



PREMIER MINISTRE

n° 972-3/SGDN/DCSSI

Paris, le 17 juillet 2003

SCHEMA DE QUALIFICATION

*des solutions de surcharge de sécurité
des disques durs*

(Problématique de « l'effacement » des signaux magnétiques)

document provisoire

Mots clés : signaux magnétiques, confidentialité, support magnétique, disque dur, surcharge, effaceur, effacement, démagnétiseur, démagnétisation, destruction.

DIRECTION CENTRALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Version : 0.911(provisoire)/2003

SOMMAIRE

1 : Références	5
2 : Avant-propos.....	6
3 : Objet du schéma.....	6
4 : Définitions	7
5 : Système de référence	7
6 : Référentiel d'exigences.....	9
6.1 : Etape n°1 : mise en ordre de marche	9
6.2 : Etape n°2 : avertissement sur la légalité de l'action engagée	9
6.3 : Etape n°3 : avertissement sur la validité des opérations de surcharge	10
6.4 : Etape n°4 : avertissement sur la pertinence de l'action engagée	11
6.5 : Etape n°5 : choix de la stratégie et des options de surcharge	12
6.6 : Etape n°6 : avertissement sur les conditions de poursuite des opérations	12
6.7 : Etape n°7 : exécution des opérations de surcharge	14
6.8 : Etape n°8 : contrôle final	15
6.9 : Etape n°9 : rapport final.....	15
6.10 : Stratégies et options de surcharge	16
7 : Application du schéma.....	18
Annexe n°1 : Conditions d'appréciation, tableaux et grilles guides	19
Annexe n°2 : Extraits du guide [2] et compléments juridiques	27

1 : REFERENCES

- [1] **Guide pratique pour la protection des supports classifiés de défense n° 972/SCSSI/SI du 09/04/98.**
- [2] **Guide technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter (Problème de l'effacement des signaux magnétiques), n° 972-1/SGDN/DCSSI du 17/07/03.**
- [3] **Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, paru au journal officiel n°92 du 19 avril 2002, page 6944.**

2 : AVANT-PROPOS

La confidentialité des informations enregistrées sur les disques durs est une obligation permanente au regard des lois et règlements concernant la protection des informations et supports classifiés de défense.

Plus généralement, elle est un besoin éprouvé légitimement par les usagers des systèmes d'information, particulièrement au moment de se séparer de leurs ordinateurs ou disques durs.

La mesure de sécurité qui vient naturellement à l'esprit est l'effacement des supports magnétiques. L'utilisateur attend de cette mesure qu'elle supprime les traces laissées par ses écritures. Or les disques durs ne possèdent que deux fonctions qui permettent, en condition normale d'exploitation, l'écriture et la lecture. L'effacement n'est pas possible, sauf à concevoir et implanter une fonction nouvelle ou définir avec les deux fonctions disponibles un processus dont les effets seraient jugés équivalents à ceux d'un effacement.

Le guide [2] identifie la surcharge comme une mesure susceptible d'assurer la confidentialité des informations écrites sur les disques durs tout en préservant le caractère réutilisable de ces supports. Cette surcharge concerne le disque dur complet.

La mise en œuvre de cette mesure au titre de la sécurité des systèmes d'information (SSI) nécessite de disposer d'une solution dont la capacité à se rapprocher suffisamment de l'objectif de sécurité qu'elle vise, soit formellement reconnue.

Une telle reconnaissance procède d'un schéma de qualification.

3 : OBJET DU SCHEMA

Ce schéma a pour objet la qualification des solutions de surcharge complète de disques durs.

Il s'applique aux solutions qui déclarent satisfaire le besoin de sécurité énoncé ci-dessous, en se rapprochant de l'objectif de sécurité énoncé ci-après.

Le **besoin de sécurité** est la confidentialité des informations écrites sur les disques durs destinés à être recyclés ou exportés (*énoncé extrait du guide [2]*).

L'**objectif de sécurité** est l'inaccessibilité des informations écrites sur les disques durs avant leur recyclage ou leur exportation (*énoncé extrait du guide [2]*).

Ce schéma est à l'usage des responsables de l'organisation de la sécurité des systèmes d'information de l'administration et de leurs collaborateurs informaticiens qualifiés.

4 : DEFINITIONS

Les définitions suivantes fixent la terminologie du schéma :

Surcharge de sécurité : opération qui ajoute des signaux magnétiques sur les plateaux des disques durs¹ de telle façon que les signaux magnétiques anciens ne peuvent plus être mesurés.

Solution de surcharge : procédé d'écriture qui vise à rendre inaccessibles les données anciennes écrites sur les disques durs tout en permettant la réutilisation de ces disques durs.

Qualification d'une solution de surcharge : reconnaissance de la capacité d'une solution de surcharge à se rapprocher suffisamment de l'objectif de sécurité qu'elle vise.

Dans ce schéma, une solution de surcharge qualifiée est appelée : **solution de surcharge de sécurité**, ou simplement **solution**.

Schéma de qualification : processus d'appréciation qui s'appuie sur un référentiel d'exigences.

Référentiel d'exigences : ensemble de spécifications qui constitue un système qui permet de comparer les performances avérées d'une solution aux performances nominales de ce système.

Une solution de surcharge candidate à la qualification est appelée : **candidat**.

5 : SYSTEME DE REFERENCE

Le référentiel d'exigences objet du paragraphe suivant, spécifie le protocole opératoire et les opérations qui constituent le système fonctionnel abstrait de référence, ou plus simplement : système de référence. Ce système approche l'objectif de sécurité aussi près que la théorie développée par Peter GUTMANN² permet de le montrer.

