Méthode

INCAS.V2
INtégration dans la Conception des Applications de la Sécurité

Version 2.0

Juin 1999

Commission Qualité et Sécurité des Systèmes d'Information

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Semard – 75009 Paris
Téléphone : 01 53 25 08 80 Fax : 01 53 25 08 88

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement **René Hanouz**, ainsi que :

Michel	**BONNEAU**	**Enseignant**
Monique	**BOUCHER**	**RATP**
Paul	**De KERVASDOUE**	**AQUIS**
Eric	**SABATIER**	**Caisse d'Epargne**
Remy	**LE CHEVALIER**	**LCS CONSEIL**
Didier	**MONNIER**	**CANSSM**
Monsieur	**NASSIET**	**SNCF**
Guy	**PICHON**	**France Télécom Transpac**
Bernard	**VALENTIN**	**Lefebvre Consultants**
Olusamni	**ADEDUJI**	**Etudiant**

TABLE DES MATIERES

1. INTRODUCTION

1.1 Préalable

Le système d'information doit être considéré comme un élément stratégique des entreprises, au même titre que son personnel, ses produits, ses marchés et ses techniques. Dans notre économie actuelle, où la mise en œuvre de nouveaux instruments de paiement ne peut se concevoir sans support informatique, le système d'information présente des risques importants, qui pour une entreprise peuvent se répercuter sur l'ensemble de la profession.

1.1.1 Les enjeux

A titre d'information, le total des pertes liées aux risques informatiques, déclarées en milliards de francs à l'Assemblée Pleinière des Sociétés d'Assurances représentait en 1996, **12,72 milliards de Francs**, répartis en :

- **accidents** (panne, incendie, dégâts des eaux d'un serveur ou centre informatique,…) qui représentent **24% des pertes**
- **erreurs** (erreurs de conception, de programmation, d'exploitation, d'utilisation,…) qui représentent **14% des pertes**
- **malveillances** (vols de postes de travail, modification illicite des données, des programmes, à des fins de fraude ou détournement de fonds, défi intellectuel,…) qui représentent **62% des pertes**

Les actes de malveillance coûtent plus cher à la nation que les incidents sur chèques, les hold-up et la contrefaçon des billets pris séparément.

Les études d'analyse de risques montrent encore en 1998 que la grande faiblesse des systèmes d'information réside principalement dans le **manque de cohérence de la sécurité mise en œuvre** (moyens humains, techniques et organisationnels).

Cette situation résulte, pour partie,

- soit d'un manque de prise en compte de la sécurité,
- soit d'une prise en compte inadaptée et trop tardive des besoins de sécurité dans le cycle de conception et de développement projets informatiques.

1.1.2 Les dispositions prises

Afin de tenter de faire évoluer ces comportements, René HANOUZ dans le cadre des travaux au CLUSIF met dès 1992 à disposition des chefs de projets informatiques, une démarche d'intégration de la sécurité dans les méthodes de conduite de projet (INCAS.V1)

Cette démarche, aujourd'hui actualisée (INCAS.V2) n'est plus tributaire des méthodes de conduite de projet et de conception existantes sur le marché, mais elle s'intègre et s'appuie sur les modélisations et standards appliqués dans les entreprise (approche MERISE et approche Objet, modèles clients serveurs,…), en effet, elle propose maintenant :

- une **suite d'actions de sécurité courtes**, allant de 1 heure à la demi-journée, réparties sur tout le cycle de conception et de développement d'une application

- ces actions sont **intégrées dans les différentes phases** des méthodes de conduite de projet et de conception au moment jugé le plus opportun, afin d'obtenir l'efficacité maximum du travail aussi bien en temps qu'en qualité

- ces actions **tissent une toile sécuritaire** sur l'ensemble du projet, de son lancement jusqu'à sa mise en exploitation, il convient donc de toutes les réaliser, dans l'ordre, et avec les acteurs concernés

- l'analyse sécurité, qui s'appuie sur les **flux, l'architecture technique, les données, les traitements et les procédures organisationnelles**, permet d'être exhaustif et de répondre aux besoins de sécurité fonctionnelle en évitant comme cela est encore trop souvent le cas aujourd'hui de faire de la sécurité pour de la sécurité, voire de la méthode pour de la méthode

- la **fiche de suivi des mesures de sécurité**, en particulier, en fin de phase conception technique permet d'éviter que les mesures décidées ne tombent pas dans l'oubli. Il est de la responsabilité des instances de suivi qualité et sécurité du projet d'y veiller

- les actions de sécurité prévues dans les phases de développement, jusqu'à la phase d'évaluation permettent aux instances qualité et sécurité du projet de **contrôler l'atteinte effective des objectifs de sécurité** (cible de sécurité et fiches de suivi des mesures, élaborées en fin d'étude préalable et mise à jour au fur et à mesure des phases)

- enfin, un certain accompagnement de l'instance qualité et sécurité (RSSI) est primordial, car elle est le garant de la **qualité du travail** effectué (analyse de la gravité des risques du métier en terme d'accidents, d'erreurs, et de malveillances, sur les quatre facteurs DICP), et il doit apporter :

    - son **expertise de l'informatique** en général (études, méthodes, exploitation), et en particulier,
    - sa connaissance **de l'état de l'art de la sécurité** (les marchés de la sécurité, la sécurité internet, les aspects juridiques (CNIL, lois Godfrain, code d'éthique de la sécurité, …), des recommandation du SCSSI (ITSEC, Profil de protection)
    - sa connaissance des **méthodes de sécurité** (Marion, Mehari, Melisa, Messedi, Cramm, Budi, etc.)
    - sa connaissance des **techniques de sécurité** (les progiciels Racf, Top-secret, Acf2, les logiciels sécurité micros, les principes de cryptographie, le chiffrement, le scellement, DES, RSA, la gestion des clés, les niveaux, moyens et outils de secours et de sauvegardes en environnement client serveur, EDI, etc.)

cet accompagnement assure un gain de temps et une efficacité importante sur la qualité, la sécurité et le déroulement général du projet.

2. PRESENTATION GENERALE

INCAS s'adresse principalement aux EQUIPES DE PROJET et implique conjointement les utilisateurs représentant de la maîtrise d'ouvrage et les informaticiens représentant de la maîtrise d'œuvre, selon les phases et les actions de sécurité déroulées, les pôles de compétences technique sont sollicités.

INCAS intègre les quatre FACTEURS DE BASE DE LA SECURITE interprétés comme suit :

- la **Disponibilité (Dn)** garantie de continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.
- l'**Intégrité(In)** garantie d'exactitude, d'exhaustivité et de validité de l'information garantie de non modification illicite de l'information
- la **Confidentialité(Cn)** garantie de non accès illicite en lecture ou en divulgation de l'information (papiers, disquettes, portables,…)
- la **Preuve et** le **Contrôle(Pn)** garantie d'auditabilité et de non répudiation [1]

INCAS s'appuie sur un SYSTEME de CLASSIFICATION de la gravité du risque :

La mesure globale du risque ne peut résulter d'une quelconque opération mathématique fonction de l'impact et de la potentialité.

L'importance d'un risque, sa "**gravité**", résulte d'une décision stratégique de l'entreprise fondée sur les valeurs d'impact et de potentialité. Cette décision peut être traduite en termes « d'aversion aux risques ».

L'équipe projet (maîtrise d'ouvrage et maîtrise d'œuvre) doit se prononcer sur la forme que revêt pour elle l'aversion au risque (A), en fonction de l'impact (I) et de la potentialité du risque (P), quel que soit celui-ci. Ceci peut être fait par une **grille d'aversion au risque**.

Cette grille traduit le comportement face au risque, tel qu'il peut s'exprimer dans la réalité avec ses composantes I et P . Un exemple d'une telle grille est donné ci-dessous :

I / P	1	2	3	4
0	0	0	0	0
1	0	1	**2**	**3**
2	0	1	**3**	**4**
3	1	**2**	**3**	**4**
4	1	**2**	**3**	**4**

Par convention, nous mesurerons la gravité d'un risque « g » par l'aversion au risque déduite de cette grille en fonction de I et de P.

Cette gravité repose sur un système de classification simple :

la cotation **(n) = 0 et 1** correspond à une **Gravité de Risque** dite **Faible et acceptée**

la cotation **(n)=2, 3 et 4** correspond à une **Gravité de Risque** dite **Inacceptable**

[1] à interpréter dans un sens plus concret que celui de la norme Iso 10-181

Règle : Dès que la gravité des risques est estimée supérieure à 1, des mesures de réduction des risques, adaptées et équilibrées à la gravité des risques et au plan économique sont à déterminer, à planifier et à mettre en œuvre dans les phases suivantes du projet.

INCAS est applicable dans les cas suivants :

- conception et développement de projets traditionnels (centralisés, décentralisés, clients serveurs, EDI, objets, Intelligence Artificielle, etc.)
- acquisition de progiciels,
- développement de projets sur micro-ordinateur.
- audit d'applications existantes par reverse engineering

Remarque : il est important de souligner que l'intégration de la sécurité dans la conception et le développement des applications ne peut, ni ne doit être perçue comme un ***projet en soi****. C'est la raison pour laquelle,* ***INCAS est partie intégrante des méthodes de conduite de projet et de conception,....***

A ce titre, les livrables de sécurité issus de cette démarche font partie des méthodes de conduite de projet et de conception, et doivent pouvoir être consultés à la demande, par les responsables concernés

3. DEMARCHE

Elle comprend TROIS ETAPES fondamentales intégrées aux phases de Conduite de Projet.

3.1 1ère Etape : dans les phases de conception du système

3.1.1 En phase de lancement

- Définir globalement à partir des grandes activités du projet, la gravité des risques en terme DICP (cf. p.10),
- Justifier cette classification et mettre en relief les risques stratégiques.

