World Lottery Association

WLA-SCS:2020

WLA – Norme de contrôle de la sécurité

Exigences en matière de sécurité et d'intégrité des informations et des opérations pour les opérateurs de loteries et de paris sportifs, et leurs fournisseurs.

Publication : octobre 2020, version 1.2
(Révisée : le 2 mai 2022)

Table des matières

Avant-propos

La World Lottery Association (WLA) reconnaît depuis sa fondation la nécessité d'une norme de sécurité et d'intégrité adaptée aux opérateurs de loteries et de paris sportifs. Elle a donc poursuivi le travail entamé par ses prédécesseurs.

Les opérateurs de loteries et de paris sportifs sont confrontés, à des fins commerciales, au besoin de développer des environnements assurant une sécurité et une intégrité visibles et documentées, de manière à gagner la confiance des joueurs et des autres parties prenantes. La norme de contrôle de la sécurité de la WLA (WLA-SCS) est conçue pour aider les opérateurs de loteries et de paris sportifs, ainsi que leurs fournisseurs, à travers le monde à atteindre des niveaux de contrôle conformes aux pratiques de qualité et de sécurité des informations généralement acceptées, ainsi qu'aux exigences spécifiques au secteur. Elle permet aux opérateurs de loteries et de paris sportifs de susciter une plus grande confiance vis-à-vis de l'intégrité de leurs opérations. La certification WLA-SCS fournit une mesure objective de la performance du contrôle de la sécurité et de la gestion des risques d'un opérateur de loteries et de paris sportifs.

La norme WLA-SCS a été rédigée par le Comité de gestion des risques et de la sécurité de la WLA (WLA SRMC). Le WLA SRMC est composé de représentants et de spécialistes en matière de sécurité des opérateurs de loteries et de paris sportifs de partout dans le monde. La comparaison des pratiques actuelles de sécurité et d'intégrité en vigueur dans le secteur avec les pratiques approuvées par des experts en loterie du monde entier a permis d'établir un cadre solide de sécurité et de gestion des risques pour les opérateurs de loteries et de paris sportifs, ainsi que pour leurs fournisseurs.

Le WLA SRMC révise toutes les normes de contrôle de la sécurité utilisées dans le secteur des loteries et des paris sportifs, agit en qualité de coordinateur pour le secteur en ce qui concerne les questions de sécurité et gestion des risques et supervise le processus de certification grâce auquel la conformité des membres et membres associés de la WLA avec la norme WLA-SCS est vérifiée.

Toutes les nouvelles normes ou les mises à jour éditées par le WLA SRMC doivent être approuvées et validées par le Comité exécutif de la WLA, puis approuvées par les délégués présents à l'Assemblée générale biennale avant leur publication.

La structure de la présente norme est alignée aux recommandations de l'Organisation internationale de normalisation (ISO) en la matière. Par ailleurs, la WLA s'engage à tenir la WLA-SCS à jour et alignée à la norme ISO/CEI 27001.

Introduction

La présente norme définit des standards de sécurité, d'intégrité et de gestion des risques pour le secteur des loteries et des paris sportifs. Elle se veut la référence du secteur pour toutes les questions de sécurité et d'intégrité. Elle décrit un processus de gestion de la sécurité qui s'appuie à la fois sur les normes reconnues au niveau international et sur une base de sécurité commune représentant les règles de l'art pour les opérateurs de loteries et de paris sportifs. Elle comprend une série détaillée de contrôles et d'exigences pour les opérateurs de loterie et de paris sportifs, ainsi que pour leurs fournisseurs.

La présente norme peut être considérée comme le fondement de relations de confiance avec les parties prenantes et les régulateurs du secteur dans le but de mener des opérations de loterie et de paris sportifs ou des jeux multijuridictionnels, et peut également offrir une aide non négligeable à la haute direction en garantissant un examen indépendant afin de renforcer la confiance accordée à la sécurité des opérations de loteries et de paris sportifs.

La version la plus récente de la norme, WLA-SCS:2020, présente un nouveau cadre de certification à deux niveaux.

La conformité au niveau 1 de la norme WLA-SCS démontre un niveau de base essentiel en matière de sécurité de l'information des opérateurs de loteries et de paris sportifs et témoigne de leur engagement à atteindre le plus haut niveau de certification dans la norme WLA-SCS, soit le niveau 2. La certification au niveau 1 de la norme WLA-SCS convient aux organisations membres de la WLA qui préfèrent une approche graduelle à la certification.