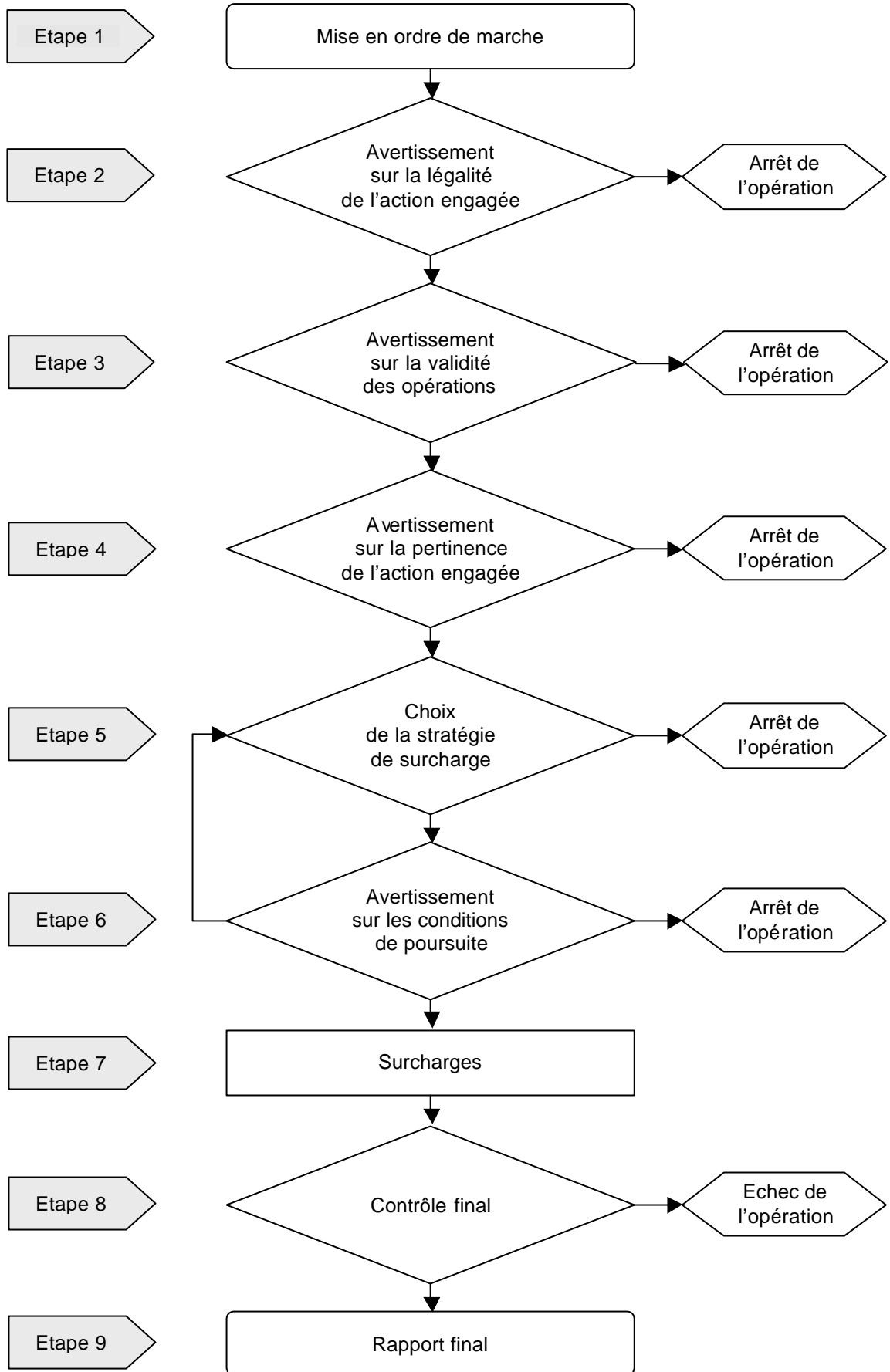
Idéalement les candidats devraient être des réalisations du système de référence. Leur qualification pourrait être alors prononcée automatiquement après validation de leur processus de développement. Si le processus de développement ne peut pas être validé ou si un candidat n'est pas développé à partir du système de référence présenté ici, il convient de l'apprécier à l'aide du présent schéma.

Ce schéma contient : l'organigramme du protocole opératoire de référence (*page suivante*), les spécifications des exigences à chaque étape des opérations (*chapitres 6.1 à 6.9*), les spécifications des stratégies et options de surcharge (*chapitre 6.10*), des modèles de tableaux et grilles d'appréciation des candidats (*annexe n°1*).

¹ Voir la définition d'un **disque dur** donnée dans le guide [2] et rappelée dans l'annexe n°2.

² Peter GUTMANN, Department of Computer Science, University of AUCKLAND, *Secure Deletion of Data from Magnetic and Solid-State Memory*, Sixth USENIX Security Symposium, San Jose, California, 22-25 juillet 1996.

Protocole opératoire de référence



6 : REFERENTIEL D'EXIGENCES

6.1 : Etape n°1 : mise en ordre de marche

- 1.1._ : La solution est accompagnée de sa documentation complète en français : 1- conditions de mise en oeuvre, 2- caractéristiques techniques, 3- déclaration de performances, 4- manuel de l'utilisateur, 5- conditions de garantie, 6- conditions d'accès à l'assistance technique.
- 1.1.1.1 : La documentation indique que l'ordinateur traitant doit être isolé et son alimentation en énergie électrique doit être stabilisée à ses valeurs nominales.
- 1.2 : L'origine et l'intégrité de la solution sont vérifiables.
- 1.3.1 : La solution s'exécute sans recourir au système d'exploitation installé sur l'ordinateur contenant le disque dur à traiter.
- 1.3.2 : Quand la solution est distribuée sur un CD-ROM, la procédure de démarrage de l'ordinateur à partir du CD-ROM est indiquée dans le manuel de l'utilisateur.

6.2 : Etape n°2 : avertissement sur la légalité de l'action engagée

- 2.1 : La solution s'interrompt immédiatement après son démarrage pour délivrer un avertissement sur la légalité de l'action engagée.

Exemple d'avertissement :

Le disque dur que vous allez surcharger contient peut être des informations classifiées de défense.

L'opération rendra ces données inaccessibles aux usagers légitimes
utilisant normalement le système d'information.

Assurez vous d'être autorisé à mener une telle opération
sans enfreindre les articles 413-9 et suivants du code pénal.

Le disque dur que vous allez surcharger contient peut être des informations sensibles.

L'opération rendra ces données inaccessibles aux usagers légitimes
utilisant normalement le système d'information.

Assurez vous d'être autorisé à mener une telle opération
sans enfreindre, une loi de la République, un règlement ou un engagement de votre administration.

- 2.2 : La solution offre la possibilité d'échapper à la poursuite du protocole ; c'est l'option par défaut en cas de mise en attente avec décompte de temps.
- 2.3._ : La solution enregistre : 1- la date et l'heure indiquées par le système, 2- le nom, la fonction et l'organisme d'appartenance de l'opérateur ; il est admis que cette identification ne soit pas authentifiée ; l'opérateur peut aussi compléter le procès verbal de surcharge, de façon manuscrite, à la fin des opérations.

