UA2401
Rapport pour l'obtention du
Certificat de spécialisation
"Maîtrise de l'archivage à l'ère numérique"

Elaboré par Marjorie CARIOU
20 juin 2016

Criticité des documents :
Ecart entre perception et évaluation.
Apport de la norme ISO 18128:2014[1]
Cas du Crips[2] Ile-de-France

Jury : Michel Cottin

[1] Norme *ISO 18128 : 2014 - Évaluation du risque pour les processus et systèmes d'enregistrement*
[2] CRIPS : Centre Régional d'Information et de Prévention du Sida

Maitriser les risques liés à la gestion des documents est un enjeu fort pour les organismes privés et publics. Ce rapport tente, à l'aide de l'évaluation définie par la norme ISO 18128 : 2014[3], de mesurer l'écart entre la perception d'un risque lié aux documents et le risque encouru par un organisme.
Les différentes étapes pour évaluer ces risques structurent ce rapport. Il fournit par ailleurs une terminologie des concepts utilisés. Enfin, toutes les références des documents consultés sont disponibles à la fin du présent document.

SOMMAIRE

[3] Norme *ISO 18128 : 2014 - Évaluation du risque pour les processus et systèmes d'enregistrement*

I. Contexte

L'organisme, utilisé pour exemple, est le Centre régional d'information et de prévention du sida (CRIPS). Son objectif est la prévention des comportements à risques dans le domaine de la vie affective et sexuelle (VIH/sida, IST, hépatites), des addictions, des inégalités et injustices liées aux singularités (lutte contre le sexisme, l'homophobie, la sérophobie). L'équipe du Crips intervient sur l'ensemble du territoire francilien dans les lycées et CFA, les structures accueillant des publics en situation de vulnérabilité (migrants, personnes en situation de handicap, milieu carcéral, LGBT…). Il met à disposition des acteurs de prévention, un espace d'information et de prévention (Pôle infodoc), un espace d'écoute d'information, d'orientation et d'animation (Cybercrips) et une unité mobile de prévention (BIP).

Contexte interne à l'organisme

Structure de l'organisme *:*

Organisme associé au conseil régional Ile-de-France, créé en novembre 1988, le Crips s'appuie sur une organisation associative décisionnelle via le Bureau, le Conseil d'administration et l'Assemblée générale [Statuts du Crips Ile-de-France]

Le conseil d'administration est composé de 21 membres, dont des représentants de l'Etat, de la région Ile-de-France, de la ville de Paris, des personnalités scientifiques désignées par l'Etat, la région et la mairie et enfin des membres élus par les adhérents. Le CA élit parmi ses membres un président, trois vice-présidents, un secrétaire et un trésorier qui forment le bureau pour trois ans. Le directeur est nommé par le président.

Finances de l'organisme *:*

Budget : 4 427 456 € (2014)

94% de financements publics et 4 % de recettes propres

La Région d'Île-de-France assure à elle seule 80 % des ressources de l'association.

L'État, par l'intermédiaire de l'ARS et le DGS, contribue au financement à hauteur de 12 % et la Ville de Paris à 2 %

Ressources humaines *:*

53 salariés (dont 43 ETP)

Public *:*

Professionnels des secteurs éducatif, sanitaire et social, association de lutte et de prévention du sida, des hépatites et des conduites à risque.

Fonctions opérationnelles *:*

Prévention, documentation, formation, communication/évènementiel

Fonctions administratives *:*

Administration, finance, Ressources Humaines

Fonctions supports *:*

Diffusion, informatique, maintenance matériel et locaux

Contexte externe à l'organisme

Les exigences règlementaires en vigueur dans la juridiction de l'organisme

– *Le Crips, en tant qu'association loi 1901*

Elle reçoit annuellement une ou plusieurs subventions dont le montant global dépasse 153 000 euros. Elle a obligation d'établir des comptes annuels comprenant un **bilan comptable**, un **compte de résultat** et une **annexe** (comptabilité d'engagement) et faire certifier ces comptes par un commissaire aux comptes. [Source : code du commerce - article L 612-4]

Par ailleurs, selon le règlement n° 99-01 adopté le 16 février 1999 par le Comité de la réglementation comptable « relatif aux modalités d'établissement des comptes annuels des associations et fondations », le Crips a l'obligation de tenir un **livre journal** dans lequel les écritures sont comptabilisées chronologiquement et jour par jour, et éventuellement plusieurs livres-journaux auxiliaires, un **grand livre** constitué par les comptes de l'association dans lesquels sont reportés les écritures des journaux.

[Source : http://associations.gouv.fr/704-comment-compter.html]

– *Le Crips, en tant qu'organisme de formation*

Selon le code du travail[4], il doit établir un **bilan pédagogique et financier (BPF)** retraçant son activité de l'année précédente avant le 30 avril de chaque année. Il l'adresse à la Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (Direccte). Le Crips doit en conserver une copie. Le **bilan comptable**, le **compte de résultat** et **l'annexe du dernier exercice clos** doivent être joints.

Les sanctions administratives pour défaut de présentation du bilan pédagogique et financier sont la caducité de la déclaration d'activité et l'absence de diffusion de l'identité du prestataire sur la liste publique des organismes de formation.

De plus, le défaut de production du bilan pédagogique et financier constitue une infraction pénale et peut être puni d'une amende de 4 500€ et à titre complémentaire, d'une interdiction d'exercer temporairement ou définitivement l'activité de dirigeant d'organisme de formation. [Source : Direction de l'information légale et administrative]

La durée de conservation des documents administratifs, comptables ou commerciaux peut être différente du « délai de reprise », c'est-à-dire de la période sur laquelle l'Administration peut contrôler l'organisme. Ainsi, si le registre du personnel ou les fiches de paie doivent être conservés pendant au moins 5 ans, il doit garder les bilans, comptes de résultats et annexes, livres et registres comptables pendant au moins 10 ans à compter de la clôture de l'exercice. [Source : AGEFOS PME - Guide des organismes de formation - Edition 2015]

– *Le Crips, en tant que producteur de support de prévention,*

Il a l'obligation de dépôt légal à l'un des organismes dépositaires.

