Brand Compliance

RÈGLEMENT DE CERTIFICATION

Table des matières

1 Introduction

En tant qu'organisme de certification (OC), Brand Compliance Belgique fournit des services liés à l'évaluation et à la certification des systèmes de gestion et des processus des organisations, sur la base des normes applicables. Brand Compliance Belgique travaille pour une certification effectuée sous accréditation, conformément aux règles de l'organisme national d'accréditation. Vous trouverez des informations sur les accréditations actuelles de Brand Compliance Belgique sur KMO, WSE & ISO certification & audits.

Dans le texte qui suit, le client est désigné par « le donneur d'ordre » et Brand Compliance België B.V. par « Brand Compliance Belgique ».

1.1 Champ d'application

Les normes auxquelles s'appliquent les présentes règles de certification sont les suivantes :

- ✓ Système de gestion des actifs informatiques (ITAM) : ISO/IEC 19770-1:2017
- ✓ Système de gestion de la sécurité de l'information (ISMS) : ISO/IEC 27001:2022
- ✓ CyberFundamentals Essential

1.2 Objectif du présent règlement de certification

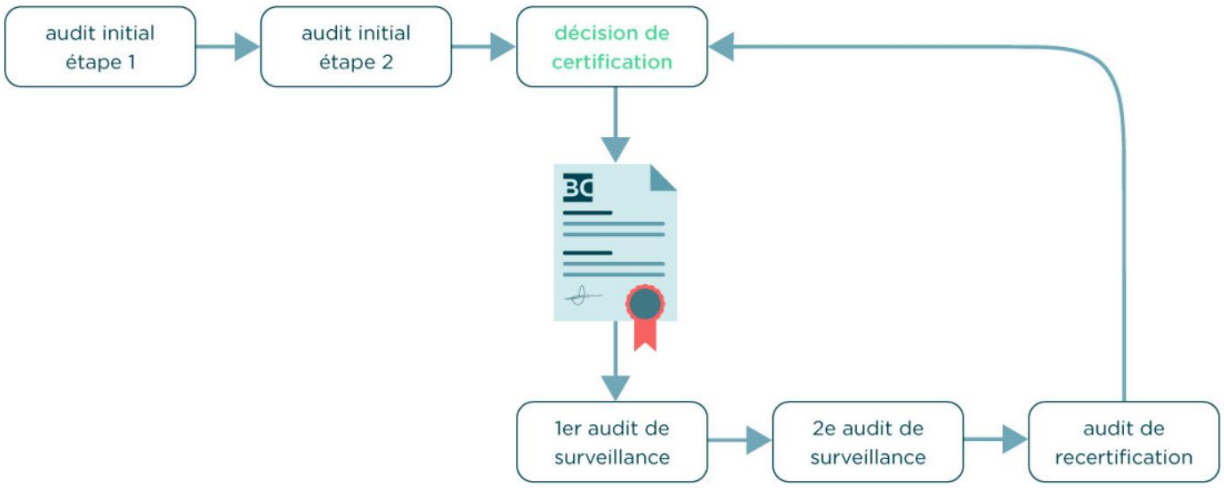
Ce règlement de certification a pour objectif de fournir à toutes les organisations qui souhaitent obtenir ou maintenir une certification auprès de Brand Compliance Belgique un aperçu de la méthode de travail, des procédures et des accords mutuels applicables.

2 Processus de certification

Ce chapitre explique en détail le processus de certification. Le processus de certification débute par une demande introduite par le client. Sur cette base, un contrat est établi. Une fois le contrat approuvé par Brand Compliance Belgique, les dates d'audit sont fixées en concertation avec le client. Les deux parties procèdent alors aux préparatifs, après quoi l'audit initial se déroule aux dates convenues. Cet audit comprend une étape 1 et une étape 2. À l'issue de l'audit initial, un rapport est établi puis évalué par une commission de certification indépendante, qui décide si le certificat peut être délivré au donneur d'ordre.

Au cours de chaque étape, le (chef) auditeur peut constater des non-conformités. Celles-ci doivent être résolues avant que la certification puisse être accordée. Voir paragraphe 2.11.

Le cycle de certification commence après l'audit initial. Ce cycle est illustré dans le schéma ci-dessous.



Pour conserver le certificat, chaque organisation certifiée doit faire réaliser chaque année, dans les douze mois suivant la réunion de clôture de l'audit précédent, l'audit suivant du cycle.
Le cycle comprend deux audits de surveillance, suivis d'un audit de re-certification à la fin de la période triennale. Après la nouvelle décision de certification, un nouveau cycle débute.

Brand Compliance Belgique informera le client en temps utile de chaque audit prévu tout au long du processus. Le client reste libre de convenir d'un rendez-vous pour le prochain audit à un stade plus précoce.

2.1 Reprise intermédiaire

Si une certification existante est reprise d'un autre CI et qu'aucune particularité n'a été constatée, comme décrit dans l'IAF MD2, le cycle de certification peut être repris. Dans tous les autres cas, un audit initial est requis. Cette situation est toujours notifiée au client.

2.2 Demande de certification

Le processus de certification commence par une demande de certification. Celle-ci est enregistrée au moyen du formulaire prévu à cet effet. Les informations consignées sont basées sur les données fournies par le client. À partir de ces informations, le temps à consacrer à la certification peut être calculé.