6.3 : Etape n°3 : avertissement sur la validité des opérations de surcharge

- 3.1._ : La solution analyse l'ordinateur traitant (BIOS³, CPU, système RAID, ...).
- 3.2._ : La solution analyse le disque dur à traiter ; elle repère : 1- le standard (SCSI ou IDE en configuration maître ou esclave), 2- les performances (vitesse de transfert, ...), 3- la taille, 4 les caches mémoires, 5- les partitions à usage exclusif du système courant⁴, 6- les fonctions de tolérance aux pannes (SMART⁵), 7- l'état du disque (elle recherche les zones endommagées).

Puis, la solution pratique une des trois heuristiques suivantes :

- 3.3 : La solution confronte les éléments de son analyse à une base d'informations ; la base d'informations et les conditions de sa mise à jour doivent être validées.
- 3.3bis : La solution applique un plan de tests capable de discriminer les disques sur lesquels elle opérera correctement ; le plan de tests et tous les tests doivent être validés.
- 3.3ter : La solution pratique une combinaison des deux heuristiques précédentes.
- 3.4 : A la fin de l'analyse, la solution enregistre pour elle-même et/ou édite immédiatement la signalétique et les réponses suivantes :

Identification du BIOS de l'ordinateur traitantobligatoire
Identification de la carte mère recommandé
Identification du processeur recommandé
Identification du contrôleur de disqueobligatoire
Identification du disque dur à traiterobligatoire

Caractéristiques du disque dur à traiter :

Standard et performances (en référence aux normes ATA)obligatoire
Configuration (maître/esclave, pour les disques IDE uniquement).....obligatoire
Nombres de cylindres/têtes/secteurs déclarés au BIOS (C/H/S)obligatoire
Taille des secteurs.....obligatoire
Capacité totale calculéeobligatoire
Existence de zones défectueusesobligatoire
Existence de mémoire cacheobligatoire
Existence d'une partition propriétaireobligatoire
Existence d'une fonction de tolérance aux pannes (SMART)obligatoire

Le modèle est-il reconnu par la solution ? ..réponse obligatoire pour l'heuristique 3.3
La mémoire cache, s'il y en a, peut-elle être désactivée ? réponse obligatoire
La solution peut-elle s'affranchir des partitions présentes ? réponse obligatoire
La fonction de tolérance au panne peut-elle être désactivée ? réponse obligatoire

³ Basic Input Output System : programme de démarrage propriétaire d'un ordinateur.

⁴ Partition associée à la fonction de mise en veille des ordinateurs portables, par exemple.

⁵ Self-monitoring, Analysis and Reporting Technology : fonction de tolérance aux pannes.

3.5 : A l'issue de son activité d'analyse, la solution s'interrompt pour délivrer sa conclusion sous la forme d'un avertissement sur la validité des opérations de surcharge à venir.

Exemple d'avertissement pour un cas favorable :

Le disque dur à traiter est un modèle connu, sans secteur défectueux,
le BIOS de l'ordinateur traitant est une version connue,
le système d'exploitation utilisé par la solution est compatible avec le disque dur et le BIOS.

Sauf défaillance de l'ordinateur traitant, les opérations de surcharge seront exécutées.

Exemple d'avertissement pour un cas douteux :

Le disque dur à traiter est un modèle inconnu
ou le BIOS de l'ordinateur traitant est une version inconnue.

Les opérations de surcharge risquent d'être exécutées partiellement et imparfaitement.

Exemple d'avertissement pour un cas défavorable :

Le disque dur à traiter est défectueux, ou est un modèle incompatible avec la solution,
ou le BIOS de l'ordinateur traitant est une version incompatible avec la solution,
ou l'ordinateur traitant a une architecture incompatible avec la solution

Les opérations de surcharge n'atteindront pas l'objectif de sécurité visé.

3.6 : La solution offre la possibilité d'échapper à la poursuite du protocole ; c'est l'option par défaut en cas de mise en attente avec décompte de temps.

6.4 : Etape n°4 : avertissement sur la pertinence de l'action engagée

4.1 : Après l'étape n°3, la solution s'interrompt pour délivrer un avertissement sur la pertinence de l'action engagée.

Exemple d'avertissement :

L'action engagée vise à rendre inaccessible les informations écrites sur le disque dur.
Toutefois, rien ne garantit l'inexistence de moyens capables de recouvrer des données surchargées.

Assurez vous⁶ de bien choisir la mesure de sécurité adaptée à votre besoin
au regard de vos obligations pénales⁷, civiles et administratives.

4.2 : La solution offre la possibilité d'échapper à la poursuite du protocole ; c'est l'option par défaut en cas de mise en attente avec décompte de temps.

⁶ Avec l'aide du guide [2], par exemple.

⁷ En particulier les articles 226-17, 413-9 et autres du code pénal (voir des extraits en annexe n°2)

6.5 : Etape n°5 : choix de la stratégie et des options de surcharge

5.1 : Après l'étape n°4, la solution s'interrompt pour permettre le choix de la stratégie et des options de surcharge.

Exemple d'interface :

<p style="text-align: center;">Choix de la stratégie de surcharge :</p> <p>Choix de la méthode de parcours :</p> <ul style="list-style-type: none">1 : application de chaque passe de surcharge sur tout le disque dur.2 : application secteur par secteur de toutes les passes de surcharge.3 : enchaînement de la méthode de parcours n°1 puis de la méthode n°2.4 : enchaînement de la méthode de parcours n°2 puis de la méthode n°1. <p>Choix combiné du nombre de passes d'écriture et des caractères à écrire :</p> <ul style="list-style-type: none">1 : Surcharge standard (une passe).2 : Surcharges renforcées.<ul style="list-style-type: none">1 : Option n°1 (sept passes)2 : Option n°2 (huit passes dont une d'aléa)3 : Option n°3 (trente six passes dont huit d'aléa) <p style="text-align: center;">Choisir une stratégie et ses options ou ECHAPPER.</p>

5.2 : La description des différentes stratégies et options de surcharge est documentée en ligne ou dans une documentation d'accompagnement⁸.

5.3 : La solution offre la possibilité d'échapper à la poursuite du protocole ; c'est l'option par défaut en cas de mise en attente avec décompte de temps.

6.6 : Etape n°6 : avertissement sur les conditions de poursuite des opérations

6.1 : La solution estime en unité de temps la charge induite par le choix de la stratégie de surcharge. Elle tient compte : 1- des performances de l'ordinateur traitant (puissance de son microprocesseur), 2- des caractéristiques du disque dur à traiter (capacité, vitesse de rotation, DMA), 3- de la stratégie et des options choisies.

6.2._ : La solution s'interrompt pour éditer le bilan des conditions de poursuite des opérations établi à partir des informations relevées entre les étapes n°2 et 6.

