.2.3 *Les généralités – Gestion des risques, du personnel et des tiers*

« La **gestion des risques** doit être mise en œuvre **tout au long du cycle de vie** du système informatisé en prenant en considération la **sécurité du patient**, **l'intégrité des données** et la **qualité du produit**. Dans le cadre du système de gestion des risques, les décisions relatives à l'étendue de la validation et aux contrôles d'intégrité des données doivent être basées sur une évaluation justifiée et documentée des risques liés au système informatisé » [11]. C'est pourquoi le guide ICH Q9 concernant la gestion des risques a été intégré aux BPF européennes (ancienne annexe 20). Ce guide permet de comprendre les principes fondamentaux de la gestion des risques, afin de mettre au point une méthode adaptée au projet. En conséquence, la conception du système (matériels, fonctionnalités des logiciels) sera optimale, et l'étendue de la validation (identification des paramètres « critiques », complexité des tests…) sera déterminée plus efficacement.

[7] Disponibles en Annexe 1 et Annexe 2.

La partie concernant **le personnel** n'a pas vraiment changé sur le fond. Elle est seulement plus précise dans l'identification des rôles clés impliqués dans la gestion des systèmes informatisés : un « responsable du processus », un « responsable du système », du « personnel qualifié » et un « service informatique ». L'ensemble du personnel doit travailler en étroite collaboration.

La partie concernant **la gestion des tiers** (fournisseurs et prestataires de services) s'est beaucoup étendue par rapport au petit paragraphe 18 de l'ancienne version. Il stipule notamment, en plus de l'établissement d'un accord sur le partage des responsabilités, la nécessité d'auditer les fournisseurs, encore une fois sur la base d'une évaluation des risques ; et la documentation de ces audits doit être disponible à l'inspection.

1.4.2.4 *La « phase projet » - Validation*

L'ancien paragraphe sur la validation a été considérablement étendu dans la nouvelle version, et compose l'intégralité de cette nouvelle « phase projet ». Les nouvelles dispositions stipulent de tenir à jour un inventaire de tous les systèmes informatisés utilisés en fonction de leur niveau de risque. Les systèmes « critiques » ou à haut niveau de risque doivent faire l'objet d'une documentation détaillée incluant une description physique et logique, les flux de données associés et les interfaces avec les autres systèmes ou processus. Les autres ajouts consistent en l'obligation :

- d'assurer que tout système a été développé en accord avec un **Système de Gestion de la Qualité** (SMQ).
- d'assurer **la traçabilité des spécifications** du besoin de l'utilisateur tout au long du cycle de vie du système ; encore une fois, ces spécifications doivent être basées sur une évaluation documentée des risques
- de contrôler les changements en cours de validation, notamment par l'enregistrement des déviations observées
- prouver la robustesse du système et sa capacité à protéger l'**intégrité de ses fonctions et de ses données** contre une utilisation inappropriée. Les méthodes de test utilisées au cours de la validation doivent être appropriées.

1.4.2.5 *La « phase opérationnelle »*

De nombreux paragraphes de l'ancienne version (particulièrement de 8 à 17) ont été modifiés, améliorés et regroupés sous cette nouvelle rubrique nommée « phase opérationnelle ». Les dispositions de cette rubrique concernent les exigences réglementaires à prendre en compte pour la conception du fonctionnement opérationnel des systèmes. Elles concernent la gestion :

- des données électroniques (méthode d'entrée, transfert, vérification, stockage, sauvegarde),
- des impressions,
- de l'audit trail[8],
- des changements et de la configuration,
- de la sécurité
- de la libération de lot de produit
- des mesures de remplacement en cas de panne.

Les principales modifications propres à chacune de ces clauses consistent en un renforcement des exigences réglementaires pour les paramètres critiques. L'utilisateur doit donc les identifier dès que nécessaire au moyen d'une évaluation des risques. Quatre nouvelles sections ont été créées. Elles concernent :

- l'évaluation périodique des systèmes
- la gestion des incidents
- la gestion des signatures électroniques
- l'archivage des données.

L'évaluation périodique des systèmes informatisés permet de s'assurer qu'ils demeurent en état validé et sont conformes aux BPF. Cette évaluation doit inclure, le cas échéant, l'étendue actuelle des fonctionnalités, les enregistrements de déviation et d'incident, l'historique de mise à jour, les rapports de performance, de fiabilité, de sécurité et de validation ». Cette nouvelle section illustre bien le souhait des autorités de renforcer le concept de **cycle de vie** des systèmes : le travail de validation ne s'arrête qu'à la fin de leur exploitation.

[8] C'est un enregistrement de l'utilisation des ressources du système informatique. Il doit enregistrer tous les accès aux données ayant un impact qualité : identification de l'utilisateur, la création / modification / suppression de données avec la date, l'heure et le motif. Cet enregistrement est la « boîte noire » du système informatique.

Le paragraphe concernant la gestion des incidents rend obligatoire l'établissement de rapports d'erreurs et de leurs évaluations. Ces rapports doivent contenir la liste exhaustive de tous les problèmes, erreurs et défauts rencontrés, mais l'analyse des causes en vue d'un CAPA[9] peut se limiter aux incidents identifiés comme « critiques ».

Depuis 1997 avec la publication du « 21 CFR Part 11 », la FDA était la seule autorité à encadrer la gestion des enregistrements et signatures électroniques. Mais la Gestion Électronique des Documents (GED) s'est considérablement développée ces dernières années avec le développement de logiciels très performants. Le gain pour les entreprises en terme de gestion est conséquent (élaboration, classement, stockage, diffusion, etc.). C'est pourquoi cette clause définit trois caractéristiques qu'une signature électronique doit avoir pour être conforme : avoir le même impact que la signature manuscrite dans le cadre de l'entreprise, être liée de façon permanente (donc irréversible) à l'enregistrement correspondant et inclure la date et l'heure de celle-ci.

Pour la première fois, un paragraphe aborde l'archivage des données. La partie « sauvegarde des données » alerte sur l'importance des sauvegardes régulières qui doivent êtres réalisées pour assurer l'intégrité des données critiques[10] ; ceci afin qu'elles soient toujours accessibles et lisibles. Les fonctions d'archivage et de restauration doivent aussi être vérifiées lors de la validation, pour garantir l'intégrité des données même en cas de modification du système.

[9] CAPA pour « Actions Correctives et Actions Préventives » est un outil de gestion de la qualité.
[10] « Critique » signifie avoir un impact direct ou indirect sur la qualité.

1.4.3 Les BPF européennes : le chapitre 4

La Commission européenne a publié par la même occasion une mise à jour du chapitre 4 concernant la gestion documentaire, devenue nécessaire en raison de l'utilisation croissante de documents électroniques dans les environnements BPF. Il n'y a pas de changement majeur, mais quelques précisions sont apportées dans la section « Génération et contrôle de la documentation ».

Les systèmes complexes ont besoin d'un grand nombre de documents dans le cadre de leur validation et de leur exploitation. Cette documentation peut être hybride, c'est-à-dire exister pour une part en format papier et pour l'autre en format électronique. Ce qu'il est important de retenir c'est que « **les mêmes exigences s'appliquent à tous les types de support documentaire** ». C'est pourquoi tous les documents électroniques (procédures, instructions, formulaires, modèles et enregistrements) doivent faire l'objet des mêmes contrôles que la documentation papier.

La nouvelle version donne aussi quelques précisions supplémentaires sur les enregistrements électroniques : « Pour les enregistrements électroniques, l'utilisateur doit définir les données qui seront utilisées comme données brutes. *A minima*, toutes les données sur lesquelles sont basées des décisions qualité doivent être définies comme des données brutes ».

1.5 CONCLUSION PARTIE 1

Tout établissement pharmaceutique appartenant à un pays de l'Union européenne doit valider ses systèmes informatisés réglementés conformément aux **BPF européennes** récemment mises à jour. Nous avons pu en extraire les orientations majeures, aux conséquences importantes :

1. La généralisation de l'approche basée sur **la gestion du risque qualité**. La gestion des risques devient la clé de voûte de la maîtrise des systèmes informatisés, comme elle est devenue incontournable dans toute la réglementation pharmaceutique depuis la parution du guide ICH Q9.

2. La validation est indissociable du **cycle de vie** du système. Elle débute par la définition du besoin de l'utilisateur et se termine à l'arrêt de l'exploitation du système. La maîtrise des changements est un élément très important.

3. La nécessité d'assurer la **traçabilité des spécifications** tout au long du cycle de vie, pour garantir la couverture du besoin de l'utilisateur.

4. La nouvelle gestion des **données électroniques**, des signatures électroniques et de la documentation.

5. Le renforcement des exigences sur le personnel et sur la **gestion des tiers**.

Notons que dans l'ensemble des textes internationaux, il n'y a jamais d'instruction détaillée sur ce qui doit être testé. Définir la stratégie de validation et évaluer les risques liés à l'activité est du ressort de l'industriel.

- DEUXIÈME PARTIE -
LA DÉMARCHE DE VALIDATION DES SYSTÈMES INFORMATISÉS

Dans cette deuxième partie, nous allons aborder en détail les différentes étapes de la validation d'un système informatisé. L'enjeu est de répondre de façon pragmatique aux dispositions réglementaires abordées dans la partie précédente, en expliquant la mise en place d'une stratégie de validation efficace.

Nous rappellerons dans un premier temps l'importance du système de gestion de la qualité pour un établissement pharmaceutique. Nous poursuivrons l'exposé par l'étude des différents facteurs qui influence le choix de la stratégie de validation, avec la gestion du risque et la gestion des projets. Enfin, nous terminerons par l'examen de la méthodologie de validation des systèmes informatisés.

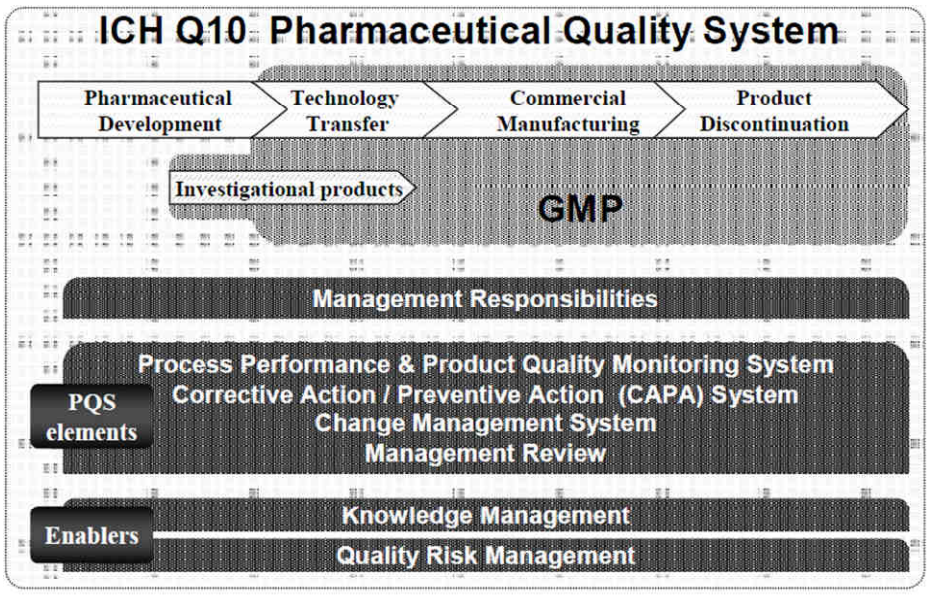
2.1 PRÉ REQUIS : LE SYSTÈME DE GESTION DE LA QUALITÉ

« Le pharmacien responsable de l'établissement de fabrication doit fabriquer des médicaments adaptés à l'emploi, répondant aux exigences du dossier d'autorisation de mise sur le marché et n'exposant les patients à aucun risque lié à des carences en matière de sécurité, de qualité ou d'efficacité. La réalisation de cet objectif de qualité engage la responsabilité de la direction de l'entreprise et du pharmacien responsable. » [28].

« Pour atteindre plus sûrement cet objectif, l'entreprise doit posséder un **système d'assurance de la qualité** bien conçu, correctement mis en œuvre et effectivement contrôlé, système incluant le concept de Bonnes Pratiques de Fabrication, de contrôle de la qualité et de gestion du risque qualité et impliquant une participation active des responsables et du personnel des divers services. » [28]

Ainsi le guide **ICH Q10** a été intégré dans les BPF européennes depuis juin 2008. Ce document s'appuie sur des concepts internationaux de normalisation de la Qualité (ISO) pour expliciter les grands principes d'un système qualité pharmaceutique. La taille et l'importance des activités de l'entreprise doivent être prises en considération lors du développement du système de gestion de la qualité. L'illustration ci-dessous, extraite de la deuxième annexe du guide en donne un aperçu général.

Figure 2 : les principes d'un Système de Gestion de la Qualité Pharmaceutique



Sources in Eudralex Volume 4 - Part III : Pharmaceutical Quality System (ICH Q10)

2.1.1 Ses objectifs

Le système de gestion de la qualité d'un établissement pharmaceutique peut être considéré comme efficace quand il permet d'atteindre trois objectifs principaux :

- La fabrication de médicaments conformes à leurs spécifications, pour répondre aux besoins des patients, des professionnels de santé et des autorités réglementaires.
- Assurer que les processus industriels en jeu soient toujours appropriés et performants en développant des systèmes de surveillance et de contrôle efficaces.
- Faciliter la démarche d'amélioration continue de tous les processus, y compris ceux gouvernant le fonctionnement du système de gestion de la qualité lui-même.

2.1.2 Ses ressources

Les fondations d'un SMQ performant reposent sur deux piliers qui sont la gestion **des connaissances industrielles**[11] ainsi que la **gestion du risque qualité**. La gestion des connaissances doit être une approche systématique destinée à acquérir, analyser, stocker et diffuser toutes les informations utiles relatives aux produits et aux processus. Il convient de multiplier les sources d'informations (qui ne se limitent pas au simple domaine de la publication scientifique). La documentation interne, regroupant les études de développement, les activités de transfert technologique, les validations de procédés tout au long du cycle de vie des produits, est la meilleure source d'informations.

La gestion du risque qualité est un outil d'une importance capitale. Cette approche permet d'identifier, d'évaluer et de contrôler rationnellement les risques qualité potentiels, et de faciliter la démarche d'amélioration continue de la qualité des produits et des processus.

[11] Les connaissances regroupent le savoir et le savoir-faire de l'entreprise.

2.1.3 Au cœur du système : une gestion volontaire

La Direction d'une entreprise pharmaceutique est entièrement responsable du bon fonctionnement de son système de gestion de la qualité. Elle doit définir sa politique qualité en décrivant ses intentions générales en la matière, et particulièrement sur le respect des référentiels réglementaires applicables.

L'engagement des responsables est donc essentiel pour respecter les objectifs de qualité et de performance. Les efforts doivent porter en priorité sur :

- La conception initiale, la mise en place, la surveillance et la maintenance du système qualité pour qu'il soit efficace à tous les niveaux de l'entreprise.
- La définition des rôles, des responsabilités et des relations de tous les membres du personnel et des sous-unités de l'entreprise, pour qu'ils soient compris de tous. Cette mesure permet en outre une communication interne efficace, et facilite la remontée des informations critiques dans les délais.
- Faciliter l'amélioration continue, par l'exécution de revues régulière de la gestion de la qualité, de la qualité des produits et des processus.
- S'assurer que le système de gestion de la qualité dispose de ressources humaine et financière suffisantes.

2.1.4 Les clés de l'amélioration continue

Selon l'ICH Q10 (voir Figure 2) quatre outils sont importants pour mettre en place une démarche d'amélioration continue. Nous ne les aborderons pas en détail, mais ils sont souvent présents dans toutes les éditions des Bonnes Pratiques de Fabrication. Ces éléments doivent être appliqués de façon appropriée à chaque stade du cycle de vie du médicament. Ces quatre outils sont :

- La surveillance des performances des processus et de la qualité des produits
- La gestion des CAPA : des actions préventives et des actions correctives
- La gestion des changements
- La gestion des revues documentaires (des processus, des produits, etc.)

2.2 LE CHOIX D'UNE STRATÉGIE DE VALIDATION

2.2.1 La politique qualité de l'entreprise comme point de départ

Nous venons de le voir, il est obligatoire pour la Direction de définir par écrit sa politique d'Assurance Qualité, dans un document appelé le manuel qualité. « L'entreprise doit posséder un système d'assurance de la qualité bien conçu, correctement mis en œuvre et effectivement contrôlé, système qui inclut le concept de bonnes pratiques de fabrication de contrôle de la qualité et de gestion du risque qualité et implique une participation active des responsables et du personnel des divers services. Ce système doit bénéficier d'une documentation complète et être dirigé avec efficacité. » [28]

Ce document est très important, car il permet de clarifier les interactions entre les processus. Concernant les systèmes informatisés, la Direction de l'entreprise prouve qu'elle comprend la nécessité de valider ses systèmes critiques et qu'en réponse, une stratégie de validation adaptée est élaborée. Le manuel qualité abordera donc les points suivants :

- Une déclaration d'engagement de la Direction concernant la politique de **validation** sur le site.
- Établir dans quelle mesure l'entreprise à recours à l'utilisation de **systèmes informatisés** pour la gestion électronique des données critiques. Quelles données et pour quels processus ?
- Identifier clairement le processus de validation des systèmes informatisés et les responsabilités associées aux différents acteurs.
- À quelles normes et à quels référentiels réglementaires la validation des systèmes sera-t-elle conforme ?

2.2.1.1 *Le processus de validation des systèmes informatisés*

La stratégie de l'entreprise concernant la validation de ses systèmes informatisés doit être définie dans une procédure standard, conforme à la politique de gestion documentaire en place. Les points importants sont :

- L'objectif et l'étendue : c'est-à-dire quels sont les systèmes concernés et leurs caractéristiques. Quels sont les critères d'inclusions et d'exclusions ?
- Les références et documents réglementaires applicables.

- Le personnel concerné et les responsabilités associées.
- La description du processus avec une approche globale en analyse de risques, les bonnes pratiques de tests à observer, les bonnes pratiques documentaires, etc.
- Les éventuelles annexes associées comme les trames documentaires.

Dans un contexte économique et financier délicat, toute entreprise doit utiliser ses ressources de façon optimale. Or, les activités de validation se révèlent souvent très coûteuses. Il est donc intéressant pour l'entreprise de prédéfinir plusieurs niveaux de validation en fonction de la criticité des systèmes. De cette façon, une **évaluation préalable des risques** permet de justifier le choix d'une stratégie de validation ayant un niveau de qualité adapté au nouveau système.

Afin de présenter plus facilement les activités de validation, nous allons commencer par définir les principaux acteurs qui y participent.

- L'établissement pharmaceutique peut être désigné par le client, par opposition au fournisseur du système responsable de son développement. Dans un grand groupe pharmaceutique, il se peut que le fournisseur en question soit un département interne à l'établissement pharmaceutique, par exemple dans le cadre d'un développement logiciel autonome.

- l'utilisateur : représentant l'ensemble du personnel qui utilisera le système dans son environnement opérationnel. Le responsable de cette équipe est généralement le détenteur du système, et est responsable de son fonctionnement et des données qui y résident jusqu'à son retrait. Il doit apporter ses connaissances spécifiques lors de l'expression du besoin utilisateur afin de décrire puis de choisir le système le plus adapté. Le détenteur du système (*system owner*) et le responsable du processus industriel (*process owner*) sont deux rôles différents pouvant être attachés à la même personne.

- un service d'Assurance Qualité, qui est responsable de l'application des Bonnes Pratiques et de la politique qualité mise en place, notamment en matière de gestion documentaire.

- un service informatique : représente le personnel compétent en matière de technologies de l'information. Ce service documente l'infrastructure informatique de l'entreprise. Durant la validation, il fournit entre autres ses compétences techniques dans le processus d'achat.

- un groupe projet (ou service de validation) : selon les besoins et les moyens de l'établissement, les opérations de validation peuvent être à la charge d'un service spécialisé, ou être menées par le comité de pilotage d'un projet. Dans ce cas, le chef de projet peut être le responsable utilisateur.

2.2.2 La gestion du risque qualité

Comme indiqué en première partie, la stratégie de validation va dépendre étroitement des résultats de l'évaluation des risques liés au système informatisé. Nous allons donc aborder dans ce chapitre la gestion du risque qualité. Nous verrons enfin la classification logicielle des GAMP[12], qui est très utile à la compréhension des risques liés uniquement aux logiciels.

2.2.2.1 *Principe général [30]*

Le guide **ICH Q9** relatif à la gestion du risque qualité fait partie des **BPF européennes** depuis 2006. Il décrit le procédé général et les méthodes à mettre en œuvre dans la gestion du risque qualité. Il est difficile de développer une approche commune à l'application de la gestion du risque qualité, car la perception du dommage potentiel, de sa probabilité d'apparition et de sa gravité peut être différente chez les différentes parties prenantes (patients, professionnels de santé, autorités politiques et industrielles). Mais pour les produits pharmaceutiques, la gestion du risque qualité doit se focaliser en priorité sur la **protection du patient**.

Les deux grands principes de la gestion du risque qualité sont donc :

- qu'elle doit reposer sur la connaissance scientifique et, est au final étroitement liée à la protection des patients,
- que le degré d'effort, de formalisation et de documentation du processus de gestion du risque qualité doit être proportionné au niveau de risque considéré.

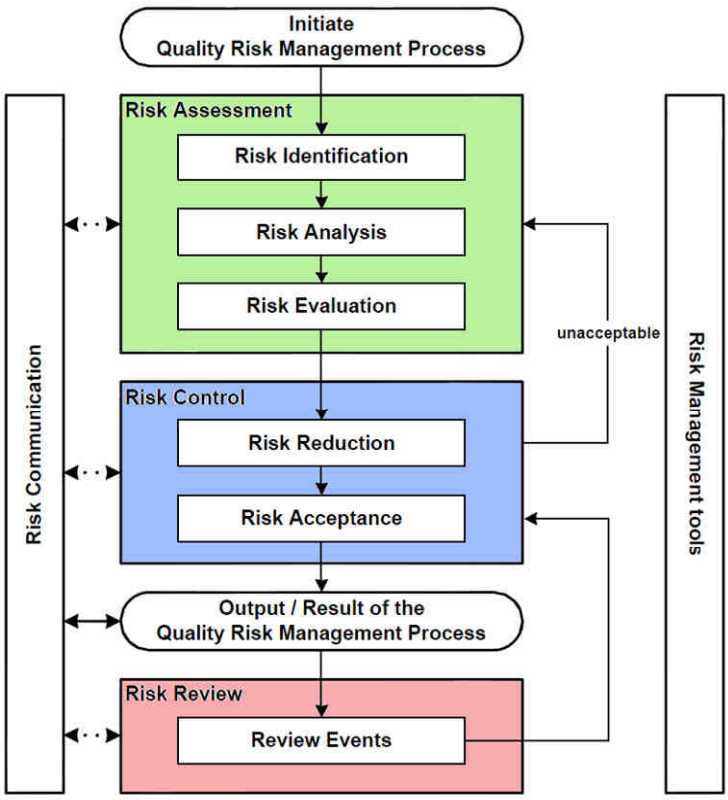
[12] Revoir Le Forum GAMP [20] [21], page 21.