Brand Compliance Belgique détermine pour chaque client le temps nécessaire à la réalisation d'un audit complet et efficace, conformément à la norme demandée. Le calcul du temps s'appuie sur le tableau des journées-homme lié à la norme concernée et tient compte des facteurs pouvant influencer cette estimation. La planification, la préparation et la rédaction du rapport font également partie du temps total consacré. Sur cette base, Brand Compliance Belgique établit une offre pour le client.

2.3 Contrat de certification

Brand Compliance Belgique enverra une offre accompagnée d'un contrat. Le client peut accepter l'offre en la renvoyant signée ou en envoyant son accord par e-mail à Brand Compliance Belgique.

2.4 Planification

Après réception de l'accord sur le contrat, Brand Compliance Belgique déterminera avec le client une date appropriée pour la réalisation de l'audit. Les étapes 1 et 2 seront planifiées en concertation, soit de manière successive (étape 1 suivie de la étape 2 après son achèvement), soit simultanément selon le cas. Pour CyberFundamentals, le « niveau de maturité » total de l'auto-évaluation finalement révisée, tel que déterminé après l'audit d'étape 1, doit être d'au moins 2,5 sur une échelle de 5 pour passer à l'évaluation de l'étape 2.

La politique de Brand Compliance Belgique consiste à fournir ses services exclusivement avec son propre personnel. L'externalisation des travaux d'audit n'est pas pratiquée. Toutefois, il peut être fait appel à des collaborateurs externes, par exemple à un expert technique. Ces collaborateurs sont qualifiés par Brand Compliance Belgique comme équivalents à son propre personnel et signent, dès leur arrivée, une déclaration de confidentialité ainsi qu'une déclaration d'indépendance, comme le fait le personnel interne.

Le contrat que Brand Compliance Belgique conclut avec les collaborateurs engagés prévoit la même obligation de confidentialité et les mêmes règles de conduite relatives aux données confidentielles du client que celles applicables à son propre personnel.

Les collaborateurs intérimaires se présentent comme des collaborateurs de Brand Compliance Belgique, mais ne jouent aucun rôle dans les services administratifs. Ils ne participent en aucun cas à la décision finale de certification. La déclaration d'indépendance prévoit que les collaborateurs intérimaires sont tenus de signaler toute situation susceptible de compromettre leur indépendance dans le cadre des missions qui leur sont confiées.

2.5 Préparation

Afin de garantir le bon déroulement des audits, une préparation est nécessaire tant de la part de Brand Compliance Belgique que du client.

2.5.1 Préparation de Brand Compliance Belgique

Afin de réaliser l'audit de manière correcte, l'auditeur principal se prépare en s'imprégnant de l'organisation. À cette fin, il peut demander au client certains documents. Le client en est informé en temps utile par l'auditeur principal.
L'auditeur principal établit ensuite un programme d'audit complet. Sur cette base, un plan d'audit est élaboré et partagé avec le client avant la réalisation de l'audit. Ce plan précise quels collaborateurs seront interrogés à quel moment et quels éléments de l'organisation seront examinés.

2.5.2 Préparation du client

Avant que l'audit puisse avoir lieu, le client doit avoir réalisé au minimum une revue de direction concernant le système de gestion à certifier, ainsi qu'un audit interne couvrant l'ensemble du périmètre de la certification.

Pour CyberFundamentals, le client est tenu de fournir, préalablement à l'audit, une auto-évaluation CyberFundamentals Essential, includant les pièces justificatives pertinentes, l'onglet « détails » dûment complété, ainsi qu'une justification pour un maximum de cinq mesures exclues.

2.6 Audit initial

Le processus de certification débute par un audit initial, composé de deux parties : un examen documentaire (étape 1) et un audit portant sur la mise en œuvre du système de gestion (étape 2). L'objectif de ces audits est de recueillir des preuves démontrant que le système de gestion est effectivement mis en œuvre et conforme à la norme pour laquelle la certification est demandée.

2.6.1 Coopération du client

Pour qu'un audit se déroule avec succès, le client doit fournir des informations suffisantes permettant de vérifier que le système de gestion ou le processus décrit est complet, mis en œuvre conformément aux exigences de la norme, et que son application peut être effectivement testée.
Cela peut impliquer la visite de certains sites afin de vérifier la maîtrise des processus. La BELAC évalue périodiquement si Brand Compliance Belgique continue de répondre aux normes fixées. Cette évaluation peut inclure une visite sur place, dont le client est toujours informé en temps utile.
Le client est tenu d'informer immédiatement Brand Compliance Belgique si un auditeur participant à l'audit a, de quelque manière que ce soit, fourni des services de conseil ou de support à l'organisation, ou a été impliqué dans des activités susceptibles de compromettre l'impartialité de l'audit.

2.6.2 Audit initial – étape 1

Au cours de l'étape 1 de l'audit initial, l'auditeur principal évalue dans quelle mesure la conception du système de gestion ou du processus répond aux exigences de la norme concernée.
Le client doit mettre à disposition de l'équipe d'audit toutes les informations générales relatives au système ou au processus de gestion, ainsi qu'aux activités couvertes par celui-ci.
Il doit également fournir une copie de toute la documentation obligatoire mentionnée dans la norme applicable et, le cas échéant, des informations complémentaires.