[Source : code du patrimoine]

[4] Code du travail : article L6352-11
https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006189924&cidTexte=LEGITEXT000006072050
Code du travail : articles R6352-22 à R6352-24
https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000018522310&cidTexte=LEGITEXT000006072050

– *Le Crips, en tant que centre de ressources,*

Il a l'obligation de respecter le droit d'auteur. Toutefois l'auteur ne dispose pas d'une universalité de droits sur l'exploitation de son œuvre. En effet, l'article L 122-5 CPI prévoit des exceptions selon lesquelles l'exploitation d'une œuvre protégée peut encore être effectuée : analyses et courtes citations, revues de presse, diffusion à titre d'information d'actualité, base de données électroniques, etc. [Source : code de la propriété intellectuelle]

– *Le Crips, en tant que responsable de traitement[5] informatique de données personnelles[6],*

Il a notamment l'obligation de s'assurer que toutes les précautions sont prises pour empêcher que les données, dès la conception des produits, services et systèmes les exploitant, ne soient déformées ou communiquées à des personnes non autorisées. Il a obligation de documentation : un **registre** détaillé des traitements de données personnelles doit être conservé à la fois par le responsable[7] de traitement et les sous-traitants (« *data processors* ») et doit pouvoir être mis à la disposition des autorités de contrôle.

[Source : Règlement général sur la protection des données (RGPD). Echéance mai 2018]

Données du RUP : les mentions portées sur le registre unique du personnel doivent être conservées pendant 5 ans à partir du départ du salarié ou du stagiaire de l'établissement.

Données du RUP :

Les parties prenantes extérieures à l'organisme qui ont un intérêt particulier dans les opérations de l'organisme.

– *Région Ile-de-France*

Convention établie tous les 3 ans, par tacite reconduction. Produire un reporting semestriel.

Audit commandé par la région tous les 4 ans. Les aspects administratifs (statuts et procès verbaux, etc.), ressources-humaines (salaires, dossier recrutement, etc.) et financiers (cohérence entre budget et l'exécuté) sont étudiés à l'appui des documents.

– *Agence régionale de santé*

Convention annuelle contractualisée suite à appel à projet. Bilan pédagogique et financier à produire chaque année.

– *Mairie de Paris*

Convention annuelle contractualisée suite à appel à projet. Bilan pédagogique et financier à produire chaque année.

– *Rectorats (Académie Ile-de-France)*

Agréments accordés pour 5 ans. Fournir les documents suivants : listing des établissements où le Crips est intervenu, nombre des interventions par thématiques réalisées, rapports d'activité sur les trois dernières années, bilans financiers et enfin un argumentaire pour renouveler l'agrément.

---

[5] Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction [Source : CNIL]

[6] Donnée personnelle : Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale…). [Source : CNIL]

[7] Le responsable d'un traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal. [Source : CNIL]

– *Agence du service civique (Ministère de la jeunesse et du sport)*

Agrément accordé pour 2 ans. Fournir les documents suivants : rapports d'activité sur les trois dernières années, bilans financiers et enfin un argumentaire pour renouveler l'agrément. Publication des offres de missions sur l'espace réservé sur le site de l'agence et obligation de répondre à toutes les candidatures proposées. [Source : Loi n° 2010-241 du 10 mars 2010]

– *IGAS – Inspection Générale des Affaires Sociales*

Peut commander un audit si notamment l'association est en difficulté.

Les facteurs politiques

En 2015, la région Ile-de-France a changé de majorité politique. Le nouveau président, conseiller régional, a pris ses fonctions en 2016. Un-e directeur-rice est en phase de recrutement. C'est le cinquième changement de direction en quatre ans.

Les facteurs économiques

Les dernières quatre années, une baisse de budget de 150 000 € oblige à faire des économies. Les budgets pour fonctionnement et le recrutement de personnel sont ciblés.

II. Terminologie

Système documentaire : système d'information qui intègre, organise, gère et rend accessibles les documents d'activité dans le temps. Ceci peut inclure les applications métiers ou les systèmes qui créent et préservent les documents d'activité. [Source : norme ISO 30301 :2011 / SGDA – Principes et vocabulaire]

Processus : une ou plusieurs séquences d'activités requises pour produire un résultat qui respecte des règles de gouvernance. [Source : norme ISO 26122: 2014 / Information et documentation — Analyse des processus pour la gestion des informations et documents d'activité]

Processus documentaire : ensemble d'activités permettant à un organisme de créer, maîtriser, utiliser, conserver et éliminer des documents d'activité. [Source : norme ISO 18128 :2014 / Information et documentation —Évaluation du risque pour les processus et systèmes d'enregistrement]

Authenticité **:** Un document d'activité authentique est un document dont on peut prouver

- qu'il est bien ce qu'il prétend être
- qu'il a été créé ou envoyé par l'acteur qui prétend l'avoir créé ou envoyé
- qu'il a été créé ou envoyé au moment prétendu.

Fiabilité **:** Un document d'activité fiable est un document

- dont le contenu peut être considéré comme la représentation complète et exacte des opérations, activités ou faits qu'il atteste
- sur lequel on peut s'appuyer lors d'opérations ou d'activités ultérieures.