Cette première action sécurité réalisée avec les responsables de l'équipe projet Maîtrise d'Ouvrage et Maîtrise d'œuvre permet d'orienter les **facteurs de sécurité sur lesquels un effort important sera à consentir**.

3.1.2 En étude préalable

- Initialisation des risques liés au développement (cf. p. 12 à 17)

Expression des besoins de sécurité liés aux scénarios envisagés pour le système futur.

- Analyser globalement la gravité des **risques survenus sur le système existant**

- Déterminer à partir de la modélisation du SI futur réalisée par l'équipe projet **les besoins en sécurité du nouveau projet informatique** (architecture technique, échanges ou flux, données, traitements, procédures organisationnels, progiciel)
- **classification de la gravité des risques**[2] en **D**isponibilité, **I**ntégrité, **C**onfidentialité, **P**reuve et contrôle
- **définition de mesures** globales et besoins de sécurité permettant une approche économique en terme de risques et mesures pour chaque scénario envisagé

- Faire une **synthèse sécurité** de deux à trois pages pour le comité de pilotage
- Définir la **cible de sécurité** visée pour l'application future
- Initier **la fiche de suivi** des mesures de sécurité

[2] d'Accident, d'Erreur, de Malveillance

3.1.3 En conception générale

- Initialisation des risques liés au développement (cf. p. 12 à 17)

  A partir de la **modélisation finalisée du système futur** (données, traitements, organisation(*)) et en fonction des besoins de sécurité retenus en étude préalable pour chacun des facteurs DICP

- procéder à une étude de la gravité des risques, **globale ou détaillée** :
  - - **globale**, sur D et/ou I et/ou C et/ou P, par regroupement, de lots de données, traitements et procédures organisationnelles (données, traitements, organisation(*)) représentant un sous-ensemble cohérent pour la sécurité et relevant exclusivement d'une classification de la **gravité des risques égale à 2**
  - - **détaillée**, sur D et/ou I et/ou C et/ou P, des données, traitements et procédures organisationnelles (données, traitements, organisation[3]) et relevant exclusivement d'une classification de la **gravité des risques égale à 3 ou 4**
- affiner et détailler les mesures de sécurité et le bilan économique établis en étude préalable
- mettre à jour la **synthèse sécurité** de deux à trois pages pour le comité de pilotage
- actualiser la **cible de sécurité** visée pour l'application future
- compléter les **fiches de suivi** des mesures de sécurité

3.2 2ème Etape : dans les phases de spécifications

3.2.1 En spécifications fonctionnelles

- Initialisation des risques liés au développement (cf. p. 12 à 17)

  A partir des mesures de sécurité exprimées en étape 1:

- traduire les besoins de sécurité **en fonctions et services de sécurité** à mettre en œuvre :

  I,C : contrôle d'accès (profils et habilitations pour le transactionnel et le traitement par lots)

  I,C : intégrité des flux (non modification des champs, des séquences,…)

  C : secret du flux (empêcher une observation de certains flux)

  P : authentification de l'entité homologue (l'entité connectée est bien celle prévue)

  P : authentification de l'origine (non répudiation)

  D : procédures dégradées informatiques et non informatiques

  C,D : fonctions de confidentialité et de pérennité des jeux d'essai

3 MCD,MCT,MOT si utilisation de MERISE

3.2.2 En conception technique

- Initialisation des risques liés au développement (cf. p. 12 à 17)
- préciser pour les fonctions et services retenus les **mécanismes de sécurité** à mettre en oeuvre :

  I,C : sécurité liée aux bases de données de l'application (protection des champs, etc.)

  I,C : chiffrement, scellement (mécanismes de distribution des clés protégeant les services de confidentialité, d'intégrité et d'authentification)

  I,C,P : signature numérique avec ou sans notarisation (dépend du niveau de confiance des entités émettrices et réceptrices)

  C : bourrage de voie pour éviter qu'un tiers puisse tirer des conclusions de l'analyse du trafic

  I,C : contrôle de routage (routes obligatoires, toutes routes sauf,…)

  D : sauvegardes liée aux données de l'application (besoins utilisateurs ou applicatifs, etc.)

  D : archivages liés aux données de l'application (archivage légal, etc.)

  D : spécificités de l'application future liée au secours techniques (back-up matériel, applicatif, serveurs, réseau local, réseau distribué, etc.) et à la continuité du service (contrat de réserve)

mettre à jour la **synthèse sécurité** de deux à trois pages pour le comité de pilotage

actualiser la **cible de sécurité** visée pour l'application future

compléter les **fiches de suivi** des mesures de sécurité avant le démarrage des phases de développement

3.3 3ème Etape : dans les phases de développement

3.3.1 En réalisation, tests, recette, installation, démarrage, évaluation

Sécurité de l'application future

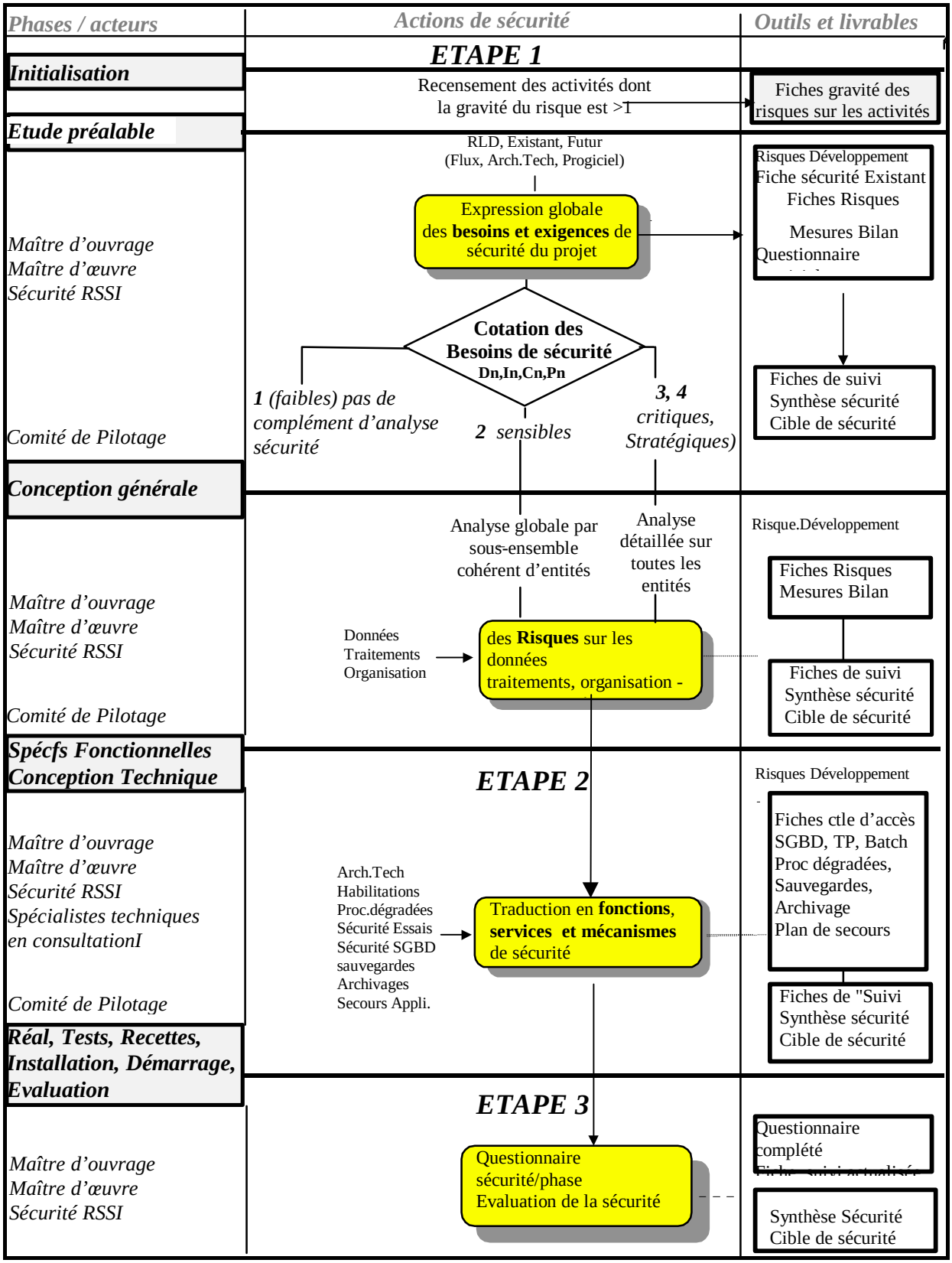
A partir des fiches de suivi mises à jour et validées en fin de phase de conception technique :

- vérifier et propager (qui fait quoi ?, quand ?, comment ?). l'ensemble des mesures retenues sur les fiches de suivi dans les dossiers de développement (dossiers de programme, manuels utilisateurs, dossiers techniques d'exploitation, etc.)
- Passer en revue les questionnaires sécurité, spécifiques au développement de chaque phase (réalisation et tests, recette, installation, démarrage et évaluation) et apporter les correctifs qualité et sécurité jugés utiles pour maintenir le niveau de sécurité de l'application future
- En phase d'évaluation, vérifier, en outre, que les **besoins de sécurité sont effectivement atteints** (**cible de sécurité**) :
  - valider la réalisation de l'ensemble des mesures répertoriées dans les fiches de suivi (Informatique et Utilisateur),
  - Valider l'efficacité[4] et la robustesse[5] des moyens de sécurité mis en oeuvre
  - rédiger une synthèse mettant en relief ce qu'il reste à faire et ce qui est fait.

[4] facile à mettre en œuvre et bon retour sur investissement sécurité

[5] résistant aux menaces, par exemple aux intrusions, etc.