2.2.2.2 *Description du processus [30]*

La gestion du risque qualité est un processus systématique utilisé tout au long du cycle de vie du médicament. La Figure 3 est extraite du guide ICH Q9. Elle décrit les étapes importantes de ce processus. Les étapes de décision n'y figurent pas parce qu'elles peuvent intervenir à tout moment du procédé. Ces décisions peuvent amener à revenir à l'étape précédente et à collecter des informations complémentaires, à ajuster le modèle utilisé ou même à clore le procédé de gestion du risque.

Les activités de gestion du risque qualité sont habituellement prises en charge par des équipes pluridisciplinaires, faisant appel à des experts dans les domaines concernés (service qualité, ingénierie, statistique, etc.). La communication relative au risque doit être efficace à toutes les étapes du processus de gestion du risque. Le point de départ est la planification du processus. Pour cela, il faut définir le problème relatif au risque, réunir les informations pertinentes liées au danger utile à l'évaluation du risque, identifier un responsable, allouer les ressources suffisantes et établir un calendrier.

Figure 3 : Schéma du processus général de gestion du risque



Sources in Eudralex Volume 4 - Part III : Quality Risk Management (ICH Q9)

Commençons par définir ce qu'est le risque. Le **risque** est « la combinaison de la probabilité d'apparition d'un dommage et de sa gravité » [28]. Le danger est défini comme la « source potentielle d'un dommage » [28].

L'estimation du risque - *Risk Assessment*

La première phase du processus est l'estimation du risque, et elle commence par l'identification des dangers afférents à la situation. L'identification du risque potentiel répond aux questions « qu'est-ce qui peut mal tourner ? » et « quelles en seraient les conséquences » ? Ensuite, l'analyse doit permettre d'estimer les risques associés aux dangers identifiés. C'est le procédé qualitatif ou quantitatif qui consiste à lier la probabilité de la survenue des dommages à leur gravité. Avec certains outils de gestion du risque, la capacité de détection des dommages (détectabilité) est également prise en compte dans l'analyse. L'évaluation du risque se termine enfin par la comparaison de cette analyse avec des critères de risques donnés. Le résultat d'une évaluation des risques est soit une estimation quantitative du risque, soit une description qualitative d'une étendue du risque potentiel.

La maîtrise du risque - *Risk Control*

La maîtrise du risque est une prise de décision visant à diminuer et/ou accepter les risques, en vue de les ramener à un niveau acceptable. La réduction du risque comprend des mesures prises pour diminuer la gravité, la probabilité des dommages voire leur détectabilité. La dernière étape formelle sera l'acceptation des risques résiduels s'ils sont tous inférieurs à un niveau spécifié acceptable.

La revue du risque - *Risk Review*

Enfin, la dernière étape du processus est la revue des résultats du processus, pour prendre en compte les nouvelles connaissances et l'expérience de terrain. En effet une fois le processus de gestion du risque qualité initié, il continue à être utilisé pour les événements qui peuvent avoir un impact sur la décision initiale de gestion du risque qualité, que ces événements soient planifiés ou non. L'examen peut inclure une nouvelle évaluation des décisions d'acceptation du risque.

La gestion du risque qualité s'appuie sur une approche scientifique et pratique de la prise de décision. Elle utilise des méthodes documentées, exhaustives et reproductibles, reconnues par l'industrie pharmaceutique et par les autorités compétentes. Ces outils peuvent être adaptés et même combinés. Les outils les plus connus sont l'**AMDEC** (analyse des modes de défaillance, de leurs effets et de leur criticité) et l'HACCP (analyse des dangers et maîtrise des points critiques).

2.2.2.3 *Gestion du risque lié aux systèmes informatisés [21] [31]*

Le guide des GAMP aborde la gestion des risques liés aux systèmes informatisés de façon pragmatique : il est nécessaire de partir du processus industriel en jeu, avant d'aborder la question du système et de ses fonctions. Car il est en effet impossible de déterminer précisément l'impact de l'utilisation d'un système informatisé sur la santé du patient, si le processus industriel n'est pas lui-même entièrement compris. Les risques associés à l'utilisation de tels systèmes ne peuvent logiquement pas être supérieurs au risque global du processus industriel. En revanche la stratégie proposée dans les GAMP n'est pas une exigence réglementaire supplémentaire. Si la politique qualité de l'entreprise est opérationnelle et efficace, et si la gestion des risques est conforme à l'ICH Q9, il est inutile d'en modifier le fonctionnement. La validation de nouveaux systèmes a pour objectif d'éviter tout risque inacceptable tant au niveau de la sécurité des patients qu'au niveau industriel, tout en maximisant les avantages industriels générés par ce nouveau système. Les entreprises doivent comprendre et gérer les risques conjointement avec les avantages, et doivent être préparées à mener plusieurs analyses de risques pendant la mise en œuvre d'un nouveau système. La stratégie du GAMP repose sur cinq étapes.

Étape n°1 : étudier le procédé industriel

Il est peu réaliste de tester complètement tous les aspects d'un système informatisé, et il convient en conséquence de concentrer les efforts sur les zones critiques. C'est pourquoi une évaluation préliminaire, basée sur l'étude détaillée du procédé industriel doit être effectuée. Il faut déterminer si le système est utilisé dans le cadre d'une activité réglementée et quels sont les référentiels applicables. Les spécifications de l'utilisateur (URS), les spécifications fonctionnelles (FS) et les exigences réglementaires forment la base du processus d'évaluation. Toutes les fonctions doivent être identifiées au cours de cette phase et être documentées avec leurs possibles relations de dépendances. Le but est

d'évaluer les risques associés à l'exploitation après projet du système, et non pas les risques inhérents au projet. Cette étape ne doit pas être négligée, car toutes les étapes suivantes en découlent, et permet de déterminer l'ampleur de l'effort. Il est essentiel de veiller à ce que les futurs utilisateurs soient impliqués activement dans le processus d'évaluation des risques, tout au long de celui-ci et qu'ils en acceptent les résultats.

Étape n°2 : identifier les fonctions à risques

Partant des informations recueillies lors de l'évaluation préliminaire, il faut déterminer à présent si les fonctions du système représentent un risque qualité, c'est-à-dire portant sur la **sécurité des patients**, la **qualité des produits** ou sur l'**intégrité des données** (notamment électroniques). Voici quelques exemples de critères :

- Qualité pharmaceutique : formule incorrecte, erreur de matière première, erreur d'étiquetage, traçabilité des lots
- Sécurité des patients : effets indésirables supplémentaires, traitement des réclamations
- Intégrité des données : calculs erronés des résultats de contrôle qualité

Le résultat de l'examen de chaque fonction à risque doit être documenté. Même si l'évaluation d'une fonction particulière ne révèle pas de risque particulier, cette conclusion doit avoir une justification.

Le second type de risque à ne pas négliger concerne l'impact économico-industriel pour l'entreprise. Cette partie ne sera pas développée.

Étape n°3 : procéder à l'analyse des risques et prendre les mesures adéquates

Après avoir déterminé les risques qualité et économico-industriel associés aux fonctionnalités du système, l'analyse de risque doit identifier les scénarios à risque, et si des mesures sont nécessaires pour réduire les dommages potentiels. Pour exécuter cette évaluation, le guide des GAMP recommande l'utilisation d'un outil appelé **AMDEC**[13], car c'est l'outil idéal pour identifier les éléments d'un système qui le rendent vulnérable.

[13] Pour « Analyse des Modes de Défaillance de leurs Effets et de leur Criticité »

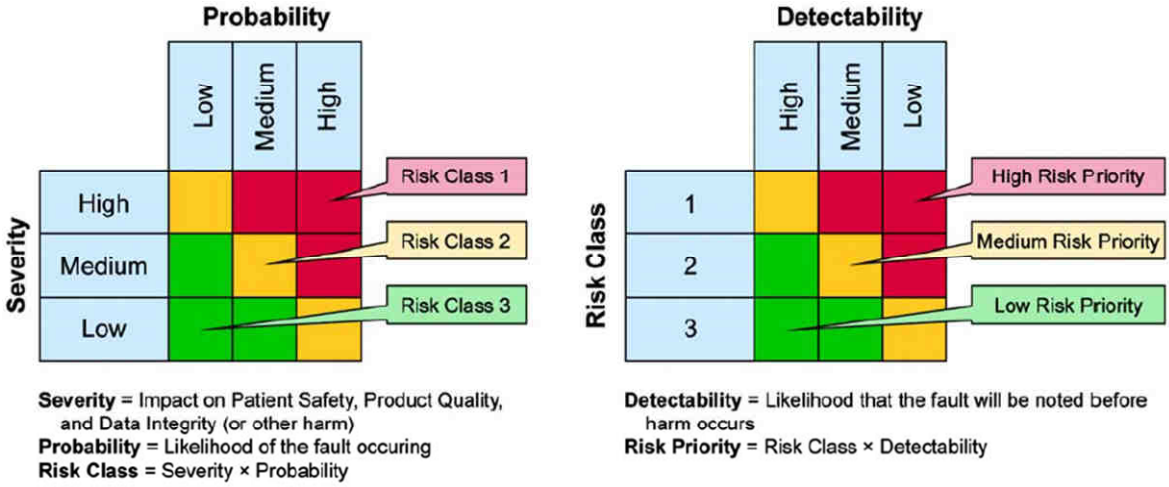
Tableau II : Exemples d'analyse des scénarios à risque

Fonction	Sous-fonction	Scénarios à risque	Effet(s)
Approvisionnement	Émission d'une commande	Entrée d'une classe de matière incorrecte lors de la saisie de la commande	Réception d'une classe de matière incorrecte Renvoi au fournisseur après analyse Pénurie de stocks
Contrôle qualité	Sécurité	Modification possible d'un résultat d'analyse d'échantillon	Certification d'un résultat erroné Libération d'un lot non conforme Impact sur la santé des patients

La méthode demande ensuite de déterminer la probabilité de survenue des scénarios à risques ainsi que leur gravité. L'estimation de la probabilité de survenue durant une période donnée peut être difficile, car dans de nombreux exemples ces événements peuvent résulter de défaillances logicielles systématiques. Quant à l'évaluation de la gravité, elle doit tenir compte à la fois des effets immédiats et de l'impact sur l'activité sur le long terme (par exemple sur les aspects réglementaire, marketing et financier). Les GAMP proposent trois niveaux d'évaluation pour chaque critère : faible, moyen et élevé. Une fois ces niveaux définis pour chacun des scénarios, il est possible de répartir les risques en trois Classes de Risques (Figure 4 - matrice de gauche).

Le dernier élément pouvant être évalué est la détectabilité, c'est-à-dire la probabilité de détection d'un dommage. Avec une probabilité de détection élevée, il sera rapidement reconnu et une action corrective appropriée pourra être prise à temps. En combinant la classification des risques avec la détectabilité, il est possible de classer par priorité les conditions de panne associées à chaque scénario de risque en fonction des zones de plus grande vulnérabilité (Figure 4 - matrice de droite). Dès lors que ces priorités ont été déterminées, il faut définir des mesures appropriées de réduction des principaux risques.

Figure 4 : Méthode d'évaluation et de classification des risques des GAMP



Sources in C. Martin K., Perez A. « *GAMP 5 Quality Risk Management Approach* ». *Pharmaceutical Engineering*. Mai/Juin 2008. Vol. 28, n°3

Il existe différentes méthodes de réduction des risques. Une solution consiste à modifier les éléments de conception du système, voire du procédé lui-même, avec l'introduction de nouvelles procédures externes comme une double vérification. D'autres solutions recourent à l'utilisation de méthodes, d'outils, de composants éprouvés ou de composants en doublon. Le contrôle de l'environnement d'exploitation est aussi un moyen de traquer les risques. Par ailleurs, la structure même du projet peut être reconsidérée, ainsi que le nombre de tests à effectuer lors des qualifications.

Étape n°4 : définir les tests de validation et vérifier les mesures de réduction du risque

Les résultats de l'analyse de risque doivent permettre de justifier les scénarios de tests à effectuer durant la validation. Globalement, les fonctions à faible risque qualité ne requièrent que peu de tests fonctionnels pour répondre aux besoins de conformité. Plus une fonction est critique, plus il convient d'examiner et de simuler des modes de défaillance pertinents, à savoir ce qu'il se passe lorsque la fonction échoue.

Des mesures de contrôles du risque peuvent être mises en place sur la base des résultats des tests, si les essais ont montré que certaines fonctionnalités ne sont pas assez fiables. Les fonctions à risques élevés peuvent faire l'objet de contrôles redondants, toujours dans un objectif de maîtrise du risque. L'efficacité et la traçabilité de ces mesures

par rapport aux risques identifiés doivent être vérifiées. Une évaluation du risque résiduel doit être effectuée au moins pour les fonctions à risque initialement élevé.

Étape n°5 : revoir périodiquement les risques

Toujours en accord avec le processus général de gestion du risque de l'ICH Q9 il convient, une fois le système opérationnel, d'effectuer la revue périodique des risques identifiés. Les points essentiels sont de :

- Constater si des risques initialement non identifiés sont présents.
- Déterminer si les risques initialement identifiés sont bien présents, et à quel niveau.
- Confirmer que les risques initialement identifiés sont toujours acceptables, en fonction des événements passés.
- Évaluer si les mesures de réduction des risques et les contrôles en place sont efficients.

C'est le niveau de risque qui détermine la fréquence des revues périodiques.

2.2.2.4 *La classification logicielle des GAMP*

Dans un système informatisé, la principale source de risque est la partie logicielle. En effet au fur et à mesure de l'évolution technologique, ils deviennent de plus en plus complexes. De nombreux facteurs, tels que les erreurs d'écriture d'un code source ou la mauvaise installation ou configuration des programmes sont autant d'éléments qui augmentent le risque de défaillance. Une caractéristique importante des logiciels à prendre en compte est l'étendue de leur distribution (très grande par exemple pour les systèmes d'exploitation). Car il est évident que si un programme fonctionne sur des centaines de milliers de machines, il est extrêmement peu probable d'observer une erreur n'ayant jamais été répertoriée.

La **classification des logiciels** issue des GAMP peut être utilisée avec les procédés d'évaluation des risques et d'évaluation des fournisseurs pour **déterminer une stratégie de validation** adaptée. Les catégories sont fondées sur le risque croissant de défaillance, c'est-à-dire à la fois sur la complexité et sur le niveau de distribution des logiciels. Les systèmes informatisés et automatisés sont souvent constitués de plusieurs éléments et, pour un même système, ces éléments peuvent être classés dans différentes catégories. À l'origine, la première classification était composée de cinq catégories. Aujourd'hui avec l'évolution des technologies, elles ont été réduites à quatre. [31]

Catégorie n°1 : les logiciels d'infrastructure (Windows®, Unix®)

Cette première catégorie concernait à l'origine uniquement les systèmes d'exploitation. Elle a été récemment étendue pour inclure l'ensemble des programmes d'infrastructures dont le rôle est de permettre le fonctionnement général et la communication de tous les systèmes d'information. Sont donc inclus de nombreux *middlewares*, comme des gestionnaires de bases de données, des indicateurs de performance réseau, des outils de traitement d'information par lot, etc. Ces logiciels sont reconnus et disponibles dans le commerce. Ils ne sont pas soumis à une validation particulière, car ils sont considérés à faible risque de par leur grande distribution. De plus, leurs fonctionnalités sont indirectement mises en question pendant les tests des autres logiciels.

L'ancienne catégorie n°2

Cette catégorie a disparu dans la dernière version des GAMP. Elle concernait les microprogrammes aussi appelés *firmwares* ou logiciel embarqué, étant un ensemble d'instructions directement intégrées dans du matériel informatique (par exemple le BIOS d'un ordinateur). Aujourd'hui ils sont devenus tellement sophistiqués qu'il n'y a plus de raison de les traiter différemment des autres logiciels. Les *firmwares* peuvent donc entrer dans n'importe quelles catégories selon leur nature.

Catégorie n°3 : les logiciels non configurés

Cette troisième catégorie était appelée « progiciels standards » avant d'être renommée « logiciels non configurés ». Ce sont des logiciels standards appelés COTS[14], offrant une solution simple et disponible en l'état à un procédé industriel. Non configuré signifie qu'il n'est pas nécessaire de paramétrer spécifiquement le logiciel pour combler les besoins de l'utilisateur ou du processus industriel. L'installation doit se limiter à l'établissement de l'environnement d'exploitation (par exemple le raccordement au réseau et à l'imprimante). Les paramètres de procédé peuvent être entrés dans l'application. Les logiciels d'analyse statistique ou ceux intégrés dans les instruments de laboratoire (comme les équipements HPLC) sont des exemples de progiciels standard.

Catégorie n°4 : les logiciels configurés (SAP®)

Les logiciels COTS se sont tellement complexifiés qu'aujourd'hui nombre d'entre eux sont configurables et s'adaptent facilement aux besoins des utilisateurs. Par conséquent, ils doivent être considérés comme appartenant à la quatrième catégorie. Ces progiciels configurables offrent des interfaces et des fonctions standard permettant de configurer très précisément les procédés industriels. Ces systèmes complexes disposent souvent de plusieurs couches logicielles, ce qui implique la configuration de modules prédéfinis et éventuellement d'autres modules logiciels développés sur mesure. Ces progiciels doivent être parfaitement reconnus et matures avant d'être considérés comme appartenant à la catégorie 4. Dans le cas contraire, la catégorie 5 est plus pertinente. Parmi les exemples de progiciels appartenant à la catégorie 4 figurent les systèmes de contrôle

[14] « COTS » pour *Commercially available Off-The-Shelf* (logiciel disponible sur le marché)

commande, les systèmes de supervision type SCADA, les systèmes d'exécution de fabrication (MES) et certains progiciels ERP, MRP II et LIMS.

Catégorie n°5 : les logiciels personnalisés

Comme la catégorie 4, la catégorie 5 reste pour l'essentiel inchangée. Les systèmes de cette catégorie sont développés pour répondre aux besoins spécifiques de l'entreprise de l'utilisateur. Les développements personnalisés peuvent concerner un système entier ou l'extension d'un système existant. Un audit du fournisseur est généralement requis pour confirmer que les systèmes qualité existants appropriés sont établis pour gérer le développement et le support permanent de l'application. Le plan de validation doit refléter l'évaluation du fournisseur et toutes les observations inscrites lors de l'audit, la criticité, la taille et la complexité de l'application. Il devra définir des stratégies pour l'atténuation de toutes les faiblesses identifiées lors du procédé de développement du fournisseur.

Les catégories de logiciels ne sont qu'un des facteurs à prendre en compte pour le choix d'une stratégie de validation. En effet, elles établissent une conclusion générale sur une large gamme de logiciels très différents.

2.2.3 La gestion de projet

L'organisation en mode gestion de projet doit résulter du choix de la stratégie de validation. En effet, elle n'est pas toujours nécessaire et sera surtout profitable pour la validation de systèmes inédits et très complexes. Les sociétés prestataires de services sont elles très concernées, car elles doivent réaliser de nombreuses validations pour le compte d'établissements pharmaceutiques aux exigences de qualité variables.

2.2.3.1 *Définition d'un projet*

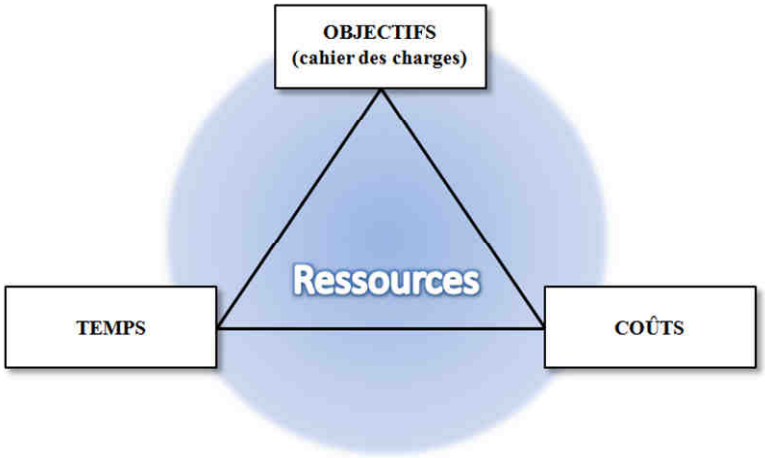
« Un projet est un ensemble unique d'actions coordonnées avec des dates définies de début et de fin, entreprises par un individu ou une entité pour atteindre des objectifs spécifiés en respectant des paramètres de coûts, de délais et de performances ». [32]

Il faut tout d'abord bien comprendre la différence fondamentale qu'il existe entre un projet et un processus (ou opération de travail). Tous deux sont réalisés par un certain nombre d'acteurs aux rôles et responsabilités définis. Ils sont contraints par une quantité limitée de ressources, et sont successivement planifiés, exécutés et contrôlés.

Mais à la différence du processus, qui est par définition répétable, continu et permanent, le projet est une activité :

- Temporaire, c'est-à-dire planifié dans le temps, avec les dates de début et de fin définies à l'avance. Le terme du projet arrive avec l'atteinte des objectifs fixés ou l'abandon de celui-ci.
- Unique, c'est-à-dire même si le « type » d'ouvrage est connu, un projet nécessite de faire quelque chose n'ayant jamais été fait avant. L'élaboration des caractéristiques de l'ouvrage est progressive (par étapes ou itérations).