Intégrité **:** l'intégrité d'un document d'activité renvoie au caractère complet et non altéré de son état. [Source : norme ISO 15489 :2016 / Information et documentation — Records management — Partie 1: Concepts et principes]

Risque : effet de l'incertitude

- un effet est un écart, positif et/ou négatif, par rapport à une attente
- l'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance
- un risque est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux.
- un risque est souvent exprimé en termes de combinaison des conséquences d'un évènement (incluant des changements de circonstances) et de sa vraisemblance.

[Source : Guide ISO 73 :2009 / Management du risque — Vocabulaire]

Perception du risque : point de vue d'une partie prenante concernant un risque. La perception du risque reflète les besoins, les questions, les connaissances, les convictions et les valeurs de la partie prenante.

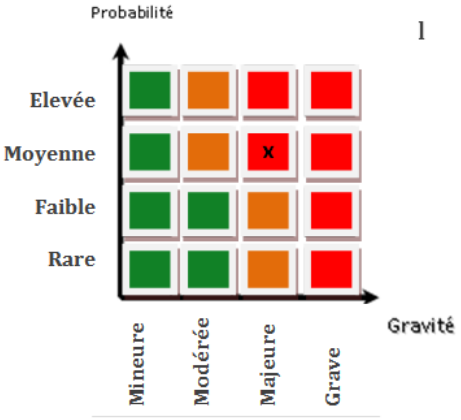
Description du risque : représentation structurée du risque contenant généralement quatre éléments : les sources, les événements (3.5.1.3), les causes et conséquences.

[Source : norme ISO 18128 :2014 / Information et documentation — Évaluation du risque pour les processus et systèmes d'enregistrement]

Criticité : Le risque se mesure par la multiplication de deux critères : la probabilité et la gravité. La **probabilité** exprime la possibilité de survenance du risque, c'est-à-dire la potentialité que l'accident se produise. La **gravité** mesure l'importance des conséquences, des impacts envisagés en cas de survenance du risque, en cas d'accident.

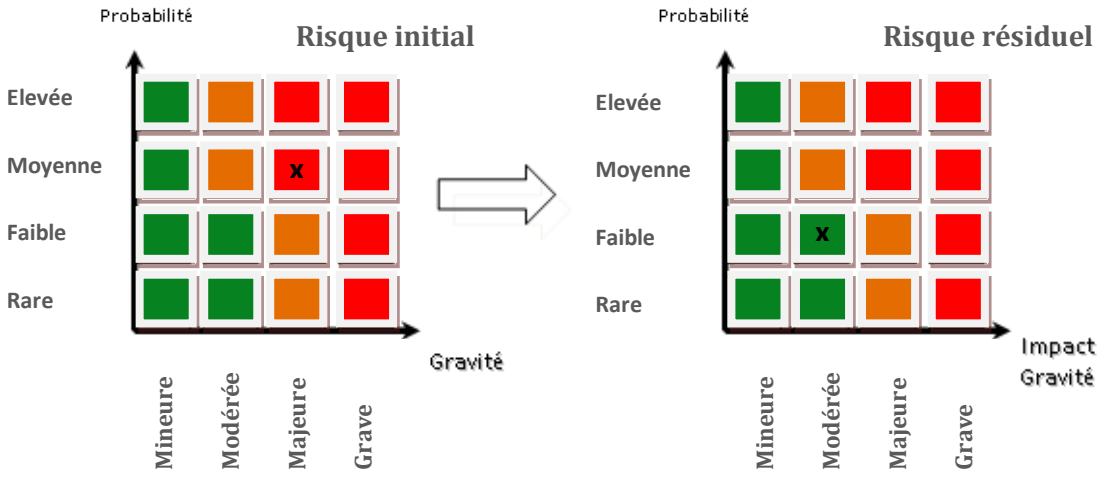
Le résultat de cette multiplication est la **criticité** du risque que, par simplification sémantique, on assimile souvent au risque lui-même. La formule de calcul correspondante est la suivante : Risque = Criticité = probabilité x gravité. La représentation graphique de cette mesure est une matrice dont l'abscisse correspond à la gravité et l'ordonnée à la probabilité.

Les termes utilisés pour graduer les axes de la matrice de risque sont ajustables et dépendant de l'organisme.



Pour lutter contre les risques, l'organisme met en œuvre des dispositifs de protection et/ou de prévention, qui constituent au final les éléments de maîtrise des risques. La protection diminue la gravité, en limitant ce que pourrait être l'impact du risque en cas d'accident. La prévention diminue la vraisemblance de l'accident, en mettant en place des mesures destinées à éviter que le risque ne survienne. Au final, protection et prévention constituent la maîtrise du risque.

Le **risque possède une valeur initiale,** jugée trop importante par l'organisme et qui existerait en l'absence de toute disposition de maîtrise du risque ou en présence de mesures de protection/prévention insuffisantes. Le **risque résiduel** est celui qui subsiste après la mise en œuvre des dispositions de maîtrise du risque, protection ou prévention satisfaisantes.
Pour formaliser cette notion de risque initial et de risque résiduel, les deux figures ci-dessous utilisent la même matrice de calcul, seul le positionnement du résultat (représenté par la croix) évoluant d'une représentation à l'autre :



[Source : Quantification des risques. In : Maitrise des risques. Bibliothèque virtuelle documents et normes. AFNOR Editions, 2016. Disponible sur : http://www.bivi.maitrise-risques.afnor.org/layout/set/print/sites-autres/maitrise-des-risques/ofm/maitrise-des-risques/ii/ii-40/ii-40-62/1]

III. Appréciation du risque

Considérant la perte ou l'endommagement des documents d'activité qui, par conséquent, ne sont plus utilisables, fiables, authentiques, complet ou inaltérés et qui donc, peuvent ne plus répondre aux objectifs du Crips, quatre personnes responsables des documents au Crips ont été interviewées afin de déterminer, dans un premier temps, les documents d'activité qui constituent des documents essentiels pour le Crips et le niveau d'importance qui s'y rattache.