3.4 Vue de synthèse



3.5 Echelle de références pour l'évaluation des risques

3.5.1 Stratégique : niveau 4

Tout incident(1) susceptible de provoquer :

- des pertes financières inacceptables (ex : centaines de millions de francs et milliards)
- des pertes immédiates d'une activité ou d'un métier de l'entreprise
- des sanctions judiciaires au plus haut niveau de responsabilité Exemple : échec de négociations de très haut niveau (politique ou économique)

3.5.2 Critique : niveau 3

Tout incident(1) susceptible de provoquer :

- des pertes financières importantes (ex : quelques dizaines de MF à 100 MF)
- une nuisance grave à l'image de marque
- une perte importante de marchés, de clientèle
- un infraction majeure à la législation
- une nuisance organisationnelle jugée importante sur l'ensemble de l'entreprise
- une gêne susceptible de fausser les décisions et les orientations des dirigeants.

3.5.3 Sensible : niveau 2

Tout incident(1) susceptible de provoquer :

- des pertes financières significatives (ex : quelques centaines de KF à 10 MF)
- une nuisance significative à l'image de marque
- une perte significative de clientèle
- une nuisance organisationnelle jugée significative par l'utilisateur
- un manque à la réglementation, comptable et/ou fiscale
- la non atteinte des objectifs visés par un projet important.

3.5.4 Faible : niveau 1

Tout incident[6] susceptible d'occasionner de faibles nuisances, interne au domaine considéré et peu gênant pour l'utilisateur.

Une évaluation plus précise, et quantifiée, des niveaux n'est en général pas immédiatement possible, elle s'appuiera au fur et à mesure du temps sur l'expérience acquise et les comparaisons entre applications.

---

[6] il s'agit de sinistres liés à une interruption prolongée de l'application (bug applicatif, panne serveur, panne réseau, perte ou vols de fichiers et sauvegardes, etc.) ou à des résultats erronés (programme fonctionnant mal, tableaux de bords de décision faux, états comptables impossibles à ajuster, taux de crédit faux, mauvais arrondis, malveillance programmée, virus, etc.), ou à une divulgation d'information confidentiel, accès illicite par le réseau, écoute téléphonique, vente d'information, etc). ou à des erreurs ne pouvant être prouvés, ou actes de malveillances (fraudes, détournements de fonds par des moyens liés à l'informatique, sabotage, défi intellectuel, etc.)

4. ANNEXES LIVRABLES

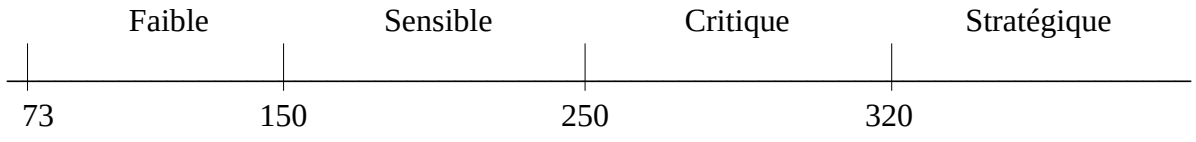
4.1 Risques Liés au Développement du projet[7]

PROJET : DATE :

PHASE :

Domaines étudiés :	Note	Pondération	Note Pondérée
RISQUES LIES à la TAILLE du PROJET			
1. Importance du développement (charges / délais)		5	
2. Nombre de directions, fonctions,... concernées		6	
3. Planification et suivi budgétaire		5	
RISQUES LIES À L'ORGANISATION			
1. Impact (%) des fonctions automatisées		3	
2. Impact des modifications de procédures		3	
3.Impact des modifications de structures utilisateurs		5	
4. Appréciation de l'utilisateur		5	
5. Participation des fonctions utilisatrices		5	
6. Existence d'une équipe de projet		4	
7.Définition, fonctionnement des structures du projet		5	
8. Expérience du management projet		6	
RISQUES TECHNOLOGIQUES :			
1. Aspect hardware (matériel, site nouveaux etc.)		3	
2. Aspect software (logiciels nouveaux ou modifiés)		5	
3. Connaissance informatique des utilisateurs		4	
4. Connaissance du domaine par les utilisateurs		6	
5. Connaissance du domaine par les informaticiens		3	
Niveau global de risques (TOTAL des NOTES PONDEREES)			

Echelle de notation du niveau de risque



Niveau de risque lié au développement du projet :

Faible **o** Sensible **o** Critique **o** Stratégique **o**

Règles d'analyse

Au-delà du seuil de notation 170 des mesures d'urgence doivent être prises.

[7] Ne pas confondre le système de rotation avec le niveau de risque défini en page 10.

Mais, même avec une moyenne satisfaisante, un ou plusieurs postes négatifs et essentiels pour le projet doivent entraîner des correctifs.

4.2 Mode d'emploi Risques liés à la taille du projet

NOTES

4.2.1 IMPORTANCE DU DEVELOPPEMENT

Délais (nbre de mois) Charge (*)	3 à 9 mois	9 à 12 mois	12 à 24 mois	+ de 24 mois
3 h / mois à 6 h / mois	1	2	3	4
6 h / mois à 30 h / mois	2	1	2	3
30 h / mois à 6 années x h	3	2	1	2
+ de 6 années x h	4	3	2	3

(*) cette charge recouvre l'ensemble des phases du cycle de développement et des intervenants (utilisateurs et informaticiens).

4.2.2 Nombres de directions concernées *Notes*

(interlocuteurs que le chef de projet a en face de lui pour mener à bien son projet)

- une ou deux 1
- trois ou quatre 2
- cinq ou plus 3

4.2.3 Planification et suivi budgétaire *Notes*

Il y a un suivi régulier tant de la planification que du budget 1

Il y a un suivi de temps à autre sans contrôle et/ou suivi budgétaire épisodique 2

Il n'y a pas de planification du projet et/ou suivi budgétaire rare 3

Remarque : La planification des projets et son suivi permettent à l'équipe projet de connaître la progression du développement notamment au regard des délais et charges prévus.

Il est important d'y porter régulièrement attention notamment sur les écarts constatés pour y remédier le plus tôt.

Il est aussi utile qu'il y ait un contrôle de ce suivi effectué par une personne, un comité qui soit extérieur au groupe projet.

De même, un dépassement important du budget alloué peut entraîner l'arrêt du projet ; aussi est-il important de connaître le budget restant pour vérifier que l'on se situe dans ce cadre. Le cas échéant, il est important d'en avertir les structures décisionnaires pour d'éventuelles augmentations ou réductions

LES PONDERATIONS RETENUES CORRESPONDENT AUX ETUDES EFFECTUEES DANS LE CADRE D'ASSOCIATIONS D'EXPERTS QUALITE ET SECURITE DES SYSTEMES D'INFORMATION ET GROUPES DE TRAVAIL UTILISATEURS DE GRANDES ENTREPRISES (MFQ, CIGREF, etc.)

4.3 Mode d'emploi Risques Structurels et liés au Management

	NOTES
1. Impact (%)des fonctions à automatiser	
0 % à 25 %	3
25 % à 50 %	2
50 % à 100 %	1
2. Impact des modifications de procédures de fonctionnement	
Formation nécessaire des personnels	3
Légères modifications	2
Sans conséquences	1
3. Impact des modifications de structure utilisateurs	
Déplacement de personnel	3
Réorganisation partielle du service	2
Modifications sans conséquences	1
4. Appréciation de l'utilisateur (direction et final)	
Réservé sur l'apport du projet informatique	3
D'accord avec quelques réserves	2
Positive (est demandeur)	1
5. Participation des fonctions utilisatrices	
Peu ou pas impliqués	3
Attitudes concernées	2
Attitudes responsables, fortement impliquées	1
6. Existence d'une équipe de projet	
Non existante	3
Représentant(s) utilisateurs temps partiel	2
Représentant utilisateurs conforme aux prévisions du projet	1
7. Définition et fonctionnement des structures du projet	
Structures et ou principes de fonctionnement non définis	3
Structures et principes de fonctionnement en partie définis	2
Structures et principes de fonctionnement clairement définis	1

Les différentes structures participantes au projet sont-elles clairement définies, leurs rôles respectifs bien précisés ? Cette question concerne la maîtrise d'ouvrage, maîtrise d'ouvrage déléguée, maîtrise d'oeuvre, maîtrise d'oeuvre déléguée et d'autre part la facilité, la rapidité de communication entre ces différentes structures.L'absence claire de définitions, de responsabilités, de procédures de communication efficaces pouvant avoir des impacts sur le déroulement du projet notamment en délais et charges. Une charte de services peut exister formalisant ces différents points.

8. Expérience du management du projet	
Expérience du management d'équipe forte	1
Expérience du management d'équipe moyenne	2
Expérience du management d'équipe faible	3

LES PONDERATIONS RETENUES CORRESPONDENT AUX ETUDES EFFECTUEES DANS LE CADRE D'ASSOCIATIONS D'EXPERTS QUALITE ET SECURITE DES SYSTEMES D'INFORMATION ET GROUPES DE TRAVAIL UTILISATEURS DE GRANDES ENTREPRISES (MFQ, CIGREF, etc.)