Figure 5 : Schématisation des paramètres critiques d'un projet

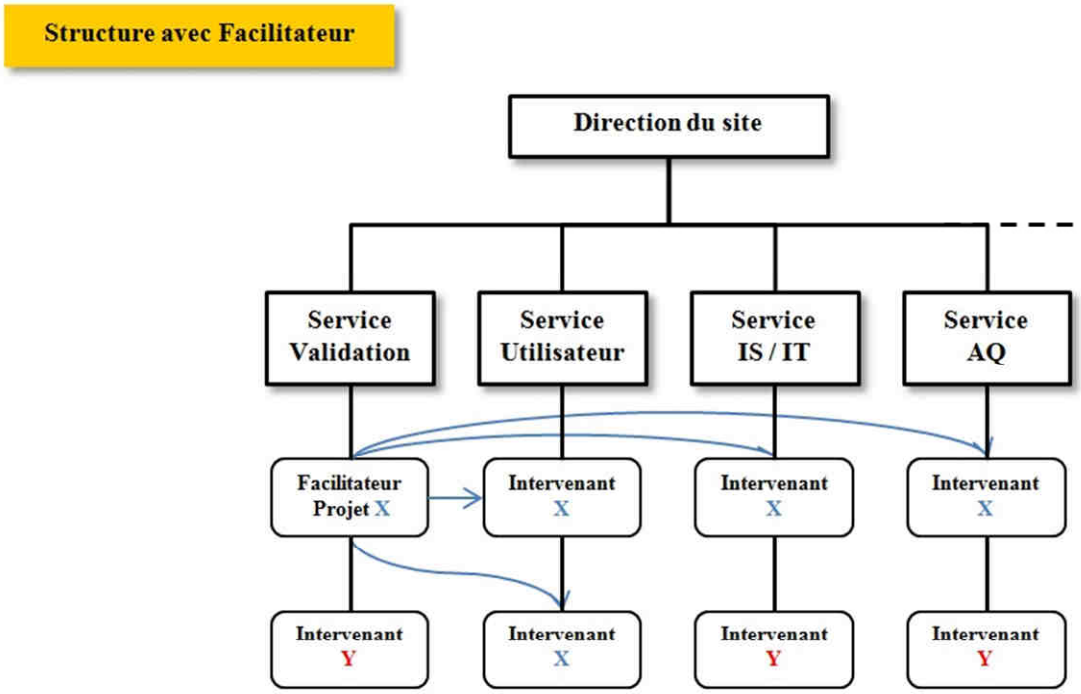


Ce schéma montre bien l'équilibre existant entre les différents paramètres d'un projet, au travers de la forme du triangle central : augmenter ou diminuer l'importance de l'un des paramètres aura un impact direct sur les deux autres. Par exemple, réduire les coûts se traduira souvent par réduire les objectifs de qualité attendus.

2.2.3.2 *Structures organisationnelles*

En fonction de la taille de l'entreprise et de l'importance des activités de validation associées, les industriels peuvent choisir de s'organiser selon différentes modalités de fonctionnement. L'organisation de base, hiérarchique, est aussi dite « fonctionnelle », car le travail est organisé par fonction ou service. Mais telle quelle, cette structure n'est pas très adaptée à la gestion de projet. Nous allons donc détailler trois types d'adaptations différentes, d'efficacité croissante en matière de gestion de projet.

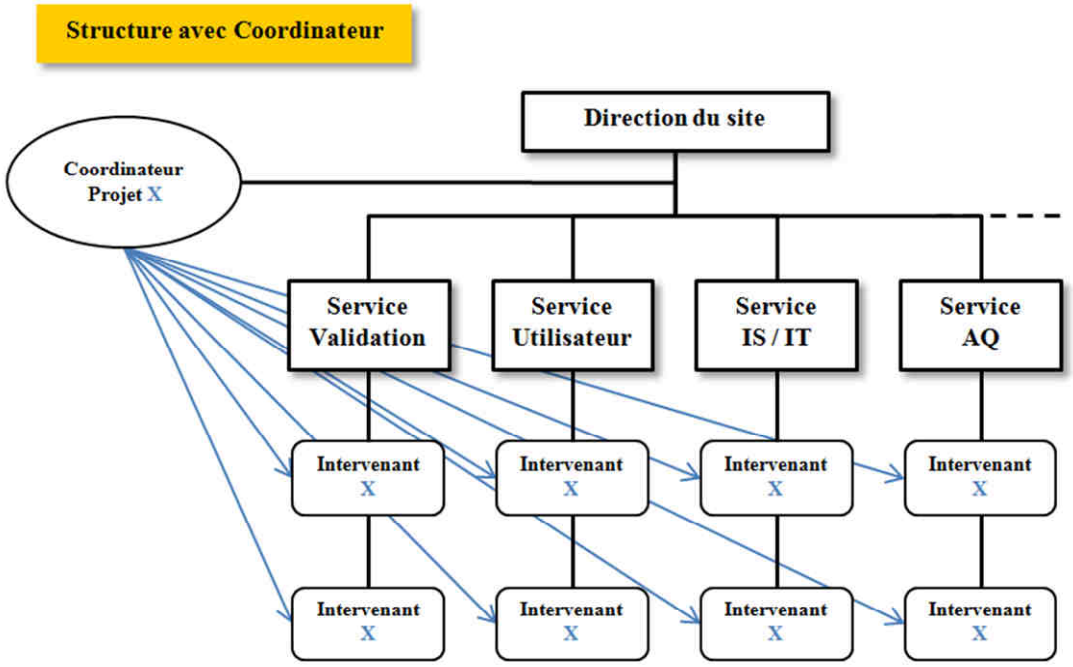
Figure 6 : Exemple de mode d'organisation avec facilitateur



Pour des projets de petite ampleur, une structure avec simplement un facilitateur est suffisante et permet d'économiser les ressources. Tous les intervenants ont pour consigne d'exécuter à la fois leur mission de routine, ainsi que le travail supplémentaire requis par le projet de validation X. Le facilitateur est aussi un intervenant du projet et fait de même. Son objectif est d'aider l'équipe à prendre des décisions de groupe, en explorant collectivement les problèmes. Il met en place un cadre propice à la communication et s'assure que chacun exprimer son opinion.

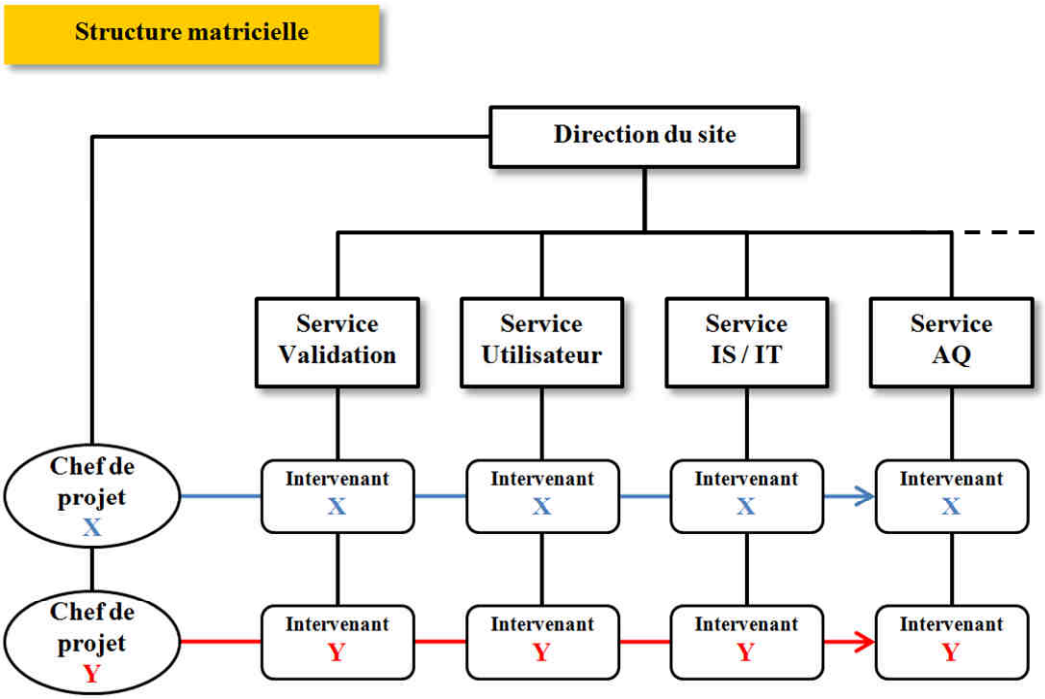
Pour les entreprises d'effectif réduit où il n'existe pas de service dédié à la validation des systèmes, il est préférable que le facilitateur soit le Responsable Utilisateur du futur système, ou un membre de l'Assurance Qualité. Dans tous les cas, le facilitateur doit être une personne formée à la gestion de projet, avec un minimum d'expérience de terrain.

Figure 7 : Exemple de mode d'organisation avec coordinateur



Pour les projets plus importants, il est préférable de remplacer le facilitateur par un coordinateur temporaire et indépendant, placé directement sous la responsabilité de la Direction. Il y a deux avantages à cela. Premièrement, cela permet de libérer l'intervenant qui jouait le rôle de facilitateur, lui permettant de se consacrer entièrement à son propre travail. Deuxièmement, le coordinateur étant indépendant, il possède une meilleure vue d'ensemble et une meilleure influence pour encadrer le travail des divers intervenants au projet.

Figure 8 : Exemple de mode d'organisation matriciel



Dans une structure matricielle, les chefs de projet sont rattachés au Directeur Général et sont indépendants les uns des autres. Ils disposent d'une équipe multifonctionnelle pour mener à bien leur projet. Cette organisation basée sur la double hiérarchisation temporaire de l'entreprise est une forme moderne et efficace de gestion de projets.

Il faut noter que tous les principaux services ne sont pas représentés sur les schémas. C'est le cas du service des achats, qui assure la gestion financière des projets et une partie de la relation client / fournisseur.

2.3 MÉTHODOLOGIE DE LA VALIDATION

Dans les chapitres précédents, nous avons vu les prérequis à la validation. En partant de la politique qualité de l'entreprise, nous avons utilisés entre autres la gestion du risque qualité pour choisir une stratégie de validation adaptée au projet industriel. Dès lors, la stratégie de validation est sélectionnée, justifiée et doit être appliquée étape par étape.

2.3.1 Le cycle de développement d'un système informatisé

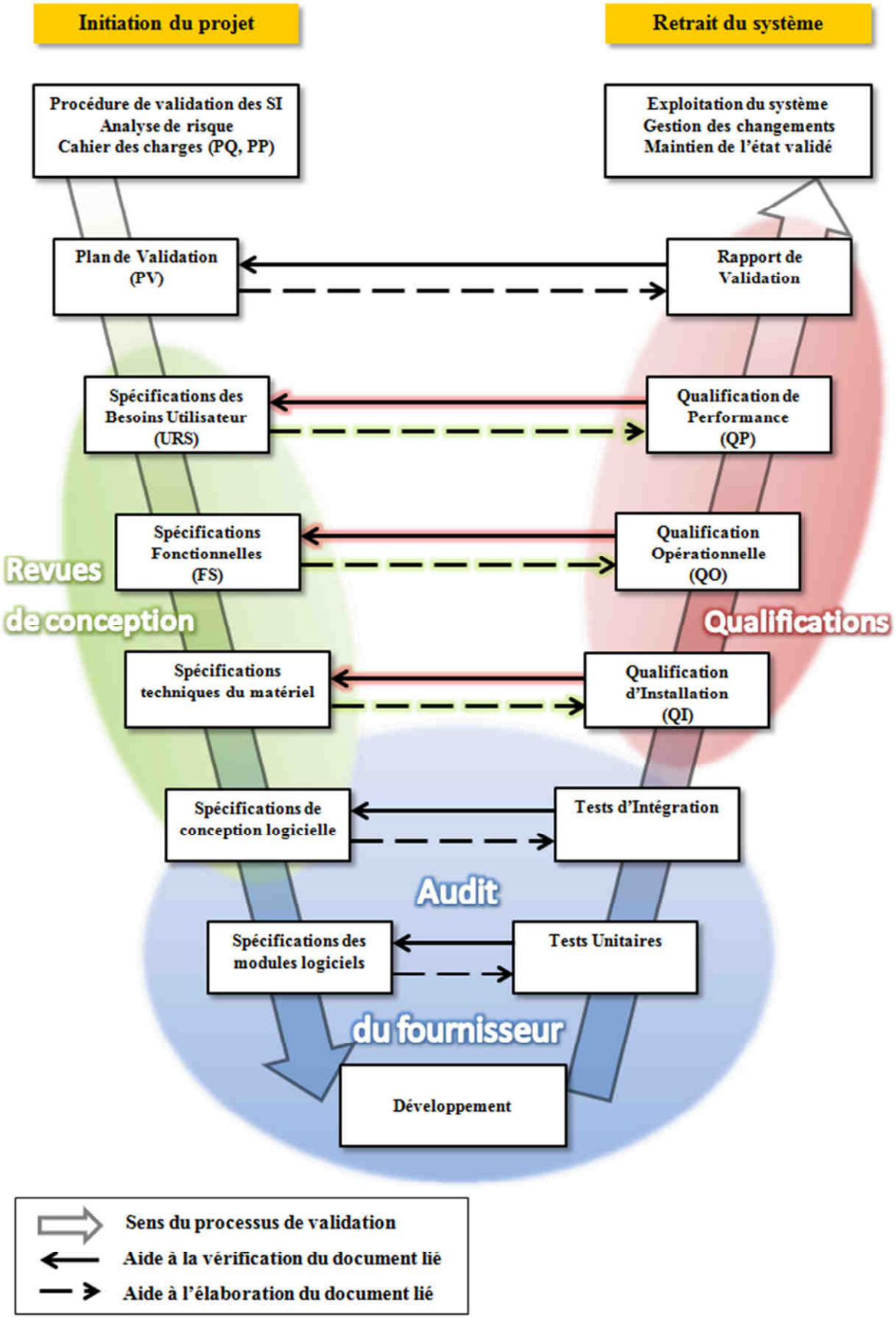
La validation ne peut pas être traitée comme une action indépendante. Elle fait entièrement partie du **cycle de vie** du système. Sans une réflexion globale sur le cycle de vie, le risque de découvrir par la suite des non-conformités est bien plus important, avec des répercussions souvent coûteuses. Que le système soit développé en interne ou par une société prestataire, ou encore acheté puis configuré par un fournisseur, il devra être intégré dans l'entreprise en utilisant une approche de cycle de vie formellement défini. Cette approche sert de base à tout processus de validation et de revalidation. C'est d'ailleurs une exigence réglementaire explicite de la nouvelle version des BPF européennes : « La documentation de validation et les rapports correspondants doivent couvrir les étapes pertinentes du cycle de vie ». [11]

Le modèle du cycle en V est devenu un modèle standard de gestion de projet depuis les années 1980 avec le développement de l'ingénierie des systèmes. Cette discipline a pour objectif de contrôler la conception de systèmes dont la complexité ne permet pas le pilotage simple, en mobilisant l'ensemble des corpus théoriques pour leur mise en cohérence (sciences de l'ingénieur, sciences humaines, sciences cognitives, génie logiciel, pharmacotechnie, etc.).

« L'ingénierie des systèmes se focalise sur la définition des besoins du client et des exigences fonctionnelles, détectés tôt dans le cycle de vie, en documentant les exigences, puis en poursuivant avec la synthèse de la conception et la validation du système. » [33].

Le modèle de cycle de vie en V est quasi systématiquement utilisé dans l'industrie du logiciel. Il est par ailleurs repris dans les guides des GAMP et du PICS.

Figure 9 : Application du modèle en V au cycle de vie d'un système informatisé



La Figure 9 est une application classique du modèle en V à la validation d'un système informatisé dans l'industrie pharmaceutique. Elle permet de visualiser les relations d'interdépendance entre les différentes étapes d'un projet de validation standard. On voit notamment comment les trois principales activités de qualification peuvent être mises en correspondance avec les principales spécifications requises. Les résultats d'un niveau ou d'une étape correspondent aux entrées du niveau ou de l'étape suivante. Bien sûr, les différentes spécifications peuvent être combinées pour les plus petits systèmes.

Les prochains chapitres suivent le découpage du travail tel que représenté en Figure 9 :

- Définition du besoin et revues de conception
- Développement et audit du fournisseur
- Qualification et maintien de l'état validé.

2.3.2 Définition du besoin et revues de conception

2.3.2.1 *L'enjeu considérable de la définition des besoins*

En réalité la question serait la même s'il s'agissait de construire un immeuble ou une voiture : il faut faire des plans. Pour notre système, un **cahier des charges** permet d'expliquer quel est le produit final attendu, et aussi de faire une estimation des coûts et des délais. Si les besoins ne sont pas assez précisément décrits, le risque d'obtenir un système qui ne répond pas aux besoins du client ou seulement de façon partielle est important. Un cahier des charges efficace évite donc d'avoir à refaire tout ou partie de ce qui a été élaboré. Même si l'établissement d'un cahier des charges nécessite beaucoup de temps et de réflexion, en pratique c'est toujours du temps de gagner. Il est tout simplement impossible de s'affranchir de formaliser ses besoins.

Selon l'importance du projet, le cahier des charges peut être subdivisé en plusieurs documents, souvent nommés **spécification des besoins utilisateur** (URS), plan qualité et plan projet. Finalement, l'essentiel n'est pas de discuter la forme, mais plutôt le contenu important à faire figurer dans ce corpus documentaire. Car ce corpus est la clé de voûte du processus de sélection du fournisseur et sera le fondement **contractuel** de cette future

relation tout au long du projet. De nombreux modèles de documents existent et peuvent être commandés sur des sites spécialisés tels que celui de l'ISPE[15].

Les **spécifications utilisateur** représentent sans conteste la partie la plus importante. En relation avec les besoins de l'utilisateur, elles décrivent ce que le système est supposé faire. Ces spécifications doivent exprimer des exigences et non des solutions de conception. Une priorisation des exigences doit permettre de différencier les exigences essentielles (impératives) de celles qui sont simplement souhaitables. Une fois le fournisseur sélectionné, une version finalisée des URS peut être rédigée en accord avec sa réponse, puis approuvée et actualisée tout au long du cycle de développement. Les URS sont directement en lien avec la qualification de performance (QP). En effet, les tests réalisés à cette étape devront permettre de vérifier que le système alors opérationnel est apte à satisfaire le besoin initialement émis par l'utilisateur.

Tableau III : Exemples d'exigences de spécification utilisateur (URS)

Fonctions	Description du procédé, mode de fonctionnement (démarrage, arrêt, reprise), contraintes quantitatives temporelles et de performance, action en cas de défaillance, sécurité…
Données	Définition des données à manipuler, identification des paramètres critiques, des plages et limites de validité, les capacités de traitements, la vitesse d'accès aux données, l'intégrité et la sécurité des données en particulier si application du 21CFR Part 11…
Interfaces	Interface avec les utilisateurs en termes de rôles ou de fonctions (opérateur, responsable métier, responsable informatique), interface avec les autres systèmes et avec l'équipement.
Environnement	Agencement, environnement de travail (stérile, poussiéreux, température, humidité, etc.)
Contraintes	Compatibilité avec le matériel existant de l'utilisateur, disponibilité, maintenance
Cycle de vie de développement	Système qualité du fournisseur (certification, méthodologie, gestion de projet, etc.), exigences de tests (données, simulations requises), définition des livrables…

Le cahier des charges contient aussi les clauses relatives à la gestion de la qualité et à la planification du projet. Pour les systèmes d'envergure et en fonction des activités de validation de l'entreprise, il peut être judicieux de séparer ces spécifications dans un **plan qualité** et dans un **plan projet** convenus entre l'utilisateur et le fournisseur. Le plan qualité permet ainsi de définir les actions et les éléments à délivrer, la distribution des responsabilités et les procédures de qualité adéquates. Le plan projet s'attachera plus à détailler les différentes phases souhaitées (Figure 9 – Audit du fournisseur), les activités et

[15] *International Society for Pharmaceutical Engineering*, dont le Forum des GAMP est membre.

les délais attendus. Ces clauses sont contractuelles et assurent la qualité du service du fournisseur. Elles ne dispensent pas pour autant d'effectuer un audit régulier de celui-ci.

2.3.2.2 *Le Plan de Validation*

Le **Plan de Validation** (PV) décrit de manière détaillée **comment** la validation doit être réalisée. Il ne faut pas le confondre avec le Plan Directeur de Validation (PDV) dont le rôle est de décrire les secteurs de l'entreprise dans lesquels la validation doit avoir lieu et de présenter l'état d'avancement de l'ensemble de l'activité de validation. Un plan directeur de validation peut toutefois être utilisé pour définir le plan global d'un projet conséquent, mais chaque système devra être documenté par son un plan de validation individuel. Le plan de validation doit résumer l'intégralité du projet. Pour cela, il doit généralement aborder les points suivants :

- La définition des rôles et des responsabilités partagées entre le détenteur du système, le chef de projet, le service d'assurance qualité. Les responsabilités attachées à chaque signature d'approbation doit être clairement définies. La structure organisationnelle est très importante et dans la mesure du possible il faut indiquer les rôles supplémentaires (par exemple techniques).

- La détermination du niveau de risque qualité et les conséquences sur la stratégie de validation retenue : modèle de cycle de vie, les entrées et sorties pour chaque étape de la validation, les critères d'acceptation associés. Tous les standards ou procédures à suivre doivent y être définis, particulièrement ceux concernant la gestion des tiers (fournisseurs).

- Les éléments à délivrer pour la validation (ou « livrables ») devant être produits.
- Les critères d'acceptation généraux du système.
- Les exigences en matière de gestion des changements avec la référence aux procédures appropriées.
- Les procédures opérationnelles standard (SOP) à créer ou à actualiser suite à la mise en œuvre du système.
- Les exigences de formation du personnel
- La gestion de la documentation : les procédures à appliquer
- Le maintien de l'état validé : les actions et les procédures à appliquer

Le plan de validation doit indiquer les différents types de rapports à produire pour couvrir les progrès réalisés à chaque étape, les points soulevés et l'acceptation des phases décisives du projet. Il sera également nécessaire de rédiger un rapport de validation final pour résumer la totalité du projet, en évaluant ses degrés de réussite et statuant sur l'acceptation du système. Le PV est un document essentiel et décisif quant au succès du projet. C'est un document vivant qui doit être actualisé si nécessaire tout au long du projet. [21]

2.3.2.3 *Différents types de spécifications*

Le fournisseur rédige des **spécifications fonctionnelles** (FS) répondant aux besoins de l'utilisateur tel que décrit dans les URS. Elles décrivent les fonctions détaillées du système sous forme d'objectifs de conception. En outre, elles doivent être suffisamment claires pour que l'équipe chargée de la conception puisse ensuite avancer sans avoir à consulter trop fréquemment le fournisseur.

