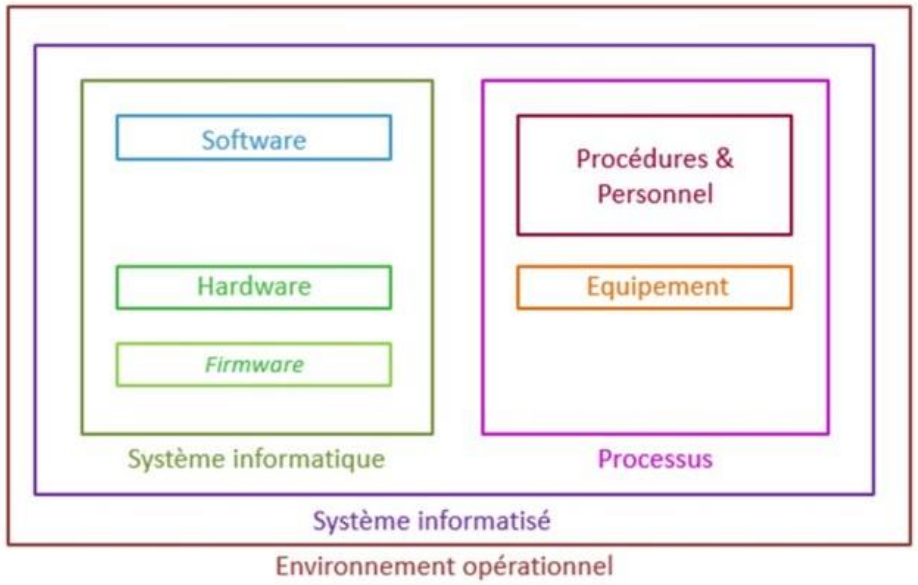
# *Validation des systèmes informatisés et automatisés (SISA)*

# GENERALITES

Qu'est-ce qu'un **système informatisé (SI) ou système automatisé (SA)** : Le système informatisé ou automatisé comprend le matériel, le logiciel, le personnel et les procédures.

- Exemple : Logiciel, HPLC liée à un système informatisé…

Ce schéma explique bien le cadre plus complet d'un système SISA par rapport à la notion de système informatique



# GENERALITES

Pourquoi **valider un SISA** ?

- Afin de respecter la règlementation liée au marché. C´est une exigence !
- Afin de prévenir de grave conséquence liée à un disfonctionnement du système

Chaque domaine d´activité (Traitement des eaux, déchets, industrie pharmaceutique, agroalimentaire, automobile… etc) est soumis à des réglementation spécifiques et donc le SISA doit se conformer à ces exigences. Dans le domaine pharmaceutique, la FDA (U.S. Food Drug Administration) fait office de référence.

Qu'est-ce que la **validation** ?

La validation porte sur le procédé / le processus tandis que la qualification porte sur les entrants du procédé / processus. Dans le domaine pharmaceutique, cette validation s´exprime au travers d´un document appelé VPP (Validation Project Plan) expliquant la stratégie dans laquelle le système ou installation va être validé. Le but de cette validation est de s´assurer que le système délivré est conçu et fonctionne en accord avec :

- La réglementation
- Les besoins utilisateurs (URS : User Requirement Specification)

La validation d'un système est formalisée sous protocole / rapport de validation. Ces documents font souvent l'objet d'une revue lors d'une inspection ou d'un audit. Dans le domaine de l´informatique et/ou automatisme nous parlerons de CSV (Computerized System Validation) qui se décline différemment selon la catégorie Gamp de 1 à 5. Un des principes fondamentaux de la validation est le model en V.

# GUIDES ET REGLEMENTATIONS

T:\SPsolutions\Normes\ISPE - Baseline, GAMP, GMP, GPG\GAMP-ISPE Automation

## REGLEMENTATION

- Europe : Les requis sont définis par **l'Annexe 11 de l'Eudralex volume 4** : «Systèmes informatisés»
- USA : Les requis sont définis par le code fédéral **21 CFR Part 11**

## Guide

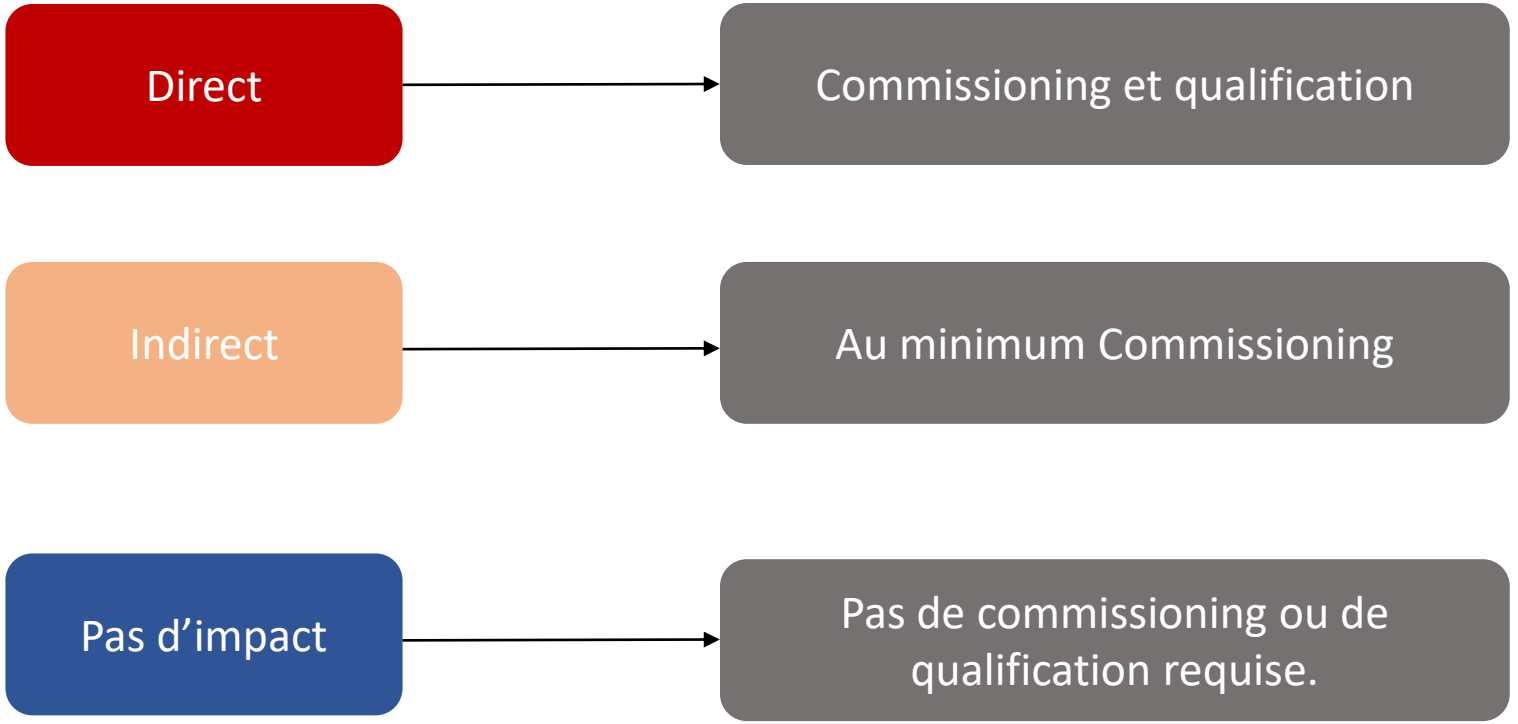
- **GAMP 5** (Good Automated Manufacturing Practices) : N'est pas un texte réglementaire. Il est tout de même un guide très utilisé en industrie pharmaceutique pour encadrer la conception, le développement et la validation d'un système informatisé ou automatisé.
- **GMP** Good Manufacturing Practice
- **BPD** Bonne pratique de documentation