Ces personnes sont les suivantes :

- La responsable du secrétariat de direction
- La responsable du service financier
- La responsable du pôle information documentation
- L'informaticien du Crips

Les informations collectées ont été organisées dans un tableau joint en **annexe 1**[8].

Les documents essentiels, dont la perte ou l'endommagement pourraient suspendre l'activité du Crips

Selon les professionnels interviewés, ce sont :

- Les bilans comptables
- Les comptes de résultat
- Les grands livres d'écritures
- Les factures
- Le fichier contacts
- Les logiciels et leurs licences
- Le registre des mots de passe administrateur
- Le site web du Crips

- **Les bilans comptables, les comptes de résultat et les grands livres d'écriture** sont sauvegardés sur un serveur dédié (serveur compta – 20 Go de données) protégé par un pare-feu et sauvegardé quotidiennement sur un autre serveur (WOOXO – 2,67 To de données) dédié exclusivement à la sauvegarde de tous les serveurs du Crips. Le serveur WOOXO sauvegarde 7 jours consécutifs de données. Ces documents sont par ailleurs envoyés à l'expert comptable et au commissaire aux comptes. Le risque est maitrisé.
- Concernant **les factures**, leur volume correspond à 7200 écritures par an soit 72.000 factures conservées sous format papier au Crips. Elles sont conservées dans le bureau de la direction financière (pour les 3 dernières années) et à la cave (pour les plus anciennes). Le risque de perte et d'endommagement est perçu comme réel et non maitrisé.
- **Le fichier contact** comprend 16000 enregistrements. Il est hébergé chez un serveur extérieur, onlinet.net. Une sauvegarde FTP est réalisée chaque semaine. Le risque d'effacer fortuitement un contact sans retour possible est perçu et l'incertitude de la responsable du fichier quant à sa localisation est évoquée.
- **Les logiciels et leur licence** sont sauvegardés sur des disques internes et externes sécurisés par des mots de passe administrateur. Le risque de se faire voler ou pirater les disques est perçu et maitrisé par des mots de passe assez complexes, lesquels sont sauvegardés et remis au directeur. Le coût financier est élevé (exemple : 50 licences Microsoft office à 100€ l'unité, 2 suites creative à 2000€ l'unité, etc.)

[8] Annexe 1 : Annexe1-UA2401_CS32_2016_CARIOU Marjorie.xls

- **Le registre des mots de passe administrateur et les procédures techniques** sont sous formats .xls et .docx, ils sont sauvegardés dans une rubrique invisible sur le serveur CBUILDER (serveur dédié aux documents d'activité de tous les collaborateurs du Crips). Le risque de vol et de piratage est prévenu par la localisation du registre dans une rubrique invisible et la remise des données au directeur.
- **Le site web** du Crips comprend tous les produits documentaires qui représentent une part de l'expertise du Crips. Ce site, sous format SPIP, est hébergé par le serveur extérieur online.net. Une sauvegarde quotidienne est réalisée par online.net et une sauvegarde hebdomadaire est réalisée par le Crips. Le risque de piratage est perçu et maitrisé par les sauvegardes quotidiennes du prestataire et la sauvegarde hebdomadaire du Crips

Les risques selon la norme ISO 18128

Il est d'abord nécessaire de déterminer les critères de risques liés aux processus et aux systèmes documentaires. Ces critères s'appuient sur

- les exigences règlementaires en vigueur dans la juridiction de l'organisme (cf. chapitre I.)
- les conséquences des évènements porteurs de risque, identifiées selon la zone d'incertitude et la façon dont elles sont mesurées. Le tableau ci-dessous classe l'appréciation des conséquences des évènements et s'inspire de celui proposé par la norme ISO 18128

Tableau 1

Mineur	Modérée	Majeure	Grave
faille normale dans la restriction d'accès	accès non autorisé. Pratique non autorisée.	accès non autorisé. Obligation d'enregistrement	accès non autorisé. Perte et endommagement
endommagement d'une petite quantité de documents d'activité dans un pôle d'activité	endommagement d'une quantité importante de documents d'activité dans un pôle d'activité	endommagement de documents essentiels aux activités se généralisant sur plusieurs pôles d'activité	endommagement de documents d'activité essentiels dans une majorité des pôles d'activité
perte limitée de donnée	perte de donnée compromettant la fiabilité. Traitement de données à caractère personnel non autorisé au-delà d'une limite et compromettant la fiabilité.	perte de donnée compromettant la fiabilité et la réputation de l'organisme	perte de données, perte de la fiabilité, perte de la confiance du public
perte recouvrable	activité non perturbée. perte recouvrable avec effort	perte reconnue et perturbante à plusieurs niveaux opérationnels	arrêt d'activité. Effort de rétablissement coûteux et chronophage. Perte définitive des documents

- le mode d'expression des probabilités : la probabilité d'un évènement porteur de risque sera mesuré sur l'axe du temps, comme ci-dessous

Tableau 2

Score de probabilité	Interprétation
1	probabilité rare, 1 fois tous les 10 ans
3	probabilité faible, 1 fois tous les 3 ans
6	probabilité moyenne, 1 fois par an
9	probabilité élevée, plus d'1 fois par mois

- la méthode de détermination du niveau de risque : (cf. chapitre II.)
  Criticité = probabilité x gravité
  Si probabilité >= x et si gravité >= Y, alors une action préventive de niveau z est à mener. L'enjeu de ces calculs est de fournir des indicateurs capables de mesurer une évolution de la situation, une progression ou une régression.
- Critères permettant de déterminer si un risque est acceptable ou nécessite un traitement : la taille du système documentaire, le nombre d'utilisateurs, l'utilisation qui est faite lors des opérations de l'organisme

1. Identification du risque

L'objectif consiste à « identifier ce qui peut se produire, susceptible d'avoir une incidence sur la capacité des documents à répondre aux besoins de l'organisme. Il convient de documenter les risques identifiés dans un registre des risques de l'organisme ».