2.6.2.1 Réunion d'ouverture

Lors de la réunion d'ouverture, l'auditeur présente à la direction du client le déroulement de l'audit, y compris la planification, les critères de certification et la méthode d'évaluation du système ou du processus de gestion. Cette réunion aborde également la manière de procéder en cas de modifications nécessaires, par exemple concernant le périmètre ou la durée de l'audit. Brand Compliance Belgique applique des directives spécifiques à cet effet et détermine, en concertation avec le client, les mesures à mettre en œuvre.

2.6.2.2 Audit – étape 1

Lors d'un audit d'étape 1, les points suivants sont au minimum examinés :

- ✓ les informations documentées relatives au système de gestion ou au processus du client ;
- ✓ les conditions spécifiques du site du client et les entretiens avec le personnel du client afin de déterminer si l'organisation est prête pour l'étape 2 ;
- ✓ l'évaluation du statut du client et de sa compréhension des exigences de la norme, plus particulièrement en ce qui concerne l'identification des principales performances du système de gestion, du processus ou des aspects significatifs, des procédures, des objectifs et de leur mise en œuvre ;
- ✓ l'obtention des informations nécessaires relatives au champ d'application du système de gestion ou du processus, y compris :
  - le ou les établissements du client ;
  - les processus et équipements utilisés ;
  - les niveaux des mesures de maîtrise mises en place (en particulier dans le cas de clients ayant plusieurs sites) ;
  - les exigences légales et réglementaires applicables ;
- ✓ l'évaluation de l'allocation des moyens pour l'étape 2 et la confirmation avec le client des détails pratiques relatifs à cette étape;
- ✓ la planification de la étape 2, afin d'obtenir une compréhension suffisante du système de gestion ou du processus et des activités du client sur site, par rapport aux normes de systèmes de management ou à d'autres documents normatifs ;
- ✓ l'évaluation visant à déterminer si les audits internes et les revues de direction ont été planifiés et réalisés, et si le degré de mise en œuvre du système de management indique que le client est prêt pour la étape 2.

L'étape 1 de CyberFundamentals « Essential » couvre spécifiquement les points suivants :

- ✓ un audit documentaire de l'auto-évaluation de niveau « Essential » et des preuves appropriées à l'appui de cette auto-évaluation. L'objectif est de déterminer si le score global de maturité de l'auto-évaluation n'est pas inférieur à 2,5/5, afin que le processus puisse passer à la étape 2.

2.6.3 Audit initial – étape 2

L'audit de étape 2 a lieu au plus tard 6 mois après la réunion de clôture de l'audit d'étape 1. Au cours de l'étape 2, l'équipe d'audit évalue l'efficacité et la mise en œuvre du système de gestion ou du processus au sein de l'organisation, au moyen d'entretiens, de demandes de documentation justificative, de visites physiques et d'observations dans les différents services. En cas de poursuite/reprise d'un cycle de certification, un rendez-vous est fixé pour un audit de suivi.

2.6.3.1. audit – étape 2

L'audit de l'étape 2 comprend au minimum :

- ✓ des informations et des pièces justificatives concernant le respect de toutes les exigences des normes de systèmes de management applicables ou d'autres documents normatifs ;

- ✓ le suivi, la mesure, le rapport et l'évaluation des performances par rapport aux principaux objectifs de performance et aux cibles (conformément aux attentes des normes de systèmes de management applicables ou d'un autre document normatif) ;
- ✓ la capacité du système de gestion ou du processus du client, ainsi que ses performances, à satisfaire aux exigences légales, réglementaires et contractuelles applicables;
- ✓ le contrôle opérationnel des processus du client ;
- ✓ les audits/évaluations internes et la revue de direction ;
- ✓ la responsabilité de la direction concernant la politique du client.

2.6.3.2 Éléments spécifiques CyberFundamentals « Essential »

L'étape 2 de CyberFundamentals « Essential » aborde spécifiquement les points suivants :

- ✓ évaluation sur place de la mise en œuvre, y compris de l'efficacité :
  - Mesures prises au regard des exigences du niveau « Essential ».
  - Mesures prises en rapport avec les niveaux de « maturité » des mesures importantes documentés dans l'auto-évaluation ;
  - Mesures prises en rapport avec les contrôles liés aux aspects de gestion du niveau « Essential ».
  - Capacité du système de gestion de l'organisation et performances relatives au respect des exigences légales, réglementaires et contractuelles applicables.
- ✓ Les informations relatives à l'auto-évaluation des mesures importantes doivent être suffisamment détaillées pour permettre d'aboutir à une conclusion d'audit.