6.3.1 : La solution offre la possibilité de revenir sur le choix de la stratégie de surcharge.

6.3.2 : La solution offre la possibilité d'échapper à la poursuite du protocole ; c'est l'option par défaut en cas de mise en attente avec décompte de temps.

⁸ Pour contrôler la qualité de la documentation, voir au chapitre 6.10 les exigences concernant les stratégies et options de surcharge.

Exemple de bilan favorable :

BILAN DES CONDITIONS DE POURSUITE DES OPERATIONS

Opérateur : **Pierre DUPONT**
 Fonction : **technicien informatique**
 Organisme : **SGDN/...../BI**

Opération engagée le : **15/01/03 à 14h00**

Désignation du disque dur à traiter : **WD Caviar 36400**
 Modèle (P/N) : **AC36400-00LC**
 Numéro de série (S/N) : **WT 420 204 8826**
 Origine : **SINGAPORE**
 Date de construction : **19/06/98**
 Standard : **Enhanced IDE U DMA ATA 66**
 Configuration (cas des disques IDE) : **maître**
 Nombre de cylindres (C) : **13 328**
 Nombre de têtes (H) : **15**
 Nombre de secteurs (S) : **63**
 Taille des secteurs **512 octets**
 Sa capacité totale calculée est de : **6,4486 giga bit**
 Le disque contient des secteurs défectueux : **non**
 Ce modèle de disque est reconnu par la solution : **oui**
 De la mémoire cache a été repérée : **oui, elle peut être désactivée**
 Une partition à usage exclusif du système a été repérée : **non**
 Des partitions ont été repérées : **oui, elles peuvent être supprimées**
 Une fonction de tolérance aux pannes a été repérée : **non**

Le BIOS de l'ordinateur est une version : **AMIBIOS HIFLEX v1.19 connue**

Le système d'exploitation utilisé par la solution est **compatible** avec le disque dur et le BIOS

Le microprocesseur de l'ordinateur traitant est cadencé à : ... **400Mhz**

La stratégie de surcharge choisie est : **surcharge renforcée à huit passes avec application de chaque passe de surcharge sur tout le disque dur.**

La charge de traitement estimée est de : **10 heures**, sans interruption

Rappel :

L'opérateur doit prendre en compte les avertissements sur la légalité (étape n°2), la validité (étape n°3) et la pertinence (étape n°4) des opérations qu'il engage.

Mise en garde : l'opérateur est censé prendre connaissance attentivement de toutes les informations éditées ; il doit relever les incohérences (exemple : différence entre les informations C, H et S marquées sur le disque dur et celles relevées par la solution) et toutes autres indications signalant des faits susceptibles d'invalider le traitement.

6.7 : Etape n°7 : exécution des opérations de surcharge

- 7.1.1 : La solution désactive la mémoire cache du disque dur, s'il y en a.
- 7.1.2 : La solution désactive la fonction de tolérance aux pannes, s'il y en a.
- 7.1.3 : La solution ne tient pas compte des partitions ou les supprime, s'il y en a.
- 7.2.1 : La solution annonce l'opération prévue par la stratégie appliquée.

Exemple d'annonce :

Stratégie : **surcharge renforcée, option n°2,**
chaque passe de surcharge est appliquée au disque dur complet avant de passer à la suivante
Passe : 4 sur 8 Ecriture du motif : **0xFF**

- 7.2.2 : La solution exécute l'opération annoncée en comptant les caractères qu'elle écrit.
- 7.2.3 : La solution s'interrompt et annonce une défaillance s'il n'y a pas de correspondance entre le nombre de caractères écrits et la taille reconnue du disque dur (*voir 3.2.3*) ou du secteur traité.
- 7.2.4 : La solution relit le disque dur, ou le secteur traité, et compte les caractères lus.
- 7.2.5 : La solution s'interrompt et annonce une défaillance si elle lit un caractère autre que celui qu'elle vient d'écrire, ou s'il n'y a pas de correspondance entre le nombre de caractères relus et la taille reconnue du disque dur (*voir 3.2.3*) ou du secteur traité.

Exemple d'annonce :

Stratégie : **surcharge renforcée, option n°2,**
chaque passe de surcharge est appliquée au disque dur complet avant de passer à la suivante
Passe : 4 sur 8 Relecture du motif : **0xFF**

Un secteur contient des caractères autres que ceux écrits lors de la passe : 4.

La solution a détecté un dysfonctionnement.

Reprendre les opérations à partir du point 3.1 ou du point 7.1.1 ou ECHAPPER

- 7.2.6 : La solution revient au point 7.2.1 ou passe au point 8.1.1.
- 7.3 : Pendant l'exécution des opérations, la solution entretient une animation permettant à l'opérateur de suivre l'avancement de l'opération et de s'assurer de la charge du microprocesseur (charge CPU).

6.8 : Etape n°8 : contrôle final

- 8.1.1 : La solution vérifie l'état du disque dur (même procédé qu'à l'étape 3.2.7).
- 8.1.2 : La solution s'interrompt et annonce une défaillance si elle découvre un secteur défectueux.
- 8.2 : La solution remet le disque dur dans sa configuration d'origine, s'il y a lieu.

6.9 : Etape n°9 : rapport final

- 9._ : La solution affiche ou imprime un rapport d'activité sous la forme d'un procès verbal.

Exemple de procès verbal favorable :

PROCES VERBAL DE SURCHARGE D'UN DISQUE DUR	
Disque dur traité :	
Désignation du disque dur :	WD Caviar 36400
Modèle (P/N) :	AC36400-00LC
Numéro de série (S/N) :	WT 420 204 8826
Nombre de cylindres/têtes/secteurs :	13 328 / 15 / 63
De capacité totale :	6,4486 giga bit
Conditions du traitement :	
Le modèle de disque a été reconnu par la solution :	oui
De la mémoire cache a été repérée :	oui, elle a été désactivée
Une partition à usage exclusif du système a été repérée :	non
Des partitions ont été repérées :	oui, elles ont été supprimées
Une fonction de tolérance aux pannes a été repérée :	non
Le BIOS de l'ordinateur est une version :	connue
La stratégie appliquée a été :	la surcharge renforcée, option n°2
Le traitement a duré :	10 heures, sans interruption
Opérateur :	Pierre DUPONT
Fonction :	technicien informatique
Organisme :	SGDN/...../BI
Opération commencée le :	15/01/03 à 14h00
Toutes les opérations ont été exécutées dans un environnement maîtrisé. L'opérateur certifie avoir surveillé leur bon déroulement.	
<u>Visa de l'opérateur :</u>	<u>Visa de l'officier de sécurité :</u>
<i>(...autres champs : à paramétrer à la demande)</i>	
Destinataires :	
Monsieur le Chef du bureau informatique	
Monsieur l'Officier sécurité du système d'information (OSSI)	

6.10 : Stratégies et options de surcharge

Le choix de la stratégie et des options de surcharge relève de la recherche d'un équilibre coût/confiance pour un procédé qui, dans tous les cas, ne protégera pas au delà de la menace M2 (voir le guide [2] ou l'annexe n°2).