- **Autres ISPE Gamp Baseline** (Risk-Based approach, Data Integrity, IT infrastructure, …)

Les systèmes utilisant des enregistrements et des signatures électroniques doivent être en conformité avec les exigences du 21 CFR Part 11 de la FDA si l'on vend des produits aux USA.  Si l'on vend ses médicaments en Europe, c'est l'annexe 11 des GMP qui s'applique et le guide du PIC/S PI011-3.
Le GAMP 5, guide reconnu par les industriels et les instances réglementaires, intègre toutes les exigences du PIC/S.

# Classification des équipements et systèmes

L'effort de justification, documentation et vérification dépend de l'impact du système sur la qualité du produit



# CATEGORIES GAMP

L'effort de justification, documentation et vérification dépend de la catégorie des éléments software du système

| Catégorie | Description | Exemple typique | Approche typique |
|---|---|---|---|
| **1. Logiciel d'infrastructure** | • « Logiciel en couche » (c'est-à-dire sur lequel les applications sont construites)<br>• Logiciel utilisé pour gérer l'environnement opérationnel | • **Systèmes d'exploitation**<br>• Moteurs de **bases de données**<br>• Middleware<br>• Langages de programmation<br>• Progiciels statistiques<br>• Tableurs<br>• Outils de surveillance de réseau<br>• Outils d'ordonnancement<br>• Outils de contrôle des versions | ▪ Enregistrement du numéro de version, vérification de la justesse de l'installation réalisée d'après des procédures d'installation approuvées<br>• Se reporter au GAMP Good Practice Guide : IT infrastructure control and compliance |
| **3. Non-configuré** | Les paramètres opérationnels peuvent être saisis et sauvegardés, mais le logiciel ne peut pas être configuré spécifiquement pour satisfaire au processus métier | • Applications basées sur un firmware<br>• Progiciels (COTS)<br>• Instruments (cf. GAMP Good Practice Guide : Laboratory computerized systems pour des informations complémentaires) | • Approche réduite du cycle de vie<br>• URS<br>• Approche pour l'évaluation du fournisseur basée sur le risque<br>• Enregistrement du numéro de la version, vérification de la justesse de l'installation<br>• Tests basés sur le risque en fonction des exigences dictées par l'utilisation (pour les systèmes simples, un étalonnage régulier peut se substituer aux tests) ; pour certains dispositifs médicaux des tests rigoureux sont requis<br>• Procédures en place pour maintenir la conformité et l'adéquation avec l'utilisation prévue |

# CATEGORIES GAMP

| Catégorie | Description | Exemple typique | Approche typique |
|---|---|---|---|
| **4. Configuré** | Logiciel, souvent très complexe, qui peut être configuré par l'utilisateur pour répondre aux besoins spécifiques du processus métier propre à l'utilisateur. Le code logiciel n'est pas altéré. | • LIMS<br>• Systèmes d'acquisition de données<br>• SCADA sans dev. spécifique<br>• ERP<br>• MRPII<br>• Surveillance des essais cliniques<br>• SNCC<br>• Rapport d'évènements indésirables<br>• CDS<br>• GED<br>• Systèmes de gestion des bâtiments<br>• CRM<br>• Tableurs<br>• **Interfaces homme-machine simples**<br><br>NB : des exemples spécifiques des types de systèmes ci-dessus peuvent contenir des éléments personnalisés significatifs | Approche du cycle de vie<br>• Approche pour l'évaluation du fournisseur basée sur le risque<br>• Démonstration que **le fournisseur possède un système de gestion de la qualité adéquat**<br>• Certains documents du cycle de vie conservés uniquement par le fournisseur (par exemple les spécifications de conception)<br>• Enregistrement du numéro de version, vérification de la justesse de l'installation<br>• Tests basés sur le risque pour **démontrer que l'application fonctionne telle que conçu dans un environnement de test**<br>• Tests basés sur le risque pour **démontrer que l'application fonctionne telle que conçu dans le cadre du processus opérationnel**<br>• Procédures en place pour maintenir la conformité et l'adéquation avec l'utilisation prévue<br>• Procédures en place pour **gérer les données** |