2.6.3.3 Éléments spécifiques à l'ITAM

En ce qui concerne spécifiquement l'ITAM, les éléments suivants doivent au moins être abordés :

- ✓ le leadership démontré par la direction et son engagement envers la politique et les objectifs en matière de gestion des actifs informatiques ;
- ✓ les exigences documentaires issues de la norme ITAM applicable ;
- ✓ une évaluation des risques liés à la gestion des actifs informatiques et la garantie que cette évaluation produit des résultats cohérents, valables et comparables lorsqu'elle est mesurée ;
- ✓ la définition des objectifs et des mesures de maîtrise basées sur l'analyse des risques liés à la gestion des actifs informatiques et la manière de les traiter (processus de maîtrise) ;
- ✓ la performance du système de gestion des actifs informatiques et l'efficacité de l'ITAM, comparées et évaluées par rapport aux objectifs formulés ;
- ✓ la conformité entre les mesures de maîtrise définies, la déclaration d'applicabilité, les résultats de l'analyse des risques et les mesures de maîtrise, ainsi que la politique et les objectifs de gestion des actifs informatiques ;
- ✓ la mise en œuvre des mesures de maîtrise. Compte tenu des risques externes et internes connexes, la surveillance, les mesures et l'analyse globales des processus et des mesures de maîtrise de la gestion des actifs informatiques. Ceci afin de déterminer si les mesures de maîtrise mises en œuvre sont efficaces et permettent d'atteindre les objectifs fixés ;
- ✓ les programmes, processus, procédures, enregistrements, rapports d'audit interne et évaluations de l'efficacité de l'ITAM afin de s'assurer qu'ils sont conformes aux décisions prises

par la direction générale ainsi qu'à la politique de gestion des actifs informatiques et aux objectifs correspondants.

Si, dans le cadre d'une certification ITAM, il est décidé de ne pas mettre en œuvre certaines mesures de maîtrise, cela doit être justifié par le client d'une part et approuvé par l'équipe d'audit d'autre part.

2.6.3.4 Éléments spécifiques de l'ISMS

En ce qui concerne spécifiquement l'ISMS, les éléments suivants doivent au moins être abordés :

- ✓ le leadership démontré par la direction et son engagement envers la politique et les objectifs en matière de sécurité de l'information ;
- ✓ les exigences documentaires issues de la norme ISMS applicable ;
- ✓ une évaluation des risques liés à la sécurité de l'information et la garantie que cette évaluation produit des résultats cohérents, valables et comparables lorsqu'elle est mesurée ;
- ✓ la définition des objectifs et des mesures de maîtrise basées sur l'analyse des risques liés à la sécurité de l'information et la manière de les traiter (processus de maîtrise) ;
- ✓ la performance du système de sécurité de l'information et l'efficacité de l'ISMS, comparées et évaluées par rapport aux objectifs formulés ;
- ✓ la conformité entre les mesures de maîtrise définies, la déclaration d'applicabilité, les résultats de l'analyse des risques et les mesures de maîtrise, ainsi que la politique et les objectifs en matière de sécurité de l'information ;
- ✓ la mise en œuvre des mesures de maîtrise. Compte tenu des risques externes et internes connexes, la surveillance globale, les mesures et l'analyse des processus et des mesures de maîtrise de la sécurité de l'information. Ceci afin de déterminer si les mesures de maîtrise mises en œuvre sont efficaces et permettent d'atteindre les objectifs fixés ;
- ✓ les programmes, processus, procédures, enregistrements, rapports d'audit interne et évaluations de l'efficacité de l'ISMS afin de s'assurer qu'ils sont conformes aux décisions prises par la direction générale ainsi qu'à la politique de sécurité de l'information et aux objectifs correspondants.

Si, dans le cadre d'une certification ISMS, il est décidé de ne pas mettre en œuvre certaines mesures de maîtrise, cela doit être justifié par le client et approuvé par l'équipe d'audit.

Le titulaire du certificat doit appliquer une procédure de réclamation documentée concernant les produits, processus et services pour lesquels un certificat a été délivré. Tous les documents relatifs aux réclamations doivent rester à la disposition de Brand Compliance Belgique pendant 5 ans après la réclamation.

2.6.3.5 Réunion de clôture

Les éventuelles non-conformités constatées sont discutées et signalées lors de la réunion de clôture. Avec la direction du client, l'auditeur principal résume les conclusions, classe les non-conformités et discute de leur résolution. Il est également indiqué si le client sera proposé pour la certification. Sur la base des conclusions de l'étape 1, Brand Compliance Belgique se réserve le droit de répéter l'étape 1 et/ou de reporter ou d'annuler l'étape 2.

2.7 Rapport

Après l'audit d'étape 1 et l'audit d'étape 2, l'auditeur principal établi un rapport présentant ses conclusions. Ce rapport traite tous les éléments de la norme, y compris la manière dont l'organisation les a mis en œuvre. Les points positifs et les points d'amélioration y sont mis en évidence, et donnent au client une vue d'ensemble de l'organisation.

2.8 Décision de certification

Une fois l'audit initial complet (étape 1 et étape 2) terminé, une commission de certification indépendante émet une recommandation, sur la base du rapport, quant à l'octroi ou non du certificat. La décision finale est prise par le directeur général. En cas de résultat positif, le client reçoit de Brand Compliance Belgique un certificat attestant que l'organisation satisfait aux exigences de la norme.

2.9 Audits de surveillance

Des audits intermédiaires ont lieu chaque année, deux fois par cycle de certification. L'objectif est de contrôler le système de gestion et/ou le processus certifié du client, afin d'en garantir la continuité. Au cours d'un audit de surveillance, des non-conformités peuvent être constatées. Cela est expliqué plus en détail au paragraphe 2.11. Les non-conformités doivent être traitées dans le délai imparti afin de permettre la poursuite de la certification.

2.10 Recertification

La recertification doit être finalisée dans les trois ans suivant l'audit initial. L'objectif d'une recertification est de confirmer la continuité et l'efficacité du système de gestion et/ou du processus, ainsi que la pertinence et l'applicabilité continues du ou des périmètres. Elle couvre le fonctionnement pendant la période certifiée. La structure d'un audit de recertification est comparable à celle d'un audit d'étape 2.