La conformité au niveau 2 de la norme WLA-SCS permet aux organisations membres de la WLA d'assurer l'intégrité, la disponibilité et la confidentialité des services et des informations indispensables à la sécurité de leurs opérations. Grâce à la conjugaison de l'évaluation des contrôles pour les opérateurs de loteries et de paris sportifs et la conformité à la norme ISO/CEI 27001 pour les systèmes de management de la sécurité de l'information, le niveau 2 de la norme WLA-SCS représente la norme de certification la plus complète et étendue disponible pour les opérateurs de loteries et de paris sportifs, et leurs fournisseurs.

L'adoption de la norme WLA-SCS est une décision stratégique. La conception et la mise en œuvre des systèmes de management de la sécurité et de l'intégrité d'une organisation sont influencées par ses besoins spécifiques, ses objectifs, ses exigences en matière de risques et de sécurité, les processus qu'elle emploie, la taille et la structure de l'organisation. Ces facteurs et les systèmes qui les soutiennent sont censés évoluer dans le temps et la mise en œuvre d'un système de management doit donc s'adapter aux besoins de l'organisation. À titre d'exemple, une situation simple nécessite un système simple.

La conformité à la norme WLA-SCS peut être utilisée par les parties internes et externes intéressées afin d'évaluer la sécurité et l'intégrité des systèmes d'un opérateur de loteries et de paris sportifs, et de leurs fournisseurs.

En plus de se aligner à la norme ISO/CEI 27001, la WLA-SCS respecte les exigences de la norme ISO 9001 afin d'assurer une mise en œuvre et une application intégrées et cohérentes avec les normes de gestion s'y rapportant.

1. Champ d'application de la norme

La norme WLA-SCS englobe tous les types d'opérations de loteries et de paris sportifs, y compris les entreprises commerciales, les agences gouvernementales et les organisations à but non lucratif.

Elle spécifie les exigences d'établissement, de mise en œuvre, d'exploitation, de surveillance, de révision, de maintenance et d'amélioration d'un système documenté de sécurité et d'intégrité dans le contexte des risques globaux de l'organisation.

Les exigences définies dans la WLA-SCS sont d'ordre général et sont destinées à être appliquées par toutes les organisations de quelque type, taille et nature que ce soient. Dans tous les cas, il ne peut être toléré d'exclure aucune des exigences spécifiées dans les annexes A, B, C ou D, lorsqu'une organisation affirme se conformer à la WLA-SCS.

Toute exclusion jugée nécessaire des contrôles établis dans les annexes A, B, C ou D doit être justifiée de façon formelle et des preuves doivent être avancées afin de démontrer que les exclusions ont été acceptées par les responsables de l'organisation. Lorsque des contrôles ont été exclus, les demandes de conformité à la norme WLA-SCS ne peuvent être reçues que dans la mesure où lesdites exclusions n'affectent pas la capacité de l'organisation ou sa responsabilité à garantir une sécurité et une intégrité répondant aux exigences déterminées par une évaluation des risques ainsi qu'aux exigences légales ou réglementaires applicables. Tous les contrôles des annexes A, B, C ou D ayant été exclus seront notés dans le périmètre de certification décrit dans le certificat WLA-SCS.

Remarque : si une organisation dispose déjà d'un système opérationnel de gestion des processus commerciaux (en rapport avec la norme ISO 9001 ou ISO 14001, par exemple), il est recommandé dans la plupart des cas de satisfaire les exigences de la WLA-SCS dans le cadre du système de management existant.

Important : la WLA-SCS ne prétend pas inclure toutes les dispositions nécessaires d'un contrat. Les membres de la WLA adoptant la norme WLA-SCS sont responsables de son application correcte. La conformité avec une norme ne dispense pas en soi de toute autre obligation légale.

2. Références normatives

Les documents ci-après servent de références normatives dans le présent document et sont indispensables à son application. Pour les références datées, s'applique uniquement l'édition citée ; pour les non datées, l'édition la plus récente du document référencé (y compris toutes les modifications).

ISO/CEI 27001 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

ISO/CEI 27017 Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage.

WLA-SCS:2020 Code de pratique – directives de bonnes pratiques relatives aux exigences et contrôles de la sécurité et de l'intégrité de la norme WLA-SCS.

Guide de certification à la norme WLA-SCS.

