|  |
| --- |
| MODE D’EMPLOI  Ce questionnaire est destiné à aider le commissaire aux comptes à la fois à prendre connaissance des spécificités du système informatique de l’entreprise et à évaluer les risques qui lui sont attachés.  Il est adapté aux systèmes simples, mais peut être, si certains points le justifient, complété grâce au questionnaire « système complexe ».  Le choix entre ces deux questionnaires dépend de la connaissance préalable du commissaire aux comptes de l’organisation informatique de l’entreprise.  Des feuilles de travail ont été également développées pour aider à la description de l’organisation informatique des PME.  L’évaluation des risques sera reportée sur le tableau récapitulatif des risques.  Ce questionnaire comporte 5 parties :   * traitements informatisés des cycles * fonction informatique * matériel * logiciels * dispositions légales et réglementaires |

1. TRAITEMENTS AUTOMATISES DES CYCLES

Pour chaque application, évaluer le degré de complexité en fonction du degré d’informatisation des tâches.

Pour chaque application, le risque sera gradué en fonction de :

* l’existence d’une documentation utilisateur plus ou moins importante,
* la facilité apparente de suivre le chemin de révision (flux, annulations, centralisations) en préservant la sécurité des informations,
* des délais de validation.

**Complexité**

**Achat ${Value1}**

**Vente ${Value2}**

**Trésorerie ${Value3}**

**Comptabilité ${Value4}**

**Paie ${Value5}**

**Stock ${Value6}**

|  |  |
| --- | --- |
| **CONCLUSIONS :**  ${CSA} | **NIVEAU DE RISQUE**  ${RSA} . |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **II. FONCTION INFORMATIQUE** | **Description (ou réf. feuille de travail)** | | | |  | | | |
| **Prise de connaissance** |
|  |  |  |  |  | |  |  |
| PERSONNEL INFORMATIQUE |  |  |  |  | |  |  |
| - Effectif, |  |  |  |  | |  |  |  | | |
| - Degré de formation, |  |  |  |  | |  |  |
| - Coût (le tableau « Budget » peut être utilisé) |  |  |  |  | |  |  |  | | |
| - Une solution simple consiste à analyser le dernier exercice clos |  |  |  |  | |  |  |  | | |
|  |  |  |  |  | |  | | | |
| **ANALYSE DES RISQUES** |  |  |  |  | |
|  | **Oui/Non** | **Risques** | | | |
| 1. La direction générale exerce-t-elle un contrôle sur le service informatique : |  |  | | | |
| - Contrôle renforcé ? | ${B1} | ${RB1} | | | |
| - Contrôle des objectifs ? | ${B2} | ${RB2} | | | |
| Est-elle impliquée dans les décisions informatiques ? | ${B3} | ${RB3} | | | |
| 2. Tous les services utilisateurs sont-ils consultés pour les décisions informatiques qui les concernent ? | ${B4} | ${RB4} | | | |
| 3. La conception interne est-elle :   * intégrale ? * partielle ? * inexistante ?   La conception externe est-elle :   * intégrale ? * partielle ? * inexistante ?   4. L’exploitation interne est-elle :   * intégrale ? * partielle ? * inexistante ?   L’exploitation externe est-elle :   * intégrale ? * partielle ? * inexistante ? | ${B5}  ${B6}  ${B7}  ${B8}  ${B9}  ${B10}  ${B11}  ${B12}  ${B13}  ${B14}  ${B15}  ${B16} | ${RB5}  ${RB6}  ${RB7}  ${RB8}  ${RB9}  ${RB10}  ${RB11}  ${RB12}  ${RB13}  ${RB14}  ${RB15}  ${RB16} | | | |

|  |  |  |
| --- | --- | --- |
| **COMMENTAIRES :**  ${CSB} | **NIVEAU DE RISQUE**  **${RSB}** . | **SCORE**  **${SSB}** |