Une recertification a lieu suffisamment à l'avance (environ 3 mois) de la date d'expiration du certificat. Les éventuelles non-conformités constatées doivent être évaluées comme résolues par l'équipe d'audit avant l'expiration du certificat, afin de garantir son maintien.

Pour CyberFundamentals Essential, une auto-évaluation mise à jour, datant de moins de quatre mois, est requise pour l'audit de recertification. Le client doit la soumettre en temps utile à Brand Compliance avant la recertification. Il doit également fournir les preuves relatives à la maturité révisée des mesures et contrôles importants associés aux aspects de gestion du niveau de sécurité « Essential ».

2.11 Non-conformités

Il peut arriver que des non-conformités soient constatées lors des différents audits. Les non-conformités sont des éléments dans la conception, la mise en œuvre du système de gestion et/ou du processus qui doivent être résolus avant qu'une certification ne puisse être accordée. Les non-conformités sont classées en deux catégories :

1) Non-conformité majeure (catégorie A) : non-respect d'une exigence qui affecte la capacité du système de gestion à atteindre les résultats prévus. Une non-conformité peut être considérée comme majeure dans les circonstances suivantes :

   - lorsqu'il existe un doute raisonnable quant à l'existence de contrôles de processus efficaces, ou quant à la capacité des produits ou services à satisfaire aux exigences prescrites ;
   - un ensemble de non-conformités mineures liées à une même exigence ou à un même problème peut indiquer une défaillance du système et constituer, de ce fait, une non-conformité majeure.

2) Non-conformité mineure (catégorie B) : non-respect d'une exigence qui n'affecte pas la capacité du système de gestion à atteindre les résultats prévus.

Peuvent également être constatés:

- Possibilité d'amélioration : indique une inefficacité et un domaine d'amélioration potentiel. Elle découle indirectement des exigences de certification et doit être prise en considération.
- Point de préoccupation (PvZ) : point faible qui pourrait être classé comme non-conformité lors de l'audit d'étape 2.

2.11.1 Éléments spécifiques pour les non-conformités CyberFundamentals Essential

Les non-conformités sont classées en deux catégories pour chaque niveau de maturité :

	non-conformité majeure Niveau de maturité	**non-conformité mineure Niveau de maturité**
Chaque mesure clé	< 3/5	
Chaque contrôle de gestion	< 3/5	
Chaque catégorie	< 3/5	
Niveau de maturité total	< 3/5	
Tous les autres contrôles		< 2/5

2.11.2 Délai de résolution des non-conformités

Pour toute non-conformité, le (Lead) Auditeur fixe, en fonction de sa catégorie, un délai dans lequel la non-conformité doit être résolue ou un plan d'action doit être soumis. Dans le cadre de la recertification, la période de validité du certificat en cours est déterminante.

Si la résolution des non-conformités lors d'une recertification n'a pas lieu pendant la période de validité du certificat en cours, elle doit être réalisée au plus tard dans un délai maximum de 5 mois (calculé à partir de la date d'expiration du certificat). Si cette condition est remplie, un nouveau certificat peut être délivré. Dans ce cas, la date d'entrée en vigueur du certificat correspond à la date de la décision de recertification , et la date d'expiration est basée sur le cycle de certification précédemment applicable. Si le délai de 5 mois n'est pas respecté, un nouvel audit initial (au minimum un audit de étape 2) doit être réalisé pour maintenir la certification.

2.11.3 Actions correctives

Des actions correctives peuvent être prises afin de résoudre la ou les non-conformités. On distingue Deux catégories d'actions correctives sont distinguées :

I. actions correctives impliquant uniquement une modification du système de gestion documenté. Dans ce cas, le rapport de non-conformité peut être clôturé sur présentation d'une preuve écrite, et une vérification sur site n'est pas nécessaire ;
II. actions correctives qui impliquant des changements tels qu'une vérification sur place est nécessaire. Dans ce cas, Brand Compliance Belgique planifiera et réalisera une enquête complémentaire.

2.11.4 Traitement

La réponse du client à la non-conformité constatée comprend toujours les éléments suivants :

- ✓ Analyse des causes ;
- ✓ Correction ;
- ✓ Action corrective.

Le donneur d'ordre peut fournir ces informations sur papier ou sous forme numérique. L'auditeur principal concerné veille à ce que, pour chaque non-conformité constatée, les éléments ci-dessus figurent clairement dans la réponse.

En cas de non-conformité majeure (catégorie A), les corrections et les actions correctives doivent être vérifiées au plus tard dans les 5 mois suivant le dernier jour de l'audit.

3 Utilisation des certificats et logos

Des règles spécifiques s'appliquent à l'utilisation des marques de certification et des logos. Lorsque l'audit de certification est réussi, le client a droit à un certificat ainsi qu'au droit d'utiliser les logos certifiés correspondant à la ou aux normes concernées. À partir de ce moment, le client peut choisir d'utiliser ces logos, par exemple dans son identité visuelle ou pour des actions marketing.

Le titulaire du certificat doit veiller à ce qu'aucune confusion ne puisse être créée auprès des tiers concernant le périmètre de la certification ou le label délivré par Brand Compliance Belgique. Si Brand Compliance Belgique constate un usage incorrect ou injustifié du label, elle demandera au client de procéder à une rectification.