Tableau IV : Exemples d'exigences de spécifications fonctionnelles (FS)

Fonctionnalités	l'objectif du dispositif, détail de son utilisation, l'identification des algorithmes critiques, les performances (réponse, précision, capacité de traitement), la sécurité (restriction des accès, autocontrôles), les fonctions configurables et limites permises…
Données	Définition hiérarchique des données (base de données, fichiers simples, formats, etc.), les accès (lecture, écriture), la capacité de stockage, d'archivage, et les mesures d'intégrité et de sécurité
Interfaces	Données transmises et reçues, synchronisation, format et débit de transfert, protocole de communication, partage (création, duplication, destruction, etc.), traitement des erreurs et encore la sécurité des interfaces…
Autres	Disponibilité (fiabilité, détection d'erreur, fonctionnement de secours, etc.)

L'utilisateur doit revoir et approuver ces spécifications contractuelles. Les FS sont directement en lien avec la qualification opérationnelle (QO). En effet après l'installation du système, les tests de QO permettent de vérifier que toutes les fonctionnalités du système fonctionnent conformément aux exigences préétablies et donc que le système est opérationnel.

Une fois les spécifications fonctionnelles formalisées, de nombreuses spécifications dites **de conception** vont en découler. Ces spécifications doivent contenir des informations suffisamment détaillées pour permettre la construction et la maintenance du système.

On y retrouve logiquement (cf. Figure 9) :

- Des spécifications techniques du matériel
- Des spécifications de conception logicielle
- Des spécifications pour les modules logiciels.

Il est intéressant d'illustrer les spécifications techniques du matériel au moyen d'un schéma annoté. Le système informatique doit être décrit (unité principale, périphériques, dispositifs de stockage, les interconnexions, la configuration, etc.) ainsi que les composants d'entrée/sortie, les exigences électriques et environnementales. Toutes ces spécifications doivent être testées en phase de qualification d'installation.

Les spécifications de conception logicielle et pour les modules logiciels relèvent de l'ingénierie du logiciel. Elles servent de base à l'écriture du code source des logiciels. L'utilisateur doit demander dans le cahier des charges (ou plan projet) au fournisseur d'appliquer une stratégie de test adéquate. Ainsi, les tests unitaires et tests d'intégration permettent d'assurer le bon développement de la solution système.

2.3.2.4 *Les revues de conception et la traçabilité des exigences*

L'objectif des revues de conception est d'évaluer l'ensemble de la documentation de conception afin d'identifier les manquements et les incohérences puis mettre en place les actions correctives identifiées. Il s'agit de revues systématiques et planifiées des documents de spécifications, de conception et de développement, devant être programmées à des phases appropriées du cycle de développement. En général elles doivent avoir lieu lors de l'élaboration des URS, des FS et pour chacune des spécifications de conception. Chaque revue doit impliquer l'utilisateur, le développeur et les membres de l'assurance qualité puisque le but de ce procédé est de faire en sorte que les spécifications répondent aux exigences. Dans la première partie, nous avons vu que la nouvelle version des BPF européennes exige le renforcement de **la traçabilité des spécifications**, qui doit être assurée tout au long du cycle de vie du système. C'est pourquoi il est recommandé que l'utilisateur développe une **matrice de traçabilité** pour démontrer que toutes les exigences sont satisfaites par la solution mise en œuvre et qu'elles seront testées de manière pertinente pendant les qualifications. [21]

La traçabilité montre que les éléments de conception en entrée sont reliés aux éléments de conception en sortie et qu'ils ont été vérifiés. En plus de la démonstration de cette vérification, une matrice de traçabilité peut apporter une aide considérable à l'évaluation et à la gestion des changements. En pratique, cette matrice se présente souvent sous la forme de tableau. Elle enregistre la relation entre deux résultats (ou plus) issus du processus de développement : par exemple la relation entre les spécifications fonctionnelles et les spécifications de conception logicielle ; ou bien entre les spécifications fonctionnelles et les tests de qualification associés.

Le travail sur les matrices de traçabilité doit être commencé conjointement avec les spécifications utilisateurs, et la (ou les) matrice(s) de traçabilité doivent être mises à jour et maintenues tout au long du cycle de vie de développement, jusqu'à l'approbation des dernières spécifications de test (qualification de performance). Les matrices de traçabilité doivent ensuite être maintenues et mises à jour en tant que partie du procédé de gestion des changements opérationnels, de manière à pouvoir continuer de refléter avec précision le système utilisé. Enfin, les matrices de traçabilité doivent être conservées en tant que preuves démontrant que les exigences ont été mises en œuvre et testées.

2.3.3 Développement et audit du fournisseur

2.3.3.1 *Encadrement*

La nouvelle version des BPF européennes a renforcé les dispositions relatives au **personnel et à la gestion des tiers**. Cette partie du cycle de développement est particulièrement importante si la partie logicielle du système informatisé est créée sur mesure (catégorie n°5 de la classification logicielle des GAMP). Comme nous l'avons vu lors de la définition du besoin, l'utilisateur doit définir avec précision ce qu'il attend du fournisseur dans le cahier des charges et/ou des plans qualité et projet. Néanmoins, ces dispositions contractuelles ne dispensent pas la surveillance des activités convenues entreprises par le fournisseur au moyen de rapports, de revues et d'audits.

2.3.3.2 *La phase de développement*

Le fournisseur doit avoir établi des techniques appropriées pour garantir que le logiciel développé ou configuré satisfait aux exigences prédéfinies dans les spécifications. Il doit avoir développé son propre système de gestion de la qualité, suffisamment performant, que l'utilisateur doit auditer. Les compétences à évaluer se déclinent autour des points suivant :

- les méthodes et les outils de développement,
- les directives qualité et les procédures opérationnelles,
- les règles et les conventions de programmation appliquées,
- les méthodes de revue, principalement du code source,
- l'exécution des tests prédéfinis, notamment d'acceptation système,
- la sécurité et la confidentialité autour du projet.

Des activités de **tests du système en cours de développement** doivent être définies et approuvées. Le but de ces tests est de statuer si l'état de construction du système est satisfaisant pour accéder à l'étape suivante. C'est une garantie supplémentaire pour éviter d'accepter un système qui ne répond pas aux premières exigences de conception. Les phases de test doivent refléter l'architecture et la complexité du système et s'articulent autour de trois documents :

- les tests des modules logiciels[16]
- les tests d'intégration logicielle
- les tests d'**acceptation** du système

Ainsi, si d'éventuels défauts ou insuffisances sont identifiés, mais qu'aucun plan d'action correctif n'a été mis en place, les tests d'**acceptation** doivent refuser le système. On parle de tests FAT (exécutés chez le fournisseur) et de tests SAT (exécutés après installation sur le site de l'utilisateur). Il incombe à l'utilisateur de décider quels rapports doivent lui être soumis pour revue et approbation formelles et de documenter cette décision dans le plan de validation.

[16] Aussi appelés « tests unitaires »

2.3.4 Qualification et maintien de l'état validé

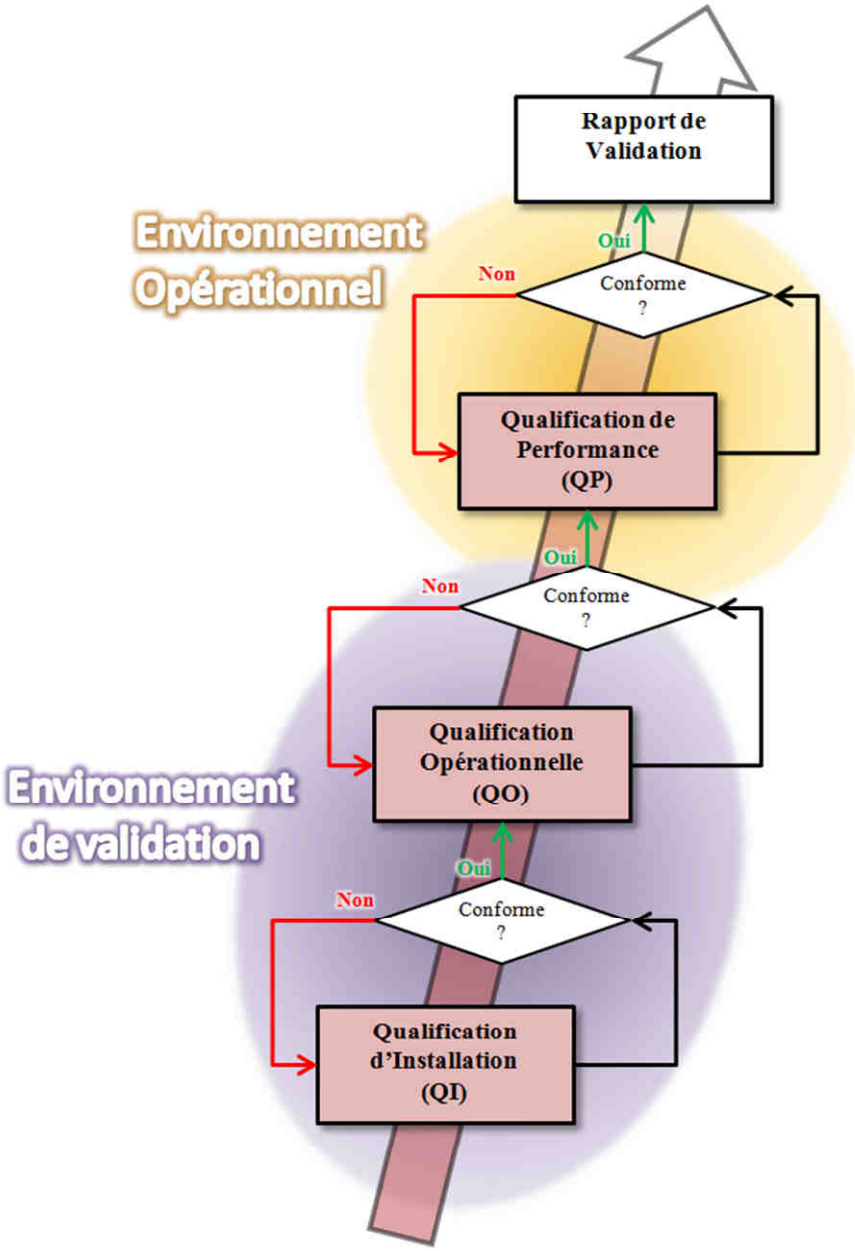
Dans cette troisième et dernière partie du cycle de vie nous allons détailler comment s'organisent les étapes de qualifications. Ces étapes sont très importantes, car elles justifient de façon documentée la couverture complète des exigences précédemment émises. Nous continuons donc après la phase de développement. Le fournisseur livre et installe le système informatique chez l'utilisateur, et le test d'acceptation final sur site (SAT) est réalisé avec succès. Le système est donc correctement installé dans son environnement de validation.

2.3.4.1 *Aperçu des activités de qualification*

Les activités de qualification et de validation font l'objet d'une ligne directrice particulière dans les Bonnes Pratiques de Fabrication. *A minima*, trois phases de qualification sont attendues : la qualification d'installation (QI), la qualification opérationnelle (QO) et la qualification de performance (QP) (cf. Figure 10, page suivante). Ces trois phases s'enchainent obligatoirement dans cet ordre logique, étant donné que les spécifications découlent les unes des autres. Il est par exemple inutile de tester la fonction d'impression si l'installation correcte de l'imprimante n'a pas été vérifiée.

Cette logique d'enchainement des phases de qualification doit être définie dans le plan de validation. Sauf exception particulière, la conformité des résultats d'une phase doit être établie avant de pouvoir passer à la phase de qualification suivante. Les tests d'acceptation exécutés par le fournisseur peuvent constituer une partie des qualifications d'installation et opérationnelle s'ils sont correctement contrôlés et documentés. Cela peut ainsi réduire le volume des tests nécessaires ultérieurement, mais cette stratégie doit être documentée dans le plan de validation.

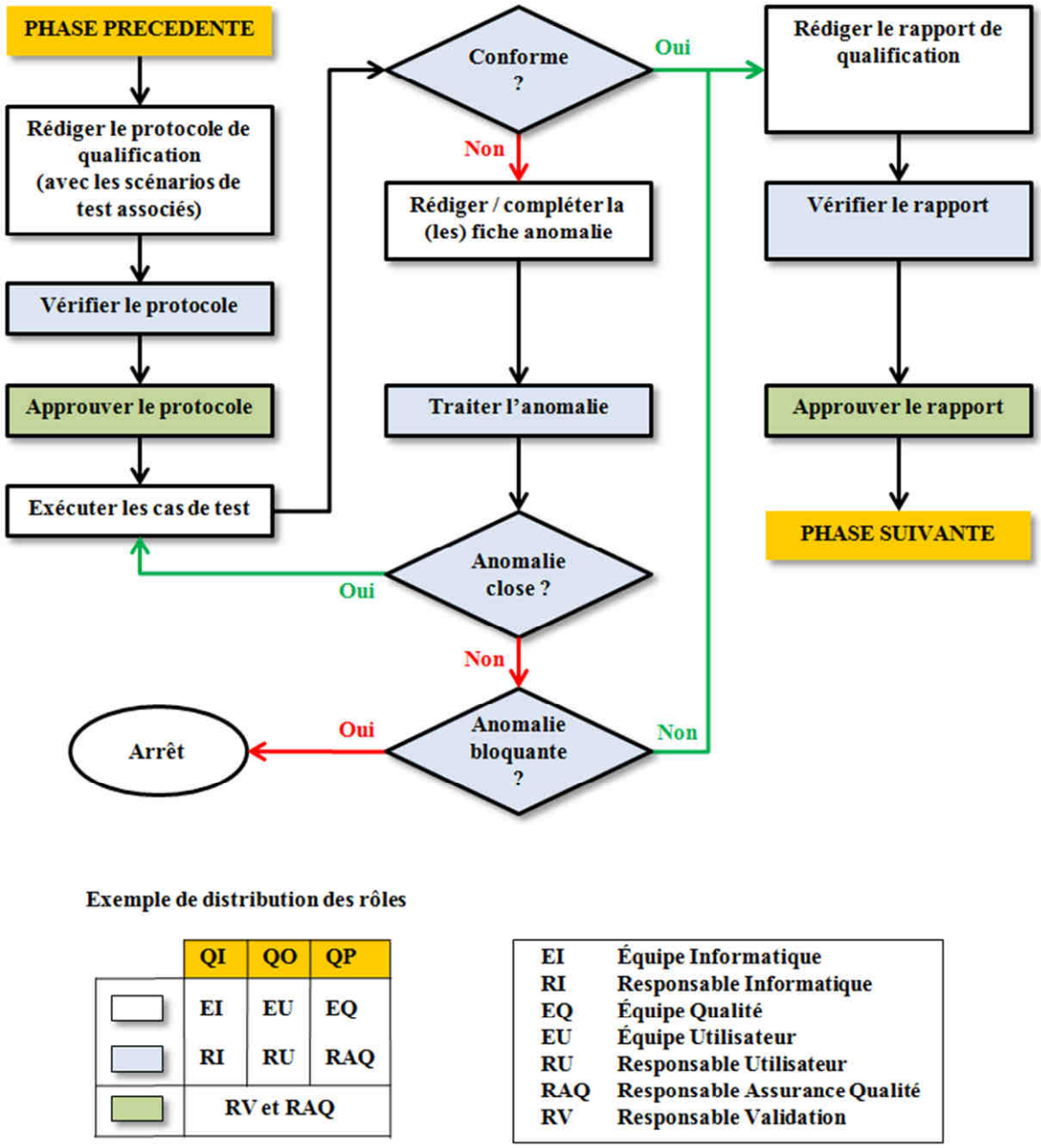
Figure 10 : Enchaînement des étapes de qualification



Les qualifications d'installation et opérationnelle s'effectuent dans un environnement « de validation », jusqu'à la libération officielle du système au terme de cette dernière. En revanche, la qualification de performance s'exécute dans l'environnement opérationnel, c'est-à-dire dans les conditions normales d'exploitation.

Toutes les activités de qualification se déroulent suivant le même procédé, qui comprend au minimum les étapes représentées ci-dessous. Ces activités doivent être décrites dans chacun des trois protocoles de qualification, dont la rédaction doit avoir commencé au moment de la finalisation des spécifications qui y sont associées (cf. Figure 9).

Figure 11 : Schématisation du déroulement classique des phases de qualification



Lors de l'exécution des tests de qualification, certains peuvent échouer, ce qui doit conduire à l'enregistrement d'une **anomalie**. La gestion de ces anomalies est primordiale : il est impossible de continuer la qualification sans les avoir toutes traitées, en évaluant leur impact et tentant de mettre en place des solutions correctives. Le pire cas de figure est une anomalie bloquante[17] pour laquelle aucune solution n'est envisageable. La cause d'une telle non-qualité se trouve très logiquement en amont, du fait d'un mauvais travail préparatoire : mauvaise évaluation du fournisseur, erreur dans la conception du système ou revue de conception inefficace. La qualification s'arrête ; l'équipe chargée du projet doit décider des changements nécessaires dans le cadre d'un processus de maîtrise des changements.

Les anomalies sont donc traitées puis clôturées ; les tests ayant échoués sont exécutés une nouvelle fois. Lorsque le système satisfait l'ensemble des tests avec succès (ou à défaut quand aucune anomalie ne reste plus bloquante) le rapport de qualification est approuvé. Son rôle est de reprendre les résultats des tests pour statuer sur la conformité de la qualification afin de permettre le passage à l'étape de qualification suivante.

Le partage des responsabilités doit être expliqué dans chaque protocoles de qualification. Un exemple classique est représenté par le code couleur de la Figure 11. Le « Responsable Validation » est le responsable du projet de validation dans son ensemble, tel qu'il est défini dans le Plan de Validation initial.

Une fois la qualification de performance terminée, l'utilisateur est responsable de l'élaboration du rapport de validation (cf. Figure 9). Ce document récapitulatif documente la revue de conformité au Plan de Validation de tous les éléments délivrés et de toutes les activités effectuées, preuves à l'appui, pour déclarer que le système est validé.

[17] La classification des anomalies est généralement binaire : bloquante ou non bloquante. Les anomalies bloquantes doivent êtres traitées sans délai pour autoriser le passage dans la phase de qualification suivante.

2.3.4.2 *Protocole de qualification [34]*

Comme toutes les activités de qualification se déroulent suivant le même procédé, la documentation utilisée dans les trois phases est semblable. La description d'une phase de qualification doit être consignée dans un protocole comportant les points suivants.

- Le recensement des documents de référence, c'est-à-dire :
  - les documents Qualité de l'entreprise (SOP[18], réglementations en vigueur)
  - les documents associés au système (l'analyse de risque, processus industriel contrôlé),
  - la documentation du fournisseur ainsi que tous les documents relatifs à la phase en question : installation (QI), utilisation (QO), exploitation (QP).

- La définition du domaine d'application.

  Les éléments du système informatisé doivent être clairement identifiés et séparés des éléments en place, pour déterminer les limites de la validation. Par exemple lors d'une impression des données réalisée sur une imprimante commune à un autre système déjà validé, la présence de cet élément devra être vérifiée en QI, mais la vérification opérationnelle de l'imprimante ne sera pas refaite en QO. Il est primordial de décrire l'organisation du système à l'aide de schémas.

- La description des rôles et responsabilités :

  Quelle que soit l'organisation choisie par l'entreprise, les rôles et responsabilités doivent être clairement définis et justifiés. C'est pourquoi il est impératif de rappeler dans cette section le Responsable de la phase. Les prestataires de services et consultants formés peuvent intervenir dans la conduite des opérations. Concernant la distribution des rôles, il faut établir qui est en charge de la rédaction, de la vérification et de l'approbation de chacun des documents livrable (cf. Figure 11) et définir la personne exécutant les tests.

[18] *Standard Operating Procedure* (Procédure opérationnelle normalisée)

- La description de la phase.
  - La première étape est de définir les prérequis nécessaires à sa mise en œuvre. Par exemple, la réussite des tests d'acceptation fournisseur. Décrire ensuite les différentes étapes envisagées, sous forme de listes[19] de tests à réaliser. Lorsque des tests sont commandés au fournisseur, la revue de son protocole est obligatoire.
  - Un point très important est d'expliquer comment seront gérées les éventuelles anomalies. En pratique une fois constatée, l'anomalie doit être enregistrée et classée selon son impact sur le système (mineur, Majeur, Critique). La correction envisagée doit être tracée et vérifiée avant la clôture de l'anomalie.
  - Enfin, il faut rappeler les règles d'exécution des tests. Ces documents font souvent l'objet de procédures ou de modes opératoires indépendants cités en référence.

- La description des critères d'acceptation.

  Il faut définir les critères pertinents qui permettront de statuer sur la conformité des opérations menées. Ils portent sur :
  - le déroulement de l'exécution,
  - la gestion des anomalies constatées,
  - la documentation d'exploitation produite,
  - la formation du personnel réalisée.

  Ces critères seront vérifiés à chaque rapport de qualification.

Le protocole rédigé, vérifié puis approuvé par l'Assurance Qualité doit être intégré dans le circuit documentaire.

[19] Ces listes sont aussi appelées « cas de test » ou « scénario de test »

2.3.4.3 *Complément d'information pratique*

L'élaboration des cas de tests

- Pour chaque de test, il faut opposer un résultat attendu, compréhensible et approuvé par tous les acteurs de la phase.
- De nombreux tests nécessitent l'adjonction d'une preuve qui garantit leur validité (par exemple un extrait d'audit trail permet de vérifier une fonction de traçabilité). Il est important de préciser directement dans le scénario de test la nature de l'enregistrement attendu ; tout manque de preuve engendrant une anomalie.
- L'utilisation d'une **matrice de traçabilité** est fortement recommandée car le nombre de spécifications à vérifier est généralement très important. Cet outil facilite beaucoup la rédaction et la revue des tests, et **réduit le risque** d'oublis.

L'exécution des cas de tests

La règle d'or est de ne pas être à la fois juge et partie : celui qui exécute les tests ne pas avoir participé à leur élaboration. L'exécution est unique et doit être référencée par un numéro qui garantit sa traçabilité. Le testeur s'engage sur la conduite des tests en apposant sa signature datée à chaque ligne de test, conformément aux règles préétablies. Sur ce point, il convient d'ailleurs d'observer quelques bonnes pratiques :

- Tout document doit être daté et signé.
- Tout document partiellement complété doit en porter clairement la mention et si nécessaire une justification (ex : N/A).
- Les corrections doivent être rayées à l'aide d'une seule ligne de telle sorte que les données d'origine soient encore lisibles ; elles doivent être paraphées, datées et accompagnées d'une brève explication.
- Les documents ne doivent pas être manuscrits, à l'exception bien évidemment des cas de tests qui seront compléter à la main de façon claire, lisible et indélébile.
- Pendant l'exécution, les résultats des tests doivent êtres enregistrés directement sur la fiche de résultat de test ou faire référence aux documents générés par l'ordinateur (par exemple des copies d'écran).
- Le statut de conformité doit être indiqué à chaque ligne de test, par comparaison du résultat et des critères d'acceptation.