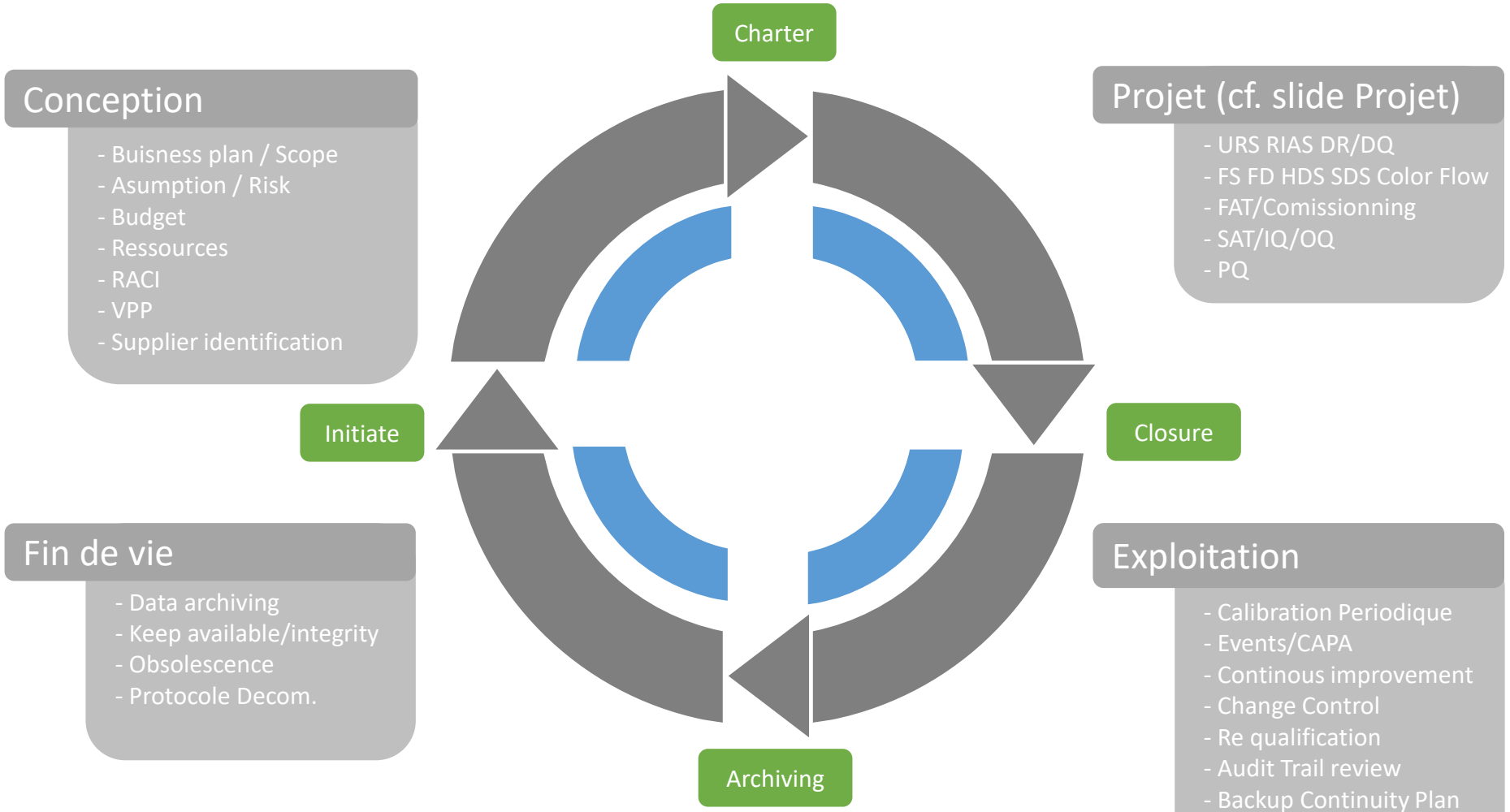
# CATEGORIES GAMP

| Catégorie | Description | Exemple typique | Approche typique |
|---|---|---|---|
| **5. Personnalisé** | Logiciel personnalisé conçu et codé pour satisfaire au processus opérationnel. | Variés mais incluant :<br>• Les applications informatiques développées en interne et en externe<br>• Les applications de contrôle de processus développées en interne et en externe<br>• **SCADA avec dev. spécifique**<br>• Les logiques (IEC 61131, ladders, etc.) personnalisées: **PLC** (Automate Prog.)<br>• Les firmwares personnalisés<br>• Les tableurs (macros) | Idem à la catégorie 4, plus :<br>• Une évaluation plus rigoureuse du fournisseur, avec un possible audit du fournisseur<br>• La possession de la totalité de la documentation du cycle de vie (FS, DS, tests structurels, etc.)<br>• **Revues de conception et de code source** |

**La validation d´un système dépend de la catégorie dans laquelle il est répertorié. Plus un système est complexe, risqué ou nouveau plus le niveau de contrôle doit être élevé. Cette validation est ainsi basée sur le risque.**

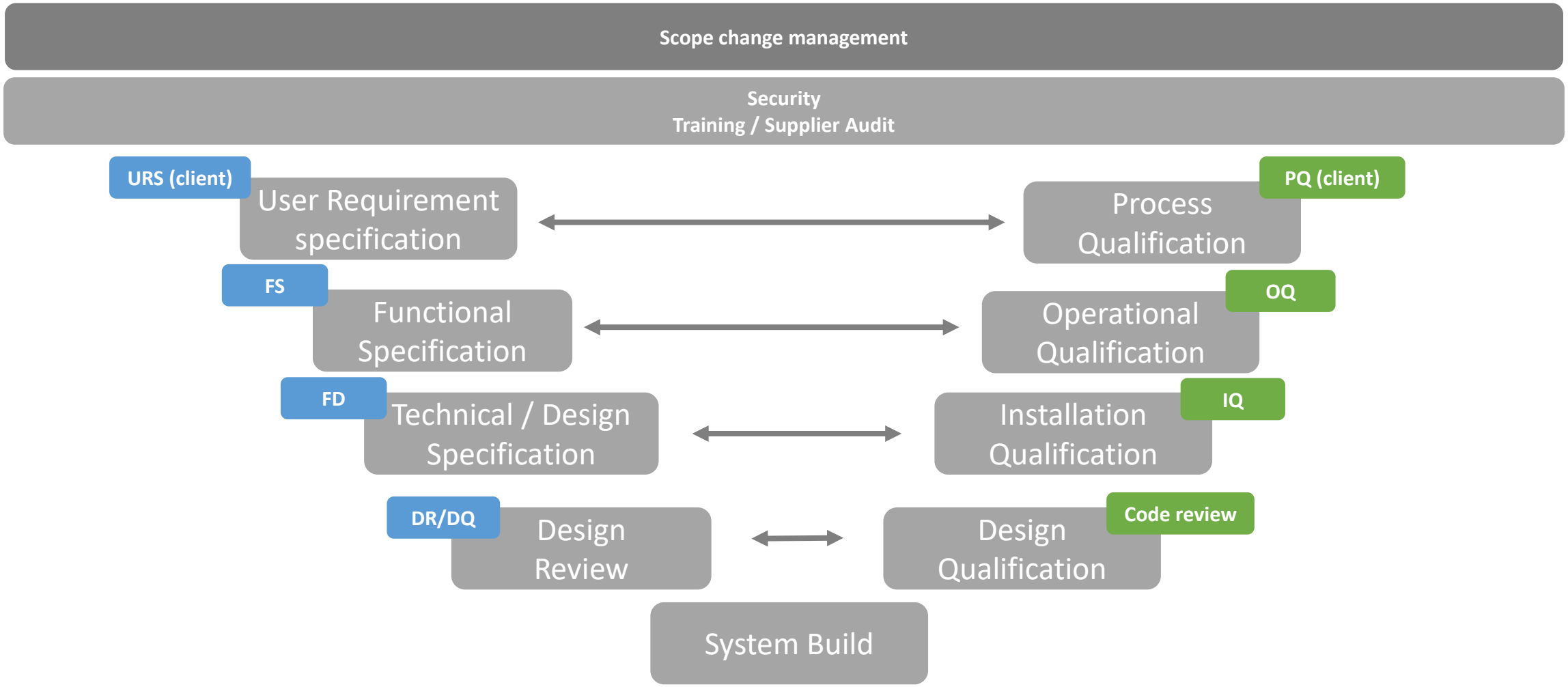
# CYCLE DE VIE D'UN SI/SA

Le cycle de vie d'un système informatisé regroupe le concept, le projet, l'utilisation et la mise hors service.