Trois degrés de liberté permettent de faire varier les stratégies et options de surcharge : 1- le choix de la méthode de parcours du disque dur à surcharger, 2- le choix du nombre d'opérations d'écriture, 3- le choix des motifs ou caractères à écrire.

Une **passé** est l'ensemble des opérations d'écriture et de lecture d'un caractère unique telles que décrites aux étapes 7.2.1 à 7.2.6. Une **passé** s'applique à tout ou partie du disque dur selon la méthode retenue.

1- Choix de la méthode de parcours du disque dur

10.1.m₁ : **Surcharge séquentielle** : la solution applique successivement chaque **passé** de surcharge à tout le disque dur.

Mise en garde : cette méthode n'est valide que si l'opérateur a les moyens de maintenir la tension électrique appliquée à la tête d'écriture à sa valeur nominale pendant tout le traitement ; une variation de cette tension est susceptible en effet de générer des surcharges inefficaces même si toutes les **passés** d'écriture et de lecture sont validées à la fin par la solution (étape n°9) ; il est recommandé d'alimenter l'ordinateur traitant avec une source électrique maîtrisée.

10.1.m₂ : **Surcharge saturante** : la solution applique successivement à chaque secteur du disque dur toutes les **passés** de surcharge.

Remarque : cette méthode vise à faire perdurer la phase de régime transitoire du courant qui circule dans les têtes ; l'effet escompté est l'augmentation du nombre de pics de tension autour de la valeur nominale de la tension appliquée aux têtes ; les opérations d'écriture qui surviennent lors d'une surtension (statistiquement la moitié des écritures) ont alors un pouvoir magnétisant supérieur aux opérations d'écriture effectuées en régime établi ; cet effet produit une « bavure » magnétique qui tend à compenser l'effet de gigue⁹ des têtes, et à camoufler mieux l'hystérésis magnétique des écritures anciennes.

Mise en garde : cette méthode n'est valide que si la solution a la capacité de repérer et désactiver les mémoires caches du disque dur.

Remarque : les deux stratégies m₁ et m₂ ne sont pas exclusives l'une de l'autre et peuvent être combinées.

2- Choix du nombre de **passés** d'écriture et des caractères à écrire

La solution propose plusieurs combinaisons de **passés** afin de permettre à l'opérateur de tirer le meilleur parti des moyens et des délais qui sont mis à sa disposition. La solution peut présenter un menu offrant tout ou partie des options suivantes.

⁹ Variations aléatoires du positionnement des têtes autour de la position nominale.

Surcharge standard

10.2.1 : Une passe d'écriture avec le caractère : 0x00.

Surcharges renforcées

Option n°1 :
(option par défaut¹⁰)

10.2.2.1 : Six passes d'écriture avec les caractères : 0x55, 0xAA, 0x00, 0xFF, 0x33, 0xCC.

Une dernière passe d'écriture avec le caractère : 0x00.

Option n°2 :

10.2.2.2 : Six passes d'écriture avec les caractères : 0x55, 0xAA, 0x00, 0xFF, 0x33, 0xCC.

Une passe d'écriture avec les caractères sortis d'un générateur pseudo-aléatoire de bonne qualité (chiffrement DES, RC4, hachages SHA ou MD5, etc.) initié par une semence d'aléa vrai.

Une dernière passe d'écriture avec le caractère : 0x00.

Option n°3 :

10.2.2.3 : Quatre passes d'écriture avec les caractères sortis d'un générateur pseudo-aléatoire de bonne qualité (chiffrement DES, RC4, hachages SHA ou MD5, etc.) initié par une semence d'aléa vrai.

Vingt sept passes d'écriture à l'aide des vingt sept motifs suivants pris dans un ordre aléatoire : 0x55, 0xAA, 0x924924, 0x492492, 0x249249, 0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88, 0x99, 0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF, 0x924924, 0x492492, 0x249249, 0x6DB6DB, 0xB6DB6D, 0xDB6DB6. L'ordre des passes est défini par le même générateur aléatoire que précédemment. Les motifs ne doivent pas être répétés.

Répétition : quatre passes d'écriture avec les caractères sortis d'un générateur pseudo-aléatoire de bonne qualité (chiffrement DES, RC4, hachages SHA ou MD5, etc.) initié par une semence d'aléa vrai.

Une dernière passe d'écriture avec le caractère : 0x00.

Remarques : Une **semence d'aléa vrai** est une suite binaire mise au point à partir d'un générateur d'aléas vrais tel qu'un générateur physique (générateur de bruits, etc.). Comme il est probable que l'ordinateur traitant possède un tel générateur, l'opérateur pourra être sollicité pour générer une suite aléatoire à partir d'opérations au clavier ou à la souris.

¹⁰ Cette option couvre les exigences du Department of Defense – USA (*ADP Security Manuel, DoD 5200.28*).

7 : APPLICATION DU SCHEMA

Ce schéma peut être utilisé pour préparer un candidat à la qualification et pour son examen.

Mettre en œuvre ce schéma au premier titre permet d'apprécier librement l'opportunité d'une candidature et de remédier à ses insuffisances éventuelles par des corrections ou des mesures particulières d'adaptation.

Mettre en œuvre ce schéma au titre d'un examen de qualification entend l'organisation d'un rendez-vous formel.

Le responsable de l'organisation de la sécurité des systèmes d'information mandaté par son autorité qualifiée¹¹ constitue une commission de qualification avec les experts qu'il juge nécessaires. Cette commission réunit trois personnes au moins : le responsable mandaté, l'administrateur informatique comptable des disques durs à traiter et un ou plusieurs experts. Les membres de la commission établissent rigoureusement leur référentiel d'exigences, puis prennent en compte et apprécient le candidat avec les mesures particulières d'adaptation qui l'accompagnent. En deçà de cinq membres, la commission travaille en suivant la règle du consensus. A partir de cinq membres, elle peut travailler par votes. Le rendez-vous se conclut sur une proposition de qualification, un ajournement ou une disqualification du candidat. La qualification d'une solution de surcharge est prononcée par l'autorité qualifiée¹³. Elle est annexée à la politique de sécurité du système d'information (PSSI) qui est mise à jour en conséquence.