L'obtention d'un certificat portant sur un système de gestion n'implique pas la certification des produits, de leurs emballages ou des services eux-mêmes.

3.1 Certificat

Une fois l'audit de certification terminé avec succès, Brand Compliance Belgique délivrere un certificat précisant la norme selon laquelle l'évaluation a été réalisée, les activités de l'entreprise évaluées (le périmètre) et la durée de validité.

Conformément aux exigences des normes d'accréditation, Brand Compliance Belgique tient à jour une liste des clients qu'elle a certifiés, accompagnée de leurs activités. Cette liste est accessible aux tiers. Toute information ne relevant pas de la norme d'accréditation ne sera transmise à des tiers qu'avec l'autorisation écrite du client.

L'ITAM Forum publiera sur son site web la liste des organisations certifiées ISO 19770-1:2017.

3.1.1 Visibilité du certificat

En cas de certification sous accréditation, le certificat porte le logo de l'organisme d'accréditation concerné. Le client peut afficher ce certificat sur son lieu de travail ou le présenter à des parties prenantes. Le logo de certification peut être utilisé à cet effet, conformément aux dispositions du paragraphe 3.2.

3.1.2 Résiliation du contrat

Le client peut résilier le contrat conformément aux conditions qui y sont stipulées. La résiliation doit être notifiée par écrit. Brand Compliance enverra ensuite une confirmation écrite. À la date de résiliation, le client est tenu de détruire tous les certificats en sa possession, de supprimer les logos, marques ou mentions de tous supports (y compris site web), afin d'éviter tout usage non autorisé.

En cas de non-suppression dans les délais impartis, la clause pénale décrite au paragraphe 3.4 s'applique.
Brand Compliance Belgique se réserve le droit d'effectuer des contrôles inopinés sur site pour vérifier l'absence d'usage non autorisé après la résiliation.

3.2 Logos certifiés

Pendant la durée de validité du certificat, le client a également le droit d'utiliser le ou les logos de Brand Compliance Belgique à des fins promotionnelles. Brand Compliance Belgique a enregistré ses logos au Registre des marques du Benelux sous le numéro 1402095. Brand Compliance Belgique fournira au client un jeu de logos originaux à cet effet. Brand Compliance Belgique vérifiera leur utilisation correcte lors des audits de surveillance et de la recertification. Les conditions d'utilisation sont décrites au paragraphe 3.2.1.

3.2.1 Utilisation du ou des logos certifiés

Le logo peut être utilisé sur la correspondance, les publicités, les supports promotionnels et les supports électroniques, sur les murs, portes, fenêtres et sur les stands d'exposition, à condition que l'utilisation ne soit pas trompeuse et soit conforme aux exigences du présent règlement. Il est interdit d'apposer le logo sur le produit, l'emballage ou de toute autre manière susceptible d'être interprétée comme une indication de conformité du produit.

Le logo Brand Compliance Belgique peut être utilisé :

- ✓ en noir sur fond blanc, ou en couleur sur fond blanc ;
- ✓ si cela n'est pas possible, en blanc sur un fond coloré ;

- ✓ avec une largeur minimale de 50 mm ;
- ✓ avec tous les chiffres et lettres du logo lisibles ;
- ✓ en maintenant une proportionnalité correcte lors d'un agrandissement (les espaces entre les caractères doivent être augmentés proportionnellement).
- ✓

Exemple :
Logo de certification de conformité incendie Belgique, ISO 19770-1:2017

(25 * 68 mm)

(25 * 68 mm)

Si le donneur d'ordre a des doutes quant à l'utilisation ou souhaite s'écarter des dimensions indiquées ci-dessus pour le logo Brand Compliance Belgique, il peut contacter be-info@brandcompliance.com .

3.2.2 Certifications sous accréditation

Lorsque Brand Compliance Belgique est accrédité pour la norme, le titulaire du certificat est autorisé à utiliser le logo BELAC qui a été spécifiquement mis à la disposition de Brand Compliance Belgique ; le règlement d'utilisation est disponible sur le site web de BELAC (BELAC-2-001).

3.3 Utilisation du nom Brand Compliance Belgique

Le client peut utiliser le nom de Brand Compliance Belgique à des fins de marketing, par exemple dans le cadre de communications sur les activités de certification via les réseaux sociaux ou par e-mail.

Lorsqu'il utilise les certificats, déclarations de conformité et/ou rapports d'audit fournis par Brand Compliance Belgique, le donneur d'ordre agit de manière à ne pas porter atteinte à la bonne réputation ni à l'indépendance de Brand Compliance Belgique. Toutes les publications doivent être conçues de façon à ne pas donner une fausse impression quant au périmètre ou aux sites auxquels la certification s'applique, ni quant aux normes et exigences concernées. Si le client souhaite partager des documents avec des tiers, ceux-ci doivent être reproduits dans leur intégralité.