4.4 Mode d'emploi Risques Technologiques et de non connaissance

	NOTES
1. Aspects Matériels : matériel, site nouveaux (notes cumulatives)	
Pas de matériel nouveau	1
Ajout d'un serveur ou CPU	3
Ajout de périphériques (imprimantes, etc.)	2
Ajout de mini-ordinateurs ou micro-ordinateurs en environnement hétérogène	3
Ajout de réseaux (LAN, WAN, etc.)	3
Création d'un nouveau site (Bâtiment + matériel)	4
Total =	
2. Aspects Applicatifs - logiciels nouveaux -(notes cumulatives)	
Pas d'outils logiciels nouveaux	1
Nouveau langage de développement (C++, etc.)	2
Nouveau S G B D (ORACLE, INGRES, etc.)	2
Nouvelle technique du développement (AGL, etc.)	3
Nouveau protocole télécommunication (TCP/IP,. ..)	2
Nouvelle technologie (Internet, Intranet, etc.)	2
Nouveau logiciel d'édition	2
Nouveau logiciel de communication (EDI, PELICAN)	2
Nouveau progiciel	2
Total =	
3. Connaissance informatique des utilisateurs	
N'utilise pas d'outils informatiques (écran passif sans plus)	3
Travaille sur micro en local avec des tableurs,..	2
Connaît une méthode de conception et la programmation	1
4. Connaissance par les utilisateurs du domaine abordé	
Connaît peu le sujet traité dans le projet	3
Le sujet traité fait partie de son travail courant	2
Connaît bien le sujet traité depuis plusieurs années	1
5. Connaissance par les informaticiens du domaine abordé	
N'a jamais traité ce type de sujet (ou informaticien débutant),	3
1er ou 2ème projet traitant du sujet (ou équipe mixte externe + interne, débutant partiellement)	2
Plusieurs projets de ce type à son actif (informaticien expérimenté)	1

LES PONDERATIONS RETENUES CORRESPONDENT AUX ETUDES EFFECTUEES DANS LE CADRE D'ASSOCIATIONS D'EXPERTS QUALITE ET SECURITE DES SYSTEMES D'INFORMATION ET GROUPES DE TRAVAIL UTILISATEURS DE GRANDES ENTREPRISES (MFQ, CIGREF, etc.)

4.5 Autres aspects des risques liés au projet

D'autres éléments sont à prendre en compte pour minimiser les risques liés au développement, "en général on le sait, mais on ne l'applique pas" il en résulte les résultats que l'on connaît :

projets abandonnés,

dépassements des délais,

dépassements des budgets,

organisation conflictuelle,

maintenances avant même que le projet soit terminé (non qualité),

mécontentement des utilisateurs,

etc.

4.5.1 L'importance du projet pour l'entreprise

Il est possible d'apprécier cette dimension à partir de certains indicateurs, par exemple :

le projet est soumis à des contraintes réglementaires,

le projet concerne tout ou une partie des clients de l'entreprise,

le projet concerne un nombre de personnel conséquent,

etc.

On peut alors dire que les risques constatés prennent une dimension plus importante en rapport avec l'importance du projet pour l'entreprise au point de devenir inacceptables.

4.5.2 La dépendance inter-projets et inter-applications

Si le projet dépend, pour être opérationnel d'un (ou plusieurs) autre(s) projet(s) en cours de développement, il faudra avoir connaissance de l'évolution de ce projet afin de pouvoir éventuellement prendre les dispositions nécessaires.

De même si ce projet dépend d'autres applications en fonctionnement, il faudra s'attacher à bien identifier les relations pour éventuellement prévoir et développer des interfaces ou mises à jour de ces applications.

4.5.3 La disponibilité des décideurs, valideurs

Dans le cadre de projets concernant par exemple plusieurs entités juridiques distinctes et pour lesquels des structures de pilotage regroupent les valideurs et les décideurs des projets, il est important que les actions de validation et de décision se déroulent avec le moindre impact notamment sur les délais du projet.

4.5.4 La définition des tâches des acteurs (non pilotes) du projet et l'adhésion

Il est important que chaque membre (utilisateurs, informaticiens, organisateurs) connaisse parfaitement ses tâches, ses responsabilités dans le cadre du projet. Une bonne communication au sein de l'équipe, une adhésion aux objectifs et à l'organisation du travail sont des éléments forts de succès.

4.5.5 La localisation de l'équipe de projet

La répartition de l'équipe de projet (études, réalisation, etc.) sur différents sites génèrent des difficultés supplémentaires qui provoquent des retards, des erreurs et des incompréhensions, voire des conflits.

4.5.6 La préparation des ressources informatiques

Les ressources spécifiques nécessaires en matériels, logiciels, espaces disques, bureaux, etc. devront être identifiées et demandées au plus tôt afin d'éviter des retards dans la mise à disposition par rapport aux besoins.

4.5.7 La disponibilité des ressources humaines techniques

Il est important que l'équipe projet soit informée de la disponibilité des ressources humaines techniques (Architecte réseau, etc.) et qu'elle puisse planifier la charge de travail nécessaire au projet avec ces spécialistes. Faute de quoi les délais risquent de ne pas être totalement respectés.

5. ETUDE PREALABLE, CONCEPTION GENERALE

PREDEFINITION DE LA GRAVITE DES RISQUES
DU SYSTEME FUTUR
(MISE EN RELIEF DES RISQUES STRATEGIQUES)

PROJET: DATE :

PHASE :

Grandes fonctions du champ d'activité du projet	Classification Dn In Cn Pn	Justification de la classification Nature du risque[8] et description de son Impact et de sa Potentialité

Classification du document : …….

[8] accidents, erreurs, malveillances (ne pas négliger l'évocation du risque de malveillance, en particulier dans les projets financiers, etc.)

RISQUES SURVENUS SUR LE SYSTEME EXISTANT

PROJET : DATE :

PHASE :

Risques <u>survenus</u> sur le système existant ou auxquels on a échappé	**Classification[9] Dn, In, Cn, Pn**	**Conséquences[10] (pertes financières, image de marque, procès, etc.)**

Classification du document : ……..

[9] Cotation de la gravité du risque.

[10] Description de l'impact et de la fréquence d'apparition (potentialité) du risque

FICHE D'ANALYSE DE RISQUE

PHASE DU PROJET : DATE :

Document d'analyse : Référence du risque : **R . .**
Référence des documents

Elément à risque :

(Objet du système d'information)

Description du risque :

(Accidents, Erreurs, Malveillances)

Conséquences :

(pertes financières, image de marque, manque à gagner, problèmes juridiques, sociaux, surcharge ou sous charge de travail, etc.)

Classification DICP de la gravité du risque	Type de préjudice[11]	Valorisation du risque (charge en moisxHomme ou montant en KF, ou qualitatif)

Mesures de sécurité recommandées (informatiques et non informatiques) :

Phase du projet pour la prise en compte de la mesure	Responsable de la mesure	Coût des mesures de sécurité	Modalités de mise en place	Classification résiduelle de la gravité du risque

[11] Préjudices : Organisationnel, juridique, financier, social, image de marque, politique, responsabilité civile, etc.
Coût : exprimé en KF ou mois x hommes, ou bien qualitatif

RISQUES LIES AU PROGICIEL RETENU

PROJET : DATE :

PHASE :

Fournisseur : Progiciel :

Fonction(s) du progiciel :

- Notation des réponses au questionnaire sécurité progiciel INCAS :

  0 : très faible

  1 : faible

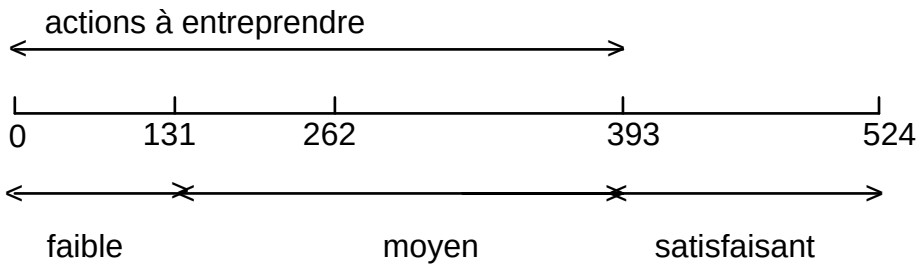
  2 : partiel ou moyen

  3 : assez satisfaisant

  4 : très satisfaisant

  Les pondérations peuvent être adaptées en fonction des exigences fonctionnelles, organisationnelles, ou de sécurité du projet.

- Résultats (total pondéré global)



Critères de sécurité	Note	Pon-déra-tion	Note pondérée	Observations

1. Sécurité du progiciel

1.1 - D,I,C,P : les facteurs de sécurité ont-ils été pris en compte lors de la conception du progiciel pour pallier les risques d'accidents, d'erreurs et de malveillances ?				
1.2 – I : la plate-forme de tests et recettes du progiciel était-elle sécurisée afin de réduire les risques de type bombe logique ?				
1.3 – I : Fréquence des versions (par an) ?				
1.4 - D : Date de la première et dernière installation du progiciel ?				
1.5 – I : Existe-t-il une assistance à la mise en œuvre et au paramétrage des éléments ou fonctions touchant la sécurité, soit du progiciel lui-même, soit de l'environnement de l'installation ?				
1.6 – D : Les programmes sources sont-ils déposés dans un organisme certifié (ex : APP) ?				
1.7 – D : Existe-t-il une maîtrise des programmes sources pour le client, ou une agence fournisseurs en France (droits de modification, correction d'anomalies) ?				
1.8 – Qualité : Quel est le coût d'une intervention en dépannage (hot-line, télémaintenance, etc.) ?				
1.9 – D : Le langage d'écriture du progiciel est-il un langage répandu ?				
1.10 – D : le développement du progiciel utilise-t-il les fonctions de COMMIT/ROLLBACK pour les transactions ?				
1.11 – P : Existe-t-il une journalisation ?				
1.12 – D : Le progiciel est-il portable sur différents environnements et système d'exploitation (UNIX, OS/400, WIN-NT, DEC, BULL, SUN, etc.) ?				