La DCSSI est tenue informée des qualifications prononcées au sein de l'administration. Elle les valide en les inscrivant dans son *Catalogue des produits de sécurité des systèmes d'information pour l'administration*, sous la rubrique : *Solutions de surcharge de sécurité*. S'il advient qu'elle ait des réserves concernant une solution de surcharge qualifiée, elle en informe les ministères sans délai par la voie fonctionnelle SSI et met à jour le catalogue.

Reconnaissance des candidats certifiés

Il n'est pas nécessaire de mettre en œuvre ce schéma pour une solution de surcharge certifiée par la DCSSI conformément au décret [3]. Pour une telle solution, le responsable de l'organisation de la sécurité des systèmes d'information produit lui-même, aux vues de la cible de sécurité et du rapport de certification, un avis de qualification qui lui sert à mettre à jour le dossier d'homologation et la politique de sécurité de son système d'information.

Précaution avec le code des marchés publics

Le cahier des charges d'une opération d'achat d'une solution peut stipuler la certification telle que prévue par le décret [3] comme une exigence de la personne publique. Il ne peut pas indiquer la qualification comme critère de choix. Si le présent référentiel d'exigences et les conditions locales d'appréciation des candidats font parties du cahier des charges, la recette du produit livré pourra tenir lieu d'examen pour proposer immédiatement une qualification.

¹¹ Ou toute autre autorité ayant reçue, de l'autorité qualifiée, délégation pour tenir ce rôle.

ANNEXE N°1

Conditions d'appréciation

L'appréciation d'une solution de surcharge candidate pour la qualification est une activité à laquelle il convient de savoir fixer des règles et des limites.

L'appréciation peut être raisonnée, c'est à dire qu'elle s'appuie sur une méthode d'analyse à caractère scientifique, ou subjective, elle s'appuie alors sur l'avis d'un ou plusieurs experts.

Une appréciation raisonnée, ou évaluation, nécessite de disposer des spécifications de toutes les réponses attendues pour chaque exigence ; ces spécifications servent à établir la **conformité** du candidat au système de référence. Une évaluation nécessite aussi de pratiquer des tests, éventuellement agressifs, sur tous les éléments critiques ; ces tests permettent de mesurer l'**efficacité** des réponses proposées par le candidat. Les niveaux de conformité et d'efficacité atteints par le candidat visent à procurer une **assurance** sur la sécurité offerte. Cette assurance est d'autant plus élevée que les exigences sont élevées.

Le bon exemple d'appréciation raisonnée est l'évaluation selon les Critères Communs IS 15408¹² dans le cadre du décret [3]. C'est pourquoi il est recommandé d'engager les auteurs de solution de surcharge à faire certifier leur produit dans le cadre de ce décret. Le certificat est un critère de choix légitime que la personne publique peut invoquer pour discriminer les offres dans une opération de marché.

Une appréciation subjective, ou expertise, nécessite de réunir des spécialistes reconnus sur le sujet traité ; le niveau d'expertise nécessaire est celui de l'ingénieur informaticien spécialisé dans les équipements informatiques et sensibilisé à la sécurité. Ce schéma contient des tableaux et grilles conçus pour ces experts afin qu'ils puissent organiser rapidement leur examen et conclure.

Les grilles d'appréciation détaillées permettent aux examinateurs d'attribuer un statut à chaque réponse apportée par le candidat examiné, au regard des exigences. On distingue a priori six statuts :

- Doute : réponse impossible à apprécier au moment de l'examen.
- Absence : exigence non satisfaite au moment de l'examen.
- Présence déclarée et admise : l'examineur a confiance dans la déclaration de l'auteur de la réponse et ne vérifie pas sa conformité.
- Présence déclarée mais non crédible : l'examineur n'a pas confiance dans la déclaration de l'auteur de la réponse et n'a pas vérifié son existence ni sa conformité.
- Présence vérifiée et réponse validée : l'examineur a constaté la présence d'une réponse à l'exigence ; son expertise lui permet de considérer que cette réponse est suffisante.
- Présence vérifiée et réponse insuffisante : l'examineur a constaté la présence d'une réponse à l'exigence ; il considère que cette réponse est insuffisante.

¹² ISO/IEC International Standard 15408 : 1999 *Common Criteria for Information Technology Security (CC)*.

**Tableaux et grilles guides d'appréciation
des solutions de surcharge candidates
à la qualification de produit SSI**

Tableau guide n°1

Observations		Oui	Non
Le candidat est une réalisation logicielle du système décrit dans ce schéma (<i>chapitres 6.1 à 6.10</i>).		●	●
Le processus de développement du candidat est validé.		●	●
Conclusions			
La qualification du candidat peut être prononcée.		←	
Il est nécessaire d'engager un processus d'appréciation (<i>voir le tableau guide n°2</i>).			←

Tableau guide n°2

Observations		Oui	Non
Le protocole opératoire du candidat est disponible et comparable à celui du présent schéma (<i>voir l'organigramme au chapitre 5</i>).		●	●
Toutes les étapes sont implémentées. Leurs spécifications techniques, ou internes, sont disponibles.		●	●
Les étapes non implémentées donnent lieu à des mesures particulières documentées et soumises au processus d'appréciation.		●	●
Conclusions			
Le processus d'appréciation du candidat peut être engagé.		←	
Le processus d'appréciation du candidat ne peut pas être engagé.			←

Grilles d'appréciation détailléesLégende des grilles d'appréciation :

Marques	Signification
X	indique le statut d'une réponse apportée par le candidat à l'exigence considérée.
MP	indique le statut d'une réponse qui n'appartient pas au candidat ; il s'agit d'une mesure particulière (MP) appréciée en même temps que les autres réponses.

Cases	Signification
X	une case grise marquée gêne ou empêche la qualification de la solution.

Statuts	Signification
?	appréciation impossible.
abs	exigence non satisfaite.
pv	présence vérifiée d'une réponse.
rv	réponse validée (*).
ri	réponse insuffisante.
pd	présence déclarée d'une réponse.
ca	confiance accordée à la déclaration et à la réponse.
pc	pas de confiance accordée à la déclaration ou à la réponse.