3. Termes et définitions

3.1 Abréviations courantes

WLA : World Lottery Association

WLA-SCS : WLA Security Control Standard (norme de contrôle de la sécurité de la WLA)

WLA SRMC : WLA Security and Risk Management Committee (Comité de gestion des risques et de la sécurité de la WLA)

3.2 Définitions

Cette section dresse uniquement la liste des termes utilisés avec un sens particulier dans les pages de la présente norme. La majorité des termes présents dans cette norme sont utilisés conformément à leur définition dans un dictionnaire ou selon leur définition communément admise, qu'il est possible de consulter dans les glossaires de sécurité de l'ISO ou d'autres recueils de termes bien connus sur la sécurité.

Actifs : informations ou ressources à protéger par des contremesures.

Personnel : désigne tout employé, entrepreneur ou autre tierce partie travaillant pour l'opérateur de loteries ou pour le fournisseur de technologie de loterie qui, par sa fonction ou son accès, pourrait affecter la confidentialité, la disponibilité ou l'intégrité de l'opérateur de loteries.

Système de jeu : désigne les systèmes requis pour le fonctionnement des jeux, qui comprend le système central de jeu et tous ses composants périphériques nécessaires au fonctionnement de ces jeux.

Systèmes de jeu numériques : désigne toute la technologie permettant l'offre des jeux par un canal de vente numérique.

4. Vue d'ensemble

Dans leur approche de sécurité et d'intégrité, les organisations membres de la WLA ont pour objectif principal de garantir un fonctionnement approprié, ainsi que d'inspirer de la confiance.

La confiance accordée au fonctionnement d'un opérateur de loteries et de paris sportifs est essentielle pour conserver les joueurs et les autres parties prenantes. Par conséquent, les organisations membres de la WLA doivent développer et entretenir un environnement visible et documenté de sécurité et d'intégrité.

Le WLA SRMC a décrit dans la WLA-SCS les exigences, les objectifs de contrôle et les contrôles considérés comme étant les règles de l'art. Un opérateur de loteries et de paris sportifs doit disposer d'un système de management de la sécurité de l'information qui met en œuvre toutes les exigences mentionnées dans l'ISO/CEI 27001, ainsi que les exigences et contrôles obligatoires de la norme WLA-SCS.

La WLA-SCS intègre des exigences et des contrôles de base au sein du processus général de sécurité, d'intégrité et de gestion des risques de l'opérateur de loteries et de paris

sportifs, tout en évitant les chevauchements avec les cadres de sécurité plus généraux. Elle fournit aux professionnels de la sécurité et de l'intégrité des opérateurs de loteries et de paris sportifs un processus grâce auquel ils peuvent formellement gérer, mettre à jour et améliorer en continu leurs contrôles. Par conséquent, les opérateurs de loteries et de paris sportifs doivent développer et maintenir un environnement visible et documenté de sécurité.

La WLA-SCS comprend quatre parties qui détaillent les contrôles minimaux requis pour la gestion efficace de la sécurité et de l'intégrité par les opérateurs de loteries et de paris sportifs, ainsi que par les fournisseurs à l'industrie.

La première partie (annexe A – contrôles «G»: contrôles pour toutes les organisations) comprend la conformité aux exigences de la norme ISO/CEI 27001 dans une étendue globale, en y ajoutant 24 contrôles de base de la WLA.

La deuxième partie (annexe B – contrôles «L»: contrôles pour les opérateurs de loteries) fournit 64 contrôles supplémentaires de sécurité et d'intégrité spécifiques aux loteries et aux paris sportifs, tous représentatifs des règles de l'art en vigueur.

La troisième partie (annexe C – contrôles «S»: contrôles pour les opérateurs et les fournisseurs de systèmes de jeu) comprend 21 contrôles basés sur les produits et services offerts par les opérateurs de loteries et de paris sportifs.

La quatrième partie (annexe D – contrôles «M»: contrôles pour les jeux multijurisdictionnels) comprend 11 contrôles exigés pour participer à des jeux gérés par la Multi-State Lottery Association (MUSL).

5. Exigences générales en matière de gestion de la sécurité et de l'intégrité

5.1 Système de management de la sécurité de l'information (SMSI)

Les organisations désirant se certifier au niveau 2 de la WLA-SCS:2020 devront utiliser un système de management de la sécurité de l'information (SMSI) répondant aux exigences de la norme ISO/CEI 27001.