# CYCLE DE VIE D'UN PROJET

## CYCLE EN V POUR UN SYSTÈME CONFIGURE (Cat n°5)



# RACI - ROLES ET RESPONSABILITES DANS LE CADRE DE LA VALIDATION

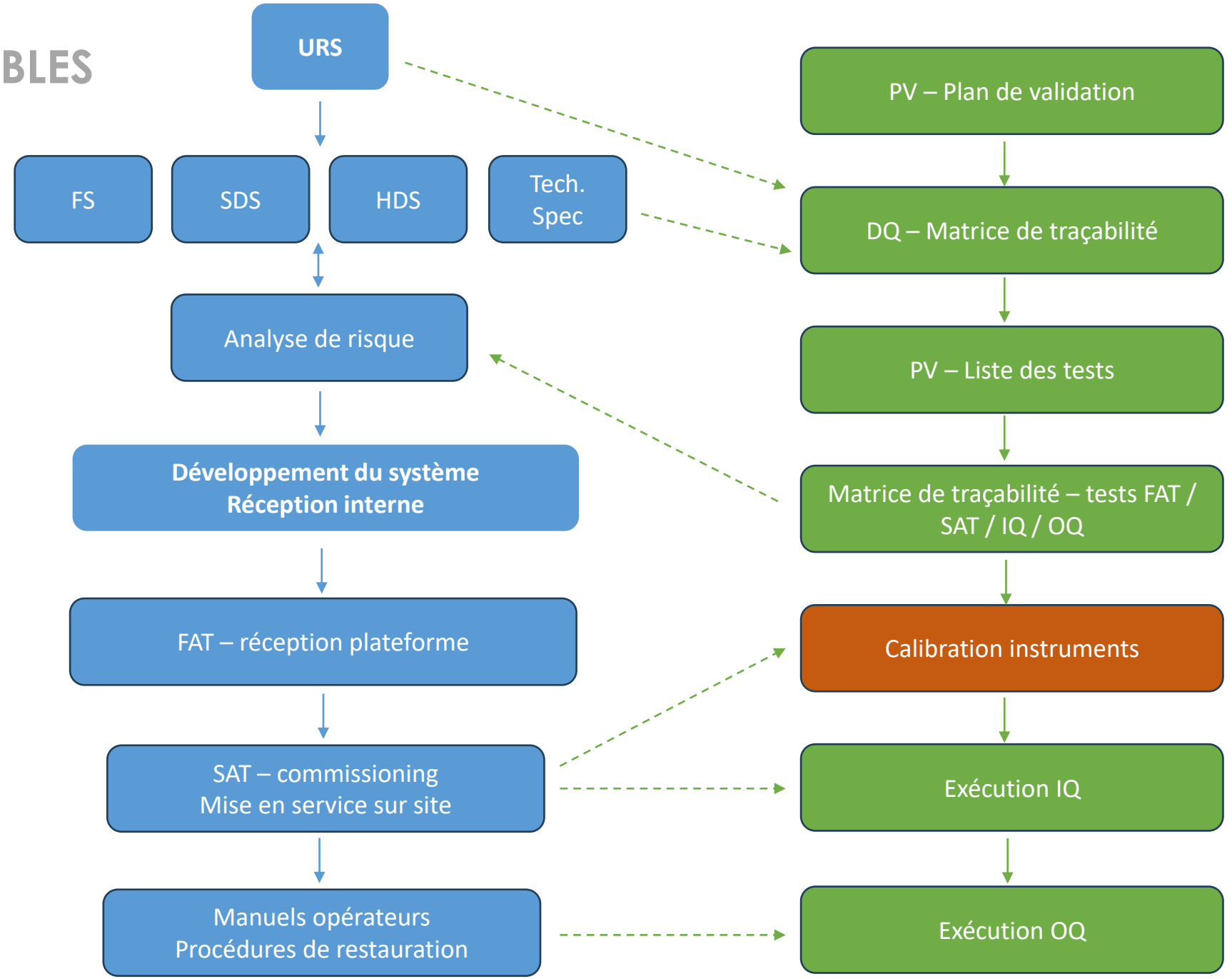
Le rôle et responsabilités des parties prenantes dans la validation d´un système SISA se décompose selon une matrice de responsabilité en fonction des activités à réaliser. Ce document sert de base à l´exécution d´un projet.

## RESPONSABILITES


## PARTIES PRENANTES
## Stackholder

| Rôle | Responsabilité |
|---|---|
| Process Owner | Utilisateur final du système, définir ses besoins, procurer des ressources au projet. |
| System Owner | Responsable de la maintenance et disponibilité du système |
| Validation Owner | Responsable de l'état validé du système |
| QA | Approuve toutes les étapes du cycle de vie d'un système, vérifie la mise en application des procédures et le respect de la réglementation |
| Supplier | Apporte son expertise sur le système, intervention en cas de défaillance |

# PROJET
# ETAPES / LIVRABLES



# PROJET
# ETAPES / LIVRABLES

| Activités | Description |
|---|---|
| URS | User Requirement Specification<br>Automation/Electrical Part/Safety/Process |
| DRDQ | Design review / Design Qualification |
| FS/FD/TS<br>HDS/SDS<br>IO List | Flow Diagram (G7) / Functional Specification<br>Technical Specification / Hardware Software Spec.<br>Liste d´entrées / sorties |
| FAT<br>Commissionning<br>SAT/IQ/OQ | Factory Acceptance Test<br>Commissionning<br>Site Acceptance Test<br>Installation Qualification<br>Operational Qualification |
| Electrical Drawing | Schématique électrique |
| Color Flow | Chemin fluidique des étapes process |
| Project doc. | Planning, RFQ, BID Analysis, Liste délivrable…. |
| RIAS | Risk Assessment |
| ---- | ------ |

# BONNE PRATIQUE DE DOCUMENTATION

Un document GMP est un document qui respecte les principes et lignes directrices liés à la fabrication de médicaments à usage humain et vétérinaire. De ce fait le scope est extrêmement large incluant toute la documentation liée à toutes les phases de la vie d´un médicament (fig. cycle de vie).