3.4 Utilisation non autorisée

Les marques, signes ou logos de certification ne peuvent pas être utilisés aux fins suivantes :

- Il est interdit d'apposer des marques de certification ou d'autres signes sur des produits, des emballages de produits ou des services qui pourraient donner l'impression que le produit concerné est certifié par Brand Compliance Belgique.
- Le donneur d'ordre ne donnera pas l'impression à des tiers que Brand Compliance Belgique est responsable de ses activités.
- Le donneur d'ordre n'apposera pas de marques susceptibles d'être confondues avec les marques de certification et/ou autres signes mentionnés dans le contrat de certification.
- Aucun logo/marque ne peut être utilisé sur des rapports d'essai de laboratoires, des rapports d'étalonnage, des rapports d'inspection ou des certificats.

En cas d'utilisation non autorisée du certificat et/ou du ou des logos de certification et/ou des marques, Brand Compliance Belgique infligera au donneur d'ordre une amende de 750 euros hors TVA par jour pendant toute la durée de l'infraction.

4 Application du certificat

Brand Compliance Belgique est et reste, pendant toute la durée de la certification, responsable de la décision qu'elle a prise en matière de certification, y compris l'octroi, le maintien, le renouvellement, l'extension, la réduction et le retrait des activités couvertes par le périmètre, ainsi que le report et le retrait du certificat. Afin de conserver le certificat obtenu, le client doit maintenir son système de gestion ou son processus, pour toutes les entités couvertes par la certification, et continuer à satisfaire en permanence aux exigences de la norme concernée.

Indépendamment du fait qu'il soit titulaire d'un certificat, le client doit toujours respecter ses obligations légales, les obligations découlant du système de gestion ou du processus certifié ainsi que les autres obligations qui pouvant être imposées à un produit, processus ou service (par exemple, d'autres documents normatifs ou exigences techniques).

4.1 Modifications intermédiaires

Si, pendant la période de validité du certificat, le client modifie de manière significative son système de gestion ou son processus, il doit en informer Brand Compliance Belgique. Cela inclut notamment des modifications relatives :

a) à la forme juridique, au statut commercial, à la forme d'organisation ou à la propriété ;
b) à l'organisation et la gestion (par exemple, le personnel clé occupant des fonctions de direction, des fonctions décisionnelles ou des fonctions techniques) ;
c) à l'adresse de contact et aux sites ;
d) au périmètre du système de gestion certifié ;
e) à des changements importants apportés au système de gestion et aux processus ;
f) à la déclaration d'applicabilité.

Brand Compliance Belgique évaluera ces modifications au regard des exigences de la norme. Des modifications importantes peuvent conduire à la réalisation d'un audit à court terme. La réception d'une plainte concernant le donneur d'ordre peut également donner lieu à la réalisation d'un audit à court terme. Les modifications mineures apportées au système de gestion, au processus ou à la documentation seront évaluées par l'auditeur (principal) lors du prochain audit régulier.

4.1.1 Activités de certification réglementaires

Pour les activités de certification réglementaires, le client doit informer Brand Compliance Belgique de toute modification envisagée du système de gestion ou du processus. Brand Compliance Belgique évalue les modifications proposées et décide si le système de garantie ainsi modifié répond toujours aux exigences de la directive ou si une nouvelle évaluation est nécessaire. Elle informe le client de sa décision. Cette notification contient les conclusions de l'enquête et la décision d'évaluation motivée.

4.2 Modification des exigences de certification

Si les exigences de certification changent pendant la période de certification, Brand Compliance Belgique en informera le client en temps utile et discutera des mesures à prendre afin que le client puisse continuer à satisfaire aux exigences de la norme. Si des modifications doivent être apportées au système de gestion ou au processus, Brand Compliance Belgique se réserve le droit de contrôler ces modifications.

En cas de modification des accréditations de Brand Compliance Belgique, ou si une accréditation venait à expirer, Brand Compliance Belgique en informera les titulaires de certificats en temps utile.

5 Suspension, restriction et retrait du certificat

Il peut arriver que Brand Compliance Belgique décide de suspendre la certification. Le client en est informé. En général, une suspension peut être envisagée lorsque le client :

- ne met pas en œuvre les actions correctives dans le délai imparti ;
- s'est révélé incapable de traiter les non-conformités constatées dans le délai imparti ;
- ne satisfait pas de manière persistante ou substantielle aux exigences de certification, y compris celles relatives à l'efficacité du système de gestion ;
- n'accepte pas que les audits de contrôle ou de recertification soient réalisés à la fréquence requise ;
- fait un usage non autorisé du certificat et/ou du ou des logos ;
- ne respecte pas ses obligations (financières) envers Brand Compliance ;
- porte atteinte à la réputation commerciale de Brand Compliance Belgique ;
- demande volontairement une suspension.
- ou lorsque, après la date d'émission, de nouveaux faits ou informations sont découverts et sont susceptibles d'influencer de manière significative l'utilisation du label CyberFundamentals « Essential », au point que le score d'auto-évaluation de maturité ne répondrait plus aux exigences nécessaires pour obtenir un certificat.

Brand Compliance Belgique fera tout ce qui est en son pouvoir pour permettre au client de prendre les mesures appropriées. Il peut arriver que Brand Compliance Belgique effectue un audit supplémentaire afin de vérifier l'efficacité des mesures.

5.1 Limitation du périmètre ISMS et ITAM

Si le client ne met pas en œuvre les actions correctives dans le délai convenu, le certificat peut être retiré ou le périmètre peut être limité.