Grille n°1

(Etape n°1 : mise en ordre de marche)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
1.1.0	Toute la documentation en français						
1.1.1	Documentation : conditions de mise en œuvre de la solution						
1.1.1.1	Avertissement sévère sur la stabilité de l'alimentation électrique ^(*)						
1.1.2	Documentation : caractéristique technique de la solution						
1.1.3	Documentation : déclaration de performances						
1.1.4	Documentation : manuel de l'utilisateur						
1.1.5	Documentation : conditions de garantie						
1.1.6	Documentation : condition d'accès à l'assistance technique						
1.2	Contrôle d'authenticité de la solution (MAC)						
1.3.1	Solution exécutable sans recours à l'OS de l'ordinateur traitant						
1.3.2	Documentation particulière pour l'amorçage à partir d'un CD-ROM						

(*) La tension électrique appliquée à la tête d'écriture doit impérativement rester à sa valeur nominale pendant tout le traitement. Une chute de cette tension est susceptible d'invalider le traitement même si toutes les passes d'écriture et de lecture sont validées par la solution. Il est nécessaire d'alimenter l'ordinateur traitant avec une source électrique stabilisée en tension (tolérance <3%) et en fréquence (tolérance <1%).

Grille n°2

(Etape n°2 : avertissement sur la légalité de l'action engagée)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
2.1	Interruption et avertissement sur la légalité de l'action engagée						
2.2	Echappement						
2.3.1	Enregistrement de la date et de l'heure du système (source BIOS)						
2.3.2	Enregistrement des éléments d'identification de l'opérateur						

Remarques : Si la solution ne réalise pas de façon logicielle l'étape n°2, une mesure de substitution doit l'accompagner. Cette mesure est à signaler en portant la marque *MP* à la ligne 2.1. Elle peut être un avertissement explicite placé en exergue dans le manuel de l'utilisateur. Le manuel doit aussi inviter l'opérateur à noter la date et l'heure de début des opérations. Tant qu'aucune opération de surcharge n'a commencé, l'arrêt brutal de l'ordinateur est l'option d'échappement d'urgence.

Grille n°3

(Etape n°3 : avertissement sur la validité des opérations de surcharge)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
3.1	Analyse de l'ordinateur traitant						
3.1.1	Analyse du BIOS						
3.1.2	Détection des performances (fréquence du CPU, ...)						
3.1.3	Détection des systèmes à redondance de disques durs (RAID)						
3.2	Analyse du disque dur à traiter						
3.2.1	Identification du standard (SCSI, IDE en position maître ou esclave)						
3.2.2	Détection des performances						
3.2.3	Reconnaissance de la taille						
3.2.4	Détection des caches mémoires						
3.2.5	Détection des partitions à usage exclusif du système courant						
3.2.6	Détection des fonction de tolérance aux pannes (SMART)						
3.2.7	Détection des zones défectueuses ^(*)						

	Heuristique						
3.3	Comparaison à une base d'informations évolutive et validée						
	ou						
3.3bis	Application d'un plan de tests validé						
	ou						
3.3ter	Tests et comparaison (combinaison des deux heuristiques précédentes)						
3.4	Enregistrement/édition de la signalétique et des réponses (cf. : §.6.3)						
3.5	Interruption et avertissement sur la validité des opérations de surcharge						
3.6	Echappement						

(*) Cette analyse est indispensable pour décider si le disque peut être traitée utilement ou non. Une zone (*cluster*) déclarée endommagée par le système d'exploitation est ensuite évitée lors des opérations d'écriture et de lecture. Elle peut pourtant contenir des données récupérables avec des outils de maintenance du commerce. C'est pourquoi, quand des zones défectueuses

sont repérées dans un disque dur, celui-ci doit être, a priori, considéré en panne. La règle n°2 de la mise en garde n°3 du guide [2] (*chapitre 7*) s'applique. Cette analyse présente une charge de temps importante, proportionnelle à la capacité du disque dur à traiter.

Remarques : Si la solution ne réalise pas de façon logicielle l'étape n°3, des mesures de substitution doivent obligatoirement l'accompagner. Elles sont à signaler en portant la marque *MP* sur les lignes concernées. Ces mesures doivent être capables de guider l'opérateur pas à pas pour qu'il effectue toutes les opérations d'analyse et de vérification que ne prend pas en charge la solution. Certaines de ces opérations nécessitent de la documentation avancée sur le disque dur à traiter et l'ordinateur traitant, de même que des outils de contrôles certifiés de l'état du disque dur à traiter. Sans cette documentation, ces outils et les compétences pour les exploiter, toute invitation à poursuivre les opérations de surcharge relève de la tromperie, voire de la malveillance.

Grille n°4

(Etape n°4 : avertissement sur la pertinence de l'action engagée)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
4.1	Interruption et avertissement sur la pertinence de l'action engagée						
4.2	Echappement						

Remarques : Si la solution ne réalise pas de façon logicielle l'étape n°4, une mesure de substitution doit l'accompagner. Cette mesure est à signaler en portant la marque *MP* à la ligne 4.1. Elle peut être un avertissement explicite placé en exergue dans le manuel de l'utilisateur.

Grille n°5

(Etape n°5 : choix de la stratégie et des options de surcharge)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
5.1	Interruption et menu						
5.2	Documentation des différentes stratégies offertes et choix						
5.3	Echappement						

Remarques : Si la solution ne réalise pas de façon logicielle l'étape n°5, une mesure de substitution doit l'accompagner. Cette mesure est à signaler en portant la marque *MP* à la ligne 5.1. L'objectif recherché à l'étape n°5 est que la stratégie appliquée par la solution soit bien celle que l'opérateur souhaite mettre en oeuvre. La solution peut, par exemple, être contenue dans une collection de supports (disquettes ou CD-ROM) telle que chaque support contienne une stratégie différente. Le choix du support à mettre en oeuvre correspond alors au choix qui peut être fait via une solution logicielle interactive.