Exemple de risque identifié par le Crips, documenté dans un registre des risques selon la norme ISO 18128 (Annexe A)

Pour identifier ce qui peut se produire sur les documents essentiels du Crips, prenons l'exemple des documents/données dont le risque est perçu mais non maitrisé :

Tableau 3

DESCRIPTION DU RISQUE	
ID du risque	1
Nom du risque	Perte des factures clients et fournisseurs
Type et/ou famille de risque	Document papier
Propriétaire du risque	Direction
Date de l'identification	01/12/2015
Description du risque	Incapacité à mettre en place une sauvegarde des factures
Circonstances de la survenue du risque	incendie, inondation, déménagement
Probabilité	Faible
Conséquence	Majeur
Stratégie d'empêchement	Acquérir un module pour émettre et intégrer les factures à la BDD compta (Sage 1000)
Stratégie de traitement	_
Date cible	_
Etat du risque	Action d'atténuation du risque non engagée car coût trop important (1500€/mois)
Date de la dernière appréciation	_

Tableau 4

DESCRIPTION DU RISQUE	
ID du risque	2
Nom du risque	Perte de contacts de l'organisme
Type et/ou famille de risque	BDD contact hébergée sur serveur externe
Propriétaire du risque	Direction
Date de l'identification	26/05/206
Description du risque	Incapacité de récupérer un contact effacé fortuitement en appuyant sur une touche du clavier
Circonstances dans lesquelles le risque peut surgir	Défaillance de la programmation qui ne propose pas de message d'alerte avant suppression de données.
Probabilité	Elevée (à chaque consultation du fichier par secrétariat direction (accès illimité) + collaborateurs Crips (accès limité)
Conséquence	Majeur : perte de contact stratégique (politique/média...)
Stratégie d'empêchement	Sauvegarde FTP hebdomadaire réalisée en interne
Stratégie de traitement	Reprogrammation de l'interface
Date cible	_
Etat du risque	Action d'atténuation du risque non engagée
Date de la dernière appréciation	_

Exemple de risque non identifié par le Crips

Au regard de la nouvelle législation relative au traitement des données à caractère personnel, il convient de pointer un risque encouru par le Crips, qui n'a pas été pointé et qui engage la responsabilité de son représentant légal (cf. chapitre I – page 5) :

Tableau 5

DESCRIPTION DU RISQUE	
ID du risque	3
Nom du risque	Traitement des données personnelles
Type et/ou famille de risque	Registre
Propriétaire du risque	Représentant légal du Crips
Date de l'identification	Non détecté
Description du risque	Incapacité à fournir un registre détaillé des traitements de données personnelles
Circonstances dans lesquelles le risque peut surgir	Contrôle de l'autorité nationale compétente (à partir de 2018) au regard du traitement des données à caractère personnel, collectées par le Crips par formulaire web et données enregistrées dans le registre unique du personnel.
Probabilité	Moyenne
Conséquence	Modérée
Stratégie d'empêchement	
Stratégie de traitement	
Date cible	_
Etat du risque	Action d'atténuation du risque non engagée
Date de la dernière appréciation	_

2. Analyse du risque

Processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. Ainsi le risque est analysé en déterminant ses conséquences potentielles et la vraisemblance de sa réalisation. Les conséquences d'évènements porteurs de risque sont identifiées selon la zone d'incertitude et échelonnées selon les critères de risque déterminés par l'organisme. La norme ISO 18128 établi une liste de contrôle[9] qui vise à identifier les zones d'incertitude.

Les zones d'incertitudes

Considérant le CRIPS, on peut identifier différentes zones d'incertitudes intervenant à différents niveaux (liste non exhaustive au regard de l'enquête succincte du fait de son fait caractère d'exercice) :

Zone d'incertitude : changements dans le contexte politique et sociale

La nouvelle règlementation pour la protection des données personnelles

Zone d'incertitude : environnement physique et infrastructure

Les inondations, les incendies

Zone d'incertitude : menaces contre la sécurité

L'intrusion/l'accès extérieur non autorisé aux systèmes documentaires et les modifications non autorisées apportées aux documents d'activité

Une intrusion physique dans le stockage des documents d'archivage ou dans l'espace informatique

Zone d'incertitude : changements organisationnels

Un plan de reprise d'activité après sinistre existant et actualisé

Zone d'incertitude : ressources humaines

Le départ d'employés clés possédant des compétences essentielles et une connaissance approfondie de l'organisme et de son historique

Zone d'incertitude : ressources financières et matérielles

La suffisance des ressources financières allouées afin d'acquérir, d'actualiser ou de préserver de systèmes adéquats

Pour chacun des risques, il faut se poser les questions :

↳ Quelle est la **vraisemblance** (**ou probabilité**) qu'un accident se produise ?

↳ Quelle est la **gravité** des conséquences ?

Il convient aussi de prendre en compte les contrôles existants, leur efficacité et leur performance.

[9] *Annexe B norme ISO 18128*

3. Evaluation du risque

Cette procédure est fondée sur l'analyse du risque pour décider si le risque tolérable est atteint *[source : Guide ISO 73].*

Décider si le risque tolérable est atteint suppose de déterminer :

- la nécessité ou non d'un traitement du risque
- les priorités de traitement
- la mise en oeuvre ou non d'une action

L'échelle des évènements porteurs de risque (tableau 1) peut être associée à un tableau de probabilité (tableau 2) afin d'identifier les évènements sur lesquels il convient d'axer des actions préventives ou/et des mesures de traitement.