Critères de sécurité	Note	Pon-déra-tion	Note pondérée	Observations
1.13 – I : Dans le cas d'échanges de données avec d'autres progiciels ou applications, la cohérence de calcul est-elle assurée ou paramétrable ?				
1.14 – D : Sur quelle architecture de réseau étendue le progiciel peut-il s'appuyer TCP/IP, SNA, DSA, etc. ?				
1.15 – I,C : L'accès au progiciel est-il partagé au niveau de son administration ?				
1.16 – I,C : L'accès aux menus généraux du progiciel est-il protégé au niveau de son administration ?				
1.17 – I,C : L'accès aux menus généraux est-il protégé par code utilisateur ? mot de passe associé au code ? autres ?				
1.18 – I,C : Existe-t-il des standards d'accès par : société ?, catégorie d'individus ? individu ? transaction ? écran ? zone d'écran ? terminal ?				
1.19 – I,C : Peut-on combiner les contrôles d'accès ?				
1.20 – I,C : sont-ils paramétrables par l'utilisateurs propriétaire de l'information?				
1.21 – I,C : Quelles sont les caractéristiques des mots de passe (taille, constitution, rythme de changement, chiffrement, etc.) ?				
1.22 – I,C : Le progiciel gère-t-il la notion de profil utilisateur permettant de définir des autorisations distinctes en fonction de l'appartenance à un groupe ?				
1.23 –C :Existe-t-il un ou plusieurs profils standard ?				
1.24 – C : est-il possible de créer de nouveaux profils ?				
1.25 – D : en cas d'accident, existe-t-il une sauvegarde automatique de la dernière zone de saisie ? liste de saisie ? écran saisie ?				
1.26 – I : Existe-t-il un mécanisme d'inter-blocage réglementant les accès multiples aux entités du dictionnaire de données ?				

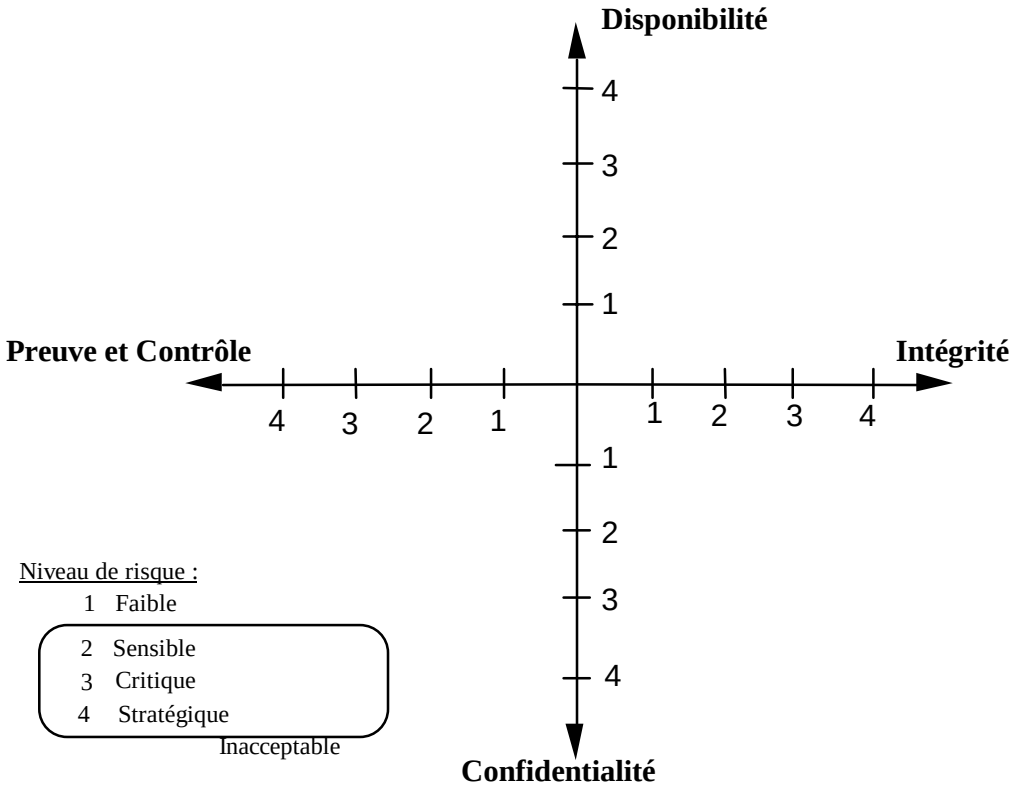
Critères de sécurité	Note	Pon-déra-tion	Note pondérée	Observations
1.27 – I : Les fichiers de la base de données doivent-ils être réorganisés régulièrement ? Quelle fréquence ?				
1.28 – I : Existe-t-il en standard des utilitaires de réorganisation et de sauvegarde de la base de donnée avec production d'un état de contrôle ?				
1.29 – I : Existe-t-il en standard des utilitaires permettant de récupérer des données stockées dans des tables relationnelles ?				
1.30 – D : Existe-t-il des outils prévus par le fournisseur pour la reprise des fichiers existants (conversion) ?				
1.31 – P : le progiciel permet-il d'obtenir un journal des accès (lecture, modifications, archivage, suppression, mise à jour) ?				
1.32 – I,C : Le progiciel permet-il via Internet des consultations, des saisies ou des modifications sécurisées ? (profils plus fin, fire-wall, etc.)				
1.33 – I : Le progiciel gère-t-il l'Euro ?				
1.34 – D : Le progiciel est-il compatible an 2000 et après ?				
1.35 – I : Existe-t-il des contrôles d'existence par rapport à des tables ?				
1.36 – I : Existe-t-il des contrôles de cohérence (ex / la clé du n°SS, etc.)				
1.37 – D : S'agit-il de contrôle informatifs ou bloquants ?				
1.38 – P : Existe-t-il des historiques ?				
1.39 – D,P : Existe-t-il un système d'archivage intégré ?				

NIVEAU DE SECURITE

PROJET : DATE :

PHASE :

	Disponibilité (D)	Intégrité (I)	Confidentialité (C)	Preuve (P)	Appréciation globale
Risques avant mesures de sécurité					
Risques après mesures de sécurité					
Cible de sécurité du futur système					



FICHE DE SUIVI DES MESURES DE SECURITE

PHASE DU PROJET,... : DATE :

PROJET :

Description des mesures de sécurité retenues	Phase d'étude concernée	Responsabilité Utilisateur ou Informatique	Date de réalisation	Date de validation

Visa du Chef de projet utilisateur et informaticien : ……...

6. SPECIFICATIONS FONCTIONNELLES

FONCTIONS ET SERVICES DE SECURITE
DEFINITION DES RESPONSABILITES

PROJET : DATE :

PHASE :

Eléments à risque (matériel, logiciel, données, procédures, etc.)	Classification Dn In Cn Pn	Propriétaire	Gestionnaire

MATRICE / FONCTIONS-ACTEURS-MODE D'ACCES

PROJET : **DATE :**
PHASE :
PROPRIETAIRE D'APPLICATION : **GLS :**
PROPRIETAIRE DE DONNEES : GESTIONNAIRE LOCAL DE SECURITE

Acteurs / **Fonctions**	***Utilisateur 1***	***Utilisateur 2***	***Utilisateur 3***	***Utilisateur 4***	***Utilisateur 5***
Fonctionnalités 1	*L*	*L,M,S*	*L*	*L*	*L,M,S,A*
Fonctionnalités 2	*L*	*L,M,S*	*L*	*L*	*L,M,S,A*
Fonctionnalités 3	*Archivage*	*LM*	*LM*	*L*	*LM*
Fonctionnalités 4			*L*		*LMS*
Fonctionnalités 5					*LM*
Autres exemples	***Administrateur***	***Propriétaire***	***Auditeur***	***GLS***	***Chef de Projet informatique***
Sauvegarde de la base	*L*				
Archivage informatique	*L*				
Archivage papier		*OUI*			
Définition des droits et habilitations		*LCM et Suppression*			
Gestion des habilitations		*L*		*Consultation*	
Contrôle de la trace technique « qui a accédé à quoi, quand, où ? ».			*Lecture*		
Contrôle trace fonctionnelle « ce qui a été fait sur les fonctionnalités,... ? »		*Lecture*			
Mise à jour système et logiciel système (Win-NT, etc.)	*LCMS*				
Mise à jour programme de l'application					*LCMS*

FONCTIONS ET SERVICES DE SECURITE TRANSACTIONNEL

PROJET : **DATE :**
PHASE :
PROPRIETAIRE D'APPLICATION : **QUESTIONNAIRE**
PROPRIETAIRE DE DONNEES : **OU ADMINISTRATEUR :**

Eléments à risque (cotation >1)	Ressources (transaction, écran, zone,...)	Classification In Cn	Utilisateurs habilités	Mode d'accès autorisé LCMSA	Mesures spécifiques de sécurité (chiffrement, scellement, cartes multi-accès, etc.)

FONCTIONS ET SERVICES DE SECURITE HORS TRANSACTIONNEL

PROJET : **DATE :**
PHASE :

Eléments à risque	Support (papier, disquette,)	Utilisateur habilité	Classification In, Cn	Fonction de sécurité recommandée
				Edition : **Diffusion :** **Sauvegarde :** **Archivage :** **Destruction :**
				Edition : **Diffusion :** **Sauvegarde :** **Archivage :** **Destruction :**
				Edition : **Diffusion** **Sauvegarde :** **Archivage :** **Destruction :**

DEFINITION DES SERVICES DE SECOURS

PROJET : **DATE :**

PHASE :

Liste des éléments à risque (traitements, programmes, procédures, …)	Classification Dn	Indisponibilité maximum acceptable	Description du service - mesures dégradées utilisateurs - normes informatiques acceptées - préparation du contrat de service,…

FONCTIONS DE PREUVE ET CONTROLE

PROJET : **DATE :**

PHASE

Eléments à risque traitements, programmes, procédures	Mode TP	Mode Batch	Classification Pn	Fonctions recommandées de preuve et contrôle
				Auditabilité : Non répudiation :
				Auditabilité : Non répudiation :
				Auditabilité : Non répudiation :
				Auditabilité : Non répudiation :

FONCTIONS ET SERVICES DE SECURITE
JEUX D'ESSAI ET TESTS

PROJET : **DATE :**

PHASE :

Eléments à risque (données d'essai et de tests)	Champ à protéger	Classification Cn	Description des fonctions et services de sécurité à mettre en oeuvre

7. CONCEPTION TECHNIQUE

FICHE D'ANALYSE DE RISQUE
(ARCHITECTURE TECHNIQUE)

PHASE DU PROJET : DATE :

Document d'analyse : Référence du risque : **R . .**
Référence des documents

Elément à risque :

(Objet du système d'information)

Description du risque :

(Accidents, Erreurs, Malveillances)

Conséquences :

(pertes financières, image de marque, manque à gagner, problèmes juridiques, sociaux, surcharge ou sous charge de travail, etc.)