|  |  |  |  |
| --- | --- | --- | --- |
| **III. MATERIEL** |  |  |  |
|  | **Oui/Non** | **Risques** | |
| **ANALYSE DES RISQUES** |  |  | |
| **1.** Les capacités sont-elles suffisantes ?  2. Les sauvegardes sont-elles exploitables et sûres :   * Les informations sont-elles sauvegardées intégralement ? * Des essais de restauration ont-ils été réalisés récemment ? * S’est-on assuré qu’aucune perte d’informations n’est intervenue ? * La périodicité des sauvegardes est-elle satisfaisante ?   Existe-t-il une conservation hors site des sauvegardes ?  3. Maintenance du matériel :  - Les charges d’entretien sont-elles bien définies ?  - Le délai d’intervention est-il convenable ?  - Les procédures de dépannage sont-elles prévues ?  4. Assurances :  - Assurance Bris de machine spécifique ?  - Assurance Protection des logiciels ?  - Assurance Perte d’exploitation ?  5. Sécurités  - Dégât des eaux ?  - Vol ?  - Accès aux locaux informatiques ? | ${C1}  ${C2}  ${C3}  ${C4}  ${C5}  ${C6}  ${C7}  ${C8}  ${C9}  ${C10}  ${C11}  ${C12}  ${C13}  ${C14}  ${C15} | ${RC1}  ${RC2}  ${RC3}  ${RC4}  ${RC5}  ${RC6}  ${RC7}  ${RC8}  ${RC9}  ${RC10}  ${RC11}  ${RC12}  ${RC13}  ${RC14}  ${RC15} | |

|  |  |  |
| --- | --- | --- |
| **COMMENTAIRES :**  ${CSC} | **NIVEAU DE RISQUE**  **${RSC}** . | **SCORE**  **${SSC}** |

|  |  |  |  |
| --- | --- | --- | --- |
| **IV. LOGICIELS** |  |  |  |
|  | **Oui/Non** | **Risque** |
| **ANALYSE DES RISQUES** |  |  |
| 1. Organisation et structure :  - La séparation des fonctions est-elle adaptée au système ?  - Les phases de développement et d’exploitation sont-elles bien définies ?  Modification de logiciels :  - Les modifications par les utilisateurs sont-elles nombreuses ?  - Les modifications par les SSII sont-elles nombreuses ?  - La phase de modification est-elle bien définie ?  2. Maintenance (voir le contrat) :  - L’assistance est-elle bien définie ?  - Les mises à jour sont-elles prévues ?  - Les mises à niveau sont-elles régulières ?  - Les délais d’intervention sont-ils corrects ?  3. Formation sur les logiciels d’exploitation :  - Faite par stage ?  - Formation autodidacte correcte ?  Formation sur les logiciels systèmes et leur utilisation :  - Faite par stage ?  - Formation autodidacte correcte ?  4. Existence de procédures écrites  Existence d’une documentation relative :  - Aux analyses ?  - A la programmation ?  - A l’exécution des traitements ?  5. Les mesures liées à la sécurité logique (codes ou mot de passe) sont-elles :  - bien définies ?  - Régulièrement mises à jour ? | ${D1}  ${D2}  ${D3}  ${D4}  ${D5}  ${D6}  ${D7}  ${D8}  ${D9}  ${D10}  ${D11}  ${D12}  ${D13}  ${D14}  ${D15}  ${D16}  ${D17}  ${D18} | ${RD1}  ${RD2}  ${RD3}  ${RD4}  ${RD5}  ${RD6}  ${RD7}  ${RD8}  ${RD9}  ${RD10}  ${RD11}  ${RD12}  ${RD13}  ${RD14}  ${RD15}  ${RD16}  ${RD17}  ${RD18} |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **COMMENTAIRES :**  ${CSD} | **NIVEAU DE RISQUE**  **${RSD}** . | **SCORE**  **${SSD}** |

|  |  |  |  |
| --- | --- | --- | --- |
| **RESUME DE LA REVUE DU SYSTEME DE CONTROLE INTERNE**  **SYSTEME D’INORMATIONS – FC9** | | | |
|  | SCORE | RISQUE | COMMENTAIRES |
| **I** | ${SSA} | ${RSA} | ${CSA} |
| **II** | ${SSB} | ${RSB} | ${CSB} |
| **III** | ${SSC} | ${RSC} | ${CSC} |
| **IV** | ${SSD} | ${RSD} | ${CSD} |

|  |  |
| --- | --- |
| **SYNTHESE**  ${SYNTH} | **RISQUE**  ${SCORE} |