5.2 Périmètre du SMSI

Le périmètre du SMSI doit couvrir toutes les activités de l'organisation liées aux loteries et aux paris sportifs, y compris tous les actifs et les systèmes d'information s'y rapportant. Il ne peut exclure que les opérations de l'organisation qui n'ont aucun rapport avec ses activités de loteries et de paris sportifs. Toutes les opérations exclues doivent alors être identifiées, en justifiant dans le détail les motifs de leur exclusion. Les fonctions organisationnelles d'ordre général (ressources humaines, planification, finances, etc.) nécessaires à la réalisation des opérations de loteries et de paris sportifs relèvent de ce périmètre.

5.3 Déclaration d'applicabilité

La déclaration d'applicabilité du SMSI de l'organisation doit inclure explicitement tous les contrôles figurant dans les annexes A, B, C et D de la WLA-SCS. Aucun contrôle ne doit être exclu, mais certains contrôles de l'annexe B et C peuvent s'avérer non applicables. Les allégations de non-applicabilité doivent être justifiées en détail.

Il est tout à fait inacceptable que l'une des exigences spécifiées dans la présente clause, ainsi que dans les annexes A, B, C et D, soit exclue dès lors qu'une organisation déclare sa conformité à la WLA-SCS.

Toute non-applicabilité des contrôles des annexes B et C jugées nécessaires doit être justifiée de façon formelle et des preuves doivent être avancées afin de démontrer que la non-applicabilité a été acceptée par les responsables de l'organisation. Lorsque des contrôles sont non applicables, les demandes de conformité ne peuvent être reçues que dans la mesure où lesdites exclusions n'affectent pas la capacité de l'organisation ou sa responsabilité à garantir une sécurité et une intégrité répondant aux exigences déterminées par une évaluation des risques ainsi qu'aux exigences légales ou réglementaires applicables.

Annexe A (contrôles «G»): contrôles pour toutes les organisations

G.1	**Organisation de la sécurité**	
G.1.1	**Attribution des responsabilités en matière de sécurité**	
Objectif:	S'assurer que les responsabilités de la fonction de sécurité sont effectivement mises en œuvre.	
G.1.1.1	Forum de la sécurité	*Contrôle* Un forum de la sécurité ou toute autre structure organisationnelle constituée de responsables seniors doit être formellement créé. Ce forum pilote et révise le SMSI afin de s'assurer qu'il soit toujours adapté, adéquat et efficace, établit des comptes rendus formels de ses réunions et se réunit au moins tous les six mois.
G.1.1.2	Fonction de sécurité	*Contrôle* Il doit exister une fonction de sécurité. Cette fonction est responsable de la conception d'une stratégie de sécurité conforme à l'organisation globale. La fonction de sécurité travaillera ensuite avec les autres divisions de l'organisation afin de mettre en œuvre les plans d'action s'y rattachant. Elle doit être impliquée dans la révision de l'ensemble de tâches et de processus nécessaires en matière de sécurité de l'organisation, y compris, sans toutefois s'y limiter, la protection des informations et des données, les communications, l'infrastructure physique et virtuelle, le personnel, ainsi que la sécurité opérationnelle globale de l'organisation.
G.1.1.3	Rattachement de la fonction de sécurité	*Contrôle* La fonction de sécurité doit être rattachée à un responsable de niveau direction et être indépendante de la fonction de technologie en ce qui concerne la gestion du risque pour la sécurité.
G.1.1.4	Position de la fonction de sécurité	*Contrôle* La fonction doit posséder les compétences nécessaires, être dotée de suffisamment de pouvoirs et avoir accès à toutes les ressources nécessaires de l'entreprise lui permettant d'évaluer, de gérer et de réduire correctement les risques.
G.1.1.5	Responsabilité de la fonction de sécurité	*Contrôle* Le responsable de la fonction de sécurité doit être un membre titulaire du forum de la sécurité et être responsable des recommandations en matière de politiques de sécurité et de changements.