Les caractéristiques d´un document GMP :

- Clair et précis
- Intègre
- Identifié/paginer/Daté/Signé

Pour compléter, un document GMP pouvant être audité, la personne remplissant ce document doit respecter certaine règle souvent appelé les BPD (Bonne Pratique de documentation).

| Exigence | Raison |
|---|---|
| Enregistrer des informations pendant ou immédiatement après l´exécution d´une tache, d´une étape ou d´une opération | Si nous comptons sur nos souvenirs pour documenter des informations, il y a de fortes chances qu´elles soient oubliées ou incorrectes. |
| Utiliser de l´encre indélébile bleue ou noire | L´encre indélébile doit pouvoir être photocopiée. Lors de la génération de photocopies, les données restent lisibles et préservées.<br>Les feutres ou autres stylos à base d´eau ne doivent pas être utilisé en raison de leur tendance à tacher et à couler. |
| Ne noircissez pas et n´utilisez pas de correcteur lorsque vous effectuez des corrections | Nous conservons toute notre documentation et nos données d´origine. Nous ne voulons pas donner l´impression que nous cachons quelque chose à un vérificateur. |

# BONNE PRATIQUE DE DOCUMENTATION

| Exigence | Raison |
|---|---|
| Enregistrer les informations de manière claire et lisible | La documentation difficile à lire peut être remise en question pour son intégrité et sa précision. Nous devons défendre ces informations lors d´un audit. |
| Enregistrer les informations directement sur les documents approuvés | Les informations transcrites à partir de post-it, de gants des wipes ou d´autres documents non approuvés peuvent être mal interprétées mal transcrites ou perdues. |
| Signez et dates toutes les entrées | Cela montre:<br>- que nous sommes responsables du travail que nous effectuons<br>- que notre traçabilité est complète |
| N´utilisez pas de flèches ou de “#” ou de guillemets pour dupliquer des informations (résultat, calculs ou autre données) | Ces symboles ne sont pas considérés comme des données valides. |
| Utiliser le format de date DD MMM YYYY<br>(Ex: 10 SEP 2012) | Format universellement accepter pour documenter les dates. |
| Utiliser l´heure au format 24 heures | Cela évite toute confusion potentielle. Il est de plus en plus courant d´utiliser le format de 24 heures comme format international. |
| Le nom d´utilisateur (ID) et le mot de passe doivent être uniques pour chaque utilisateur d´un système validé. | Le nom d´utilisateur et le mot de passe sont considérés comme une signature électronique et la signature électronique équivaut à une signature manuscrite. Il indique la présence physique de cette personne. |

Voir en annexe des exemples de documents GMP

# ALCOA PRINCIPE

Le processus d'évaluation et d'examen, entre l'organisme de contrôle et l'industriel, repose sur le fait que les informations soumises dans les dossiers et utilisées dans la prise de décision quotidienne sont complètes, exhaustives et fiables.

Mais aussi attribuables, lisibles, contemporaines, originales et exactes, communément appelées "ALCOA".


Parmi les observations justifiant le principe ALCOA, on peut citer :
- l'incapacité des organisations à appliquer des systèmes robustes qui empêchent les risques liés aux données
- d'améliorer la détection des situations dans lesquelles la fiabilité des données peut être compromise, et/ou d'enquêter sur les problèmes liés aux données
- s'appuie sur des systèmes informatisés validés mais nombre de sociétés n'examinent et ne gèrent pas de manière adéquate les enregistrements électroniques originaux se contentent souvent d'examiner et de gérer des impressions incomplètes et/ou inappropriées.

Ces observations soulignent la nécessité pour l'industrie de moderniser les stratégies de contrôle et d'appliquer des méthodes modernes de gestion des risques liés à la qualité (QRM) et des principes scientifiques solides aux modèles d'entreprise actuels (tels que l'externalisation) ainsi que les technologies actuellement utilisées (telles que les **systèmes informatisés**).

# ALCOA PRINCIPE

**Attribuable**. Attribuable signifie que l'information est capturée dans l'enregistrement de telle sorte qu'elle soit identifiée de manière unique comme ayant été exécutée par l'auteur des données (par exemple, une personne ou un système informatique).

- bonne pratique documentaire (initiales, signature manuscrite complète, la date et, le cas échéant, l'heure)
- signature au moment de la revue ou de l'action par un identifiant unique et la personne qui a fait l'action
- image numérique stockée de la signature non acceptée
- signature électronique avec date et heure
- utilisateur unique et gestion des accès
- audit trail
- identification de la personne qui effectue la tâche et la personne qui remplit l'enregistrement, la personne qui effectue la tâche contresigne

**Lisibles, traçables et permanents**. Ces termes font référence aux exigences selon lesquelles les données doivent être lisibles, compréhensibles, permanentes et permettre de se faire une idée claire de l'enchaînement des étapes ou des événements de ces enregistrements afin que toutes les activités GXP menées puissent être entièrement reconstituées par les personnes qui examinent ces enregistrements à tout moment au cours de la période de conservation des enregistrements fixée par le GXP applicable.

- l'utilisation d'une encre permanente et indélébile
- pas d'utilisation de crayons ou d'effacements
- l'utilisation de ratures d'une seule ligne pour enregistrer les changements avec le nom, la date et la raison (c'est-à-dire l'équivalent papier de la piste d'audit)
- pas d'utilisation de liquide correcteur opaque ou de correction opaque ou d'obscurcissement de l'enregistrement
- émission contrôlée de documents (annexes, notes, …) avec des pages numérotées séquentiellement (c'est-à-dire qui permettent de détecter les pages manquantes ou sautées)
- la préservation du papier/de l'encre qui se décolore au fil du temps et dont l'utilisation est inévitable.

- enregistrement des données au moment de l'activité
- audit trail
- gestion des accès aux données, pas d'écrasement ou suppression de données
- pas de masquage des données affichées ou imprimées
- archivage  sécurisé et contrôlé; sauvegarde validée des enregistrements électroniques pour assurer la reprise après sinistre

# ALCOA PRINCIPE

**Contemporaines**. Les données contemporaines sont des données enregistrées au moment où elles sont générées ou observées.

- s'applique aux procédures, formation, audit, auto-inspection des contrôles liés à des documents officiels (Logbook)
- les documents doivent être conçus de manière appropriée et la disponibilité de formulaires/ documents vierges dans lesquels les activités sont enregistrées
- l'enregistrement de la date et de l'heure des activités à l'aide de sources de temps synchronisées (horloges de l'établissement et du système informatisé) qui ne peuvent pas être modifiées par du personnel non autorisé. Dans la mesure du possible, l'enregistrement des données et de l'heure des activités manuelles (par exemple, le pesage) doit être effectué automatiquement.
- des contrôles qui permettent de déterminer la chronologie d'une activité par rapport à une autre (par ex. les contrôles de fuseaux horaires)
- la disponibilité du système pour l'utilisateur au moment de l'activité.