- L’étalonnage des instruments de mesure et des appareils de test est obligatoire. La preuve documentée de l’étalonnage est requise.

Pour chaque exécution, la conformité des résultats obtenus est évaluée à la fois par le testeur et par un vérificateur, et cette vérification s’appuie sur les résultats des tests et sur les preuves de validation associées.

La conclusion de l’exécution

Un rapport est rédigé au terme de chaque phase de qualification. Il doit contenir la liste de toutes les anomalies closes et en cours de traitement rencontrées au cours de l’exécution, et indiquer les actions associées. Le Responsable de la validation doit statuer sur la conformité de la qualification par rapport aux critères d’acceptation définis dans le protocole.

2.3.4.4 *La gestion des changements pour le maintien de l'état validé*

Le maintien de l'état validé est une étape importante du cycle de vie du système. Elle nécessite à la fois de maîtriser les changements apportés au système et d'effectuer des revues périodiques [34]. Par ailleurs, l'utilisateur doit établir des plans et des procédures définissant la manière dont toutes les activités de soutien doivent être effectuées et gérées après l'acceptation du système. Ces procédures et ces plans peuvent impliquer le fournisseur dans les activités de support et de maintenance. Dans ce cas, l'engagement du fournisseur est formalisé dans une charte de service (SLA) qui définit la manière dont le service doit être fourni.

La **gestion des changements** est fondamentale au maintien de l'état de validation des systèmes, et ce processus est étroitement lié à celui de la gestion des configurations (évolution de version). Tous les changements doivent être revus, évalués au niveau des impacts et des risques, autorisés, documentés, testés et approuvés avant leur mise en œuvre. La première étape de ce processus est la demande de changement effectuée par l'utilisateur. Cette demande est acceptée ou rejetée par la hiérarchie et le service d'assurance qualité. Les risques associés à l'application du changement et les éventuels plans de retour arrière si la mise en œuvre échoue doivent être évalués, de même que les tests nécessaires à garantir le maintien d'un fonctionnement satisfaisant. L'effet sur les utilisateurs doit aussi être pris en considération (par exemple la mise en place d'un nouveau plan de formation) ainsi que la communication autour du changement. Une fois tous les changements implémentés et testés, la demande est revue pour l'approbation finale et archivage. [21]

Les **revues périodiques** sont utilisées pour vérifier qu'un système informatisé reste en l'état validé et qu'il fonctionne conformément aux réglementations applicables ainsi qu'aux directives et aux procédures de l'entreprise. Elles doivent être planifiées à un intervalle adapté à la criticité et à l'historique opérationnel du système.

Le maintien du niveau de validation est donc maintenu par la gestion des modifications de l'ensemble des composants du système, et par l'évaluation de la revalidation à mener.

- TROISIÈME PARTIE -

VALIDATION D'UN SYSTÈME INFORMATISÉ DE LABORATOIRE

Cette dernière partie vient en complément de notre analyse réglementaire et méthodologique de la validation des systèmes informatisés. La démarche de validation proposée est issue d'une unité de recherche et de développement pharmaceutique du groupe Sanofi Pasteur.

Nous commencerons par présenter l'activité de ce laboratoire et le contexte d'acquisition du nouveau système. Nous commenterons ensuite la stratégie de validation mise en place, avec une attention particulière autour de la méthode de gestion du risque qualité. Enfin, une sélection d'exemples représentatifs des spécifications du besoin et des tests de qualification illustrera les points clés de la validation des systèmes informatisés.

3.1 CONTEXTE PROFESSIONNEL DE LA MISSION [35]

Au sein de l'organisation Recherche & Développement de Sanofi Pasteur, le département ARD EU[20] apporte un support analytique au développement de nouveaux vaccins. Il est en charge de la recherche, du développement, de la validation et du transfert des méthodes analytiques, de la libération et du contrôle en stabilité des produits en développement. Le département est organisé autour de cinq plateformes opérationnelles et d'une plateforme de support qualité. Les **GMP européennes** sont appliquées pour assurer la qualité des produits et la libération des lots destinés à des essais cliniques dans l'Union européenne.

Un projet d'extension des laboratoires a vu le jour courant 2010. Après livraison et qualification des nouveaux locaux, le laboratoire a réceptionné les nouveaux équipements. La validation abordée ici concerne un système informatisé de spectrophotométrie UV-visible, piloté par le logiciel du fournisseur Spectra Manager CFR®. Le laboratoire prévoit d'en faire une double utilisation :

- une utilisation « GMP » destinée aux contrôles libératoires des lots cliniques de phases I, II et III : c'est-à-dire parfaitement sécurisée, avec des méthodes analytiques préétablies et verrouillées.

- une utilisation « non GMP » destinée à la recherche. L'utilisation doit être plus souple et permettre la modification de tous les paramètres de mesure.

[20] *Analytical Research & Development Europe*

3.2 PLANIFICATION DE LA VALIDATION

3.2.1 Évaluation préalable du système

Un formulaire d'évaluation de la criticité et de la complexité a été conçu pour faire une **évaluation préalable des risques** de tous les systèmes entrant dans les laboratoires de recherche et de développement. Cette évaluation est le point de départ de la validation et permet de justifier le type de qualification à réaliser. Le formulaire est rempli par une équipe pluridisciplinaire constituée des signataires finaux : utilisateur, responsable validation et assurance qualité.

Le système est évalué selon deux modalités :

- la **criticité** de son impact qualité sur le processus industriel,
- sa **complexité** liée aux logiciels utilisés.

Le formulaire d'évaluation définit trois niveaux de criticité : Critique, Majeur et mineur. Les différentes utilisations possibles des systèmes sont indiquées dans le formulaire (voir Annexe 3, page 101). À chacune d'elles correspond un niveau de criticité relatif. Le niveau le plus élevé définit la criticité globale du système.

Deux attributs sont possibles pour la complexité : standard ou spécifique, selon les logiciels d'exploitation utilisés. S'ils appartiennent à la catégorie 3 des GAMP, la complexité du système est « standard ». S'ils appartiennent aux catégories 4 ou 5, la complexité du système est « spécifique ».

La combinaison des scores de criticité et de complexité permet de choisir un type de qualification préétabli selon la matrice suivante.

Tableau V : Matrice de choix de la qualification après évaluation des risques

COMPLEXITÉ				
	Spécifique			
	Standard			
		mineur	**Majeur**	**Critique**
		CRITICITÉ		

- **en vert** : qualification « type 1 », correspondant à des vérifications fondamentales.
- **en orange** : qualification « type 2 », initiée par la rédaction d'une SBU[21] suivie par un protocole regroupant : PV, QI, QO, QP et traçabilité SBU / tests de qualification, puis un rapport associé. Représente 90% des systèmes.
- **en rouge** : qualification de « type 3 », initiée par la rédaction d'une SBU, suivie par une analyse de risques détaillée et une qualification de conception avec traçabilité documentée. La qualification nécessite un plan de validation et des protocoles de QI, QO, QP indépendants.

Notre système analytique de spectrophotométrie à un impact qualité critique et sa complexité est standard. Il nécessite une qualification de type 2. Une étape complémentaire est souhaitée : il s'agit de tests d'acceptation sur site (SAT). Le fournisseur a proposé son propre protocole de test, qui peut être accepté après évaluation de sa pertinence.

Tableau VI : les relations entre l'évaluation de criticité / complexité des systèmes informatisés et les étapes de validation

Niveau de criticité du système		**Critique**			**Majeur**			**mineur**		
Étapes	**Catégorie GAMP**	**3**	**4**	**5**	**3**	**4**	**5**	**3**	**4**	**5**
Définition du projet - évaluation de criticité		**X**	**X**	**X**	**X**	**X**	**X**	**X***	**X***	**X***
Définition des besoins (SBU)		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Évaluation des fournisseurs			**X**	**X**						
Spécifications fonctionnelles (FS)			**X**	**X**		**X**	**X**		**X**	**X**
Évaluation des risques / matrice traçabilité			**X**	**X**						
Conception, développement, test, réception			**X**	**X**		**X**	**X**		**X**	**X**
Organisation de la validation			**X**	**X**		**X**	**X**			
Revue de conception			**X**	**X**		**X**	**X**			
Qualification d'installation (QI)		**X**	**X**	**X**	**X**	**X**	**X**			
Qualification opérationnelle (QO)		**X**	**X**	**X**	**X**	**X**	**X**			
Qualification de performance (QP)		**X****	**X**	**X**	**X****	**X**	**X**			
Bilan de validation			**X**	**X**		**X**	**X**			
Maintenance / Exploitation		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Révisions périodiques d'exploitation			**X**	**X**						
Définition des activités de retrait		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**

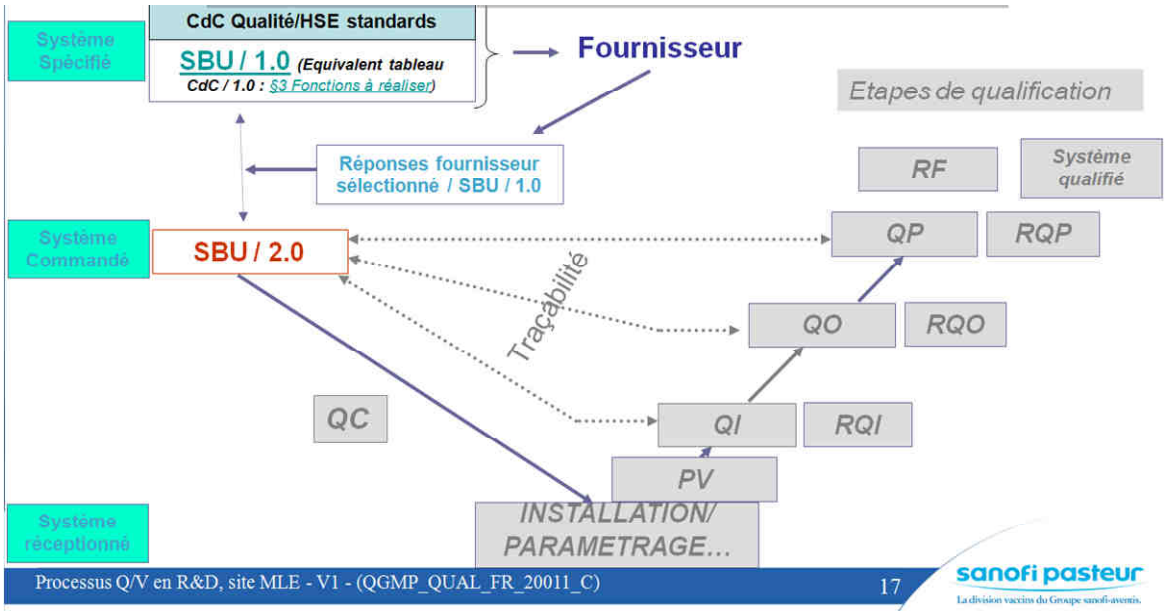
X = applicable systématiquement - **X*** évaluation criticité seule - **X**** = QP1 seule

[21] Pour « spécifications du besoin utilisateur », équivalent en français des URS

Le Tableau VI représente la stratégie de gestion documentaire adoptée par le laboratoire. On retrouve à gauche les principales étapes du modèle en V. Pour le système en question, la volonté du laboratoire est de limiter la documentation des étapes de conception. Cette **simplification du cycle de vie** est logique ; les logiciels de catégorie 3 disponibles dans le commerce étant conçus et testés pour fonctionner invariablement sur un large panel de systèmes.

La SBU est le document clé rassemblant l'ensemble des spécifications du système. C'est pourquoi tous les tests de qualification lui font référence et vérifieront ses spécifications.

Figure 12 : Extrait du support de formation - Chargé de Qualification / Validation



3.2.2 Aperçu de la stratégie de validation du laboratoire

3.2.2.1 *Avant l'achat du système*

La SBU « version 1.0 » est envoyée accompagnée d'un cahier des charges aux fournisseurs potentiels. Le cahier des charges formule les exigences liées au déroulement de la validation et décrit également les contraintes HSE[22] que le fournisseur s'engage à respecter en cas d'intervention sur le site.

Les besoins, exigences et contraintes spécifiés dans la SBU sont référencés pour permettre la traçabilité avec les tests de qualification. Le document est approuvé par le service d'assurance qualité puis envoyé aux fournisseurs potentiels. Chaque fournisseur répond sur la capacité de son système à satisfaire les spécifications définies. Le choix du meilleur système s'est réalisé sur les critères de qualité, de coûts et de délais.

3.2.2.2 *Après l'achat du système*

Après réception et prise en main du système retenu, la SBU « version 1.0 » est mise à jour. L'objectif est de vérifier que le système fonctionne bien comme décrit par le fournisseur dans sa réponse. En pratique, si une spécification n'est pas couverte, une solution alternative doit être mise en place. Ce passage en SBU « version 2.0 » permet de renforcer la connaissance des caractéristiques du système et assure la couverture effective de tous les besoins utilisateurs.

La SBU est tenue à jour durant toute la vie du système informatisé et permettra de retracer l'évolution de son utilisation.

[22] Hygiène ; Sécurité et Environnement

Pour les systèmes non complexes tel que le nôtre, la stratégie de validation n'est pas documentée dans un Plan de Validation indépendant. Les responsabilités, l'enchainement des étapes de validation, la documentation à fournir et les référentiels applicables sont directement documentés dans le protocole de qualification. Le système est référencé dans le Plan Directeur de Validation du laboratoire où sont listés tous les systèmes à valider et les stratégies retenues pour chacun d'eux.

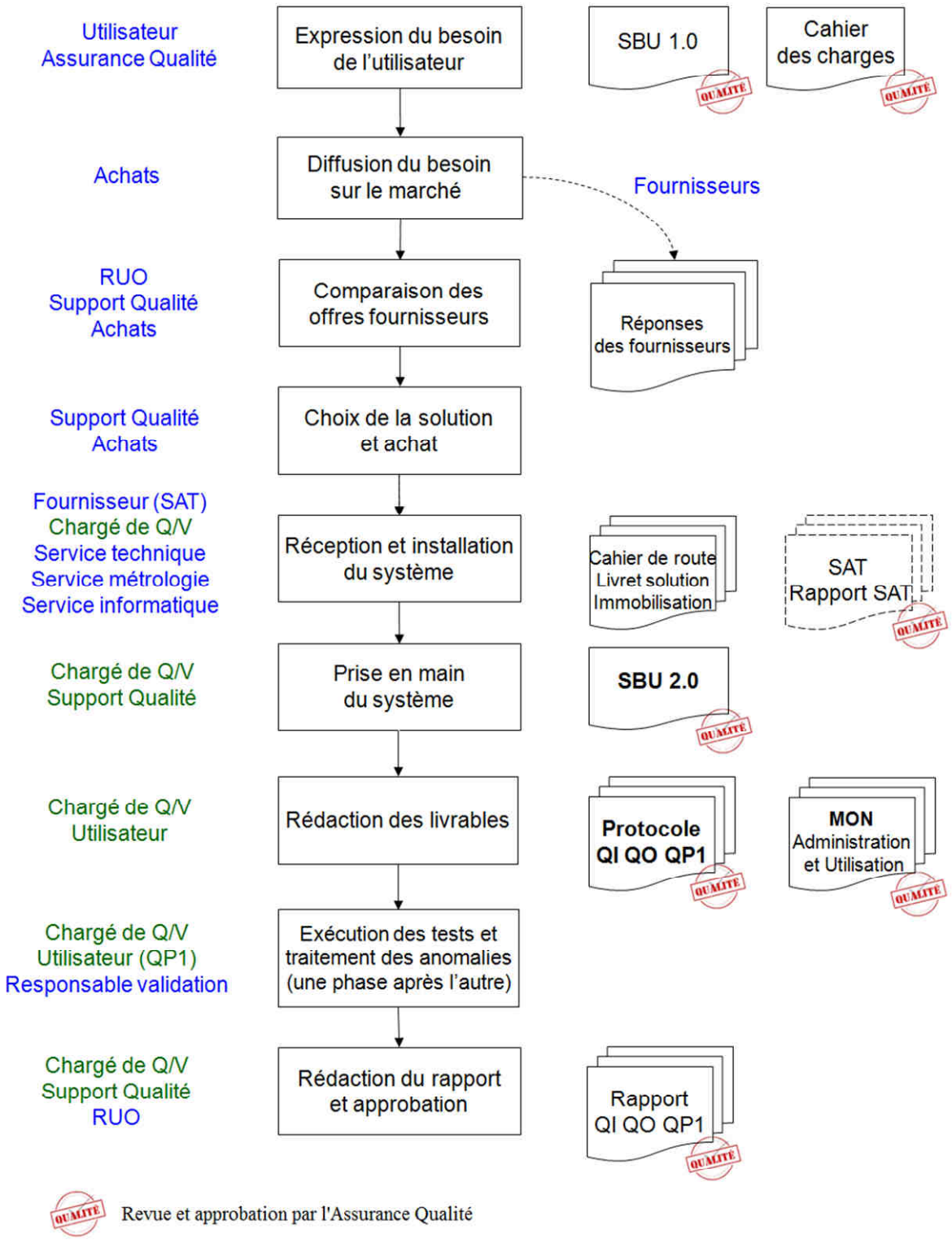
Un **protocole de qualification unique** est rédigé pour les trois étapes de qualification pour réduire le volume documentaire et faciliter la rédaction et les échanges. Par conséquent, un seul rapport de qualification est nécessaire. En revanche, l'approbation d'un responsable est indispensable à chaque étape de qualification pour passer à la suivante. L'autorisation d'utilisation définitive est conclue par l'approbation du rapport de qualification.

La **maîtrise des anomalies** est réalisée conformément à une procédure préétablie ; celles-ci sont systématiquement notifiées à l'Assurance Qualité. Les anomalies bloquantes doivent être résolues avant le passage à l'étape de qualification supérieure. Les actions correctives sont revues et approuvées avant leur mise en œuvre sous couvert du responsable de validation et de l'assurance qualité.

Des **documents d'exploitation** doivent être crées, approuvés et disponibles pour la qualification. Parmi ces documents se trouvent les Modes Opératoires Normalisés (MON).

- Le MON d'utilisation est destiné à l'ensemble du personnel amené à utiliser l'appareil. Il a pour objectif de décrire les opérations nécessaires au lancement d'une analyse en routine, l'exploitation des résultats obtenus, l'enregistrement des données générées et les actions de maintenance.
- Le MON d'administration du système informatisé est destiné aux utilisateurs administrateurs du système. Les notions abordées dans ce document concernent principalement la gestion de la sécurité et des droits d'accès, la sauvegarde et restauration des logiciels et des données ainsi que l'archivage et la restitution des données sur le long terme. Sa diffusion est restreinte.
- Un cahier de route assure la traçabilité des interventions effectuées sur toute la durée de son utilisation.

Figure 13 : résumé des étapes de la validation du système informatisé de spectrophotométrie avec les acteurs et les documents attendus



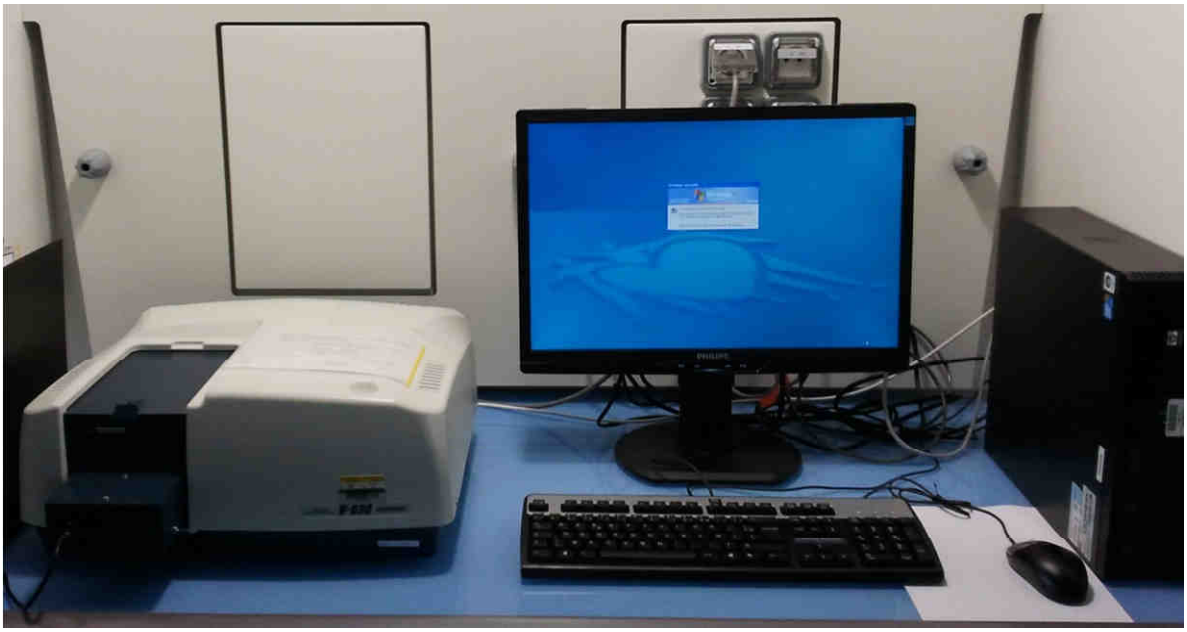
3.3 LA VALIDATION DU SYSTÈME INFORMATISÉ DE SPECTROPHOTOMÉTRIE

3.3.1 Description du système

La partie matérielle du système est composée d'un spectrophotomètre UV-visible de marque JASCO et d'un poste informatique de laboratoire standard ayant pour référence « LabPC ». Ce poste informatique possède une suite logicielle de base configurée par le service informatique de Sanofi Pasteur pour une utilisation en laboratoire. L'utilisateur n'a donc pas besoin de tester les logiciels utilitaires préinstallés (sécurité, archivage de données, etc.). Il peut se concentrer sur le logiciel de pilotage du spectrophotomètre livré par le fournisseur.