G.2	Sécurité des ressources humaines	
G.2.1	**Mise en œuvre d'un code de conduite**	
Objectif :	S'assurer qu'un code de conduite adapté est effectivement mis en œuvre.	
G.2.1.1	Code de conduite	*Contrôle* Un code de conduite doit être diffusé à tout le personnel lors de leur embauche. Tout le personnel doit donner une acceptation formelle de ce code.
G.2.1.2	Adhésion et mesures disciplinaires	*Contrôle* Le code de conduite comprend des déclarations selon lesquelles toutes les politiques et procédures sont respectées et que toute infraction ou autre violation du code peut entraîner des mesures disciplinaires.
G.2.1.3	Conflit d'intérêts	*Contrôle* Le code de conduite doit comprendre des déclarations affirmant que le personnel doit déclarer les conflits d'intérêts avec leur travail dès qu'ils apparaissent. Des exemples précis de conflits d'intérêts sont mentionnés dans le code.
G.2.1.4	Invitations et cadeaux	*Contrôle* Le code de conduite doit comprendre une politique anticorruption traitant également des invitations et cadeaux fournis par ou donnés à des personnes ou des entités avec lesquelles l'organisation entretient des relations d'affaires.
G.2.1.5	Politique de l'organisation sur le jeu	*Contrôle* Il doit exister une politique interne, conforme aux exigences légales et réglementaires, abordant le droit au jeu du personnel et de ceux qui en dépendent financièrement. Les membres du personnel dont leur fonction pourrait affecter l'intégrité des jeux sans collusion ne bénéficieront pas de ce droit. La politique doit définir explicitement les fonctions concernées par l'interdiction de jeu, qui doit être définie par voie contractuelle avec le personnel ou son employeur (si ce n'est pas l'opérateur de loteries).
G.2.1.6	Sécurité du personnel	*Contrôle* Il doit exister une politique et un processus permettant, par une vérification de sécurité, d'établir la confiance dans les individus qui pourraient affecter l'intégrité des jeux. Il doit y avoir également une politique et un processus associés pour superviser l'activité du personnel sur le système afin de détecter et examiner les activités pouvant affecter l'intégrité du jeu. Ces politiques doivent garantir un équilibre entre le droit à la vie privée de l'individu et l'obligation de la loterie de protéger l'intégrité des jeux.
G.2.1.7	Séparation des responsabilités	*Contrôle* Il doit exister une politique de séparation de fonctions décrivant les fonctions et les responsabilités respectives des personnes responsables des processus critiques pouvant affecter l'intégrité d'un jeu, comme entre autres, le processus de tirage et le paiement des gains. Le but est d'éviter les collusions possibles. De plus, aucun groupe ni équipe n'aura un contrôle global, sans la supervision de la direction, lui permettant d'affecter l'intégrité du jeu. Dans le cas d'un fournisseur de technologie de loterie, ce contrôle doit être appliqué aux aspects critiques du code pouvant affecter l'intégrité d'un jeu, tel que, sans s'y limiter, la gestion des entrés-sorties du générateur des nombres aléatoires utilisée pour déterminer le résultat des jeux.

G.2.2	Protection du personnel	
Objectif :	S'assurer que le personnel reçoit un niveau de protection adéquat.	
G.2.2.1	Politique sur la protection du personnel	*Contrôle* Une politique doit être établie afin de s'assurer que tout le personnel, qui travaille en solitaire, à distance en extérieur, ou à l'intérieur des locaux de l'opérateur de loteries dans les zones accessibles au public, reçoit un niveau de protection adéquat pour sa sécurité et son intégrité physique.

G.3	Sécurité physique et de l'environnement	
G.3.1	**Zones protégées**	
Objectif :	S'assurer que les zones permettant l'accès aux centres de production des données de jeux ou à d'autres systèmes effectivement importants pour les opérations de jeux sont correctement protégées.	
G.3.1.1	Contrôles physiques d'entrée	*Contrôle* L'accès physique aux centres de production des données de jeux, aux salles informatiques, aux centres d'exploitation des réseaux et à d'autres zones définies comme critiques sera restreint et sécurisé adéquatement ou il y aura du personnel pour les surveiller en tout temps. Bien que ce contrôle soit fondé sur les risques, dans la pratique il devra y avoir un processus vérifiable d'authentification à deux facteurs, minimum.

G.4	Contrôle d'accès aux systèmes de jeu	
G.4.1	**Gestion d'accès des utilisateurs**	
Objectif :	Permettre l'accès autorisé des utilisateurs et interdire l'accès non autorisé aux systèmes de jeu. Pour les fournisseurs de technologie, les contrôles établis dans la section G.4 doivent être appliqués aux dépôts de code employés pour développer les systèmes de jeu.	
G.4.1.1	Fonctions d'accès des utilisateurs	*Contrôle* La gamme de fonctions offertes à l'utilisateur sera définie en lien avec le propriétaire du processus, la fonction informatique et la fonction de sécurité.
G.4.1.2	Journal d'accès des utilisateurs	*Contrôle* Toutes les actions exécutées sur les systèmes de jeu, soit par des comptes système ou par des comptes d'utilisateurs, doivent être enregistrées et ces enregistrements doivent être supervisés et analysés régulièrement. En cas de besoin, des mesures appropriées seront prises.