Classification DICP de la gravité du risque	Type de préjudice	Valorisation du risque (charge en moisxHomme ou montant en KF, ou qualitatif)

Mesures techniques de sécurité recommandées:

Phase du projet pour la prise en compte de la mesure	Responsable de la mesure	Coût des mesures de sécurité	Modalités de mise en place	Classification résiduelle de la gravité du risque

MECANISMES LIES AUX HABILITATIONS SGBD

PROJET : DATE :

PHASE :

NOM DU SGBD OU DU FICHIER :

Eléments à risque (champ, enregistrement, vues, etc.)	Classification In Cn Pn	Fonctions habilitées	Modes d'accès autorisé (L,C,M,S,…)	Habilitations spécifiques retenues pour la base de données

MECANISMES DE SAUVEGARDE ET D'ARCHIVAGE DE L'APPLICATION

PROJET : DATE :

PHASE :

Eléments à risque (fichiers, programmes, etc.	Type de sauvegarde (standard, THS, de recours, etc.) [12]	Nombre de version de sauvegarde demandée [13]	Périodicité demandée de prise des sauvegardes	Archivage, durée de conservation demandée	Stockage demandé (sur site , hors site, …).

[12] Typologie des sauvegardes des centres informatiques (CTI1, CTI2, etc..)

[13] Normes des centres informatiques en matière de conservation (CTI1, CTI2, CTI3, etc.)

MECANISMES LIES AU SECOURS DE L'APPLICATION

PROJET : DATE :

PHASE :

Description des actions	Cible retenue pour l'application	Fonction Responsable de la mise en place
Classification de l'application nouvelle : • stratégique D = 4 pas d'interruption supérieure à 15 minutes • critique D = 3 reprise souhaitée sous 4 heures maximum • sensible D = 2 reprise souhaitée sous 4 à 36 heures maximum • faible risque D= 1 reprise souhaitée sous 36 heures à 14 jours		
Solutions de secours retenues pour l'application nouvelle: <u>Non informatique</u> : • plan de reprise d'activité (procédures dégradées utilisateurs, etc.) <u>Informatique</u> : • intégration dans le plan de back-up technique du centre, etc.		
Niveaux de reprise retenus pour l'application nouvelle • dégradé au niveau de l'application (applications prioritaires, etc.) • dégradé au niveau des postes de travail (réduction en nombre, etc.) • dégradé au niveau des informations stockées (accès limité, etc.) • reprise totale		
Précautions spécifiques pour la relance de l'application nouvelle • planning de stabilisation • médias et documents à protéger • participation impérative des utilisateurs pour le contrôle des résultats		

Implication des études informatiques • indispensable compte tenu des risques • non indispensable		
Exercices de secours • validation des résultats de l'application nouvelle par les utilisateurs • contrôles des études informatiques nécessaires • contrôles techniques effectués par l'exploitation suffisants		
Confidentialité et intégrité lors des exercices • conservation du même niveau de contrôle d'accès logique • acceptation d'un niveau de contrôle dégradé sur la période		

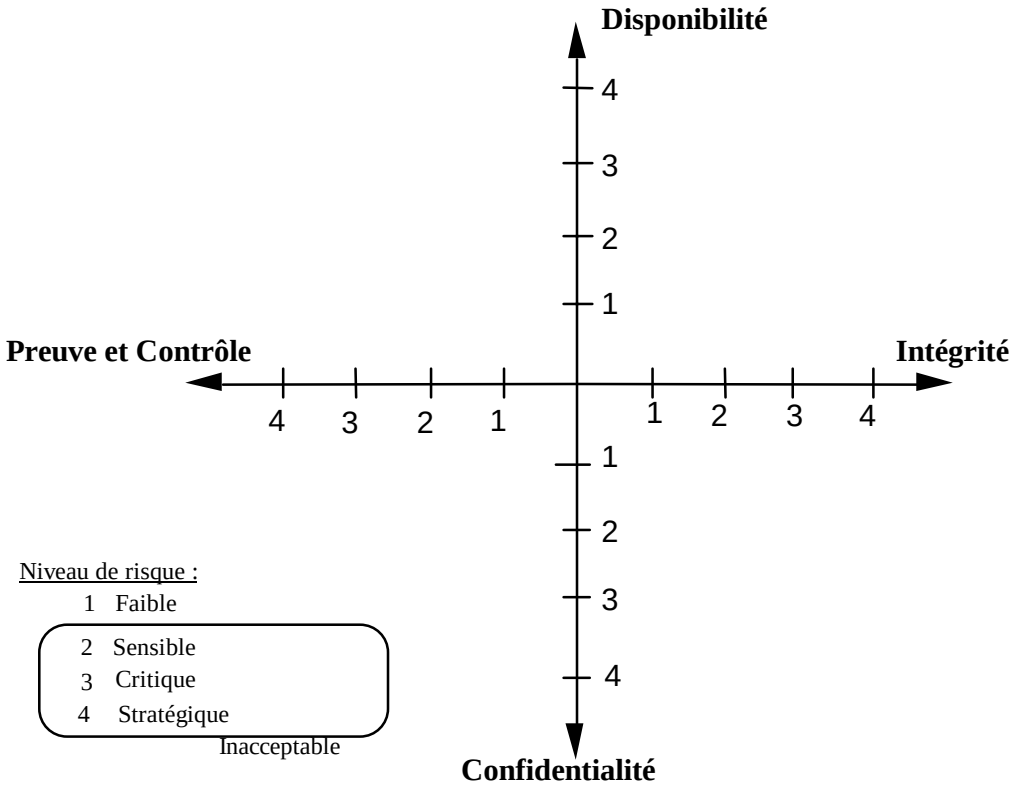
Répondre par oui ou non, dans le cas d'une réponse positive, indiquer la fonction responsable chargé du suivi et de la mise en place des actions.

CIBLE DE SECURITE

PROJET : **DATE :**

PHASE :

	Disponibilité (D)	Intégrité (I)	Confidentialité (C)	Preuve (P)	Appréciation globale
Objectif pour le futur					
Risques avant mise en œuvre des fonctions et mécanismes de sécurité					
Risques après mise en œuvre des fonctions et mécanismes de sécurité					



FICHE DE SUIVI DES MESURES DE SECURITE

PHASE DE CONDUITE DE PROJET : **DATE :**

PROJET :

Description des fonctions et mécanismes de sécurité applicables aux programmes, fichiers, JCL, etc.)	Phase de dévelop-pement concernée	Responsable Utilisateur ou Informatique	Date réalisée	Date recette et validation

Visa du chef de projet utilisateur et informaticien : ……..

Visa du Pôle de compétence sécurité informatique : ……..

Questionnaire spécifique sécurité de la phase Réalisation et Tests

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. Les contrôles programmés sont-ils prévus dans des tables ou programmes indépendants (modules externes aux applications) ?			
2. Dans le cas de données provoquant un problème bloquant, a-t-on prévu le rejet sur une liste d'anomalies afin d'éviter l'arrêt, en production, des chaînes de traitement qui en seraient dépendantes ?			
3. La documentation programme intégrant notamment, les contrôles programmées destinés à assurer l'intégrité de l'information, est-elle protégée, standardisée et régulièrement mise à jour ?			
4. Tous les paragraphes et fonctions de programmes assurant des contrôles programmés liés à la sécurité sont-ils testés (contrôle exhaustif des aiguillages) ?			
5. La règle d'épuration du code mort des programmes est-elle appliquée (codes tests ou codes abandonnés) ?			
6. Conserve-t-on la trace des tests réalisés sur les contrôles programmés liés à la sécurité ?			
7. Réalise-t-on des revues de ces traces ?			
8. Une évaluation réciproque, entre analystes programmeurs, est-elle effectuée tant sur la forme (squelette des programmes, normes, aspects techniques, sécurité) que sur le fond (appréciation des résultats, jeux d'essai de programme, voire d'enchaînement, etc.) ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
9. Les droits d'accès aux applications sont-ils externes aux programmes (exemple : logiciel de sécurité, etc.) ?			
10. Si des programmes sensibles[14] ont été identifiés Indiquez en observation quelles dispositions spécifiques ont été prises pour les protéger (scellement, bibliothèque spécifique, etc.).			
11. Les programmes sensibles sont-ils sauvegardés dans une bibliothèque externe protégée ?			
12. Les normes de sécurité, en terme de préconisation sécurité sur l'emploi des langages ont-elles été suivies (revues qualité du code)15 ?			
13. Dispose-t-on de tableaux croisés contrôle/données qui permettent de vérifier l'adéquation des contrôles programmés par rapport à la classification de la gravité des risques sur les données : stratégiques, critiques, sensibles ?			
14. La cohérence des contrôles programmés est-elle assurée aussi bien dans l'application que vis-à-vis des autres applications ? (les contrôles sur des données sensibles doivent être reproduits dans les autres programmes utilisant ces mêmes données)			
15. En cours de réalisation, l'analyste programmeur reçoit-il encore des demandes de modifications ?			
16. A-t-on défini et fait accepter un plan de test incluant les aspects de sécurité ? Par exemple : • pérennité de la base d'essai (réutilisation) ? • exhaustivité relative de la base d'essai ? • droits et modes d'accès à la base d'essai ? • trace des essais effectués ?			
17. Les analystes programmeurs de la sous-traitance ont-ils connaissance des engagements contractuels liés à la confidentialité des informations qui leur sont communiquées (dossiers d'étude, jeux d'essai, etc.)?			
18. A t-on prévu des cycles de relecture ou de revue du développement (documentation, code,…) ?			