Grille n°6

(Etape n°6 : avertissement sur les conditions de poursuite des opérations)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
6.1	Capacité d'estimation de la charge de temps des opérations à venir						
6.2.1	Edition : identification de l'opérateur						
6.2.2	Edition : date et heure de début des opérations						
6.2.3	Edition : identification et bilan du disque dur à traiter						
6.2.3.1	Identification commerciale du disque dur						
6.2.3.2	Affichage des paramètres CHS et de la capacité du disque dur						
6.2.3.3	Résultat de la détection des caches mémoires						
6.2.3.4	Résultat de la détection des partitions à usage exclusif du système						
6.2.3.5	Résultat de la détection des fonctions de tolérance aux pannes						
6.2.3.6	Résultat de la détection des zones défectueuses						
6.2.3.7	Edition : identification et performances du système traitant						
6.2.3.7	Résultat sur la compatibilité de la solution avec le système traitant						
6.2.3.8	Performances (fréquence du CPU, ...)						
6.2.3.9	Affichage de la charge de traitement estimée						
6.3.1	Possibilité de retourner à l'étape n°5.1						
6.3.2	Echappement						

Remarques : Si la solution ne réalise pas de façon logicielle l'étape n°6, des mesures de substitution doivent l'accompagner. Ces mesures sont à signaler par la marque *MP* sur toute les lignes du tableau ci-dessus qui font l'objet d'une mesure particulière de substitution. A défaut d'implémenter cette étape, la solution de surcharge candidate passe directement à l'étape n°7. L'absence d'interruption entre l'étape n°1 et 7 est susceptible de disqualifier la solution ou de la réserver aux spécialistes avertis.

Grille n°7

(Etape n°7 : exécution des opérations de surcharge)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
7.1.1	Capacité de désactivation de la mémoire cache du disque dur		(*)				
7.1.2	Capacité de désactivation des fonctions de tolérance aux pannes						
7.1.3	Capacité de s'affranchir de toutes les partitions						
7.2.1	Annonce de l'opération élémentaire à venir						
7.2.2	Passage d'écriture et comptage des caractères écrits						
7.2.3	Interruption et annonce d'un dysfonctionnement s'il n'y a pas de correspondance entre le nombre de caractères écrits et la taille reconnue du disque dur (voir : 3.2.3) ou du secteur traité						
7.2.4	A l'issue de la passe, relecture et comptage des caractères lus						
7.2.5	Interruption et annonce d'un dysfonctionnement si un caractère lu est différent de ceux qui viennent d'être écrits, ou s'il n'y a pas de correspondance entre le nombre de caractères lus et la taille reconnue du disque dur (voir : 3.2.3) ou du secteur traité						
7.3	Animation du traitement						

(*) Si cette capacité est absente, le candidat ne pourra pas être qualifié pour la stratégie de traitement secteur par secteur (voir le paragraphe 6.10 : *Stratégies et options de surcharge*).

Grille n°8
(Etape n°8 : contrôle final)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
8.1.1	Détection des zones défectueuses et relecture						
8.1.2	Interruption et annonce d'un dysfonctionnement si des secteurs défectueux sont découverts, ou si des caractères autres que 0x00 apparaissent						
8.2	Remise en configuration d'usine, s'il y a lieu						

Grille n°9
(Etape n°9 : rapport final)

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
9	Edition (affichage/impression) du procès verbal de surcharge						
9.1	Identification du disque dur traité						
9.2	Description des conditions du traitement						
9.3	Description du traitement appliqué						
9.4	Résultat du traitement						

Remarque : La qualification d'une solution n'apporte aucune garantie sur la qualité de l'environnement où elle est mise en œuvre. La qualité de l'environnement, de la mise en œuvre et de la surveillance du bon fonctionnement de la solution sont aussi nécessaires pour obtenir l'assurance d'un rapprochement de l'objectif de sécurité. C'est pourquoi, à la fin des opérations, il appartient à l'opérateur de s'engager sur la qualité de son action et des moyens qu'il a mis en œuvre.

Grille n°10
(les opérations de surcharges)

Il s'agit de reconnaître que les différentes opérations déclarées implémentées dans la solution sont effectivement présentes et mises en œuvre correctement aux cours des traitements.

N°	Exigences	Réponses					
		?	abs	pv		pd	
				rv	ri	ca	pc
10.1.m ₁	Application successive des passes à tout le disque dur						
10.1.m ₂	Application secteur par secteur de toutes les passes de surcharge						
10.2.1	Application d'une surcharge standard						
10.2.2.1	Application d'une surcharge renforcée, option n°1						
10.2.2.2	Application d'une surcharge renforcée, option n°2						
10.2.2.3	Application d'une surcharge renforcée, option n°3						

Remarques : Il est peut probable que les responsables de l'organisation de la sécurité des systèmes d'information puissent expertiser le code source d'un candidat ou faire des investigations sur les plateaux pour mesurer la qualité des surcharges. Dans les cas où ils ne sauraient accorder immédiatement leur confiance au candidat, il leur est recommandé d'avoir recours à une évaluation selon les Critères Communs.

ANNEXE N°2

Extraits du guide [2] et compléments juridiques

Définition (extrait du guide[2]) :

Disque dur : système constitué d'un ou plusieurs supports magnétiques, appelés **plateaux**, et d'un sous système, appelé **têtes**, composé d'éléments mécaniques, électroniques et logiques, qui effectue les transcriptions, l'écriture et la lecture des données.

Les menaces (extrait du guide[2]) :

[M1] Accès logique aux données en utilisant des droits «utilisateur » et les commandes du système d'exploitation courant.

[M2] Accès logique aux données en utilisant des droits «administrateur » et les commandes du système d'exploitation courant, ou en utilisant des commandes «bas niveau » d'un système d'exploitation connu.

[M3] Accès logique aux données en utilisant un programme spécial capable de prendre le contrôle des têtes du disque dur attaqué.

[M4] Accès physique aux signaux analogiques et reconstitution des données.

[M5] Accès physique aux traces et reconstitution des données.

Extraits du code pénal :

Article 226-17

(Ordonnance n° 2000-916 du 19/09/00)

Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 €d'amende.

Article 413-9

(Loi n° 94-89 du 01/02/94)

Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion.

Peuvent faire l'objet de telles mesures les renseignements, procédés, objets, documents, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat.

Article 413-10

(Ordonnance n° 2000-916 du 19/09/00)

Est puni de sept ans d'emprisonnement et de 100 000 € d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé détruire, détourner, soustraire, reproduire ou divulguer le renseignement, procédé, objet, document, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45 000 € d'amende.

Article 413-11

(Ordonnance n° 2000-916 du 19/09/00)

Est puni de cinq ans d'emprisonnement et de 75 000 € d'amende le fait, par toute personne non visée à l'article 413-10 de :

- 1°- S'assurer la possession d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui présente le caractère d'un secret de la défense nationale ;
- 2°- Détruire, soustraire ou reproduire, de quelque manière que ce soit, un tel renseignement, procédé, objet, document, donnée informatisée ou fichier ;
- 3°- Porter à la connaissance du public ou d'une personne non qualifiée un tel renseignement, procédé, objet, document, donnée informatisée ou fichier.

Article 413-12

La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines.