

PREMIER MINISTRE

Secrétariat général  
de la défense  
nationale

Paris, le 6 janvier 2004

000007/SGDN/DCSSI/SDR  
Référence : CCN-MQ.01

*Direction centrale de la  
sécurité des systèmes  
d'information*

MANUEL QUALITE DU CENTRE DE CERTIFICATION VERSION 1.0

Objet : Manuel qualité du centre de certification version 1.0

Application : A compter du 1<sup>er</sup> janvier 2004

Diffusion : Publique

Vérifié par	Validé par	Vu l'avis du comité directeur Approuvé par Le Directeur central de la sécurité des systèmes d'information
<u>Le responsable qualité</u> ORIGINAL SIGNE	ORIGINAL SIGNE	ORIGINAL SIGNE
<u>Le chef du centre de certification</u> ORIGINAL SIGNE		

## Suivi des modifications

<b>Révision</b>	<b>Date</b>	<b>Modifications</b>
1.0	01/12/2003	Création

## TABLE DES MATIERES

<b>Chapitre 1 Engagement de la direction .....</b>	<b>5</b>
<b>Chapitre 2 Généralités.....</b>	<b>6</b>
2.1. La sécurité des technologies de l’information en France .....	6
2.2. Sécurité et qualité.....	6
<b>Chapitre 3 Le manuel qualité .....</b>	<b>7</b>
3.1. Objet du manuel .....	7
3.2. Elaboration, mise à jour et diffusion.....	7
<b>Chapitre 4 Le schéma de certification .....</b>	<b>8</b>
4.1. Contexte réglementaire .....	8
4.2. Le comité directeur de la certification .....	8
4.3. Le centre de certification .....	8
4.3.1. Statut .....	8
4.3.2. Impartialité.....	8
4.3.3. Organisation.....	9
4.3.4. Responsabilités.....	9
4.3.5. Personnel du centre de certification.....	10
<b>Chapitre 5 Système qualité .....</b>	<b>11</b>
5.1. Politique qualité .....	11
5.1.1. Objectif.....	11
5.1.2. Exigences.....	11
5.1.3. Moyens .....	11
5.2. Système qualité .....	11
5.3. Responsable qualité .....	12
5.4. Planification de la qualité .....	12
5.4.1. Revues de direction .....	12
5.4.2. Groupe de pilotage de la qualité.....	12
5.4.3. Audits internes.....	12
5.5. Architecture documentaire.....	13
5.5.1. Structure documentaire .....	13
5.5.2. Maîtrise de la documentation.....	13
5.5.3. Enregistrements liés à la certification.....	14
<b>Chapitre 6 Modalités de la certification .....</b>	<b>15</b>
6.1. Accès et traitement non discriminatoires.....	15
6.2. Documents de référence.....	15
6.3. Critères d’évaluation.....	15
6.4. Modification des exigences de certification .....	15
<b>Chapitre 7 Demande de certification .....</b>	<b>17</b>
7.1. Contenu du dossier d’évaluation.....	17
7.2. Enregistrement de la demande .....	17
<b>Chapitre 8 Evaluation.....</b>	<b>18</b>
8.1. Les centres d’évaluation .....	18
8.1.1. Rôles et responsabilités.....	18
8.1.2. Procédure d’agrément.....	18
8.2. Réalisation des travaux d’évaluation par le centre d’évaluation .....	18
8.3. Le Rapport Technique d’Evaluation.....	19
<b>Chapitre 9 Certification .....</b>	<b>20</b>
9.1. Préambule.....	20
9.2. Rapport de certification .....	20

9.3. Décision de certification .....	20
9.4. Publication du certificat .....	20
9.5. Annulation du certificat .....	20
<b>Chapitre 10 Utilisation du certificat .....</b>	<b>21</b>
10.1. Règles de communication .....	21
10.2. Règles d'utilisation de la marque .....	21
<b>Chapitre 11 Surveillance et maintenance .....</b>	<b>22</b>
11.1. Surveillance.....	22
11.2. Maintenance.....	22
11.3. Surveillance ou maintenance ?.....	22
<b>Chapitre 12 Confidentialité des informations traitées .....</b>	<b>23</b>
12.1. Accès aux locaux .....	23
12.2. Accès aux informations.....	23
<b>Chapitre 13 Anomalies, réclamations .....</b>	<b>24</b>
13.1. Au près du centre de certification .....	24
13.1.1. Enregistrement et traitement.....	24
13.1.2. Litiges.....	24
13.2. Au près des commanditaires .....	24
<b>Annexe A Documents de référence.....</b>	<b>25</b>
<b>Annexe B Définitions et acronymes.....</b>	<b>27</b>
<b>Annexe C Table de correspondance avec la norme NF EN 45011:1998 .....</b>	<b>28</b>

# Chapitre 1

## Engagement de la direction

### Déclaration du Directeur central de la sécurité des systèmes d'information

Nos trois objectifs fondamentaux, en matière de qualité de certification, sont :

- garantir la rigueur et l'impartialité de nos méthodes,
- garantir la confidentialité des informations qui nous sont confiées dans le cadre des évaluations,
- assurer la conformité de nos activités aux normes internationales pour assurer la reconnaissance de nos certificats à l'extérieur de nos frontières.

Je m'engage à mettre en œuvre les moyens nécessaires à la réalisation de ces objectifs et je veillerai à ce que soient respectées les dispositions du système qualité décrites dans le manuel qualité et dans la documentation associée.

Ces dispositions comprennent notamment l'évaluation régulière de l'efficacité et de la pertinence du système qualité, afin d'en permettre l'amélioration continue : la sécurité des technologies de l'information est un domaine en évolution constante et rapide, aussi, chacun doit participer à l'adaptation des pratiques.

Les actions engagées seront vérifiées lors des revues de direction au cours desquelles le plan qualité sera analysé en vue de définir les objectifs à atteindre. La qualité doit progresser dans les domaines technique et administratif. Cet engagement concerne l'ensemble du personnel du centre de certification.

J'apporterai tout mon soutien au centre de certification pour atteindre les objectifs fixés. Le sous-directeur régulation a pour mission de m'assister dans cette tâche et je délègue la gestion opérationnelle du système qualité au chef du bureau certification.

Paris, le 6 janvier 2004

Le Directeur central de la sécurité des systèmes  
d'information  
Henri Serres

ORIGINAL SIGNE

## Chapitre 2

### Généralités

#### 2.1. *La sécurité des technologies de l'information en France*

La montée de la menace, en particulier dans le domaine informatique, et la nécessité d'une coordination entre les secteurs gouvernemental et commercial ont conduit le Gouvernement à créer, dès 1986, une organisation spécifique chargée de la sécurité des technologies de l'information en France.

L'organisation nationale comprend les instances et les organismes suivants :

- la *Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI)*, présidée par le Secrétaire général de la défense nationale, a pour mission d'assurer la concertation entre les départements ministériels sur les questions relatives à la sécurité des systèmes d'information ;
- le *Secrétariat Général de la Défense Nationale*, placé sous l'autorité du Premier ministre, veille à la cohérence des actions entreprises en matière de sécurité des systèmes d'information dans le cadre de la politique définie par le Gouvernement ;
- la *Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI)*, placée sous l'autorité du Secrétaire général de la défense nationale, est chargée, en particulier, d'apprécier le niveau de protection des systèmes d'information et d'entretenir les relations avec ses homologues étrangers.

#### 2.2. *Sécurité et qualité*

La généralisation de l'usage des moyens informatiques et de télécommunications augmente la vulnérabilité de l'information. Il est donc indispensable de renforcer les mesures de sécurité de l'information de manière à assurer :

- sa *confidentialité*,
- son *intégrité*,
- sa *disponibilité ou celle du système*.

La protection offerte par un produit ou par un système est assurée par des mesures techniques complétées éventuellement par des mesures physiques, organisationnelles ou relatives au personnel. Les mesures techniques peuvent faire l'objet d'une évaluation pouvant donner lieu à une certification.

La démarche qualité a pour but d'assurer la traçabilité des travaux réalisés, d'harmoniser les pratiques et d'assurer le niveau de rigueur requis pour la certification.

## Chapitre 3

### Le manuel qualité

#### 3.1. *Objet du manuel*

Le manuel qualité a pour objet de présenter les méthodes et les procédures du centre de certification en vue d'assurer et de maintenir la qualité et la continuité de ses prestations en matière de certification de la sécurité des produits et des systèmes des technologies de l'information.

Le manuel qualité constitue la référence pour :

- toute personne ou entité de la DCSSI exerçant une fonction relative à l'activité de certification, quant à son rôle et à ses responsabilités ;
- toute personne nouvellement recrutée, pour l'informer de la politique de la DCSSI et faciliter son intégration ;
- l'évaluation réciproque entre la DCSSI et les autres organismes, étrangers notamment, en vue d'une reconnaissance mutuelle.

#### 3.2. *Elaboration, mise à jour et diffusion*

Le manuel est élaboré par le responsable qualité, vérifié par le chef du centre de certification, validé par le sous-directeur « Régulation » puis approuvé par le Directeur central de la sécurité des systèmes d'information. Il est soumis à l'avis du comité directeur de la certification.

L'opportunité de mise à jour du manuel est examinée une fois par an.

Les mises à jour du manuel qualité suivent le circuit de validation de la rédaction initiale.

Le responsable qualité assure la diffusion du manuel qualité : les règles de diffusion du manuel sont les mêmes que celles des autres documents du système qualité.

Toutes les versions sont conservées sous forme électronique. Toutefois, la version française originale sous forme papier constitue la version de référence.

## Chapitre 4

### Le schéma de certification

#### 4.1. Contexte réglementaire

Le 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 précise le contexte réglementaire et l'organisation nécessaire à la conduite d'une évaluation par une tierce partie et à son contrôle, conduisant à la délivrance de certificats.

Ces règles sont mises en œuvre dans un schéma de certification tierce partie.

#### 4.2. Le comité directeur de la certification

L'article 15 du décret 2002-535 indique que le comité directeur de la certification en sécurité des technologies de l'information a pour mission :

- de formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;
- d'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;
- d'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;
- d'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers.

Le comité directeur se réunit au moins une fois par an. Il est présidé par le Secrétaire général de la défense nationale ou son représentant. Il rapporte au Premier ministre.

#### 4.3. Le centre de certification

##### 4.3.1. Statut

La DCSSI, créée par le décret n° 2001-693 du 31 juillet 2001, instruit les certifications.

La DCSSI est placée sous l'autorité du Secrétaire général de la défense nationale. Elle comprend plusieurs sous-directions et bureaux, conformément à l'arrêté du 15 mars 2002 portant organisation de la direction centrale de la sécurité des systèmes d'information, parmi lesquels se trouve le centre de certification.

##### 4.3.2. Impartialité

Deux éléments principaux concourent à l'indépendance du centre de certification :

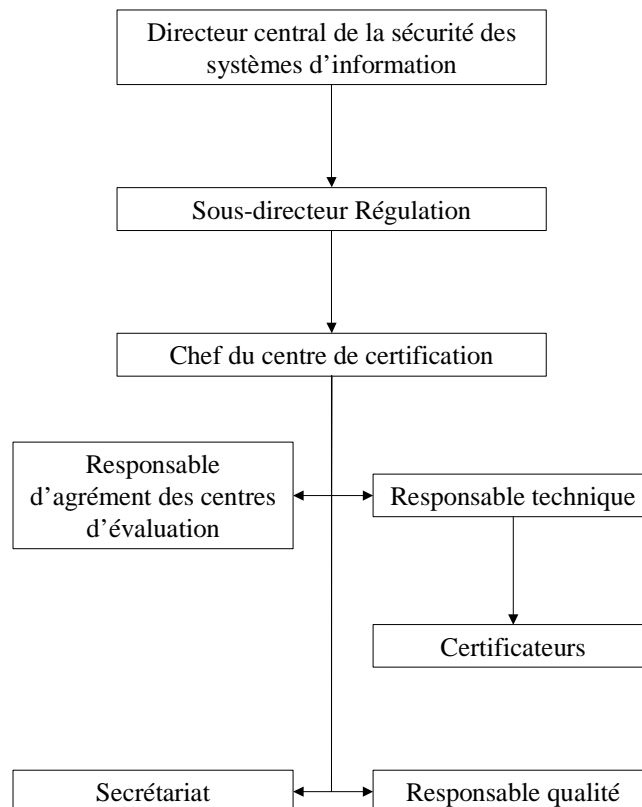
- son statut d'administration ;
- ses ressources financières, assurées par l'État, qui contribuent à consolider cette indépendance. La certification est, jusqu'à notification contraire, libre du paiement de tout droit.

Par son statut, le centre de certification n'a aucun engagement contractuel, au sens commercial du terme, avec ses partenaires impliqués dans le processus de certification : commanditaire, centre d'évaluation ou développeur.

Par ailleurs, le centre de certification ne fournit pas de prestations de conseil ou de formation visant à l'obtention ou au maintien d'une certification.

De plus, il est soumis à la décision de la Commission européenne 2000/709/CE du 6 novembre 2000 pour les organismes nationaux chargés d'évaluer la conformité des dispositifs sécurisés de création de signature.

### 4.3.3. Organisation



### 4.3.4. Responsabilités

Les rôles et responsabilités pour l'activité de certification sont répartis de la façon suivante :

- **Le Directeur central de la sécurité des systèmes d'information** a délégation du Premier ministre pour signer les certificats.
- **Le Sous-directeur Régulation** a autorité sur le centre de certification.
- **Le chef du centre de certification** a pour fonction la gestion opérationnelle du centre de certification. Il participe au recrutement de son personnel et s'assure de sa compétence pour les fonctions occupées en tenant à jour un dossier relatif à l'expérience et à la formation du personnel. Il est responsable de la définition de la procédure d'agrément des centres d'évaluation. Il s'assure de la reconnaissance des certificats à l'extérieur des frontières et entretient les relations avec ses homologues étrangers. Il participe à la gestion des critères d'évaluation et de certification. Il est responsable de la proposition de certification (positive ou négative) qu'il transmet pour décision à la Direction.  
Il est également chargé de la gestion du système qualité.

- **Le responsable technique** a pour fonction d'assurer le fonctionnement technique quotidien du système de certification. Il forme les certificateurs, assure un contrôle régulier de leurs compétences et gère leur plan de charge. Il instruit les demandes de certification puis suit l'ensemble des dossiers de certification afin d'assurer l'homogénéité technique de l'ensemble. Il valide techniquement les rapports de certification.
- **Le responsable d'agrément des centres d'évaluation** est chargé du suivi, du contrôle et de la formation continue des centres d'évaluation.
- **Le responsable qualité** est chargé de la mise en place, de la maintenance et de l'amélioration du système qualité. Il assure également la formation qualité du personnel du centre de certification.
- **Les certificateurs** sont chargés de suivre les évaluations afin de vérifier le respect des règles et procédures de certification. Ils n'interviennent ni dans les travaux d'évaluation, ni dans la décision finale de certification.
- **Le secrétariat** est attaché à la sous-direction Régulation. Il participe en particulier aux procédures de réception et d'envoi du courrier du centre de certification.

#### 4.3.5. Personnel du centre de certification

Le recrutement et le suivi de la qualification du personnel du centre de certification font l'objet d'une procédure<sup>1</sup>.

On distingue notamment deux niveaux de qualification parmi les certificateurs :

- le niveau « confirmé » qui permet d'effectuer les activités de certification sous sa propre responsabilité ;
- le niveau « junior » qui nécessite d'effectuer ces activités sous la responsabilité de certificateurs « confirmés ».

Le centre de certification n'emploie pas de personnel temporaire pour les activités de certification.

---

<sup>1</sup> Procédure PER/P/01 « Recrutement et qualification du personnel »

## Chapitre 5

# Systeme qualite

### 5.1. Politique qualite

#### 5.1.1. Objectif

Le centre de certification evolue dans un milieu ou confiance, rigueur et continuite prennent tout leur sens. De par l'etendue geographique de ses activites et la dispersion culturelle de ses clients, le centre de certification doit, au travers de son systeme qualite, donner la plus grande confiance dans les travaux qu'il mene afin d'assurer la reconnaissance de ses certificats, notamment en raison du cadre international dans lequel il s'inscrit.

Ses objectifs sont axes sur la reconnaissance des certificats emis :

- une reconnaissance nationale, pour etablir la confiance dans les travaux de certification qu'il mene aupres de toutes les parties concernes ;
- une reconnaissance internationale, afin d'entrer dans le cadre des accords de reconnaissance mutuelle sur lesquels il s'engage.

#### 5.1.2. Exigences

Pour obtenir et conserver durablement cette reconnaissance, le centre de certification doit prouver qu'il repond aux exigences suivantes :

- traçabilité : toute evaluation doit etre reproductible et l'ensemble des elements de preuves lie a la delivrance du certificat doit etre identifie et conserve ;
- continuite : le centre de certification doit pouvoir assurer ses missions quels que soient les changements internes (organisation, personnel) ;
- homogeneite : les certificats doivent rendre compte d'un niveau d'assurance comparable, quel que soit le personnel charge du suivi et quel que soit le centre d'evaluation qui a mene l'evaluation ;
- confidentialite : le centre de certification doit assurer le respect de la confidentialite des informations sensibles qui lui sont confiees ou qu'il elabore dans le cadre de la certification.

Se conformer au referentiel NF EN 45011 :1998 « Exigences generales relatives aux organismes procedant a la certification de produits » est un moyen de garantir le respect de ces exigences.

#### 5.1.3. Moyens

Le centre de certification, pour satisfaire ces exigences, dispose d'un schema d'evaluation par une tierce partie de confiance, de personnels competents au centre de certification ainsi que dans les centres d'evaluation.

### 5.2. Systeme qualite

Le systeme qualite se veut conforme a la norme NF EN 45011 et respecte les textes reglementaires qui instituent les missions du centre de certification.

Le centre de certification s'engage à :

- publier et tenir à jour les règles et exigences relatives au schéma d'évaluation et de certification ;
- publier et tenir à jour la liste des certificats et des centres d'évaluation agréés.

La DCSSI s'engage à :

- s'assurer de la compétence des centres d'évaluation qui procèdent à l'évaluation des produits ;
- n'agréer que des laboratoires accrédités selon la norme ISO/IEC 17025 pour les travaux entrant dans le cadre du décret 2002-535 ;
- travailler avec du personnel compétent et qualifié.

Les membres du centre de certification s'engagent enfin à respecter la confidentialité des informations sensibles échangées dans le cadre du schéma d'évaluation et de certification de la sécurité des technologies de l'information.

### **5.3. Responsable qualité**

Le responsable qualité est chargé de :

- assurer que le système qualité est défini, mis en œuvre et respecté à tous les niveaux concernés du centre de certification et maintenu conforme aux exigences applicables ;
- assurer la formation qualité du personnel et vérifier régulièrement ses connaissances ;
- rendre compte des performances du système à la direction pour effectuer une revue et servir de base à l'amélioration permanente.

### **5.4. Planification de la qualité**

#### **5.4.1. Revues de direction**

Les revues sont assurées lors d'une réunion annuelle organisée par le Directeur central de la sécurité des systèmes d'information et tenue en début d'année<sup>2</sup>.

Le compte-rendu des revues de direction est rédigé par le responsable qualité et diffusé aux personnes concernées.

#### **5.4.2. Groupe de pilotage de la qualité**

Un groupe de pilotage de la qualité assure la mise en œuvre et le suivi du système qualité<sup>3</sup>.

#### **5.4.3. Audits internes**

Des audits périodiques du système qualité sont organisés par le chef du centre de certification et conduits par des auditeurs qualifiés et indépendants des fonctions auditées<sup>4</sup>.

Le responsable qualité planifie et gère les audits de manière à ce que toutes les exigences de la norme NF EN 45011 soient auditées au moins une fois par an.

---

<sup>2</sup> Procédure QUA/P/01 « Revues de Direction »

<sup>3</sup> Procédure QUA/P/02 « Groupe de pilotage de la qualité »

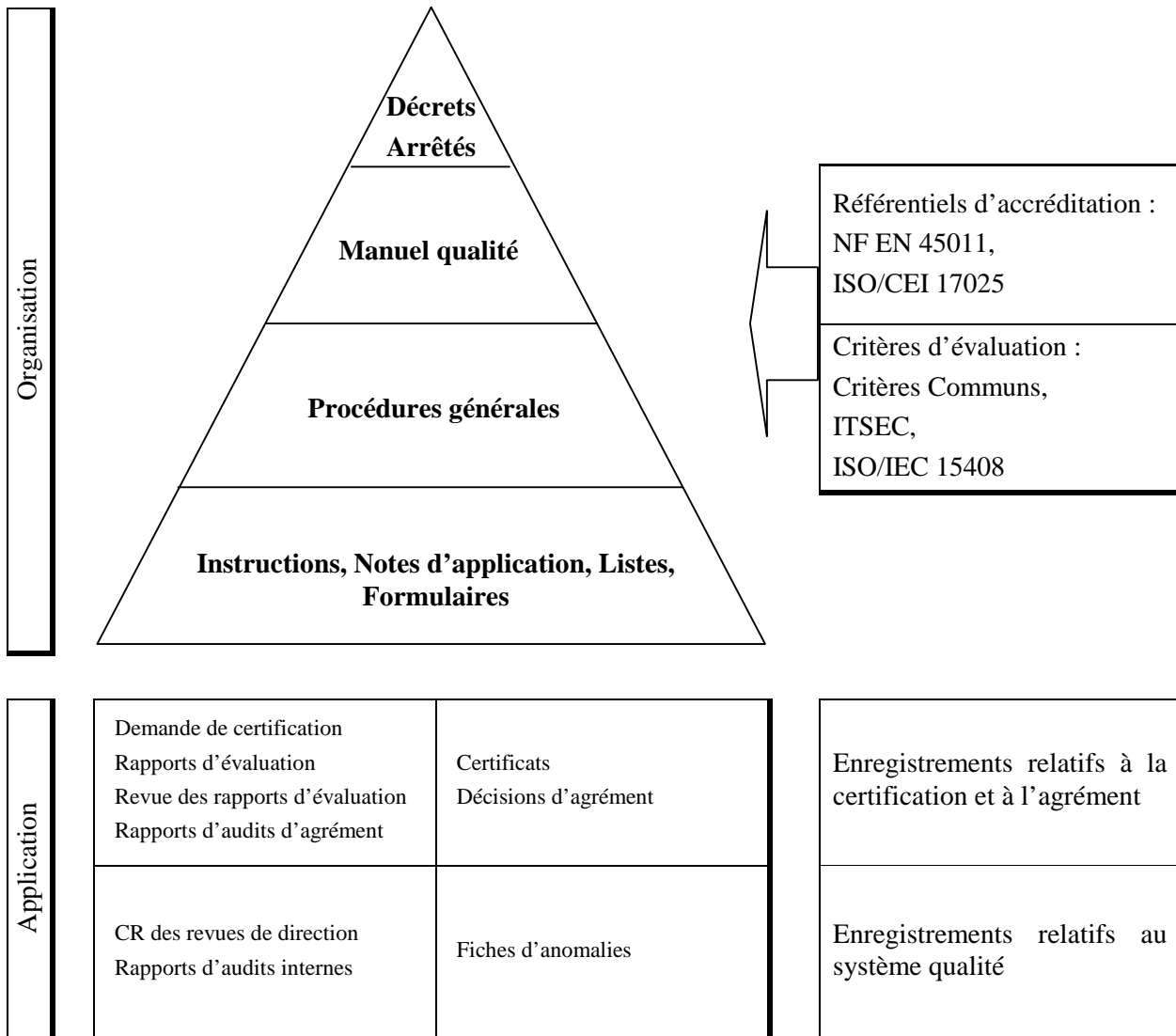
<sup>4</sup> Procédure QUA/P/03 « Audits internes »

## 5.5. Architecture documentaire

Le centre de certification dispose d'une collection documentaire couvrant l'ensemble de l'activité de certification.

### 5.5.1. Structure documentaire

La structure de cette collection documentaire est la suivante :



### 5.5.2. Maîtrise de la documentation

Le centre de certification possède des règles d'élaboration et de maîtrise de la documentation liées à son activité de certification<sup>5</sup>.

Le responsable qualité tient à jour la liste de tous ces documents qualité établis par le centre de certification.

<sup>5</sup> Procédure DOC/P/01 « Elaboration et mise à jour des documents »

### **5.5.3. Enregistrements liés à la certification**

La gestion des enregistrements liés à la certification dépend de leur nature et de la procédure à laquelle ils se rapportent. Par conséquent, la gestion des enregistrements est définie dans chaque procédure concernée.

Il existe deux sortes d'enregistrements démontrant que toutes les procédures et instructions relatives à l'activité de certification ont bien été appliquées :

- les enregistrements sur support papier conservés au centre de certification ou dans un local d'archives,
- les enregistrements stockés sur support informatique.

Le responsable qualité est garant de la conservation et de la sauvegarde de tous les enregistrements.

## Chapitre 6

### Modalités de la certification

#### 6.1. Accès et traitement non discriminatoires

Tous les développeurs et fournisseurs de produits ou de systèmes des technologies de l'information ont accès aux services de certification de la DCSSI.

La DCSSI veille à l'égalité de traitement entre les différents produits ou systèmes soumis à la certification.

L'attribution de la certification n'est subordonnée qu'au respect des règles de fonctionnement du schéma et à la satisfaction des critères d'évaluation.

#### 6.2. Documents de référence

L'ensemble des documents relatifs à la certification est disponible sur le site Internet de la DCSSI : [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

Ces documents sont notamment :

- les textes réglementaires relatifs à la certification de la sécurité des produits et des systèmes des technologies de l'information,
- les documents de fonctionnement (procédures, instructions ou notes d'application) du centre de certification,
- les critères d'évaluation.

#### 6.3. Critères d'évaluation

Les critères et méthodologies d'évaluation utilisés sont approuvés par le comité directeur de la certification.

Ces critères d'évaluation sont susceptibles d'évoluer ou d'être complétés par des guides techniques en fonction de la technologie considérée ou de contextes particuliers.

#### 6.4. Modification des exigences de certification<sup>6</sup>

Les exigences relatives à la certification peuvent être amenées à évoluer dans le temps.

Ces évolutions peuvent être :

- des évolutions des critères d'évaluation provenant des instances normatives internationales, européennes ou nationales : dans ce cas, ces évolutions sont directement disponibles sur les sites Internet de ces instances de normalisation ;
- des adaptations des exigences pour un domaine particulier : ces adaptations sont notifiées par une note d'application du schéma qui précise le délai d'application ;

---

<sup>6</sup> Procédure MOD/P/01 « Modification des exigences de certification »

- des évolutions des pratiques ou du fonctionnement du schéma de certification : ces évolutions peuvent nécessiter de recueillir l'avis du comité directeur de la certification en cas d'évolution majeure.

## Chapitre 7

### Demande de certification

#### 7.1. Contenu du dossier d'évaluation

Le commanditaire, après avoir sélectionné un centre d'évaluation, demande l'ouverture d'un dossier de certification au centre de certification par le biais d'un dossier d'évaluation (formulaire CER/F/01 : Dossier d'évaluation).

Le dossier d'évaluation comprend :

- les conditions générales de la certification,
- une description du produit ou du système à évaluer (incluant sa cible de sécurité),
- le programme de travail prévisionnel élaboré par le centre d'évaluation lors de la préparation de l'évaluation.

#### 7.2. Enregistrement de la demande

Dès réception du dossier d'évaluation, le centre de certification :

- procède à une revue documentaire approfondie, notamment pour ce qui concerne la cible de sécurité et le programme de travail prévisionnel ;
- s'il estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, il notifie au commanditaire qu'il ne pourra pas en l'état du dossier procéder à la certification envisagée ;
- indique le nom du certificateur désigné pour assurer le suivi de l'évaluation.

Par défaut, l'existence même de l'évaluation est considérée comme confidentielle par le centre de certification. L'évaluation ne fait donc l'objet d'aucune publicité par le centre de certification.

## Chapitre 8

### Evaluation

#### 8.1. Les centres d'évaluation

##### 8.1.1. Rôles et responsabilités

Les centres d'évaluation réalisent les évaluations : ils agissent en tant que tierce partie indépendante des développeurs de produits et des commanditaires.