[14] A effectuer en début de phase réalisation
Programmes sensibles : programme accèdant à des données classifiéés sensibles, ou programme représentant d'un savoir faire
[15] Ex : imbrication de boucle : perform ranging, alter to proceed to

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
19. A t-on vérifié la complexité du programme par rapport aux normes de complexité maximum admise ? (un des objectifs est d'éviter la difficulté de maintenance)			
20 .Des procédures de reprises programmées sont - elles prévues pour éviter une perte éventuelle d'information en cas d'interruption, en particulier pour le TP ? (exemple : commit / rollback, etc.)			
21. Ces procédures prennent-elles en compte les contraintes d'exploitation, en particulier dans le cas de programmes temps différé (enchaînement, planning, etc. ?			
22 Les programmes prennent-ils en compte les contrôles de base suivants : • les cadrages (dates, montants à droite, sur la virgule)? • présence de l'information ? • type d'information (numérique, alphabétique, etc.) ? • limite de valeurs (plages, fourchettes) ? • la vraisemblance (exemple : année de naissance < à l'année en cours, ratios, etc.) ? • la cohérence, suivi de l'évolution (bilan) ? • contrôle de validation (balance carrée) • attribution d'indice de gravité des contrôles qui débranche sur des actions (code retour,…)/ - arrêt du traitement, - listes d'erreurs, - modules de contrôle,			
23 A -t-on vérifié que tous les contrôles programmés garantissant l'intégrité des données sont prévus dans les dossiers d'analyse et répercutés dans les programmes ?			
24 En langage objet profite t-on de la possibilité d'encapsulation pour intégrer les règles et contrôles de sécurité dans les objets sensibles ?			
25 A t-on effectué une classification et protection des programmes, fichiers, JCL en cohérence avec les spécifications de sécurité du projet ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
Aspects qualitatif de la sécurité 26. Les programmes sont-ils réalisés en prenant en compte les normes suivantes : Normes de CLARTE, c'est-à-dire : • court ? • logique de programme algorithmique ? • programme structuré ? • déclarations de données et formats de lecture/écriture dans une partie réservée ? • profondeurs des instructions conditionnelles, boucles, activation de modules peu importantes (imbrication < à 3 ou 4)?			
27. Normes de LISIBILITE et MAINTENABILITE, c'est-à-dire : des commentaires sont-ils placés en tête de chaque partie importante de programme ? l'écriture des programmes comporte-t-elle : une seule instruction par ligne ? des marges normalisées (indentation) ? une présentation en escalier des instructions de déclaration des variables ? des noms mnémoniques et des normes pour les étiquettes ? des normes et standard de présentation des programmes ?			
28. Normes d'OPTIMISATION, c'est-à-dire : peu important en mémoire ? rapide en temps d'exécution ? temps de réponse optimum ? sans instructions inutiles ou périmées ? sans redondances de séquences d'instruction (notions de sous-programme) ? - éviter l'usage d'instruction déconseillée ?			
29 Utilise t-on des outils automatisés de contrôle de la bonne écriture et optimisation du code (Exemple : LOGISCOPE, etc.) ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
30. Le dossier de programme est-il complet, exhaustif, et rédigé au plus tard dès la fin de la phase de réalisation ?			
31. A t-on prévu à chaque nouvelle version la conservation de la trace de toute modification de versions de programmes (gestion de configuration, historisation des versions, etc.) ?			

TESTS

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. A t-on vérifié que toutes les mesures de sécurité retenues sur les fiches de suivi sont incluses dans les tests ?			
2. La sécurité logique a t-elle été testée (habilitations, menus sécurisés, profils particuliers, restriction des accès à des champs ou enregistrement de bases de données, etc.) ?			
3. A t-on vérifié que les tests de sécurité TP et Batch sont conformes aux exigences de sécurité prévues dans le plan de test (reprises sur incident, modules de contrôleur.) ?			
4. Les résultats des tests de sécurité sont-ils matérialisés dans la documentation (traçabilité et auditabilité possible) ?			
5. Les exigences de sécurité des tests ont-elles été définies : disponibilité de la plate-forme de tests ? récupération des données, sauvegardes ? confidentialité des données utilisées pour les tests ? trace et conservation des jeux d'essai ?			
6. A t-on testé la procédure de séparation des pouvoirs propriétaire, administrateur fonctionnel et technique ? (exemple : accès au mot de passe des administrateurs, suivi et contrôle des interventions sur les niveaux d'habilitations, etc.) ?			
7. A t-on testé que les données sensibles, sont mises en relief (surbrillance, encadrement, confirmation, etc.) pour attirer l'attention sur l'importance de l'exactitude à la saisie ?			
8. A t-on testé la règle de dévalidation automatique (retour à la mire d'accueil) après un laps de temps prédéfini d'inactivité du poste de travail ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
9. A t-on prévu les tests suivants : tests unitaires - normes de programmation, traitement des erreurs, ...? tests d'intégration avec les interfaces applicatifs ? tests d'homologation sur la documentation, les aides en ligne, ergonomie,...? tests de non-régression tant pour les fonctionnalités que les performances (en cas de migration ou maintenance prévisible) ? tests statiques : revue de code, ...? tests dynamiques : suivi pas à pas du déroulement des instructions, ...? tests d'exécution aveugle de modules pour suivre le comportement extérieur,...?			
10. A t-on matérialisé dans le dossier de tests les résultats des tests de sécurité, Exemple : reprise sur atteinte à l'intégrité des données ? secours et reprise sur une indisponibilité prolongée ? robustesse face à la malveillance ?			
11. A t-on testé que tous les accès aux programmes comportant de la sécurité (exemple programmes d'administration des profils, contrôles programmés de limites de valeurs, etc.) génère une preuve qui permet d'identifier les acteurs (horodatage, terminal, etc.) ?			

RECETTES

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. Le propriétaire (utilisateur) a t-il donné les règles et instructions concernant les droits et habilitations à mettre en œuvre par le gestionnaire ou administrateur ?			
2. En matière d'intégrité et de confidentialité • le GLS a t-il préparé la mise en place des autorisations d'accès aux transactions, données et programmes sensibles ? • les utilisateurs ont-ils préparé la mise en place de la sécurité sur les autres supports (papier,disquette, etc.) ?			
3. En matière de disponibilité, a-t-on, précisé dans le manuel des procédures, la mise en œuvre des procédures dégradées (qui, quoi, quand, comment, où) ?			
4. A-t-on spécifié dans le manuel utilisateur les responsabilités en matière de sauvegarde et d'archivage des données et programmes sensibles (postes de travail, serveur, …) ?			
5. A-t-on préparé la mise à jour du plan de secours pour les spécificités de sécurité propres au nouveau projet (durée maximum d'indisponibilité acceptable, reprise à chaud, etc.) ?			
6. A-t-on préparé la mise en œuvre des mesures complémentaires de sécurité en matière de constitution de jeux d'essai (modification des champs confidentiels de la base d'essai, pérennité de la base d'essai, etc.) ?			
7. A-t-on préparé la formation relative aux exigences de sécurité à respecter sur le nouveau projet ? (information des utilisateurs et des exploitants) • l'environnement technique de formation est-il préparé ? • la documentation est-elle prête ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
• les règles spécifiques de sécurité en matière de contrôles non informatiques sont-elles préparées (contrôle à la saisie, contrôle par bilan de sortie de traitement, contrôle par écran, etc.) ?			
8. A-t-on décrit dans le manuel utilisateur les mesures de sécurité liées à l'organisation (séparation des pouvoirs, vérification et audit, partage des tâches, etc.) ?			
9. Est-ce que la préparation des locaux et des matériels nécessitant la mise en place d'organisation et d'outils de sécurité est prête ?			
10. le contrat de service est-il préparé et les engagements de sécurité clairement formulés en terme disponibilité, intégrité, confidentialité, preuve et contrôle ?			
11. Si des copies de fichiers de production sont nécessaires pour la constitution des jeux d'essai, le propriétaire a t-il donné les autorisations d'obtention en tenant compte des exigences de sécurité ?			

INSTALLATION

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. Le dossier de recette contient-il les résultats de tests liés à la sécurité : • tests d'accès illicités à l'information en modification, ou en copie ? • tests de plantage et reprise à chaud ? • examen de la lisibilité des traces par un non informaticien ? • accès aux transactions utilisateurs interdit à la fonction d'administration du serveur ? • trace systématique de toutes les actions effectuées par l'administration ?			
2. Le propriétaire a-t-il donné son aval sécurité pour : • les outils de contrôle et de suivi du bon fonctionnement de l'application ? • l'organisation du contrôle (qui, quoi, comment) ?			
3. Est-ce que les règles de gestion (paramétrage Win-NT) retenues pour les droits d'accès ont fait l'objet de la recette : • couple identifiant/authentifiant unique et propre à chaque utilisateur ? • mot de passe non trivial ? • remise à jour périodique de la table des droits d'accès ? • alarme signalant une opération réalisée sous la contrainte, par l'exécution d'une transaction fictive dédiée ? • stockage et circulation sur les lignes, des mots de passe, sous forme chiffrée ? • changement, au moins tous les 2 mois, des mots de passe ? • dévalidation automatique en cas de non utilisation d'un terminal ou après un certain nombre d'essais de connexion infructueux ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
4. La validité de la granularité des droits d'accès a t-elle fait l'objet d'une recette, notamment, en architecture client serveur et en environnement de partage réseau (Microsoft, Netware, etc.)?			
5. A t-on fait la recette des paramétrages de sécurité suivants : • le compte d'administrateur Win-NT est-il verrouillé ? • le mot de passe de l'administrateur est – il particulièrement robuste ? • toutes les connexions de compte d'administration à partir du réseau sont- elles interdites, voire très limitées ? • l'administration du serveur est-elle possible uniquement à partir de la console du serveur ? • le mot de passe de secours est-il réparti entre au moins deux ou trois individus ? • les comptes invités sont-ils systématiquement désactivés ? • les connexions avec Internet, si elles existent sont sous surveillance 24H sur 24 ? • etc.			
6. La recette sécurité permet-elle de confirmer les critères de sécurité prévus dans le contrat de service (production/utilisateurs) ?			
7. Si des modifications sur les mesures de sécurité ont été effectuées en recette la fiche de suivi a t-elle été mise à jour ?			
8. Les résultats de recette incluant les aspects de sécurité sont-ils archivés ?			
9. A-t-on fait la recette de la cohérence sécurité des interfaces avec les autres applications ?			
10. Pour les tests de sécurité touchant à la malveillance (mascarade, débranchement inactif dans un programme, etc) la robustesse de la sécurité a t-elle fait l'objet de la recette ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
11. A t-on vérifié que l'indisponibilité d'un composant technique de l'installation n'arrête pas le fonctionnement des services utilisateurs sur une durée jugée inacceptable ?			
12. A t-on fait la recette des procédures de secours **immatériels** (exemple : incident grave de programmes pendant les congés ou maladies, etc.) ?			
13. A t-on vérifié pour les envois et réception entre établissements de fichiers classifiés sensibles qu'ils sont difficilement « violables ou détournables » ? à l'envoi ? pendant le transport ? à la réception ?			
14. A t-on vérifié l'impossibilité de ressaisir le même mot de passe plusieurs fois de suite ?			
15. A t-on vérifié l'impossibilité de se connecter après un nombre d'essai infructueux du mot de passe? (en général après trois essais) ?			
16. A t-on vérifié la procédure d'initiation d'un nouveau mot de passe en cas d'oubli : - obligation pour l'utilisateur d'en changer à la 1ère connexion et dès l'initiation ?			
17. A t-on vérifié la bonne utilisation des mots de passe par le personnel : • jamais écrit ? • pas de touches claviers programmés ? • etc.			
18. A t-on vérifié qu'une trace est disponible en cas de modification d'information ou de dossiers sensibles ? (exemple : suppression de contentieux, etc.) ?			