**Original**. Les données originales comprennent la première saisie ou la saisie à la source des données ou des informations, ainsi que toutes les données ultérieures nécessaires à la reconstitution complète de la conduite de l'activité de GXP. Les exigences du GXP en matière de données originales comprennent ce qui suit :
■ les données originales doivent être examinées ;
■ les données originales et/ou les copies véridiques et vérifiées qui préservent le contenu et la signification des données originales doivent être conservées
■ à ce titre, les enregistrements originaux doivent être complets, durables et facilement récupérables et lisibles tout au long de la période de conservation des documents.

- copies de sauvegarde de routine des documents électroniques originaux stockées dans un autre lieu
- des zones de stockage contrôlées et sécurisées
- une/des copie(s) est/sont faite(s) de l'ensemble des données électroniques originales, en préservant le format d'origine du document, le format dynamique, selon les besoins (par ex. copie d'archivage en utilisant un processus de sauvegarde validé)
- processus de contrôle de la réussite de la copie de la sauvegarde ou de l'archivage
- la mise à disposition d'un environnement approprié pour consulter les données électroniques archivées

# ALCOA PRINCIPE

**Exactitude.** Le terme "exact" signifie que les données sont correctes, véridiques, complètes, valides et fiables.

- la qualification, l'étalonnage et l'entretien des équipements, tels que les balances et les pH-mètres, qui génèrent des impressions
- la validation des systèmes informatisés qui génèrent, traitent, conservent, distribuer ou archiver des enregistrements électroniques
- les systèmes doivent être validés pour garantir leur intégrité
- l'investigation des déviations et des résultats douteux et hors spécifications

- introduction des données critiques dans un système nécessite un contrôle qui peut par exemple être effectué par une deuxième personne (notion de double validation)
- une fois vérifiés, ces champs de données critiques seraient verrouillés pour empêcher toute modification ultérieure, lorsque cela est possible et approprié et modifiées uniquement dans le cadre d'un processus formel de contrôle des modifications
- les tableaux (par exemple, les unités et les échelles) doivent être contrôlés
- Le processus de transfert des données entre les systèmes doit être validé
- Le temps n'est pas forcément un facteur critique pour toutes les activités. Lorsque l'activité est critique du point de vue du temps, les documents imprimés doivent indiquer l'heure et la date.

Les exigences susmentionnées pour l'ALCOA impliquent implicitement que les archives doivent être complets, cohérents, durables et disponibles (pour souligner ces exigences, on parle parfois d'ALCOA-plus).

# GESTION DES UTILISATEURS

L'accès aux systèmes GMP doit être limité aux **utilisateurs autorisés** :

- Système de badgeage à l'entrée des zones (système de contrôle d'accès)
- Accès du système sous identifiant et mot de passe

Des rôles sont attribués en fonction de l'expertise, du grade et de la formation de chaque personne :

- Des accès dits **« key user» ou «admin»** sont donnés aux administrateurs du système, en général le département IT ou automation. Ils n'ont accès qu'aux fonctions système et n'ont pas d'autorisation pour piloter l'installation.
- Des accès «**Superviseurs»**, permettant de réaliser des opérations de routines avec des droits supérieurs (exemple : ajout d'une recette, modifications de paramètres de réglage)
- Des accès «**opérateurs»** permettant de réaliser des opérations de routine, ils ne peuvent ni supprimer ni modifier des données critiques

Le tableau des droits d'accès est vérifié en FAT et en OQ.

Chaque personne doit avoir une certification de formation qui est liée à son rôle et son accès au système (vérifié lors des tests de PQ, par le client)

Ces requis sont testés lors de la validation du système.

Toutes les actions doivent être tracées dans le système via l'**audit trail.**

# FDA 21cfr part 11 – Electronic Records ; Electronic Signatures (ERES)

Le 21 CFR part 11, norme américaine de la **F**ood & **D**rug **A**dministration, porte sur les enregistrements de données soumis à la règlementation.

La gestion des données est soumise à un certain nombre de règles destinées à offrir des garanties de pérennité, d'authenticité, de confidentialité et de traçabilité. Sont donc concernées les données critiques amenées à être créées, modifiées, conservées, archivées, retirées, transmises.

Les règles, une fois interprétées et adaptées au système, se décline autour des principaux thèmes suivants :

**La gestion des accès et des droits utilisateurs** : sécurité, attributions, connexions, déconnexions
**L'horodatage des données**
**L'audit trail** dont l'objectif est de conserver la trace de toute action ou modification survenue sur les données.
**L'accessibilité et la consultation des données électroniques**
**L'archivage et la restauration des données électroniques**
**La signature électronique** visant à attester de la fiabilité des documents critiques.

# SIGNATURES ELECTRONIQUES

Lorsqu'elles sont utilisées pour de l'approbation de document GMP, les signatures électroniques doivent **être validées** par un organisme tiers permettant de justifié de son authenticité. (DocuSign …). Pour ce faire, l´obtention d´un certificat lié à la signature est nécessaire.

Par abus de langage, on parle aussi de signature électronique au niveau de la traçabilité des actions sur un SISA. Cette traçabilité permet de faciliter les revues périodique d´Audit Trail à savoir l´origine des actions (System/Operateur).

La signature doit :

- Permettre **d'identifier la personne signataire**
- Être **unique**, non utilisable par une autre personne (identifiants de connexion unique)

Deux types de signatures : biométrique et non biométriques

Les signatures biométriques utilisent une partie du corps humain pour l'identification.

Les signatures non biométriques doivent :

- Avoir au moins deux composants d'identification : **un mot de passe et un identifiant**
- **Être uniques à un utilisateur**

Les **mots de passes** doivent :

- respecter un nombre de caractère minimal,
- Être changés à une fréquence définie
- Stockés dans des endroits sécurisés
- Ne jamais être partagés

Ces requis sont vérifiés lors de la validation du système.

# FDA 21cfr part 11

**Chaque point nécessite une réponse technique ou documentaire**

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.10(a)** | Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | S'assurer que le système est soumis à validation et à des tests fonctionnels<br>S'assurer que les données ne peuvent pas être altérées.<br>S'assurer que l'emplacement des données est protégé.<br>S'assurer que les saisies sont contrôlées selon leur type et leurs valeurs limites. | Le système est soumis à qualification FAT. IQ. OQ<br>Les données enregistrées ne sont pas modifiables depuis l'application.<br>Il n'y a **pas d'accès en suppression et modification aux données enregistrées** depuis l'application.<br>**L'administrateur de l'application n'est pas l'administrateur du support des données électroniques.**<br>Les types et valeurs limites sont définies au niveau de la spécification fonctionnelle. |
| **11.10(b)** | The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. | S'assurer que les données électroniques et rapports sont disponibles pour revues. | Les données électroniques sont **consultables et imprimable** depuis l'application :<br>- Archives courbes<br>- Archives alarmes<br>- Audit trail<br>Les rapports sont accessibles et imprimables depuis le système. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.10(c)** | Protection of records to enable their accurate and ready retrieval throughout the records retention period. | S'assurer qu'il est possible de récupérer des données inactives.<br><br>S'assurer que le système dispose de mécanisme pour protéger les données. | Les **lieux de stockage** des données électroniques sont mentionnés **dans la Spécification de Design** SCADA et IT.<br><br>Les données électroniques sont non modifiables depuis l'application :<br><br>- Courbes<br>- Alarmes<br>- Audit trail<br><br>Les données électroniques sont visualisables et imprimables immédiatement sur la période de rétention souhaitée.<br><br>Les données électroniques sont **sauvegardées** dans un environnement virtualisé dont la **capacité de stockage** peut s'étendre selon les besoins (procédure client).<br><br>Sur le long terme et en cas de besoin, les données électroniques peuvent être externalisées du système actif via **archive** de la base de données (procédure interne client).<br><br>En cas de consultation de données présentent sous format archive, se référer à la procédure interne du client de gestion des archives. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.10 (d)** | Limiting system access to authorized individuals. | S'assurer que le système décrit les autorisations d'accès.<br>S'assurer que l'accès au système est soumis à autorisation. | Les **groupes utilisateurs et les actions possibles** sont décrites dans le document de spécification de Design Logiciel (SDS_22134-001). |
| **11.10 (e)** | Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. | S'assurer que la date et heure du système est contrôlé par rapport à une référence.<br>S'assurer que la date et heure ne peut pas être modifié par l'utilisateur du système.<br>S'assurer que chaque enregistrement d'Audit Trail s'effectue en mémorisant la date et heure de l'évènement au moment de l'action.<br>S'assurer que l'audit trail lest capable de tracer toutes actions de création, modification ou suppression de la part d'un utilisateur.<br>S'assurer qu'un changement de valeur ne fasse pas perdre la précédente valeur.<br>S'assurer que le système est capable de fournir une copie de l'audit trail selon une période donnée.<br>S'assurer que le système défini une période de rétention | Les serveurs du système sont connectés au **serveur de temps NTP** du site.<br>La date et heure de l'automate est synchronisée sur l'heure du serveur du système.<br>L'application ne permet **pas de modifier la date/heure**.<br>Le système enregistre dans **l'audit trail** :<br>- Le système<br>- L'utilisateur<br>- La date/heure du changement<br>- La valeur avant changement<br>- La nouvelle valeur<br>L'audit trail est consultable depuis l'application sur une période donnée et imprimable.<br>La rétention des données sur la période requise doit être assurée par le client sous forme de procédure. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.10(f)** | Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | S´assurer que le système vérifie les autorisations pour le séquencement des étapes | Le système vérifie les autorisations de démarrage, le séquencement et monitore les alarmes conformément aux spécifications du système.<br>Les limites de saisie sont aussi spécifiées et testées. Ces **spécifications sont testées et validées** durant tout le cycle de qualification de l´application (FAT, SAT. IQ, OQ) |
| **11.10 (g)** | Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. | S´assurer que seules les personnes autorisées sont habilitées à utiliser le système, accéder aux enregistrements. | Le système est livré avec un **manuel utilisateur** servant de support pour les formations du personnel avant mise en production.<br>L´attribution des droit d´accès se fait en fonction du niveau de formation et du groupe auquel l´utilisateur appartient. |
| **11.10(h)** | Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | S´assurer que les données saisies sont valides | Les limites de saisie sont décrites dans les spécifications du système et validées lors des protocoles de qualification. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.10(i) | Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. | S´assurer que les personnes qui développe, maintiennent et utilise les enregistrements et signature électronique ont les compétences, l´éducation et l´expérience pour exécuter leur tâche. | Ce point doit être **assuré par le client** en termes de procédures, formation, récurrence des formations. |
| 11.10(j) | The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. | S´assurer de la mise en place d´une politique de sécurisation des données. | Il est de la responsabilité du client de mettre en place une politique de sécurisation des comptes électronique.<br>Sensibilisation aux enjeux de la sécurité des données avec comme moyen d´action : **durée de validité des mots de passe, complexité des mots de passe** |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.10(k)** | Use of appropriate controls over systems documentation including:<br><br>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.<br><br>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | Utilisation appropriée de la documentation système :<br><br>Contrôle adéquate des accès à la documentation système et de sa distribution<br><br>Versioning et gestion du document pour maintenir une traçabilité du changement dans le temps | Dans le cadre du projet, les **documents et programmes sont versionnés**. Les versions sont tracées au niveau des protocoles ou par un document de **changement de version logiciel**.<br><br>Point à la charge du client :<br><br>Mise en place d´un système de copie contrôlée. De point de distribution, de gestion documentaire.<br><br>Mise en place du versioning des documents (historique, track change, description du changement) |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.30** | Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. | S´assurer de l´intégrité des données dans des système ouvert | **La solution fournit par SP Groups est un système fermé**.<br>Toute utilisation des enregistrements électroniques est de la responsabilité du client : mise en place de procédure permettant de garantir l´intégrité des données. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.50** | Signature manifestations.<br>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:<br>(1) The printed name of the signer;<br>(2) The date and time when the signature was executed; and<br>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.<br>(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout). | S´assurer du format de la signature électronique permet d´identifier le signataire, le moment et la raison | L'identification unique est gérée par le client. SP Groups ne permet l'accès à l'application qu'à une seule personne préalablement identifiée au travers de **l'Active Directory** du client.<br>Toute action dans l'application trace le nom de l'identifiant, la date et heure de l'évènement.<br>Les **rapports générés par l'application doivent être signés manuellement** : mise en place d´un cadre de signature pour approbation. La notion de signature électronique ne s'applique pas dans le cadre d'une signature automatique de document (comme par exemple Adobe Sign). |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.70** | Signature/record linking.<br>Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. | S´assurer de l´intégrité de la signature électronique | Application ne permet pas la copie de signature.<br>Les utilisateurs de l'application sont gérés par le client. |
| **11.100 (a)** | Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | Chaque signature électronique doit être propre à une personne et ne doit pas être réutilisée par quelqu'un d'autre ou réattribuée à quelqu'un d'autre. | Cette garantie est de **la responsabilité du client.**<br>Une procédure d'attribution de l'identifiant à une personne physique doit être mise en place.<br>Des règles de protections des mots de passes doivent être mise en place. |
| **11.100 (b)** | Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. | S'assurer qu'une personne physique ne peut pas usurper l'identifiant d'un autre utilisateur. | Une procédure d'attribution de l'identifiant à une personne physique doit être mise en place.<br>Une procédure de suppression d'un identifiant doit également être mise en place. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.100 (c)(1) | Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.<br>(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. | S'assurer que la personne physique a déposé sa signature manuscrite pour permettre l'utilisation d'un identifiant électronique. | Une procédure d'attribution de l'identifiant à une personne physique doit être mise en place. |
| 11.100 (c)(2) | (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. | S'assurer que la personne physique a déposé sa signature manuscrite pour permettre l'utilisation d'un identifiant électronique. | Une procédure d'attribution de l'identifiant à une personne physique doit être mise en place. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.200(a)(1)** | Electronic signatures that are not based upon biometrics shall:<br>(1) Employ at least two distinct identification components such as an identification code and password. | S'assurer que l'accès à l'application se fait par un login identifiant et un mot de passe. | Tout accès à l'application nécessite un **login et un mot de passe**.<br>La gestion des mots de passes par identifiant est sous la responsabilité du client (connexion **Active Directory** du client et **règles de sécurités du client**). |
| **11.200(a)(1)(i)** | (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. | S'assurer que sur une certaine durée d'utilisation, un autre utilisateur ne peut pas se substituer au premier identifiant connecté. | L'application permet à l'utilisateur de **se déconnecter** afin de forcer un autre utilisateur à s'identifier.<br>L'application dispose d'un **logout automatique** afin d'éviter qu'un utilisateur non identifié puisse réaliser des actions sur la dernière identification. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| **11.200(a)(1)(ii)** | (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. | S'assurer que sur des périodes non continues d'utilisation, l'utilisateur doit s'identifier avec un login et un mot de passe. | L'application permet à l'utilisateur de se déconnecter afin de libérer son identification (procédure client de bonne pratique).<br>L'application dispose d'un logout automatique afin d'éviter qu'un utilisateur non identifié puisse réaliser des actions sur la dernière identification. |
| **11.200(a)(2)** | Be used only by their genuine owners | S'assurer qu'aucun utilisateur ne peut utiliser l'identification d'un autre utilisateur. | L'application permet à l'utilisateur de se déconnecter afin de forcer un autre utilisateur à s'identifier.<br>L'application dispose d'un **logout automatique** afin d'éviter qu'un utilisateur non identifié puisse réaliser des actions sur la dernière identification. |
| **11.200(a)(3)** | Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | S'assurer d'un double niveau minimum de sécurité | **L'utilisateur est mettre de son mot de passe et peut le changer à sa demande.**<br>Un administrateur système gère les accès utilisateurs. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.200(a)(1)(ii) | (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. | S'assurer que sur des périodes non continues d'utilisation, l'utilisateur doit s'identifier avec un login et un mot de passe. | L'application permet à l'utilisateur de se déconnecter afin de libérer son identification (procédure client de bonne pratique).<br>L'application dispose d'un logout automatique afin d'éviter qu'un utilisateur non identifié puisse réaliser des actions sur la dernière identification. |
| 11.200(a)(2) | Be used only by their genuine owners | S'assurer qu'aucun utilisateur ne peut utiliser l'identification d'un autre utilisateur. | L'application permet à l'utilisateur de se déconnecter afin de forcer un autre utilisateur à s'identifier.<br>L'application dispose d'un logout automatique afin d'éviter qu'un utilisateur non identifié puisse réaliser des actions sur la dernière identification. |
| 11.200(a)(3) | Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. | S'assurer d'un double niveau minimum de sécurité | L'utilisateur est mettre de son mot de passe et peut le changer à sa demande.<br>Un administrateur système gère les accès utilisateurs. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.200(b) | Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | N/A Pas de biométrie | N/A Pas de biométrie |
| 11.200(a) | Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:<br>(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. | S'assurer de la sécurité et intégrité des mots de passes, ainsi que du caractère unique de chaque mot de passe. | Le système ne gère **pas d'utilisateur générique**. Chaque utilisateur est unique de par son identifiant et mot de passe.<br>Les règles de gestion des mots de passe sont assurées par le client dans l'Active Directory du site. |
| 11.200(b) | Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | S'assurer du renouvellement des mots de passe. | Les règles de gestion des mots de passe sont assurées par le client dans l'Active Directory du site. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.200(c) | Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | S'assurer de la présence d'un support interne pour la gestion des utilisateurs et mots de passes. | L'accès au système se fait uniquement au travers de la saisie manuelle de l'identifiant et de son mot de passe. Pas de carte d'identification.<br>Management et procédure sous la responsabilité du client. |
| 11.200(d) | Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | S'assurer de la présence de mesure de protection pour l'utilisation non autorisée d'un identifiant. | Les règles de tentatives de saisie de mots de passe sont assurées par le client dans l'Active Directory du site. |
| 11.200(e) | Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. | S'assurer d'une revue périodique de la mise en œuvre et utilisation des identifiants. | L'accès au système se fait uniquement au travers de la saisie manuelle de l'identifiant et de son mot de passe. Pas de carte d'identification.<br>Management et procédure sous la responsabilité du client. |