Les centres d'évaluation sont agréés par la DCSSI et, à ce titre, sont tenus de respecter toutes les règles du schéma<sup>7</sup>.

Les centres d'évaluation sont constitués d'équipes d'experts et de responsables, intégrés le plus souvent dans un organisme à vocation plus large. Toutefois, les critères d'agrément imposent un cloisonnement vis-à-vis des autres activités de l'organisme auquel le centre d'évaluation est rattaché.

Un centre d'évaluation doit être impartial et indépendant de toute pression extérieure. Il ne doit en aucun cas être impliqué dans le développement (y compris à titre de conseil) et l'évaluation d'un même produit. Cependant il peut proposer des prestations de conseil, qui ne devront en aucun cas affecter son impartialité dans le cadre des évaluations qu'il est amené à conduire.

##### 8.1.2. Procédure d'agrément

Les critères d'agrément comprennent, entre autres, l'accréditation du centre d'évaluation par le COFRAC (comité français d'accréditation) selon la norme ISO/CEI 17025 « Prescriptions générales concernant la compétence des laboratoires d'étalonnage et d'essais ». Des guides techniques d'accréditation, élaborés par le COFRAC, précisent le domaine particulier de l'évaluation de la sécurité des technologies de l'information.

L'agrément impose des exigences complémentaires qui permettent de s'assurer de la maîtrise par le laboratoire de certaines techniques particulières ainsi que de sa capacité à traiter des informations sensibles.

L'agrément d'un centre d'évaluation est ensuite accompagné d'une procédure de suivi qui permet de s'assurer de la pérennité du respect des exigences d'agrément au sein du centre d'évaluation.

#### 8.2. Réalisation des travaux d'évaluation par le centre d'évaluation

Le centre d'évaluation mène les travaux d'évaluation conformément aux critères d'évaluation choisis et au plan de travail prévisionnel. Ces travaux sont suivis par le centre de certification.

Le commanditaire de l'évaluation est responsable de la livraison des fournitures nécessaires à l'évaluation. La liste exacte des fournitures à livrer au centre d'évaluation et au centre de certification dépend des critères d'évaluation choisis. La liste est spécifiée dans le dossier d'évaluation.

Le centre d'évaluation analyse le produit ou le système et sa documentation afin de vérifier que les exigences spécifiées dans les critères d'évaluation sont satisfaites. Certains critères d'évaluation peuvent exiger une visite des sites de développement ou de production du produit ou du système à évaluer.

Lorsqu'une tâche d'évaluation est terminée, un rapport de fin de tâche est émis à destination du certificateur et du commanditaire.

---

<sup>7</sup> Procédure AGR/P/01 « Agrément des centres d'évaluation »

### **8.3. *Le Rapport Technique d'Evaluation***

Lorsque toutes les tâches d'évaluation ont été menées par le centre d'évaluation, l'évaluation est considérée comme terminée.

Le centre d'évaluation rédige alors le rapport technique d'évaluation (RTE) qu'il transmet au centre de certification et au commanditaire.

Ce rapport décrit les travaux effectués lors de l'évaluation et expose les résultats obtenus.

Le RTE contient des données sensibles couvertes par le secret industriel et commercial. Sa diffusion est contrôlée : les clauses de confidentialité sont définies contractuellement entre le centre d'évaluation et le commanditaire lors de la phase de préparation de l'évaluation.

## Chapitre 9

# Certification

### 9.1. *Préambule*

La certification est un processus global qui permet, par un ensemble d'actions, de s'assurer que l'évaluation s'est déroulée avec la compétence et l'impartialité requises<sup>8</sup>.

### 9.2. *Rapport de certification*

Après examen du RTE, le certificateur rédige un rapport de certification qui propose ou refuse la certification. Le rapport de certification est, avec la cible de sécurité, le seul document qu'un acheteur potentiel est normalement amené à consulter.

Le rapport de certification décrit fidèlement le produit ou le système évalué et recommande éventuellement la mise en œuvre de mesures nécessaires à une utilisation sûre du produit ou du système certifié. Si la certification est refusée, le rapport précise l'ensemble des non-conformités identifiées.

Le rapport de certification constitue, avec la cible de sécurité, la documentation minimale à fournir pour la reconnaissance internationale du certificat.

### 9.3. *Décision de certification*

Le centre de certification transmet le projet de rapport de certification et la cible de sécurité, avec sa proposition de verdict, au Directeur central de la sécurité des systèmes d'information.

S'il décide la certification, le Directeur central de la sécurité des systèmes d'information ou la personne qui en a reçu délégation par le Premier ministre signe le certificat et son rapport de certification.

Le certificat porte la date de la décision de certification mais ne mentionne aucune période de validité.

### 9.4. *Publication du certificat*

Si le commanditaire en fait la demande, le certificat, son rapport de certification ainsi que la cible de sécurité sont publiés sur le site Internet de la DCSSI : [www.ssi.gouv.fr](http://www.ssi.gouv.fr).

### 9.5. *Annulation du certificat*

La DCSSI peut annuler un certificat si, par exemple, un fait nouveau lui permet de démontrer que des informations transmises par le commanditaire ou le développeur au cours de l'évaluation n'étaient pas exactes, et qu'elles ont pu fausser le jugement des évaluateurs et donc le résultat final.

---

<sup>8</sup> Procédure CER/P/01 « Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information »

## Chapitre 10

# Utilisation du certificat

### 10.1. Règles de communication

Le commanditaire et, le cas échéant, les développeurs, ont le devoir d'informer fidèlement et honnêtement les utilisateurs de produits certifiés. En particulier, le commanditaire a le devoir de :

- fournir le rapport de certification et la cible de sécurité chaque fois qu'un utilisateur en fait la demande ;
- ne pas faire d'annonce trompeuse sur le produit, en annonçant ou en laissant entendre par exemple que le produit est certifié alors qu'il n'est qu'en cours d'évaluation ;
- signaler aux utilisateurs potentiels les problèmes de sécurité dont le développeur ou le commanditaire a connaissance ;
- informer sans délai tous les utilisateurs déclarés d'une nouvelle vulnérabilité.