DEMARRAGE

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. Les transferts d'information s'effectuent-ils en accord avec les dispositions de sécurité prévues : • transferts informatiques (bandes, disquettes, etc.) ? • télécommunications ? • transferts administratifs (documents papier, micro-fiches, etc.) ?			
2. Le comportement des programmes, est-il rigoureusement identique en environnement de test et de production, en particulier les dispositifs ayant trait à la sécurité ?			
3. Les mesures de sécurité liées à la télémaintenance, soit dans le cadre éventuel de logiciels, soit dans le cadre des matériels sont-elles opérationnelles ?			
4. Pour le fonctionnement dégradé, les consignes utilisateurs sont-elles opérationnelles, par exemple : • reprise d'activité manuelle ? • conservation de la trace des mouvements ? • etc.			
5. Le contrat de service est-il validé (signature) et sa période de révision actée ?			
6. Le GLS dispose-t-il de toutes les justifications et autorisations d'accès validées ?			
7. Dispose-t-on d'un plan de démarrage : • méthode d'installation (graduelle, totale, en parallèle, etc.) ? • possibilité de retour à l'ancienne version ? • moyens humains (représentants utilisateurs, chef de projet, exploitation, réseau, système, analyste, etc.) ? • contraintes organisationnelles (temps, période de pointe, limitation de la durée du parallélisme) ?			
8. Les plans de sécurité ont-ils été actualisés : • plan de secours ? • plan de sauvegarde ? • plan de reprise ?			

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
• sauvegarde de 1er niveau (pour reprise sur le site) ? • sauvegarde de 2ème niveau (pour backup externe) ? • sauvegarde de 3ème niveau (THS) ? • sauvegarde de la documentation ? • transferts sécurisés ? • sécurité des locaux de télécommunication (autocommutateurs, concentrateurs, serveurs, têtes de ligne) etc.) ?			
9. A t-on les moyens de vérifier le niveau de service prévu dans le contrat de service ? • performances (temps de réponse) • continuité de service (respect des délais de livraison, secours, modes dégradés réseau, informatique, organisationnel, etc.) • qualité des résultats fournis (intégrité des informations, exactitude, etc.) • respect de la confidentialité (surveillance des lignes contre les écoutes, non divulgation d'information confidentielles avant terme, etc.) • preuve et contrôle (possibilité d'audit des situations ambigües)			

EVALUATION

PROJET : DATE :

Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
1. D,I,C : L'utilisateur est-il satisfait de la documentation sécurité qu'il utilise (compréhension, exhaustivité des réponses aux cas rencontrés, utilité, etc.) ?			
2. D,I,C : Un suivi précis des incidents (A,E,M) (2) liés à la sécurité est-il effectué et archivé (date de l'incident, date de résolution, intervenant, etc.) ?			
3. I,C ,P : Les procédures de sécurité fondées sur les doubles signatures, l'archivage et la classification des documents, disquettes, etc. sont-elles opérationnelles et appliquées ?			
4. D,I,C : Les modifications urgentes touchant la sécurité, faites au cours de la période de démarrage ont-elles été ajoutées à la documentation et soumises à la validation des utilisateurs et des pôles de compétences sécurité concernés ?			
5. D : Dans le cadre du plan de secours, a-t-on défini, en consensus avec les utilisateurs, les critères qui permettent de conclure à un succès de l'exercice du backup, hors du domaine technique ?			
6 D : L'information et la représentation des fonctions concernées par les exercices de secours de l'application est-elle prévue et la forme définie ?			
7. I,C : La procédure de vérification des modules objets et sources est-elle en application sur les programmes sensibles ?			

(1)A effectuer pendant la phase évaluation

(2) Accident, Erreur, Malveillance

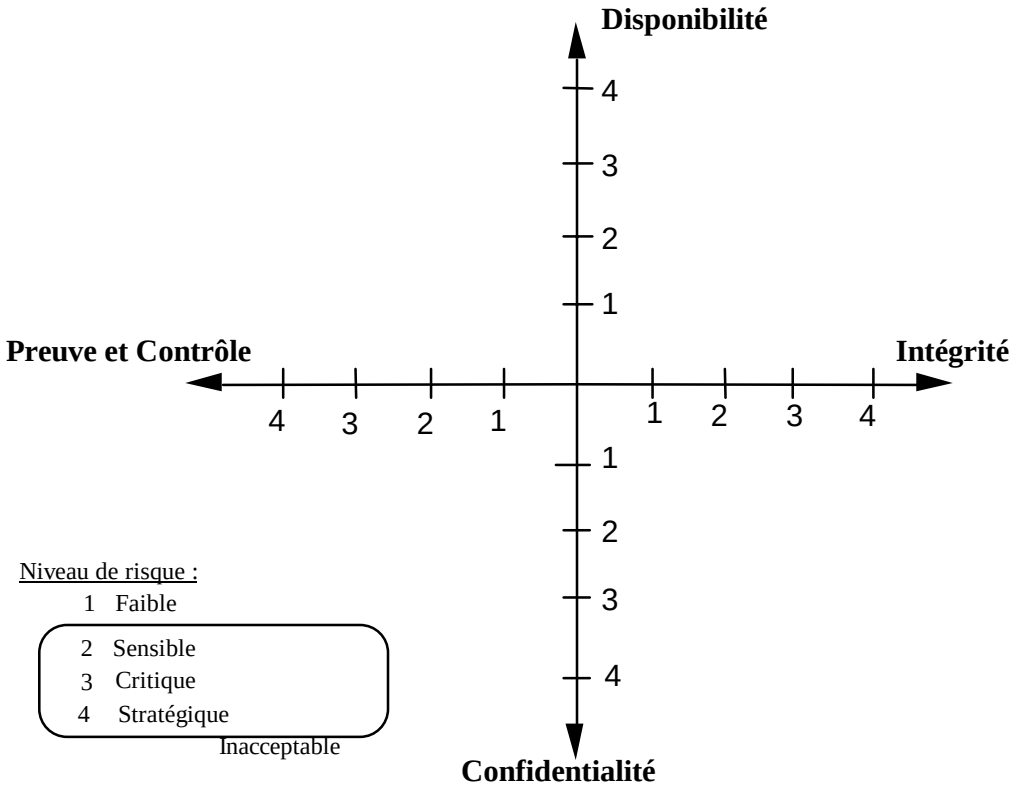
Aspect de sécurité à traiter	*Oui*	*Non*	*Observations*
8. P : Les journaux d'exploitation sont-ils archivés pour répondre aux besoins de contrôle sécurité ?			
9. I,P : Dispose-t-on de tableaux de bord de suivi sécurité pour l'application (accidents et incidents, erreurs, malveillances) ?			
10. P : Un systèmes de type audit-trail (système de pistage intégré) est-il opérationnel ? • prélèvements de données ? • édition d'états ? • mise à jour de fichiers d'audit ?			
11. D,I,C,P : La procédure d'intervention à chaud est-elle définie et opérationnelle ?			
12. D,P : Les réunions de qualification du contrat de service sont-elles planifiées ?			
13. I,C : Les mots de passe sont-ils conformes dans leur utilisation aux prescriptions de sécurité ?			
14. DICP :L'actualisation de la cible de sécurité a t-elle été réalisée et les résultats commentés et diffusés au Responsable Sécurité Informatique ?			

CIBLE DE SECURITE

PROJET : **DATE :**

PHASE :

	Disponibilité (D)	Intégrité (I)	Confidentialité (C)	Preuve (P)	Appréciation globale
Gravité du risque avant mise en œuvre des mesures INCAS					
Gravité du risque après la phase d'évaluation					



FICHE DE SUIVI DES MESURES DE SECURITE

PHASE DE PROJET : **DATE :**

PROJET :

Description des mesures restant à mettre en œuvre pour atteindre la cible de sécurité visée	Phase de maintenance concernée	Responsable Utilisateur ou Informatique	Date de réalisation prévue	Date de validation

Visa du chef de projet utilisateur et informaticien : ……..

Visa du Pôle de compétence sécurité informatique : ……..