Un score chiffré est attribué aux conséquences et à la probabilité. Cela indique la priorité assignée à l'action préventive/traitement que l'on souhaite appliquée à l'évènement porteur de risque.

Exemple d'évaluation des risques

Tableau 6

EVENEMENT (*)			PROBABILITE	CONSEQUENCES			
Contexte	Système	processus	Fréquence	Mineur	Modéré	Majeur	Grave
	Défaillance de programmation de la BDD contacts		Elevée : à chaque consultation			perte reconnue et perturbante à plusieurs niveaux opérationnels	
Economie faite sur le budget fonctionnement ne permettant pas l'acquisition d'un module (complément du logiciel Sage 1000) pour l'intégration et l'émission de factures			Faible : au moins tous les 5 ans à l'occasion d'un déménagement			perte reconnue et perturbante à plusieurs niveaux opérationnels	
	Obsolescence du support		Moyenne			Perte de documents essentiels	
Changement de la loi sur les données personnelles			Moyenne : 1 fois par an à partir de 2018		Traitement de données à caractère personnel non autorisé au-delà d'une limite et compromettant la fiabilité.		

* Les évènements porteurs de risque ont été identifiés dans le contexte de l'organisme, les systèmes ou les processus, trois catégories impliquées dans la création et le contrôle des documents d'activité de l'organisme.

Echelle de cotation utilisée pour l'évaluation des risques

On attribue à chaque niveau de probabilité et de gravité un certain nombre de points, la criticité étant le produit des deux. La couleur est définie en fonction de seuils sur le produit

Tableau 2 – possibilité de survenance de risque ou Probabilité

Score	Interprétation
1	probabilité rare, 1 fois tous les 10 ans
3	probabilité faible, 1 fois tous les 3 ans
6	probabilité moyenne, 1 fois par an
9	probabilité élevée, plus d'1 fois par mois

Tableau 8 – Importance des conséquences ou Gravité

Score	Appréciation des conséquences
1	Mineure
3	Modérée
6	Majeure
9	Grave

Il est convient parfois de coter la détection d'un risque, c'est-à-dire la capacité d'un système à détecter ou prévenir un risque.

Tableau 9 – capacité de détection d'un risque

Score	Détection
1	détectable
2	non détectable

Une valeur importante dans l'un des trois facteurs _probabilité (P), gravité (G), détection (D)_ montre une faiblesse qu'il convient de corriger. Faire le produit P*G*D donne le seuil de criticité.
Les seuils de criticité acceptés sont définis par l'organisme et sont représentés par une couleur dans un tableau d'évaluation des risques :
Niveau 3 : Risque acceptable – niveau de 1 à 9 – couleur verte
Niveau 2 : Risque moyen – niveau de 12 à 36 – couleur orange
Niveau 1 : Risque inacceptable – niveau de 54 à 162 – couleur rouge

Selon le niveau de criticité obtenu, des actions préventives sont dès lors mises en place :
Risque acceptable : pas d'action à mener
Risque moyen : action préventive fortement conseillée (ex : documenter les processus, mettre en place une fonction opérationnelle adaptée au besoin, etc.)
Risque inacceptable : action préventive obligatoire (ex : sauvegarde sécurisée, archivage externalisé, etc.)

Tableau 10 – actions préventives à mener

Score	Actions préventives
1	AP obligatoire
2	AP fortement conseillée
3	AP non prioritaire

Tableau 11 – grille d'évaluation des risques *(tableau complet disponible en **annexe 1**)*

Ce tableau reprend les documents perçus, par leurs responsables respectifs, comme étant essentiels et encourant potentiellement un risque.
A été ajouté un document manquant, qui au regard de la législation, devra à court terme être produit par toute entreprise. Le CRIPS, organisme commercialisant une offre de formation et salariant 53 personnes, traite des données à caractère personnel : Il collecte, enregistre, organise, structure, conserve (peut-être au-delà de la durée d'utilité administrative), modifie, consulte, efface, détruit des données à caractère personnel concernant les stagiaires, les candidatures sans suite collectées via formulaire web, et celles du registre unique du personnel (RUP). Le CRIPS a l'obligation, dès 2018, de documenter ce traitement (cf. chapitre I – page 5).

↳ Cette nouvelle obligation règlementaire bientôt effective n'est pas connue et **le risque** de ne pouvoir présenter le registre des traitements **n'est pas détecté**. Une veille législative, effectuée au niveau de la direction administrative, peut prévenir ce type de risque.