### 10.2. Règles d'utilisation de la marque<sup>9</sup>

La marque "certification sécurité TI" reproduite ci-dessous est la marque de certification française de la sécurité offerte par les technologies de l'information accordée par la Direction centrale de la sécurité des systèmes d'information (DCSSI). Cette marque est déposée à l'Institut National de la Propriété Industrielle sous le numéro 023 175 658.



Elle identifie les produits et systèmes certifiés dans le cadre du décret 2002-535.

---

<sup>9</sup> Procédure MAR/P/01 « Règles d'utilisation de la marque « Certification Sécurité TI » »

# Chapitre 11

## Surveillance et maintenance

Le certificat atteste, au jour de sa signature, de la conformité d'un produit ou d'un système aux exigences listées dans sa cible de sécurité. Pour prolonger la confiance dans cette conformité ou faciliter la certification des évolutions d'un produit précédemment certifié, le centre de certification propose des programmes de surveillance ou de maintenance.

### ***11.1. Surveillance<sup>10</sup>***

Le centre de certification propose un programme de surveillance des certificats qui consiste à effectuer un suivi du produit pour maintenir la confiance dans le certificat émis.

Ce suivi consiste à réaliser régulièrement (la période dépend du domaine technique concerné) des travaux de mise à jour de l'analyse de vulnérabilité du produit certifié et de faire des tests si nécessaire.

La surveillance est facultative, laissée à l'initiative du commanditaire. Dans certains cas particuliers (pour les dispositifs de création de signature électronique par exemple), elle peut être rendue obligatoire.

### ***11.2. Maintenance<sup>11</sup>***

Un certificat s'applique uniquement à la version et à la configuration évaluées du produit. Or, il est probable que le produit, son environnement de développement ou de production sont amenés à changer.

Le commanditaire peut demander l'évaluation de ces nouvelles versions du produit.

Le centre de certification propose une procédure de maintenance des certificats qui permet de réduire la charge liée à la certification de ces nouvelles versions.

### ***11.3. Surveillance ou maintenance ?***

La surveillance s'adresse particulièrement aux commanditaires ou acheteurs qui souhaitent s'assurer qu'une version donnée d'un produit ou d'un système continue de répondre dans le temps aux exigences de sécurité identifiées lors de l'émission du certificat.

La maintenance s'adresse plus particulièrement aux développeurs de produits ou de systèmes qui souhaitent réduire l'effort nécessaire à la certification de chaque nouvelle version de leur produit ou de leur système.

---

<sup>10</sup> Procédure SUR/P/01 « Surveillance des produits certifiés »

<sup>11</sup> Procédure MAI/P/01 « Maintenance des certificats »

## **Chapitre 12**

# **Confidentialité des informations traitées**

### ***12.1. Accès aux locaux***

Le centre de certification est situé dans l'enceinte du Secrétariat général de la défense nationale ; il bénéficie donc des mesures de protection et de sécurité élevées de ce dernier.

### ***12.2. Accès aux informations***

Les informations échangées pendant l'évaluation présentent, le plus souvent, un caractère sensible. Le centre de certification traite ces informations selon des règles de protection adéquates.

Dans le cadre de l'agrément, le centre de certification s'assure que les centres d'évaluation appliquent des règles similaires pour la gestion des informations sensibles qu'ils traitent.

## Chapitre 13

### Anomalies, réclamations

#### *13.1. Au près du centre de certification*

##### **13.1.1. Enregistrement et traitement**

Le centre de certification conserve un enregistrement des appels, des réclamations ou des contestations en matière de certification afin de prendre les mesures qui s'imposent et d'agir sur la cause et sur les facteurs précurseurs ou prédisposants<sup>12</sup>.

##### **13.1.2. Litiges**

Le comité directeur de la certification examine, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le décret 2002-535 qui lui est soumis par les parties.

#### *13.2. Au près des commanditaires*

Le centre de certification exige pour les produits ou systèmes certifiés que le commanditaire l'avise de toute plainte portée à sa connaissance à propos de la conformité du produit ou du système aux exigences listées dans sa cible de sécurité.

---

<sup>12</sup> Procédure ANO/P/01 « Traitement des plaintes et des anomalies »

## Annexe A

### Documents de référence

#### Textes réglementaires

##### Certification

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.
Arrêté du 28 février 2003 portant nomination au comité directeur de la certification en sécurité des technologies de l'information.
Arrêté du 9 septembre 2002 portant délégation de signature.

##### SGDN/DCSSI

Décret 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information.
Arrêté du 15 mars 2002 portant organisation de la direction centrale de la sécurité des systèmes d'information.
Arrêté du 15 mars 2002 relatif à l'organisation en bureaux des sous-directions de la direction centrale de la sécurité des systèmes d'information.

##### Signature électronique

Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.
Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
Décret 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
Décision de la Commission (2000/709/CE) du 6 novembre 2000 relative aux critères minimaux devant être pris en compte par les Etats membres lors de la désignation des organismes visé à l'article 3, paragraphe 4, de la directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques.

#### Textes relatifs à l'accréditation

NF EN 45011:1998	Exigences générales relatives aux organismes procédant à la certification de produits (reproduction intégrale du guide ISO/CEI 65:1996)
IAF G65	Guide IAF pour l'application du guide ISO/IEC 65:1996, mars 1999.
CPS-Ref-02	Critères d'accréditation concernant les organismes de certification procédant à la certification de produits et de services, révision 01, novembre 2002.