Le service informatique (IS) veille sur l'intégrité du système informatique pendant toute la durée d'utilisation. Toute demande de modification logicielle doit être approuvée par un responsable informatique et s'effectue obligatoirement en sa présence. Le système complet a été réceptionné le 21 avril 2011 dans le nouveau laboratoire.

Figure 14 : Le système informatique : PC de laboratoire avec son spectrophotomètre



3.3.2 La SBU

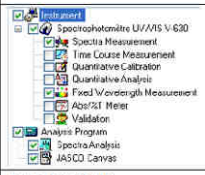
Dans le cadre de la double activité du laboratoire, le système doit être validé et paramétré pour permettre à la fois une activité réglementée dite « GMP », et une activité plus libre « non GMP ». La création de plusieurs types de profil utilisateur ayant chacun différents privilèges et restrictions est donc nécessaire.

Figure 15 : SBU 2.0 – Les trois types de profil utilisateur définis par l'utilisateur

Type de profil utilisateur	Niveau d'accès système	Niveau d'accès workgroups	Rôles
Admin_labo	Administrator	Manager	Gestion des comptes utilisateurs et de leur accès aux groupes de travail (workgroups). Création et validation des méthodes GMP N'a pas le droit de lancer d'analyse
nGMP	Power User	Analyst	Création / modification de méthodes utilisables seulement dans un contexte nGMP. Lancement d'analyses nGMP
GMP	Power User	Operator	Lancement d'analyses selon des méthodes GMP

Tous les paramètres de fonctionnement du système informatisé ont fait l'objet de discussions entre l'utilisateur et le service informatique. Une fois définis, ils sont enregistrés dans la SBU et seront activés avant l'exécution de la qualification de performance.

Figure 16 : SBU 2.0 – Les paramètres critiques du logiciel Spectra Manager CFR®

Emplacement	Paramètre	Valeur
Administrative tools System Policy	Longueur minimale du mot de passe	8 caractères
	Temps d'inactivité avant déconnexion	15 minutes
	Temps avant péremption des mots de passe	60 jours
Administrative tools Instrument : spectrophotometer	Onglet "Adjustement" ☐ Enable the start button	Décoché
	Onglet "Calibration" Wavelength calibrations	UV/Visible
Administrative tools Workgroup [GMP]	Registered instruments and programs	
	Workgroup folder	D:\Archive\GMP
	Registered Users	Au moins "AdminIS", Admin_labo" et Administrator" en tant que managers
	General	N/A
Administrative tools Workgroup [nGMP]	Registered instruments and programs	
	Workgroup folder	D:\Archive\nGMP
	Registered Users	Au moins "AdminIS", Au moins "AdminIS", Admin_labo" et Administrator" en tant que managers
	General	N/A

Les spécifications du besoin utilisateur sont regroupées selon les thèmes suivants :

- Les composants, fonctions et paramètres d'analyse du spectrophotomètre
- La documentation attendue
- Les matériaux spécifiques et l'étalonnage constructeur du spectrophotomètre
- Les contraintes environnementales à respecter
- Les points relatifs au contrat de maintenance
- Les exigences relatives à la partie logicielle du système (compatibilité, gestion des enregistrements électroniques des données, des signatures, des accès, des connexions, gestion de la sauvegarde et la restauration des données, de l'audit trail).

La SBU contient au total 94 spécifications **référencées individuellement** par un code alphanumérique (cf. Figure 17). Cette référence est utilisée dans le protocole de qualification pour assurer **la traçabilité** « spécification – test ».

A la prise en main du système, plusieurs spécifications se sont révélées non satisfaites. En réalité, les réponses techniques apportées par le fournisseur sur les capacités de son système n'étaient pas toujours exactes. En accord avec la stratégie de validation, l'impact de ces écarts sur les besoins initiaux a été évalué et des solutions alternatives mises en œuvre. Les extraits suivants illustrent quelques exemples de spécifications intéressantes.

Figure 17 : SBU 2.0 – Spectrophotomètre V-630 (extraits)

N°	Composants / Modules	Spécification du besoin	Valeurs Critères d'acceptabilité	Acceptabilité	Réponse fournisseur et adaptation du besoin par rapport au système réceptionné	Référence protocole
B1	Composants optiques	Montage	Double faisceau	Impératif	Oui ☒ Double faisceau	Non testé
B2	Composants optiques	Lampes	Deutérium Halogène (tungstène)	Impératif	Oui ☒ Lampe deutérium : de 190 à 350 nm Lampe halogène : de 330 à 1100 nm	Non testé
B3	Modes de fonctionnement	Bande passante	Fixe : 1 nm	Impératif	Non ☒ Accepté à **1,5 nm** (fixe)	Non testé
B4	Modes de fonctionnement	Types de lecture	Spectres (scan) Longueurs d'ondes fixes (5 minimum en simultanée)	Impératif	Oui ☒ Mesure de spectres (spectra measurement), longueurs d'ondes fixes jusqu'à 8 en simultané (fixed wavelength measurement)	AQI0921 2.6 2.4.6
B17	Longueurs d'ondes	Exactitude des longueurs d'onde	Le système est conforme au test "*Contrôle des longueurs d'onde*" de la Pharmacopée européenne en vigueur chapitre 2.2.25 "spectrophotométrie d'absorption dans l'ultraviolet et le visible"	Impératif	Oui ☒ Conforme au test "*Contrôle des longueurs d'onde*" de la Pharmacopée européenne (cf. voir Annexe 3)	AQI0921 2.1

La dernière colonne fait toujours référence au protocole de tests du fournisseur utilisé pour la SAT. Ici, le fournisseur a indiqué qu'il prend en charge le test vérifiant la

spécification **B4**. Ce test peut donc être capitalisé sous réserve d'approbation du protocole par l'AQ. La spécification **B17** exige que le spectrophotomètre soit conforme au standard de la Pharmacopée européenne sur l'exactitude des longueurs d'onde.

Figure 18 : SBU 2.0 – Documentation

N°	Spécification du besoin	Critères d'acceptabilité	Réponse fournisseur et adaptation du besoin par rapport au système réceptionné	Réf. protocole
DOCUMENTS DE QUALIFICATION FOURNISSEUR				
D14	Les protocoles de Qualification fournisseur	Contenu conforme au système livré et conforme aux exigences du Cahier des Charges 129 830 Documentation en français Délai attendu pour les protocoles : 1 mois avant la réception du système	Documentation en **anglais** Protocoles de qualification fournisseur (AQI0976, AQI0930, AQI0921) Documents de tests avec les méthodes utilisées décrites (P/N : 0302-7458B) Photocopies des certificats d'étalonnage du matériel utilisé pour la qualification, avec le raccordement aux étalons officiels La certification du formateur du fournisseur	Non testé
D15	Les documents de tests avec les méthodes utilisées décrites ou référencées			Non testé
D16	Les certificats d'étalonnage de l'équipement avec le raccordement aux étalons officiels			Non testé
D17	La certification éventuelle du fournisseur/constructeur			Non testé

Ci-dessus figurent quelques exemples de spécifications sur la documentation exigée. D'autres spécifications portent sur les documents de conception, les fiches techniques des matériels et du logiciel, les informations contenues dans les manuels d'utilisation, la liste des pièces de rechange ou encore les consignes de sécurité et de maintenance.

Figure 19 : SBU 2.0 – Partie logicielle ; les enregistrements électroniques

N°	Description du besoin	Acceptabilité	Réponse fournisseur et adaptation du besoin par rapport au système réceptionné	Réf. Protocole
ENREGISTREMENTS ELECTRONIQUES				
L6	Les données critiques que le système devra gérer en format électronique sont les suivantes : - Base utilisateurs / comptes utilisateurs et droits (niveaux d'accès) - Base de données si applicable - Configuration - Méthodes d'analyse, séquences, paramétrages et calculs - Données brutes et retraitées - Rapport d'analyse - Rapports d'activité (audit-trail)	Impératif	Les données critiques que le système gère en format électronique sont les suivantes : (formats cf. **L41**) - Comptes utilisateurs et droits (niveaux d'accès) -> **NON. Gestion papier (Cf. L5).** Méthodes d'analyse -> **OUI intégré dans le fichier** - Paramétrages -> **N/A Pas de paramétrage spécifique** - Calculs -> **Evolution du besoin, utilisation de feuilles de calculs Excel (Cf. L16)** - Données brutes et retraitées -> **OUI. intégré dans le fichier.** - Rapport d'analyse (trames CANVAS personnalisables en mode spectre -> **OUI. intégré dans le fichier** ; pas de calculs) - Rapports d'activité -> **L'audit système est exportable en fichier texte.** Les audits méthodes, données et rapports sont intégrés dans les fichiers correspondants.	Non testé

Figure 19 – L'étude approfondie des capacités du système a permis de choisir le format de gestion des données critiques : format papier ou électronique selon le type de donnée. Les calculs associés à l'exploitation des résultats d'analyse seront gérés à l'aide de feuilles de calcul Excel® validées selon un protocole indépendant, du fait des possibilités limitées du logiciel. La **gestion des données électroniques** est un point majeur de la validation des systèmes informatisés. L'utilisateur doit être en mesure de justifier ses choix grâce à son expertise du système.

Figure 20 : SBU 2.0 – Partie logicielle ; les données d'entrée (extrait)

N°	Description du besoin	Acceptabilité	Réponse fournisseur et adaptation du besoin par rapport au système réceptionné	Réf. Protocole
DONNEES D'ENTREE (SAISIES ou RECUES) : PARAMETRAGE ET DONNEES				
L13	**Alertes** : L'insertion de paramètres d'analyse hors des spécifications de l'appareil est impossible (longueur d'onde et vitesse d'acquisition).	Impératif	Oui ☒ Paramètres d'analyses concernés : No of cycles, cycle interval, changeover wavelength, wavelengths (fixed wavelength), scan range, vertical scale (spectra measurement)	Non testé

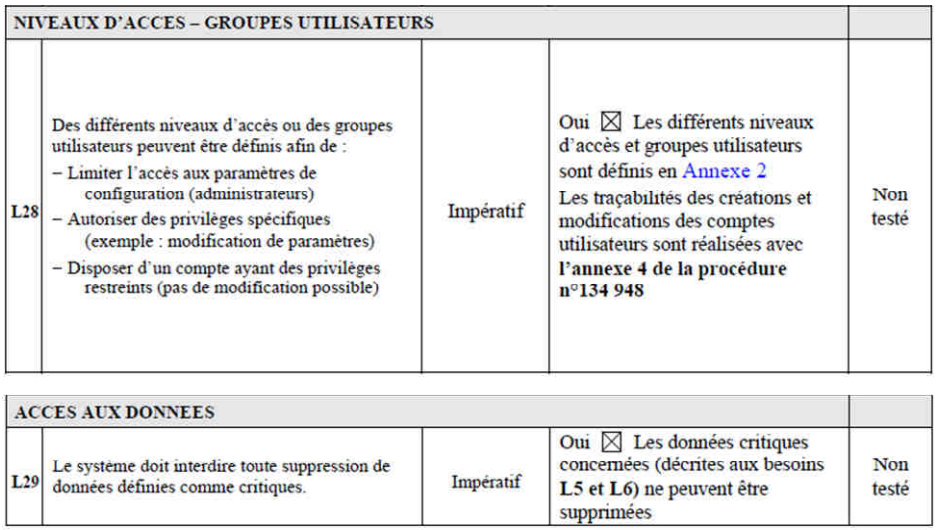
Ce type de spécification est très utile pour **réduire le risque qualité** lié à l'insertion involontaire de données erronées.

Figure 21 : SBU 2.0 – Partie logicielle ; les données en sortie (extrait)

DONNEES EN SORTIE : RESULTATS D'ANALYSE & RAPPORTS				
L21	Le rapport doit contenir les informations suivantes : - Date et Heure d'impression - Analyste - Date et heure d'analyse - Paramètres utilisés pour la mesure (+ nom et version de la méthode d'analyse) - Pagination - Identifiant de l'équipement - Identifiant du produit analysé - Calculs (si applicable) - Expression des résultats dans différentes unités - Statut du résultat (si applicable) - Champs personnalisés	Impératif	Oui ☒ Informations **manquantes** sur le rapport d'analyse : - Date et heure d'impression => **La signature du rapport sera obligatoirement faite le jour du test (Cf. MON n°148 680)** - Version de la méthode d'analyse => **Enregistrement sous un nouveau nom à chaque version (incrémentation)** - Pagination (mode fixed wavelength et spectral measurement) => **la pagination sera celle du dossier analytique** - Statut du résultat = N/A - Champs personnalisés (mode fixed wavelength) -> **Accepté en l'état**	Non testé

Figure 21 – En répondant favorablement à cette spécification, le fournisseur s'est engagé à tort sur les capacités de son système. Le logiciel ne permet pas l'affichage de toutes les informations demandées sur le rapport d'analyse. La solution alternative retenue est l'ajout de consignes supplémentaires dans les documents d'exploitation du système (MON d'utilisation n°148 680).

Figure 22 : SBU 2.0 – Partie logicielle ; les niveaux d'accès (extraits)

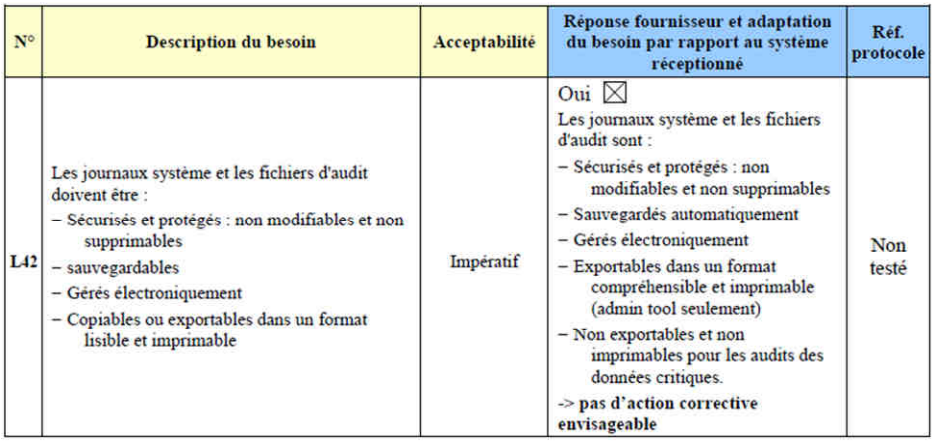


NIVEAUX D'ACCES – GROUPES UTILISATEURS				
L28	Des différents niveaux d'accès ou des groupes utilisateurs peuvent être définis afin de : – Limiter l'accès aux paramètres de configuration (administrateurs) – Autoriser des privilèges spécifiques (exemple : modification de paramètres) – Disposer d'un compte ayant des privilèges restreints (pas de modification possible)	Impératif	Oui ☒ Les différents niveaux d'accès et groupes utilisateurs sont définis en Annexe 2 Les traçabilités des créations et modifications des comptes utilisateurs sont réalisées avec **l'annexe 4 de la procédure n°134 948**	Non testé

ACCES AUX DONNEES				
L29	Le système doit interdire toute suppression de données définies comme critiques.	Impératif	Oui ☒ Les données critiques concernées (décrites aux besoins **L5 et L6**) ne peuvent être supprimées	Non testé

Figure 22 – Au besoin **L28**, le laboratoire précise qu'il assure **la traçabilité** des créations et modifications des comptes utilisateurs à l'aide d'un formulaire papier. La spécification **L29** est d'une importance capitale pour le système, car l'altération ou la perte de données critiques est catastrophique. Les tests doivent anticiper tous les cas de figure, volontaires ou non, pouvant menacer l'intégrité de ces données.

Figure 23 : SBU 2.0 – Partie logicielle ; l'audit trail (extrait)



N°	Description du besoin	Acceptabilité	Réponse fournisseur et adaptation du besoin par rapport au système réceptionné	Réf. protocole
L42	Les journaux système et les fichiers d'audit doivent être : – Sécurisés et protégés : non modifiables et non supprimables – sauvegardables – Gérés électroniquement – Copiables ou exportables dans un format lisible et imprimable	Impératif	Oui ☒ Les journaux système et les fichiers d'audit sont : – Sécurisés et protégés : non modifiables et non supprimables – Sauvegardés automatiquement – Gérés électroniquement – Exportables dans un format compréhensible et imprimable (admin tool seulement) – Non exportables et non imprimables pour les audits des données critiques. **-> pas d'action corrective envisageable**	Non testé

L'audit trail du système ne répond pas complètement au besoin car il est divisé en plusieurs parties. Les connexions au système sont par exemple enregistrées séparément des modifications sur les données critiques, ce qui complique l'élaboration des tests de vérification.

3.3.3 La SAT

Le laboratoire a souhaité capitaliser la qualification proposée par le fournisseur. En effet les tests proposés sur la conformité du système au standard de la Pharmacopée européenne répondent parfaitement aux spécifications de l'utilisateur (cf. besoin **B17** de la Figure 17, page 83). Une fois le protocole de qualification fournisseur approuvé par l'assurance qualité, le fournisseur est autorisé à exécuter les tests.

3.3.4 Les tests de qualification

Pour chacune des étapes de qualification les tests sont regroupés en « fiches de tests » selon leur objectif de vérification. Sur la figure suivante, la dernière colonne référence les spécifications couvertes par leur code alphanumérique assurant la **traçabilité des exigences de l'utilisateur**.

Figure 24 : PQ – Liste des fiches de tests de qualification d'installation (extrait)

N° fiche	Libellé	Objectif	A tester	Capitalisation tests fournisseur	Réf.SBU
FQI 01	Composants	Relever les caractéristiques des composants installés. Vérifier la présence de la documentation technique, l'installation et le repérage des composants. Hors logiciels et programmes.	Oui	Pas de capitalisation	**B1, B2, B3 B5, B7 B10, B11 B12, B14 C4, C5 Annexe 1**
FQI 02	Documentation	Vérifier que les documents sont présents et conformes au système installé.	Oui	Pas de capitalisation	**B8 D1 à D17 L1, L4**

3.3.4.1 *Qualification d'installation*

Les tests de qualification d'installation vérifient les caractéristiques des composants installés, la présence de la documentation technique attendue, les applications logicielles installées avec leur version d'installation, les connexions entre les matériels, le respect des contraintes environnementales d'installation et l'enregistrement du système sur le site (cahier de route, suivi métrologique). La qualification d'installation s'est déroulée sans anomalie.

3.3.4.2 *Qualification opérationnelle*

La qualification opérationnelle représente le volume de tests le plus important. Pour rappel, la qualification opérationnelle est la vérification documentée établissant qu'un système **fonctionne** conformément aux spécifications écrites préalablement approuvées, cela dans l'**ensemble du domaine d'exploitation spécifié**. Il s'agit donc d'élaborer les scénarios de tests permettant de vérifier les fonctionnalités du système définies dans la SBU (liste des fiches de tests en Annexe 4).

La vérification des fonctionnalités du système nécessite l'utilisation de ressources électroniques telles que des données critiques préenregistrées et des comptes d'accès temporaires. C'est pour cela que **l'environnement de validation** doit être anticipé au moment de l'élaboration des tests.

Figure 25 : PQ – FPG : les prérequis généraux à la qualification opérationnelle (extrait)

PRÉ-REQUIS A L'EXÉCUTION DES TESTS QO	
L'ensemble des tests de QI sont exécutés et vérifiés	OUI ☐
Les anomalies bloquantes pour le passage en QO sont soldées	N/A ☐ OUI ☐
Les modifications en cours sont sans impact sur le statut qualifié QI	N/A ☐ OUI ☐

EXÉCUTION DU TEST					
MODE OPERATOIRE		EXECUTION DU TEST			
		CRITERE D'ACCEPTABILITE	RESULTAT OBSERVE	C/ NC	DATE / VISA
1	Le système est inaccessible pour les autres utilisateurs pendant l'exécution des tests QO	Système inaccessible pour d'autres utilisateurs pendant les tests QO			
2	Le poste dispose d'un utilitaire de copie d'écran (Impr Ecran) fonctionnel	Utilitaire de copie d'écran fonctionnel			
3	Vérifier les versions des logiciels faisant l'objet de ce protocole de qualification	Spectra Manager Version 2.08H	Spectra Manager		
4	Des comptes **utilisateur Windows** de test pour accéder au poste métier existe et est fonctionnel. *Précisez le nom des comptes*	Ce compte existe et est opérationnel	Compte utilisateur Windows :		
5	Un compte **administrateur Windows** de test pour accéder au poste métier existe et est fonctionnel. *Précisez le nom du compte*	Ce compte existe et est opérationnel	Compte administrateur Windows :		

En tout début de qualification opérationnelle, une fiche de vérification documentaire reprend la liste des mesures correctives mise en place suite à l'analyse des écarts à la SBU. C'est un test des documents d'exploitation pour vérifier qu'ils sont rédigés, approuvés, disponibles et qu'ils mentionnent bien les actions correctives.

Figure 26 : PQ – FVD : la vérification documentaire

FVD N°IMMO : 122865	VERIFICATION DOCUMENTAIRE	EXECUTION N°.....

Table 1 : Recommandations d'utilisation émises en qualification et mesures correctrices mises en place suite à SBU

Mesures correctives Recommandations d'utilisation Facteurs d'atténuations	Etape	Document de référence Numéro / Version et chapitre
Actions correctrices mise en place suite à l'analyse des écarts à la SBU :		
- La création, modification ou suppression de compte utilisateur doit être tracé en utilisant l'annexe 4 de la procédure n°134 948.	L5, L6 L28 L43	.....
- Les informations initialement manquantes sur les rapports d'analyses du logiciel doivent être manuellement apportées afin de couvrir le besoin.	L21	.....
- Rappeler à l'utilisateur de respecter les règles de sécurité concernant les mots de passe, tels que définis dans la procédure n°134 948	L30	.....
- Rappeler à l'administrateur du système que l'audit trail ne trace pas les blocages de compte. Chaque intervention pour réinitialisation doit être mentionnée dans le cahier de route de l'appareil.	L43	.....

Par exemple, pour le besoin **L21** (revoir la Figure 21, page 85), il faut vérifier dans le document n°148 680 que l'opérateur a pour consigne de dater manuellement et de signer les résultats directement après impression d'un rapport d'analyse.

Toutes les fiches de tests de qualification opérationnelle possèdent une « annexe de traçabilité » semblable à la suivante.

Figure 27 : PQ – FQO03 : gestion des comptes utilisateurs, annexe de traçabilité

FQO 03 N°IMMO : 122 865	GESTIONS DES COMPTES & DES PROFILS UTILISATEURS DANS SPECTRA MANAGER	EXECUTION N°.....