Mise à jour du document : 20/06/2016						Évaluation initiale			Priorité à donner aux actions préventives		Gestion des actions préventives				Réévaluation après actions préventives		
Fonction	Processus	Donnée	Est-ce un document d'activité ?	Risque identifié	conséquence	Probabilité de survenance du risque	Gravité= importance des conséquenc	Criticité = risque initial	Non-détection	Priorité pour les Actions Préventive	Définition de l'action	Pilote de l'action	Date cible	Avancement de l'action	Fréquence	Gravité	Criticité = risque résiduel
SECRETARIAT DE DIRECTION	partenariat & communication	fichier contacts	non	_suppression fortuite des contacts sans possibilité de les récupérer	perte de contacts stratégiques (politique/média...)	9	6	54	1	1	Sauvegarde FTP hebdomadaire réalisée en interne	administrateur informatique	hebdomadaire	action programmée et méconnaissance de cette sauvegarde hebdomadaire par le secrétariat de direction	9	6	54
POLE INFODOC	prévention	audiovisuel	oui pour les productions CRIPS	obsolescence du format	illisibilité des productions audiovisuelles du CRIPS (patrimoine)	6	6	36	1	2	dépôt légal à la BNF	pôle infodoc	ND. en cours	partenariat engagé	3	3	9
	_communication _aide à l'action	site web	non	piratage et perte de produits documentaires à valeur ajoutée (expertise Crips)	Inviibilité des productions documentaires et pédagogiques du CRIPS - aide à l'action remise en cause temporairement	1	6	6	2	Pas d'action à mener							6
INFORMATIQUE	traitement des données à caractère personnel	**Registre**	oui	conservation de données non autorisée	contrôle et sanction à partir de 2018 (responsabilité du représentant légal engagée)	6	3	18	2	2	tenir à jour un registre du traitement des données à caractère personnel collectées	administrateur informatique	d'ici 2018 (règlement européen)				18
DIRECTION FINANCIERE	comptabilité	**Factures** (achats & ventes)	oui	vol, inondation, feu	obligation légale non respectée, impossibilité de justifier des écritures comptables dans un litige	3	9	27	1	2	Acquérir un module pour émettre et intégrer les factures à la BDD compta (Sage 1000)	direction financière	1 décembre 2015	action non engagée car coût trop important (1500/mois)	3	9	27

IV. Traitement du risque

Lorsqu'une action satisfaisante a été engagée pour prévenir la probabilité de survenance du risque, il subsiste un risque qualifié de résiduel.

La perte des productions audiovisuelles du CRIPS, documents considérés essentiels, a été perçue comme majeure par la responsable du pôle infodoc. Le risque identifié est l'obsolescence du support utilisé, risquant d'empêcher la lecture. Comme action préventive, la responsable a engagé un partenariat avec la BNF afin de déposer les productions audiovisuelles du CRIPS. La BNF s'engage, au titre du dépôt légal, à garantir la lisibilité du support de conservation. L'action préventive est satisfaisante, le risque est donc devenu résiduel pour le CRIPS.

Mise à jour du document : 20/06/2016						Évaluation initiale			Priorité à donner aux actions préventives		Gestion des actions préventives				Réévaluation après actions préventives		
Fonction	Processus	Donnée	Est-ce un document d'activité ?	Risque identifié	conséquence	Probabilité de survenance du risque	Gravité= importance des conséquenc	Criticité = risque initial	Non-détection	Priorité pour les Actions Préventive	Définition de l'action	Pilote de l'action	Date cible	Avancement de l'action	Fréquence	Gravité	Criticité = risque résiduel
	prévention	audiovisuel	oui pour les productions CRIPS	obsolescence du format	illisibilité des productions audiovisuelles du CRIPS (patrimoine)	6	6	36	1	2	dépôt légal à la BNF	pôle infodoc	ND. en cours	partenariat engagé	3	3	9

La perte des factures du CRIPS, documents considérés essentiels, a été perçue comme grave par la directrice financière. Le risque identifié est l'endommagement lié à l'environnement physique et l'infrastructure (feu, inondation). Comme action préventive, elle a fait le choix d'acquérir un module pour émettre et intégrer les factures dans la BDD comptabilité Sage 1000. Le coût représente 1500€/mois. L'action préventive n'a pu être réalisée car le coût est jugé trop important compte-tenu des économies à réaliser sur le budget fonctionnement. C'est non-satisfaisant, le risque reste de niveau 2 (moyen) pour le CRIPS. Une action préventive reste fortement conseillée.

Une seconde solution a été envisagée, celle qui consiste à numériser au moins les nouvelles factures chaque mois. Cela représente environ 600 factures (ou 7200/an et 72000/10 ans). Cela devait débuter en janvier mais rien n'a pu être fait par manque de temps. Recruter, même temporairement, une personne dédiée à cette tâche n'est pas possible. Les recrutements sont gelés pour l'instant. Si cette option peut en effet constituer une démarche de réduction des risques, le CRIPS aura toutefois l'obligation de constituer une piste d'audit. Cela consiste, *« pour l'assujetti, à mettre en place des contrôles permanents – à chaque étape du traitement de la facture – permettant de garantir le lien entre la facture reçue, l'opération commerciale réalisée et le paiement de la facture. Les preuves de ces contrôles (manuels ou informatisés) doivent être conservées par l'entreprise et suffisamment documentées pour convaincre l'administration fiscale de la validité et de la bonne maîtrise de ses flux de factures »* (Loi du 18 octobre 2013).

↳ **Une option qui n'a pas été envisagée** consisterait à externaliser la dématérialisation des factures. Un tiers archiveur, comme Locarchives, peut s'avérer une solution économique pour numériser les factures et garantir leur conformité.

Mise à jour du document : 20/06/2016						Évaluation initiale			Priorité à donner aux actions préventives		Gestion des actions préventives				Réévaluation après actions préventives		
Fonction	Processus	Donnée	Est-ce un document d'activité ?	Risque identifié	conséquence	Probabilité de survenance du risque	Gravité= importance des conséquenc	Criticité = risque initial	Non-détection	Priorité pour les Actions Préventive	Définition de l'action	Pilote de l'action	Date cible	Avancement de l'action	Fréquence	Gravité	Criticité = risque résiduel
DIRECTION FINANCIERE	comptabilité	**Factures** (achats & ventes)	oui	vol, inondation, feu	obligation légale non respectée, impossibilité de justifier des écritures comptables dans un litige	3	9	27	1	2	Acquérir un module pour émettre et intégrer les factures à la BDD compta (Sage 1000)	direction financière	décembre 2015	action non engagée car coût trop important (1500)/mois)	3	9	27

La perte des contacts du CRIPS, données considérées essentielles, a été perçue comme grave par la responsable du secrétariat de direction. Le risque identifié est la suppression fortuite de contacts du fait d'une défaillance au niveau de la programmation de la BDD. Aucun message d'alerte ne prévient la suppression. L'utilisation de cette base est très fréquente, son volume est de 16.000 contacts, certaines données ne sont accessibles qu'en accès limité et d'autres sont accessibles par tous les collaborateurs du CRIPS. L'action préventive consiste à une sauvegarde hebdomadaire, inconnue des utilisateurs. Ainsi, même s'ils ont 1 semaine pour récupérer le(s) contact(s) supprimé(s), ne le sachant pas, ils ne le feront pas. L'action préventive n'est pas satisfaisante, le risque reste de niveau 1 (inacceptable) pour le CRIPS. Une action préventive est obligatoire.

↳ **Communiquer sur le risque** avec l'administrateur système lui a permis de prendre connaissance de cette défaillance. Il propose de contacter le prestataire extérieur, en charge de la programmation de la base contacts, et lui commander un code pour un message d'alerte, prévenant le risque de suppression fortuite.

Mise à jour du document : 20/06/2016						Évaluation initiale			Priorité à donner aux actions préventives		Gestion des actions préventives				Réévaluation après actions préventives		
Fonction	Processus	Donnée	Est-ce un document d'activité ?	Risque identifié	conséquence	Probabilité de survenance du risque	Gravité= importance des conséquenc	Criticité = risque initial	Non-détection	Priorité pour les Actions Préventive	Définition de l'action	Pilote de l'action	Date cible	Avancement de l'action	Fréquence	Gravité	Criticité = risque résiduel
SECRETARIAT DE DIRECTION	partenariat & communication	fichier contacts	non	_suppression fortuite des contacts sans possibilité de les récupérer	perte de contacts stratégiques (politique/média...)	9	6	54	1	1	Sauvegarde FTP hebdomadaire réalisée en interne	administrateur informatique	hebdomadaire	action programmée et méconnaissance de cette sauvegarde hebdomadaire par le secrétariat de direction	9	6	54

En conclusion, le CRIPS court aujourd'hui des risques à cause d'une analyse et une communication des risques insuffisantes. Identifier et prioriser les risques pour **prendre les mesures appropriées** est un enjeu important pour le CRIPS. Pour **garantir la détection des risques**, il conviendrait de réaliser une veille stratégique, notamment règlementaire et technologique, de surveiller les risques et de communiquer dessus. Un registre des risques est un document qui permettrait au CRIPS de maîtriser les risques qu'il encoure.

V. Bibliographie

Article L 612-4. In : Code du commerce. Légifrance. Disponible sur : https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000029321702&cidTexte=LEGITEXT000005634379

Article L6352-11. In : Code du travail. Légifrance. Disponible sur : https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000006189924&cidTexte=LEGITEXT000006072050

Articles R6352-22 à R6352-24. In : Code du travail. Légifrance. Disponible sur : https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000018522310&cidTexte=LEGITEXT000006072050

Code de la propriété intellectuelle. Légifrance. Disponible sur : https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414&dateTexte=20090204

Déclaration d'activité des formateurs ou organismes de formation [fiche pratique]. Paris : Direction de l'information légale et administrative, 5 octobre 2015. Disponible sur : https://www.service-public.fr/professionnels-entreprises/vosdroits/F19087

ISO Guide 73:2009. Management du risque – vocabulaire. Genève : Organisation Internationale de Normalisation, 2009.

ISO 15489 :2016. Information et documentation - Records management - Partie 1: Concepts et principes. Genève : Organisation Internationale de Normalisation, 2016.

ISO/TR 18128:2014. Information et documentation - Évaluation du risque pour les processus et systèmes d'enregistrement. Genève : Organisation Internationale de Normalisation, 2014.

ISO 26122: 2014. Information et documentation - Analyse des processus pour la gestion des informations et documents d'activité. Genève : Organisation Internationale de Normalisation, 2014.

ISO 30301 :2011. SGDA – Principes et vocabulaire. Genève : Organisation Internationale de Normalisation, 2011.

Législation : Code du patrimoine. In : Qu'est-ce que le dépôt légal ? Paris : Bibliothèque Nationale de France. Disponible sur : http://www.bnf.fr/fr/professionnels/depot_legal_definition/i.depot_legal_loi/s.depot_legal_loi_code.html?first_Rub=non

Le Règlement Général sur la Protection des Données adopté définitivement [Article]. In : La revue. Cabinet Squire Patton Boggs, 18 avril 2016. Disponible sur : http://larevue.squirepattonboggs.com/Le-Reglement-General-sur-la-Protection-des-Donnees-adopte-definitivement_a2856.html

Loi n° 2010-241 du 10 mars 2010 relative au service civique. Disponible sur : http://www.service-civique.gouv.fr/uploads/content/files/62e7beb5b01d63981097e854af03cf38f8efdbeb.pdf

Quantification des risques. In : Maitrise des risques. Bibliothèque virtuelle documents et normes. La Plaine Saint-Denis : AFNOR Editions, 2016. Disponible sur : http://www.bivi.maitrise-risques.afnor.org/layout/set/print/sites-autres/maitrise-des-risques/ofm/maitrise-des-risques/ii/ii-40/ii-40-62/1

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 : dispositions générales. Commission Nationale de l'Informatique et des Libertés, 27 avril 2016. Disponible sur : https://www.cnil.fr/reglement-europeen-protection-donnees/chapitre1#Article4

Responsable de traitement. In : Définition. Commission Nationale de l'Informatique et des Libertés. Disponible sur : https://www.cnil.fr/fr/definition/responsable-de-traitement