Brand Compliance Belgique limitera le périmètre de la certification de manière à exclure les parties qui ne satisfont pas aux exigences, si le client ne satisfait pas de manière persistante ou substantielle aux exigences de certification pour les parties concernées du périmètre. Une telle limitation doit être conforme aux exigences de la norme utilisée pour la certification.

En cas de limitation du domaine d'activité mentionné sur le certificat, que ce soit à la demande du client ou sur constatation de l'auditeur principal, les supports de communication (par exemple le certificat affiché sur le site web) doivent être adaptés, afin de ne pas donner l'impression que l'organisation reste certifiée pour les activités exclues.

5.2 Maintien du certificat

Si, au cours de la période de certification de trois ans, le client ne souhaite plus conserver le certificat ou estime ne plus être en mesure de le faire, Brand Compliance Belgique retirera le certificat après réception d'une telle notification.

En cas de suspension ou de retrait, le donneur d'ordre est tenu de cesser immédiatement d'utiliser le certificat, le label de certification ou la déclaration concernés, ainsi que de s'abstenir de toute communication pouvant laisser penser qu'il est encore autorisé à les utiliser. Il en va de même en cas de résiliation du contrat par l'une des parties. À la demande de Brand Compliance Belgique, le client sera alors tenu de restituer le certificat ou la déclaration.

5.3 Publication

La suspension, le retrait et la limitation du périmètre du certificat sont mis en œuvre par Brand Compliance Belgique, qui en informe le client par écrit. Brand Compliance Belgique publiera la notification de suspension et de retrait du certificat. Pour les certifications sous accréditation, cette information est publiée dans la base de données données IAF CertSearch; pour les certifications sans accréditation, sur le site web de Brand Compliance. Brand Compliance Belgique n'a aucune influence sur les registres en ligne, tenus par des tiers, relatifs aux certificats délivrés, expirés ou éventuellement retirés. Les documents et données fournis par le client (y compris les supports d'information) peuvent être consultés, chez Brand Compliance Belgique, par des tiers lors d'un audit de ces derniers (par exemple, BELAC ou la Commission d'impartialité).

5.4 Réclamations, objections et recours contre le retrait d'un certificat/la limitation du périmètre

Si le client n'est pas d'accord avec la décision de Brand Compliance Belgique de retirer ou de suspendre le certificat, la procédure décrite au chapitre 6 s'applique.

6 Plaintes, objections et recours

6.1 Réclamations

Si le client n'est pas satisfait de la manière dont Brand Compliance Belgique a réalisé l'évaluation, il peut introduire une plainte en utilisant le « formulaire de plainte Brand Compliance Belgique » disponible sur notre site web : Compliment, plainte ou conseil » Brand Compliance Belgique.

6.2 Procédure

Les plaintes sont traitées conformément à notre procédure interne de traitement des plaintes. Dans les 5 jours ouvrables suivant leur réception, un accusé de réception écrit est envoyé à l'auteur de la plainte. L'examen de la plainte prend au maximum 10 jours ouvrables. La décision prise est communiquée par écrit au plaignant.

Toutes les plaintes reçues sont enregistrées. Le directeur général désigne un responsable pour le traitement de la plainte. Lors de cette désignation, il est explicitement garanti que cette personne n'a pas été impliquée auparavant dans la décision de certification contestée, ni dans l'objet du recours, afin de garantir l'indépendance et l'impartialité requises vis-à-vis du plaignant. Le responsable de la plainte veille à la vérification et à la traçabilité du traitement.

La procédure complète est publiée sur le site web de Brand Compliance : Procédure de réclamation et d'appel

6.3 Objection et recours

Si le client souhaite introduire un recours contre une décision de Brand Compliance Belgique concernant:

- Le refus d'accepter une demande de certification ;
- La décision de ne pas recommander la certification
- La suspension, le retrait ou l'annulation du certificat ;
- L'opposition de tiers à l'octroi d'un certificat ;

ce recours doit être introduit dans un délai de quatre semaines à compter du fait concerné. Les recours sont traités comme des plaintes. La soumission, l'examen et les décisions relatives aux recours n'entraînent aucune mesure à l'encontre du client.

7 Indépendance et objectivité

Brand Compliance Belgique est consciente du fait que l'organisation doit adopter et maintenir une position impartiale dans le cadre de ses activités de certification. C'est pourquoi des mesures ont été prises pour éviter tout conflit d'intérêts.

En conséquence :

- Brand Compliance Belgique peut dispenser à ses clients, pour lesquels des activités de certification sont réalisées, des formations fournissant des informations générales également accessibles au public, mais aucune formation spécifique à l'entreprise n'est dispensée ;
- Brand Compliance Belgique ne peut pas fournir à ces clients des audits ou revues internes ni d'autres services de conseil relatifs au système de management à certifier ;
- Brand Compliance Belgique adopte une position indépendante vis-à-vis des personnes ou organismes qui réalisent des audits ou revues internes, ou qui fournissent d'autres services de conseil chez des clients à certifier ;
- Brand Compliance Belgique peut identifier les points d'amélioration dans le système de gestion des clients pour lesquels des activités de certification sont réalisées, mais ne peut pas conseiller sur la manière de mettre en œuvre les mesures à prendre ;
- Brand Compliance Belgique ne peut pas certifier d'organismes de certification et ne peut pas être elle-même certifiée par eux ;
- la politique d'impartialité de Brand Compliance Belgique exige que les employés n'acceptent aucun cadeau de la part des clients.