NF EN ISO/CEI 17025	Prescriptions générales concernant la compétence des laboratoires d'étalonnage et d'essais (remplace la norme NF EN 45001)
---------------------	--

## Critères d'évaluation

ITSEC	Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC), version 1.2, juin 1991.
ITSEM	Manuel d'évaluation de la sécurité des technologies de l'information (ITSEM), version 1.0, juin 1995.
JIL	ITSEC Joint Interpretation Library (ITSEC JIL), version 2.0, novembre 1998.
CC	Common Criteria for Information Technology Security Evaluation : <ul style="list-style-type: none"><li>• Part 1 : Introduction and general model, version 2.1, août 1999 ;</li><li>• Part 2 : Security functional requirements, version 2.1, août 1999 ;</li><li>• Part 3 : Security assurance requirements, version 2.1, août 1999.</li></ul>
CEM	Common Methodology for Information Technology Security Evaluation: <ul style="list-style-type: none"><li>• Part 1 : Introduction and general model, version 0.6, janvier 1999 ;</li><li>• Part 2 : Evaluation Methodology, version 1.0, août 1999.</li></ul>
ISO/IEC 15408	Information technology — Security techniques — Evaluation criteria for IT security : <ul style="list-style-type: none"><li>• ISO/IEC 15408-1:1999(E) : Part 1 : Introduction and general model ;</li><li>• ISO/IEC 15408-2:1999(E) : Part 2 : Security functional requirements ;</li><li>• ISO/IEC 15408-3:1999(E) : Part 3 : Security assurance requirements.</li></ul>

## Annexe B

### Définitions et acronymes

#### Définitions

Centre de certification	Bureau de la DCSSI instituée par le décret 2001-693 et les arrêtés 15-02-2002-1 et 15-02-2002-2, dont les membres instruisent les dossiers de certification.
Centre d'évaluation	Organisme accrédité selon le référentiel ISO/CEI 17025 et agréé par le centre de certification pour conduire des évaluations de la sécurité en vue d'une certification dans le cadre du décret 2002-535.
Certificateur	Personnel du centre de certification chargé de l'instruction des dossiers de certification.
Certificat	Il atteste que l'exemplaire d'un produit ou d'un système répond aux exigences de sécurité spécifiées dans sa cible de sécurité. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8 du décret 2002-535).
Certification	Action de fournir l'assurance de conformité à des normes et autres documents normatifs.
Commanditaire	Personne ou organisme qui demande l'évaluation en vue de la certification.
Comité directeur de la certification	Comité directeur de la certification en sécurité des technologies de l'information défini par le Chapitre III du décret 2002-535.
Cible de sécurité	Ensemble d'exigences de sécurité constituant le référentiel de certification pour les évaluations ITSEC, Critères Communs ou ISO/IEC 15408.

#### Acronymes et abréviations

DCSSI	Direction centrale de la sécurité des systèmes d'information
RTE	Rapport technique d'évaluation
SGDN	Secrétariat général de la défense nationale

## Annexe C

### Table de correspondance avec la norme NF EN 45011:1998

Paragraphe de la norme	Chapitre du manuel
<b>4 Organisme de certification</b>	
<b>4.1 Dispositions générales</b>	
4.1.1	4.3.2
4.1.2	6.1
4.1.3	6.3
4.1.4	4.1
<b>4.2 Organisation</b>	Chapitre 4
<b>4.3 Fonctionnement</b>	Chapitre 6
<b>4.4 Sous-traitance</b>	8.1
<b>4.5 Système qualité</b>	
4.5.1	Chapitre 1
4.5.2	Chapitre 5
4.5.3	Manuel qualité
<b>4.6 Conditions et procédures pour l'octroi, le maintien, l'extension et le retrait de la certification</b>	
4.6.1	Chapitre 9
4.6.2	Chapitre 9
<b>4.7 Audits internes et revues de direction</b>	
4.7.1	5.4.3
4.7.2	5.4.1
<b>4.8 Documentation</b>	
4.8.1	5.5
4.8.2	5.5.2
<b>4.9 Enregistrements</b>	
4.9.1	5.5.3
4.9.2	5.5.3
<b>4.10 Confidentialité</b>	
4.10.1	Chapitre 12
4.10.2	Chapitre 12
<b>5 Personnel de l'organisme de certification</b>	
<b>5.1 Généralités</b>	
5.1.1	4.3.5
5.1.2	4.3.4
<b>5.2 Critères de qualification</b>	
5.2.1	4.3.5
5.2.2	4.3.5
5.2.3	4.3.5
<b>6 Modification des exigences pour la certification</b>	6.4

<b>7 Appels, réclamations et contestations</b>	
7.1	13.1
7.2	13.1
<b>8 Demande de certification</b>	
<b>8.1 Information sur la procédure</b>	
8.1.1	Chapitre 6
8.1.2	Chapitre 7
8.1.3	Chapitre 7
8.1.4	Chapitre 7
<b>8.2 La demande</b>	
8.2.1	7.1
8.2.2	7.1
<b>9 Préparation de l'évaluation</b>	
9.1	7.2
9.2	7.2
9.3	7.2
9.4	7.2
<b>10 Evaluation</b>	Chapitre 8
<b>11 Rapport d'évaluation</b>	8.3
<b>12 Décision de certification</b>	
12.1	Chapitre 9
12.2	Chapitre 9
12.3	Chapitre 9
12.4	11.2
<b>13 Surveillance</b>	
13.1	Chapitre 11
13.2	Chapitre 11
13.3	Chapitre 11
13.4	Chapitre 11
<b>14 Utilisation des licences, certificats et marques de conformité</b>	
14.1	Chapitre 10
14.2	Chapitre 10
14.3	Chapitre 10
<b>15 Plaintes auprès du fournisseur</b>	13.2