FQO 03 – Annexe TRACABILITE						
N°	DATE	HEURE	ACTION	QUI	AVANT	APRES
12			Création d'un compte utilisateur			
14			Modification d'un compte utilisateur (accès workgroup) ou modification d'un workgroup			
54			Création d'un workgroup			
55			Suppression d'un workgroup			
66			Modification d'un compte utilisateur (accès système)			
69			Suppression d'un compte utilisateur			

Au fur et à mesure des tests, les informations critiques rencontrées sont enregistrées sur ce document. La comparaison de ces informations avec le contenu de l'audit trail permettra de valider celui-ci en fin de qualification opérationnelle.

En plus de l'annexe de traçabilité, les fiches de tests possèdent un espace de « synthèse d'exécution ». Cet espace est réservé aux commentaires, tels que l'explication des erreurs pouvant survenir au cours des tests.

3.3.4.3 *Gestion d'une anomalie*

Lors de l'exécution des tests de qualification opérationnelle, une faille a été détectée au niveau de l'audit trail du logiciel. Celui-ci n'enregistre pas la déconnexion automatique d'un compte utilisateur quand elle a lieu après un temps d'inactivité trop important. Le test en question est le suivant :

Figure 28 : Rapport – FQO04 : test de déconnexion automatique

Déconnexion automatique				
9	Se connecter au logiciel avec le compte administrateur : ....QO.adminlabo. *Noter la date et l'heure :* ...09/08/11.. 14H49 ☒			
10	Ne pas utiliser l'application pendant 15 min. ☒			
11	Vérifier que l'application se déconnecte automatiquement au bout de 15 min d'inactivité. *Noter la date et l'heure :* 09/08/11 à 15H14	Déconnexion automatique effective	C	0 9 AOUT 2011 JFR/JFo

La déconnexion automatique fonctionne donc bien. Mais l'enregistrement de la déconnexion attendu au 09/08/2011 à 15h14 est absent du journal d'audit. Ce test de vérification a lieu lors de l'exécution de la fiche de test suivante.

Figure 29 : Rapport – FQO10 : vérification de l'audit trail (extrait)

Vérification des Annexes Audit trail de ce protocole				
15	S'assurer que toutes les annexes « Audit trail » de chaque FQO ont été correctement remplis ☒			
16	S'assurer que toutes les impressions d'audit issues de chaque application sont disponibles. Sinon, réaliser les impressions complémentaires à celles déjà imprimées. Cf. Ann...5.....p...15 à 22 et p 11 à 14 + p 24 ☒			
17	Pour toutes les actions listées dans chaque annexe de FQO. Vérifier que toutes les informations sont tracées dans le système.	☑ Les actions tracées sur les annexes de ce protocole se retrouvent toutes dans le système.	NC FA n°1	1 1 AOUT 2011 JFR/JFo

SYNTHÈSE D'EXÉCUTION DU TEST		
N° d'étape	**Observations / Anomalies**	**Date/Visa**
17	Le test de déconnexion automatique effectué en FQO04 test n°11 n'est pas tracé dans l'audit trail. Voir FA n°1 ouverte le 11 août et soldée le 17 août. La fiche d'anomalie est soldée sans actions correctives particulières, le système est accepté en l'état. 17/08/2011 JFo	1 1 AOUT 2011 JFR/JFo

Cette non-conformité engendre l'ouverture d'une fiche d'anomalie (cf. Annexe 5 page 105). Comme aucune solution simple ne peut être apportée et que l'impact qualité est **minime**, l'anomalie est clôturée en l'état sans action corrective.

3.3.4.1 *Qualification de performance*

Les tests de qualification de performance vérifient que le système informatisé est prêt à piloter le processus analytique qui lui incombe dans l'environnement opérationnel spécifié et conformément au besoin de l'utilisateur.

Figure 30 : PQ – Liste des fiches de tests de qualification de performance

N° fiche	Libellé	Objectif	Réf.SBU.
FPG	Pré-requis Généraux	Vérifier les conditions générales permettant de débuter l'exécution des tests de Qualification des Performances du système informatisé	N/A
FQP 01	Qualification du personnel	Vérifier que les personnes utilisatrices du système ont leurs droits d'accès configurés dans le logiciel Spectra Manager, qu'elles sont formées à l'utilisation de l'équipement et du logiciel, et que leur niveau de formation est en adéquation avec leur profil utilisateur.	N/A
FQP 02	Documents d'exploitation	Vérifier la présence et la mise à disposition d'une structure documentaire appropriée	N/A

La qualification de performance est essentiellement documentaire. La deuxième fiche de tests est particulièrement importante car elle demande de vérifier l'état de la documentation liée au système informatisé (cf. Annexe 6).

3.3.1 Maintien de l'état validé

En cas de changement d'utilisation du système, une réévaluation de la criticité devra être faite pour identifier les éventuels tests complémentaires ou le nouveau type de qualification applicable.

3.4 CONCLUSION PARTIE 3

Le laboratoire a su définir une stratégie de validation cohérente basée sur la gestion du risque qualité en plusieurs étapes. La simplification du cycle de vie est justifiée et la traçabilité des spécifications permet de revenir à tout moment sur le besoin de l'utilisateur. En revanche, cet exemple montre combien l'absence d'audit du fournisseur peut être problématique : il est plus difficile de contester le fonctionnement d'un système accepté.

CONCLUSION GÉNÉRALE

Finalement, l'évolution récente de la réglementation européenne concernant les systèmes informatisés dans l'industrie pharmaceutique apporte de nombreux changements. Cette refonte réglementaire est articulée autour du concept de gestion du risque qualité, introduit pour la première fois dans le référentiel européen en 2006. C'est pourquoi cette mise à jour ne devrait pas fondamentalement bousculer les habitudes des entreprises. En revanche, elle définit le nouveau standard de qualité acceptable sur lequel les autorités compétentes de l'Union européenne s'appuieront pour mener les inspections.

L'élaboration d'une stratégie de validation efficace est un processus complexe qui repose sur la connaissance des processus industriels et des technologies associés. L'expérience extraite des activités de validation passées participe à l'enrichissement de ces connaissances favorisant ainsi l'amélioration continue de la stratégie de validation.

La méthodologie de validation que nous avons développée est basée sur les principes fondamentaux communément admis. La méthode parfaite n'existe pas car l'objectif industriel est de tendre vers le meilleur rapport bénéfices / risques, en fournissant un effort contrôlé, nécessaire et suffisant. Le véritable enjeu de la validation des systèmes informatisés repose sur cet équilibre. L'assurance qualité n'a pas pour vocation de freiner l'innovation technologique en augmentant toujours plus le nombre de contrôles et le volume de documents. Sa mission est de garantir la qualité des médicaments et la sécurité des patients.

La validation des systèmes informatisés est un marché en pleine expansion, dans lequel les sociétés de consulting sont déjà bien installées. Le développement croissant de l'informatisation industrielle laisse à penser que dans les années à venir, les compétences techniques liées à l'automatisation et à la programmation logicielle seront de plus en plus recherchées.

- ANNEXES -

Annexe 1 : les BPF Européennes - Annexe 11 - Version 1992
(Page 1 sur 2)

LD.11. SYSTÈMES INFORMATISÉS

PRINCIPE

L'introduction des systèmes informatisés dans les systèmes de fabrication comprenant le stockage, la distribution et le contrôle de la qualité n'enlève rien à l'obligation d'appliquer les principes figurant dans le guide. Lorsqu'un système informatisé remplace une opération manuelle, il ne faut pas que la qualité du produit ou l'assurance de la qualité en soit affectée. Il faut tenir compte du risque de perdre certains aspects du système précédent en réduisant l'implication des opérateurs.

PERSONNEL

1. Il est essentiel de veiller à ce qu'il y ait une coopération étroite entre le personnel occupant les postes clés et le personnel chargé des systèmes informatisés. Les personnes assumant des responsabilités doivent recevoir une formation appropriée en vue de la gestion et de l'utilisation de systèmes informatisés dans leur domaine de responsabilité. Cela devrait garantir que la compétence appropriée est disponible et mise à profit pour fournir toute assistance dans le domaine de la conception, de la validation, de l'installation et du fonctionnement des systèmes informatisés.

VALIDATION

2. Le degré de validation nécessaire dépend d'un certain nombre de facteurs et notamment de l'usage auquel le système va être destiné, de sa nature prospective ou rétrospective et de l'introduction ou non de nouveaux éléments. La validation doit être considérée comme une partie de l'ensemble du cycle de vie d'un système informatique. Ce cycle comprend plusieurs étapes qui sont la planification, la spécification, la programmation, les essais, la réception, la documentation, l'exploitation, le contrôle et les modifications.

SYSTÈME

3. Le matériel doit être installé dans un cadre approprié de sorte que des facteurs extérieurs ne puissent causer des interférences.

4. Une description écrite et détaillée du système doit être établie (éventuellement avec des diagrammes) et mise à jour régulièrement. Les principes, les objectifs, les mesures de sécurité et la portée du système, ainsi que les principales caractéristiques du fonctionnement de l'ordinateur et de son interaction avec d'autres systèmes et procédures devront être décrits.

5. Le logiciel est un composant primordial de tout système informatisé. L'utilisateur du logiciel doit prendre toute les mesures qui peuvent être raisonnablement requises pour s'assurer que le logiciel a été produit conformément à un système d'assurance de la qualité.

6. Le cas échéant, le système doit comprendre des contrôles automatiques de la saisie et du traitement exacts des données.

7. Avant sa mise en service, tout système informatisé doit être minutieusement contrôlé et jugé capable d'atteindre les objectifs fixés. S'il doit remplacer un système manuel, les deux doivent fonctionner en parallèle pendant un certain temps dans le cadre de la procédure d'essai et de validation.

8. Les données ne doivent être introduites ou modifiées que par des personnes autorisées. Afin d'éviter l'introduction non autorisée de données, les moyens les plus appropriés comprennent l'usage d'une clé, d'une carte d'accès ou d'un code personnel ou encore la limite d'accès aux terminaux. Il faut prévoir une procédure pour l'octroi, le retrait et le changement de l'autorisation d'introduire et de modifier les données, y compris pour la modification des mots de passe personnels. Il convient d'envisager des

Annexe 1 : les BPF Européennes - Annexe 11 - Version 1992
(Page 2 sur 2)

systèmes permettant l'enregistrement des tentatives d'accès de personnes non autorisées.

9. Lorsque les données importantes sont introduites manuellement (par exemple, le poids et le numéro du lot d'un ingrédient au cours d'une préparation), il est nécessaire de prévoir un contrôle supplémentaire pour vérifier l'exactitude de ce qui est enregistré. Ce contrôle peut être effectué par un deuxième opérateur ou par des moyens électroniques validés.

10. Le système doit enregistrer l'identité des opérateurs qui introduisent ou confirment des données importantes. L'autorisation de modifier les données introduites doit être réservée à des personnes désignées nommément. Toute modification de données importantes doit être autorisée et enregistrée, avec le motif du changement. Il convient d'envisager le système capable de produire un enregistrement complet de toutes les entrées et modifications (« succession d'audits » ou « piste pour audits »).

11. Toute modification d'un système ou programme informatisé doit être réalisée conformément à une procédure définie prévoyant des dispositions relatives à la validation, au contrôle, à l'autorisation et à la mise en œuvre de la modification. Cette modification ne peut être exécutée qu'avec l'autorisation de la personne responsable de la partie du système concernée et doit être enregistrée. Toute modification importante doit être validée.

12. En vue d'un audit sur la qualité, il doit être possible d'obtenir des sorties en clair de données stockées électroniquement.

13. Les données doivent être protégées par des moyens physiques, ou électroniques contre les dommages accidentels ou volontaires et ce conformément au point 4.9. du guide. Les données stockées doivent être contrôlées en vue de garantir leur accessibilité, leur stabilité et leur précision. Si des modifications de l'équipement informatique ou des programmes sont proposées, les contrôles susmentionnés doivent être effectués à une fréquence appropriée au support du stockage de l'information.

14. Les données doivent être protégées par des opérations de sauvegarde effectuées à intervalles réguliers. Les données sauvegardées doivent être stockées aussi longtemps que cela est nécessaire dans des emplacements séparés et sûrs.

15. Il convient de prévoir des mesures de remplacement adéquates permettant le fonctionnement des systèmes qui doivent être mis en oeuvre en cas de panne. Le temps nécessaire à la mise en place des mesures de remplacement doit être en rapport avec le degré d'urgence. A titre d'exemple, les données nécessaires aux rappels doivent être disponibles rapidement.

16. Les procédures à suivre en cas de défaillances ou d'arrêts doivent être définies et validées. Toutes les défaillances et les mesures prises pour y remédier doivent être enregistrées.

17. Une procédure doit être établie pour l'enregistrement et l'analyse des erreurs et pour leur correction.

18. Lorsqu'il est fait appel à une entreprise extérieure pour une prestation de service dans le domaine de l'informatique, il faut prévoir un accord formel précisant clairement les responsabilités de ce contractant (cf. chapitre 7).

19. Lorsque la libération des lots en vue de la vente ou de la distribution est effectuée au moyen d'un système informatisé, ce système devra être programmé de sorte que seul le pharmacien responsable ou le pharmacien qu'il a autorisé à le faire puisse libérer ces lots. L'identité de la personne qui a libéré ces lots doit être clairement relevée et enregistrée.

Annexe 2 : les BPF Européennes - Annexe 11 - Version 2011
(Page 1 sur 4)

Commission Européenne, B-1049 Bruxelles / Europese Commissie,
B-1049 Brussel - Belgium
Telephone: (32-2) 299 11 11

Principle

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

The application should be validated; IT infrastructure should be qualified.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

General

1. *Risk Management*

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

2. *Personnel*

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

3. *Suppliers and Service Providers*

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

Project Phase

4. *Validation*

4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.

For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

Operational Phase

5. ***Data***

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

6. ***Accuracy Checks***

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

7. ***Data Storage***

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.

8. ***Printouts***

8.1 It should be possible to obtain clear printed copies of electronically stored data.

8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

9. ***Audit Trails***

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

10. ***Change and Configuration Management***

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

11. ***Periodic evaluation***

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

12. ***Security***

12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

12.2 The extent of security controls depends on the criticality of the computerised system.

12.3 Creation, change, and cancellation of access authorisations should be recorded.

12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

13. ***Incident Management***

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

14. ***Electronic Signature***

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

15. ***Batch release***

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

16. ***Business Continuity***

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

17. ***Archiving***

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Glossary

Application: Software installed on a defined platform/hardware providing specific functionality

Bespoke/Customized computerised system: A computerised system individually designed to suit a specific business process

Commercial of the shelf software: Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.

IT Infrastructure: The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Life cycle: All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

Process owner: The person responsible for the business process.

System owner: The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.

Third Party: Parties not directly managed by the holder of the manufacturing and/or import authorisation.

Annexe 3 : Formulaire d'évaluation de la criticité et de la complexité des systèmes (Page 1 sur 2)

EVALUATION DE LA CRITICITE ET COMPLEXITE DES SYSTEMES					Rapport n° : 148 681 Annexe 1. page 2
IDENTIFICATION DU SYSTEME A EVALUER (* : les données pourront être complétées après approbation avec date et visa)					
Système (*)	*Type :* Spectrophotomètre UV-Visible *Fournisseur/Modèle :* Jasco / V630 *Nom/version logiciel :* Spectra Manager / V.2.08.04		**Localisation** (bâtiment-salle)/ **N°IMMO (*)**	Temporary Lab (F') local 105 n° immo 122865	
			Propriétaire *(Fonction / Nom)*	RUO du laboratoire / Sandrine Lemoine	L-Granger 01 Sep 2011 (Gr
Département PF/ Service	**Recherche** ☐ - **ARD EU** ☒ - **BRD EU** ☐ - **Autres** ☐ : ..... **PF :** Biochimie **Service :** Laboratoire de Biochimie				

EVALUATION DE CRITICITE					
SYSTEME UTILISE POUR :	**C**	**M**	**m**		**Justification**
I - La fabrication d'un lot				**N/A** ☒	
• 1-Utilité/Gaz à usage pharmaceutique en contact produit	☐			N/A☐	
• 2-Pendant l'étape de purification du produit	☐	☐		N/A☐	
• 3-Pendant l'étape d'inactivation du produit	☐			N/A☐	
• 4-Après le stade Vrac de fabrication du produit	☐			N/A☐	
• 5-Avant étape de purification et/ou inactivation		☐	☐	N/A☐	
• 6-Utilité/Gaz à usage pharmaceutique sans contact produit			☐	N/A☐	
II - Tester / contrôler le produit ou son environnement				**N/A** ☐	
• Utilisé dans le processus de contrôle du produit avec impact direct sur le résultat de :					
1-tests « libératoires » (décrits dans la spéc. de contrôle du produit)	☒			N/A☐	
2-tests de stabilité	☒			N/A☐	
3-contrôles en cours de fabrication (*IPC*)	☒			N/A☐	
4-tests de suivi du procédé (*PMT*, tests non critiques permettant de surveiller le procédé et/ou garantir sa performance)		☒	☐	N/A☐	
• 5-Utilisé dans le processus d'analyse du produit avec impact potentiel sur le résultat		☐		N/A☒	
• 6-Utilisé dans le processus d'analyse du produit sans impact sur le résultat			☐	N/A☒	
III - Le stockage de produit				**N/A** ☒	
• 1-au cours de la fabrication (avant étape de répartition)		☐		N/A☐	
• 2-au cours de la fabrication (après étape de répartition)	☐			N/A☐	
• 3-pour étude de stabilité	☐			N/A☐	
• 4-en contrôle		☐		N/A☐	

Annexe 3 : Formulaire d'évaluation de la criticité et de la complexité des systèmes (Page 2 sur 2)

EVALUATION DE LA CRITICITE ET CATEGORISATION DES SYSTEMES					Rapport n°: 148 6 Annexe 1. page 3
EVALUATION DE CRITICITE				Type système ou N°IMMO (*) : Spectrophotomètre UV-Visible	
SYSTEME UTILISE POUR :	C	M	m		Justification / Commentaires
IV - Le nettoyage, la stérilisation ou la dépyrogénation				N/A ☒	
• 1- en fabrication	☐			N/A ☐	
• 2- en contrôle		☐		N/A ☐	
V - La décontamination				N/A ☒	
• 1-des locaux	☐			N/A ☐	
• 2-des déchets, effluents		☐		N/A ☐	
VI - Environnement				N/A ☒	
• 1-Les locaux / HFL / PSM / HVAC	NB1(C)☐ NB2(M)☐ NB3(m)☐ Autre :..... ..... ou N/A ☐				
• 2-Préparation du matériel destiné à zone en	NB1(C)☐ NB2(M)☐ NB3(m)☐ Autre :... .... ou N/A ☐				
• 3-Suivi environnemental de zones en	NB1(C)☐ NB2(M)☐ NB3(m)☐ Autre :..... ... .. ou N/A ☐				
VII - Autre utilisation				N/A ☒	
.....	☐	☐	☐		
Niveau le plus élevé déterminé :	**Critique(C) ☒- Majeur(M) ☐- mineur(m) ☐**				
EVALUATION DE LA COMPLEXITE					
Quelle est la Complexité du système ?	☒ Standard		☐ Spécifique (« à façon »)		
Si logiciel, Catégorie GAMP 5 ? ou N/A ☐ (sans logiciel)	☒ Catégorie 3		☐ Catégorie 4	☐ Catégorie 5	
DETERMINATION DU TYPE DE QUALIFICATION et DOCUMENTS APPLICABLES (voir § 7.1.3.3 et 7.1.3.4)					
Type de Qualification :	DOCUMENTS APPLICABLES				
QUALIFICATION TYPE 1 ☐	PQ TYPE 1 ☐				
QUALIFICATION TYPE 2 ☐	SBU ☒ PQ TYPE 2 ☒				
QUALIFICATION TYPE 3 ☐	FAT ☐ SAT ☐ SBU ☐ PV ☐ AR ☐ QC ☐ QI ☐ QO ☐ QP ☐				
+ ETAPES COMPLEMENTAIRES : SF ☐ - Audit ☐ - QC ☐ - FAT ☐ SAT ☒ - AR ☐ ou ☐ N/A					
☐ CCR n°...../ Indiquer la nature du changement : Changement d'utilisation ☐ - Evolution du besoin utilisateur ☐ - Autre ☐					
Rationnel/Commentaires : SAT acceptés selon la pertinence du protocole fournisseur .... **A titre indicatif** : Dans le cadre du projet NV :.....Date fin validation cible :.....	**Date fin Qualif. cible** (QO ou QP système) : 30 Juil. 2011 **Garant** (Nom/Prénom): GRANGER Laurent				
APPROBATION					
Représentant Utilisateur	Nom/P. : GRANGER L.	Date 02/Août/2010	Signature :		
Propriétaire du système	Nom/P. : LENOINE S.	Date 02/Août/2010	Signature :		
Responsable Q/V	Nom/P. : PECHARD A	Date 02/08/2010	Signature :		
AQ R&D Q/V	Nom/P. : C. BERTHILLER	Date 02/08/10	Signature :		

Annexe 4 : Liste des fiches de tests de qualification opérationnelle
(Page 1 sur 2)

N° fiche	Libellé	Objectif	Capitalisation tests fournisseur	Réf.SBU
FPG	Pré-requis Généraux	Vérifier les conditions générales permettant de débuter l'exécution des tests de qualification opérationnelle	Pas de capitalisation	**N/A**
FVD	Vérification documentaire	Vérifier que les documents nécessaires à l'utilisation du système sont approuvés Vérification de la prise en compte des recommandations d'utilisation dans les documents d'exploitation	Pas de capitalisation	**L5, L6, L21, L20, L28, L30, L35, L40, L41, L43** **Annexe 5**
FQO 01	Etalonnage	Vérifier que les chaines de mesure critiques sont identifiées et étalonnées.	Capitalisation selon SBU	**B4, B13 B15, B16 L30**
FQO 02	Configuration du logiciel	Vérifier la prise en compte des paramètres de configuration du logiciel	Pas de capitalisation	**L30, L34, L36, L38** **Annexe 4**
FQO 03	Gestion des comptes & profils utilisateurs dans Spectra Manager	Vérifier le paramétrage des profils dans Spectra Manager permet d'assurer la sécurisation du logiciel	Pas de capitalisation	**L27, L28 L30, L32 L11** **Annexe 2**
FQO 04	Gestion des accès et des connexions aux applications	Vérifier que le paramétrage des accès et des connexions permet de sécuriser les accès aux applications liées à l'utilisation du système et donc l'intégrité des données	Pas de capitalisation	**L25, L26 L30, L31 L33, L34 L35, L36 L37**
FQO 05	Gestion des données critiques	Vérifier la prise en compte de la configuration et la traçabilité lors de la création, modification de paramètres des données critiques : méthodes, données, rapports et audit trail	Pas de capitalisation	**L5, L6 L17, L29 L38**

Annexe 4 : Liste des fiches de tests de qualification opérationnelle
(Page 2 sur 2)

N° fiche	Libellé	Objectif	Capitalisation tests fournisseur	Réf.SBU
FQO 06	Fonctionnalités principales	Vérifier la prise en compte de la configuration des paramètres d'accès aux données, l'intégrité des données acquises et la communication des modules du système	Pas de capitalisation	**B4, B6, B9 B21, L3 L9, L10 L11, L14 L23**
FQO 07	Gestion des conditions de stress et alarmes	Vérifier que le système réagit conformément aux spécifications fournisseur lors de situations non familières	Pas de capitalisation	**B6, C4**
FQO 08	Paramétrage de valeurs aberrantes	Vérifier que le système refuse de prendre en compte les paramètres lorsque ceux-ci sont hors des limites fixées	Pas de capitalisation	**L13**
FQO 09	Impression	Vérifier que les impressions des méthodes et résultats, sont intègres, exactes et contiennent toutes les informations nécessaires selon les besoins utilisateurs	Pas de capitalisation	**L5, L21 L22**
FQO 10	Traçabilité	Vérifier que toutes les actions critiques réalisées sur le système sont tracées et qu'elles ne sont ni modifiables ni supprimables	Pas de capitalisation	**L7, L42 L43, L44**
FQO 11	Tests Pharmacopée et tests capitalisés	Vérifier la conformité des tests par rapport au protocole fournisseur et à la Pharmacopée Européenne en vigueur § 2.2.25	Capitalisation selon SBU	**B17, B18 B19, B20 Annexe 3**

FICHE D'ANOMALIE N°1 EN COURS DE VALIDATION (Page 1 de 1) QC ☐ QI ☐ **QO** ☑ QP ☐ VN ☐

Equipement / système : **Spectrophotomètre UV-Vis V-630 JASCO** N° d'immatriculation : **122865**

N° protocole : **148 681** 148 327 N° d'exécution : 1 FQO : **10** N° Test(s) : **17**

Rédigé par : **Jean-François ROUSSEAUX / Jessica FOREST** Date : 11 août 2011 Signature : JFR .....

Emission / Définition du plan d'action

Description de l'anomalie	Evaluation impact / Recherche de cause	Action(s) corrective(s)	Fiche(s) de test à exécuter
Le test de déconnexion automatique effectué en FQO04 test n°11 n'est pas tracé dans l'audit trail.	**Recherche de cause :** configuration logiciel : lors de la déconnexion : la session sur le logiciel est bloquée. Seule l'entrée du mot de passe réactive et redonne accès aux fonctions. Cependant l'audit du système n'enregistre pas cette action. **Evaluation impact :** Minime : la déconnexion, vérifiée dans la FQO04 tests 9 à 11, fonctionne correctement et le logiciel trace les déconnexions volontaires.	Aucune, système accepté en l'état	Aucune

Autorise la poursuite de la production oui ☐ non ☐ **NA** ☑ numéro PR..... Responsable Qop / AQ R&D Nom :..... Date.... / .... / .... Visa :.....

Validation du plan d'action

Statut de l'anomalie : non-Bloquante ☐ Bloquante ☐
Si bloquante, préciser étape *(QC/QI/QO/QP/VN/démarrage production ou test de Validation* : N/A

Responsable Validation : Nom : PECHARD A. Date 17 / 08 / 2011 Visa :.....
Responsable SQO / AQ R&D : Nom : Cigna Cyril Date 17 / 08 / 2011 Visa :.....
~~: Nom : ..... Date ..... Visa : .....~~

Bilan et approbation du plan d'action

Fiche(s) de test exécutée (s)	N° exécution	Statut	Autre(s) action(s) réalisée (s)
—	—	—	—

Responsable Validation : Nom : PECHARD Rémi Date 17 / 08 / 2011 Visa :.....
Responsable SQO / AQ R&D : Nom : Cigna Cyril Date 17 / 08 / 2011 Visa :.....
~~: Nom : ..... Date ..... Visa : .....~~

Annexe 6 : Fiche de tests de qualification de performance : documents d'exploitation

FQP 02 N°IMMO : ---	DOCUMENTS D'EXPLOITATION	EXÉCUTION N°.....

Table 3 : Documents d'exploitation associés au système

PROCESSUS / THEMES	DOCUMENT ASSOCIE	VERSION	§	DATE D'APPLICATION	COMMENTAIRES (si document N/A : justification obligatoire)
Utilisation du système	.....	.....	.....	...../...../.....	
Instruction d'administration	.....	.....	.....	...../...../.....	
Gestion des SI des laboratoires de l'ARD EU	134 948	.....	.....	...../...../.....	
Gestion des données critiques	.....	.....	.....	...../...../.....	
Gestion de la sécurité et des droits d'accès aux logiciels et aux données	.....	.....	.....	...../...../.....	
Sauvegarde et restauration des données	.....	.....	.....	...../...../.....	
Sauvegarde et restauration des logiciels	.....	.....	.....	...../...../.....	
Archivage et la restitution des données	.....	.....	.....	...../...../.....	
Maintenance du système (contrat, garantie, suivi utilisateur,...)	.....	.....	.....	...../...../.....	
Gestion des anomalies	140 826	.....	.....	...../...../.....	
Gestion des dysfonctionnements et plan de secours	.....	.....	.....	...../...../.....	
Maîtrise des modifications	061 206	.....	.....	...../...../.....	
Gestion de la configuration et des versions logicielles	.....	.....	.....	...../...../.....	
Formation au système	099 921	.....	.....	...../...../.....	
Retrait du système	134 948	.....	8.6	...../...../.....	

Table complétée le ... / ... / ..... par ..... Visa .....

GLOSSAIRE

Audit [GAMP]
Processus systématique, indépendant et documenté mené en vue d'obtenir des preuves d'audit et de les évaluer objectivement afin de déterminer quels critères convenus sont satisfaits.

Audit trail / Piste pour audit
Enregistrement de l'utilisation des ressources du système informatique. Un audit trail doit enregistrer tous les accès aux données ayant un impact BPF : identification de l'utilisateur, la création/modification/suppression de données avec la date, l'heure et le motif. Cet enregistrement est la « boîte noire » du système informatique.

Cas de test / scénario de test [GAMP]
Ensemble d'entrées de test, de conditions d'exécution et de résultats attendus, élaborés pour un objectif particulier, par exemple pour employer un chemin de programme particulier ou pour vérifier la conformité à une exigence spécifique.

Client
Entreprise ou personne recevant un produit ou un service. Voir aussi « Utilisateur ».

Code source [GAMP]
C'est la version lisible par l'homme, des instructions d'un programme informatique permettant à l'ordinateur, après assemblage, compilation ou toute autre méthode de traduction, d'effectuer une tâche précise.

Conception [GAMP]
La conception est le processus permettant de définir l'architecture, les composants, les interfaces et autres caractéristiques d'un système. Ce processus transforme les exigences en spécifications.

Cycle de vie d'un système [GAMP]
Période commençant dès la conception d'un système et se terminant lorsque le système n'est plus utilisé.

Enregistrement [36]
Preuve tangible documentée de la réalisation d'une activité ou de l'atteinte d'un résultat qui assure la traçabilité (AFNOR).
Un enregistrement électronique est toute combinaison de textes, graphiques, données, sons, images ou autres informations sous forme électronique créées, modifiées, utilisées, archivées, restaurées ou diffusées par un système informatisé (21CFR Part11).

Environnement opérationnel
(Ou « environnement d'exploitation ») Toutes les influences extérieures en contact avec le système informatique.

Exigence
Condition ou aptitude nécessaire pour répondre à un besoin.

Fournisseur
Entreprise ou personne fournissant un produit (matériel ou logiciel).

Gestion des changements [GAMP]
Processus formel par lequel les représentants qualifiés de disciplines appropriées revoient les changements proposés ou effectifs apportés à un système informatique. L'objectif principal consiste à documenter les changements et à assurer que le système est sous contrôle.

Gestion des fournisseurs [GAMP]
Processus continu d'évaluation d'un fournisseur par rapport à des standards établis de qualité, de gestion des défauts observés et de travail en collaboration, afin d'améliorer la qualité de ses produits ou de ses services et de sa documentation.

Plan de validation [GAMP]
Document décrivant la stratégie globale ainsi que les parties (intervenants) responsables de la validation d'un système dans son environnement opérationnel.

Plan Qualité [GAMP]
Document spécifiant quelles procédures et quelles ressources afférentes doivent être appliquées, par qui et quand, à un projet, à un produit, à un processus ou à un contrat particulier.

Projet [32]
Un projet est un ensemble unique d'actions coordonnées avec des dates définies de début et de fin, entreprises par un individu ou une entité pour atteindre des objectifs spécifiés en respectant des paramètres de coûts, délais et performance.

Progiciel / Logiciel standard du commerce [Wikipedia]
Logiciel applicatif défini d'après un besoin induit par le marché, disponible dans le commerce et dont l'adéquation à un usage a été démontrée par un vaste éventail « d'utilisateur-clients ». Egalement connu sous le nom de COTS (*Commercial Off-the-Shelf Software*), ce terme s'oppose au « logiciel sur mesure » développé en interne par une entreprise et conçu pour répondre à un besoin spécifique et inédit.

Progiciel de Gestion Intégré [Wikipedia]
Progiciel qui intègre les principales composantes fonctionnelles de l'entreprise : gestion de production, gestion commerciale, logistique, ressources humaines, comptabilité, contrôle de gestion. À l'aide de ce système unifié, les utilisateurs de différents métiers travaillent dans un environnement applicatif identique qui repose sur une base de données unique. Ce modèle permet d'assurer l'intégrité des données, la non-redondance de l'information, ainsi que la réduction des temps de traitement.

Qualification [GAMP]
Processus permettant de démontrer la capacité de satisfaire à des exigences spécifiées.

Réseau [GAMP]
Système comprenant des voies de transmission, du matériel et des logiciels de support, permettant de relier plusieurs ordinateurs distants à l'aide de moyen de télécommunication.

Revue [GAMP]
Activité entreprise pour établir la pertinence, l'adéquation et l'efficacité d'un objet en question à remplir ses objectifs prédéfinis.

Revue périodique [GAMP]
Evaluation documentée de la documentation, des procédures, des enregistrements et des performances d'un système informatique pour déterminer s'il se trouve toujours dans un état validé et quelles actions sont éventuellement nécessaires pour le remettre dans un état validé. La fréquence des revues dépend de la complexité, de la criticité et de la rapidité des changements (nombre de changements) du système.

Sécurité [GAMP]
Protection des matériels et des logiciels informatiques contre des accès, des utilisations, des changements, des destructions ou des divulgations d'information de nature accidentelle ou malveillante. La sécurité s'étend aussi au personnel, aux données, aux communications, et à la protection physique des installations informatiques.

Spécifications [GAMP]
Document qui spécifie, de manière complète, précise et vérifiable, les exigences, la conception, le comportement ou les autres caractéristiques d'un système ou d'un composant, et souvent les procédures permettant de déterminer si ces dispositions ont été satisfaites.

Spécifications utilisateur [GAMP]
Spécifications des exigences émises par l'utilisateur, décrivant ce que le système est censé faire, et contenant de ce fait au moins un ensemble de critères ou de conditions devant être satisfaits.

Système

- **Informatique** voir page 14
- **Informatisé** voir page 16
- **Système automatisé**
  Synonyme de « Système informatisé ». Ce terme était bien plus souvent employé avant la généralisation de l'outil informatique, car l'informatique « industrielle » se limitait alors à l'automatisme (simples systèmes de contrôle-commande).

Tests d'acceptation [Wikipedia]
Tests effectués pour déterminer si un système satisfait ou non à ses critères d'acceptation afin de permettre au client de déterminer s'il doit accepter ou non le système. Les tests d'acceptation fournisseur (FAT) sont exécutés dans l'usine du fournisseur, tandis que les tests d'acceptation sur site (SAT) sont exécutés chez le client utilisateur. Dans les deux cas, l'utilisateur doit s'impliquer dans la démarche.

Tests d’intégration [Wikipedia]
Dans un projet informatique, les tests d’intégration se déroulent dans la phase suivant les tests unitaires. Cela consiste, une fois que les développeurs ont chacun validé leurs développements ou leurs correctifs, à regrouper ensemble leurs modifications dans le cadre de la livraison au client. Ces tests ont pour but de valider le fait que toutes les parties développées indépendamment fonctionnent bien ensemble de façon cohérente.

Traçabilité [GAMP]
Capacité de tracer l’historique, l’application ou l’emplacement de ce qui fait l’objet de l’investigation.

Tests unitaire [Wikipedia]
Les tests unitaires ont pour but de prouver le fonctionnement correct d'un module ou sous-partie d’un logiciel. On écrit un test pour confronter une réalisation à sa spécification. Une « unité » peut ici être vue comme « le plus petit élément de spécification à vérifier ».

Utilisateur [GAMP]
Personne ou groupe de personnes opérant ou interagissant directement avec le système. Souvent, l’utilisateur ou les utilisateurs et le(s) client(s) ne sont pas la (les) même(s) personne(s), mais peuvent l’être.

Validation [GAMP]
Établir la preuve documentée démontrant avec un haut degré d’assurance qu’un processus spécifique va produire systématiquement un produit conforme à ses spécifications et critères de qualité préalablement définis.

BIBLIOGRAPHIE

[1] LE GOYAT A. *Le concept de validation dans l'industrie pharmaceutique. Application à la validation de méthodes de dosages.* Thèse d'exercice. Nantes : Nantes, 1992.

[2] FOOD AND DRUG ADMINISTRATION. *Guideline on general principles of process validation.* mai 1987.

[3] Leveson N. *Medical Devices: The Therac-25*. [En ligne]. 1995. Disponible sur : < http://sunnyday.mit.edu/papers/therac.pdf > (consulté le 5 janvier 2012)

[4] LE FORESTIER E. *Les Systèmes d'Information dans l'Industrie Pharmaceutique*. Thèse d'exercice. Nantes : Université de Nantes, 2002.

[5] *Définition de « Matériel »*. [En ligne]. *LAROUSSE*. Disponible sur : < http://www.larousse.fr/dictionnaires/francais/matériel/49844 > (consulté le 24 janvier 2012)

[6] *Définition de « Logiciel »*. [En ligne]. *LAROUSSE*. Disponible sur : < http://www.larousse.fr/dictionnaires/francais/logiciel > (consulté le 24 janvier 2012)

[7] *Définition de « Software »*. [En ligne]. *Searchsoa Techtarget*. novembre 1997. Disponible sur : < http://searchsoa.techtarget.com/definition/software > (consulté le 24 janvier 2012)

[8] Rannou H., Ronai M. *Etude sur l'industrie du logiciel*. [En ligne]. 22 octobre 2003. Disponible sur : < http://www.csti.pm.gouv.fr/elements/etude_AUSI_22oct03.pdf > (consulté le 24 janvier 2012)

[9] FOOD AND DRUG ADMINISTRATION. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*. [En ligne]. 11 janvier 2002. Disponible sur : < http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf > (consulté le 24 janvier 2012)

[10] FOOD AND DRUG ADMINISTRATION. « Inspection Guides - Glossary of Computer Systems Software Development Terminology ». [s.l.] : [s.n.], 1995. Disponible sur : < http://www.fda.gov/iceci/inspections/inspectionguides/ucm074875.htm > (consulté le 25 janvier 2012)

[11] European Commission. *Eudralex Volume 4 - Part I : Annex 11 (Computerised Systems).* janvier 2011.

[12] PIC/S. *Good Practices for Computerised Systems in Regulated « GXP » Environments - PI 011-3*. 25 septembre 2007.

[13] FOOD AND DRUG ADMINISTRATION. « Food Safety Modernization Act (FSMA) - Coup d'oeil sur les étapes décisives de la sécurité sanitaire des aliments dans l'histoire de la FDA ». [s.l.] : [s.n.], [s.d.]. Disponible sur : < http://www.fda.gov/Food/FoodSafety/FSMA/ucm242852.htm > (consulté le 12 mars 2012)

[14] LeMonde.fr. « La réforme du contrôle des médicaments adoptée par le Parlement ». Disponible sur : < http://www.lemonde.fr/politique/article/2011/12/20/la-reforme-du-controle-des-medicaments-adoptee-par-le-parlement_1620650_823448.html > (consulté le 12 mars 2012)

[15] *Commission européenne*. [En ligne]. Disponible sur : < http://fr.wikipedia.org/wiki/Commission_europ%C3%A9enne > (consulté le 15 mars 2012)

[16] *Polepharma - Les bonnes pratiques de fabrication*. 22 novembre 2007.

[17] AFSSAPS. *PICS*. [En ligne]. Disponible sur : < http://www.afssaps.fr/Activites/Engagement-europeen-et-international/Engagement-international/Engagement-international/PICS > (consulté le 15 mars 2012)

[18] PIC/S. *Pharmaceutical Inspection Co-operation Scheme - PIC/S 1/95 (Rev. 5)*. 7 novembre 2011.

[19] World Health Organization. *Quality assurance of pharmaceuticals - Volume 2, 2nd updated edition*.

[20] « GAMP Standards For Validation Of Automated Systems ». *11 mars 2008* [En ligne]. Disponible sur : < http://www.pharmpro.com/Articles/2008/03/GAMP-Standards-For-Validation-Of-Automated-Systems/ > (consulté le 18 janvier 2011)

[21] GAMP Forum (ISPE). *Guide GAMP 4*. Décembre 2001.

[22] *Harmonisation internationale*. [En ligne]. Disponible sur : < http://www.edqm.eu/fr/International-Harmonisation-614.html > (consulté le 16 mars 2012)

[23] FOOD AND DRUG ADMINISTRATION. *FDA Guide to the Inspection of Computerised Systems in Pharmaceutical Processing*. Février 1983.

[24] FOOD AND DRUG ADMINISTRATION. *TITLE 21-- SUBCHAPTER A -- PART 11: ELECTRONIC RECORDS; ELECTRONIC SIGNATURES*. [En ligne]. 1997. Disponible sur : < http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11 > (consulté le 23 janvier 2012)

[25] AKTEHOM. *Réglementation EU-GMP Annexe 11 – Computerised Systems*. [En ligne]. Disponible sur : < http://www.aktehom.com/reglementation-eu-gmp-computerised-systems/ > (consulté le 20 mars 2012)

[26] *Passage informatique à l'an 2000*. [En ligne]. *Wikipedia*. Disponible sur : < http://fr.wikipedia.org/wiki/Passage_informatique_%C3%A0_l'an_2000#cite_note-1 > (consulté le 26 mars 2012)

[27] Maas & Peither AG - GMP Publishing. *EU GMP Guide Annex 11 Computerised Systems*. février 2011.

[28] AFSSAPS. *Bonnes Pratiques de Fabrication*. Juillet 2011.

[29] European Medicines Agency. *Eudralex Volume 4 - Part III : Pharmaceutical Quality System (ICH Q10)*. 31 janvier 2011.

[30] European Medicines Agency. *Eudralex Volume 4 - Part III : Quality Risk Management (ICH Q9)*. 31 janvier 2011.

[31] C. Martin K., Perez A. « GAMP 5 Quality Risk Management Approach ». *Pharmaceutical Engineering*. Mai/Juin 2008. Vol. 28, n°3,.

[32] M. Renaudin - CVQ Consulting. *Management de projet*. 2 janvier 2011.

[33] Wikipedia. *Ingénierie des systèmes*. [En ligne]. Disponible sur : < http://fr.wikipedia.org/wiki/Ing%C3%A9nierie_des_syst%C3%A8mes > (consulté le 12 mars 2012)

[34] M. Hessman. *Validation et audit des systèmes informatisés*. 2010.

[35] ROUSSEAUX J.-F. *Support qualité & Validation de système informatisé de laboratoire*. 30 septembre 2011.

[36] JOUVE J.-L. *La gestion des enregistrements électroniques : un nouveau défi pour l'industrie pharmaceutique ?* [En ligne]. 17 octobre 2006. Disponible sur : < http://62.244.84.28/UserFiles/File/base_documentaire/19eme_congres_A3P/JouveRHUNE 15h30.pdf > (consulté le 25 mars 2012)

[37] *FDA 21 CFR Part 210-211*. [En ligne]. *Master CONTROL compliance accelerated*. Disponible sur : < http://www.mastercontrol.com/21_cfr_regulations/210_211.html > (consulté le 10 juin 2012)

UNIVERSITÉ DE NANTES
FACULTÉ DE PHARMACIE

Année de la soutenance
2012

Nom – Prénoms : ROUSSEAUX Jean-François, Pierre, Jean-Marie

Titre de la thèse : La validation des systèmes informatisés dans l'industrie pharmaceutique : réglementation, méthodologie et application au laboratoire de contrôle.

Résumé de la thèse :

L'informatique a révolutionné notre quotidien et celui des grandes organisations, au point d'être aujourd'hui indispensable pour toute opération. Pour les industries réglementées, auxquelles appartiennent les établissements pharmaceutiques, la question de la maîtrise de cet outil pose la problématique : permet-il d'assurer véritablement la qualité des médicaments produits ?

Les établissements pharmaceutiques sont tenus de respecter certaines Bonnes Pratiques pour garantir la qualité du médicament et la sécurité des patients. En janvier 2011, la réglementation européenne concernant l'utilisation des systèmes informatisés dans l'industrie pharmaceutique a évoluée. Dans ce contexte, il est intéressant de déterminer l'impact de ces nouvelles dispositions réglementaires sur la mise en place d'une stratégie de validation efficace.

MOTS CLÉS :

VALIDATION
SYSTÈME INFORMATISÉ
INDUSTRIE PHARMACEUTIQUE
ASSURANCE QUALITÉ

JURY

PRÉSIDENT : **M. Alain PINEAU**
Professeur de Toxicologie à la Faculté de Pharmacie de Nantes

ASSESSEURS : **M. Frédéric DEHAUT**
Pharmacien Responsable à l'Établissement Français du Sang

M. Loïs REYMOND
Chargé de mission aux Laboratoires Chiesi