# FDA 21cfr part 11

| Références | Exigences | Objectifs | Réponses |
|---|---|---|---|
| 11.300(a) | Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. | S'assurer du caractère unique de chaque combinaison de code d'identification et de mot de passe | Les règles de gestion des mots de passe sont assurées par le client dans l'Active Directory du site. |
| 11.300(b) | Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | S'assurer que les mots de passe soient périodiquement vérifiés, rappelés ou révisés. | Les règles de gestion des mots de passe sont assurées par le client dans l'Active Directory du site (renouvellement périodique imposé). |
| 11. 300(d) | Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. | S'assurer de la présence de mesure de protection pour l'utilisation non autorisée d'un identifiant. | Les règles de tentatives de saisie de mots de passe sont assurées par le client dans l'Active Directory du site. |

# REVUE PERIODIQUE (Exploitation Client)

Pour s'assurer que les requis mentionnés dans les 21 cfr part 11 et l'annexe 11 des GMP sont respectés et que le risque de modification de donnée est maitrisée, une revue périodique du système doit être réalisée.
Les revues périodiques sont réalisées par le client lors de l'utilisation du système. Lors de la conception du système, il faut vérifier que le client ait accès pour effectuer cette revue.
La revue périodique permet de vérifier qu'un système informatisé est maintenu dans un état validé tout au long de son utilisation.

Elle comprend :

- **La revue du contenu de l'audit trail**
- **La revue des formations aux systèmes**
- **La revue des accès (si la traçabilité a bien été faite lors de la suppression, création ou modification d'un utilisateur).**
- **L'application des procédures**
- **L'efficacité du système de sauvegarde**
- **La revue des actions préventives (ex: calibration / maintenance) et correctives du système**
- **La revue des changements**


**GENÈVE**
Route des Jeunes 9
1227 Les Acacias
Suisse
+41 22 792 70 00

**MARTIGNY**
Rue du Châble-Bet 41
1920 Martigny
Suisse
+41 27 722 70 00

info@spgroups.ch
www.spgroups.ch