G.5	Maintenance des systèmes d'information	
G.5.1	**Contrôles cryptographiques**	
Objectif :	Protéger la confidentialité, l'authenticité et l'intégrité des clés cryptographiques et des informations importantes relatives aux clients, aux jeux et à la loterie au moyen de techniques cryptographiques.	
G.5.1.1	Contrôles cryptographiques pour la confidentialité et l'intégrité des données entreposées sur les systèmes portables et les terminaux de loterie	*Contrôle* Des procédés cryptographiques doivent être appliqués afin de protéger la confidentialité des informations sensibles entreposées sur les systèmes informatiques portables (dans les dispositifs d'utilisateur final, comme les ordinateurs portables, et dans les supports amovibles, comme les clés USB et d'autres similaires) et pour assurer l'intégrité des données entreposées sur les terminaux de loterie.
G.5.1.2	Contrôles cryptographiques pour la confidentialité et l'intégrité des données en transit sur les réseaux	*Contrôle* Des procédés cryptographiques doivent être appliqués afin de protéger la confidentialité et l'intégrité des informations sensibles transférées dans des réseaux, dont l'analyse de risque a montré qu'ils ne présentaient pas un niveau de protection suffisant. Les informations sensibles comprennent, sans toutefois s'y limiter, les données de validation ou toute autre information importante relative aux jeux, aux clients et aux transactions financières.
G.5.1.3	Contrôles cryptographiques pour l'intégrité des informations sensibles des tickets	*Contrôle* Des contrôles cryptographiques d'intégrité doivent être appliqués pour le stockage des informations relatives aux tickets gagnants et à la validation. Ce contrôle s'applique à tous les types de jeux.

G.5.2	**Test du système**	
Objectif :	Activer et effectuer des tests sur le système.	
G.5.2.1	Méthodologie et données de test	*Contrôle* La méthodologie de test doit comprendre des mesures permettant d'empêcher l'utilisation des données créées en environnement de production pour la période du tirage en cours et d'empêcher l'utilisation des informations personnelles de joueurs, de détaillants ou du personnel. Dans ce contexte, la période de tirage doit être interprétée comme la période pendant laquelle les gains peuvent encore être réclamés.
G.5.2.2	Tests de sécurité sur le système de jeu	*Contrôle* Des tests complets sur la fonctionnalité de sécurité du système de jeu doivent être effectués avant l'utilisation de l'environnement de production et lors de tout changement significatif.

G.5.3	Sécurité du cloud	
Objectif :	Assurer la sécurité de l'information des systèmes de loterie hébergés dans le cloud.	
G.5.3.1	Sécurité du cloud	*Contrôle* Les environnements cloud qui hébergent les systèmes de jeu doivent être conformes à la norme ISO/CEI 27017. Un environnement cloud est défini comme une plateforme externe, gérée par une tierce partie, offrant une suite d'applications auxquelles l'organisation s'abonne pour recevoir des services tels que : infrastructure en tant que service, plateforme en tant que service, logiciel en tant que service, entre autres, qui sont nécessaires à son fonctionnement. Pour les fournisseurs de technologie, les contrôles établis dans la section G.5.3 de la norme WLA-SCS doivent être appliqués aux dépôts de code source employés pour développer les systèmes de jeu.

G.6 Disponibilité du système et continuité d'exploitation

G.6.1	Disponibilité des services et continuité de l'exploitation	
Objectif :	Assurer la protection de l'image et de la réputation de l'organisation et réagir face à des interruptions des activités d'exploitation.	
G.6.1.1	Exigences de disponibilité et résilience	*Contrôle* L'organisation disposera d'une liste de services essentiels aux joueurs (canaux de vente au détail et numériques) nécessaires au fonctionnement continu des jeux de loterie, ainsi que des exigences de disponibilité et de résilience de ces services. Les systèmes doivent être conçus conformément à ces exigences.
G.6.1.2	Continuité d'exploitation	*Contrôle* L'organisation doit préparer un plan documenté de continuité d'exploitation couvrant, à tout le moins, le fonctionnement continu des jeux de loterie et la confiance continue des parties prenantes dans l'intégrité des opérations de loterie. L'organisation doit également planifier, réaliser et évaluer des exercices de continuité d'exploitation à intervalles réguliers afin de se préparer aux situations de crise, couvrant les éléments inclus dans le plan de continuité d'exploitation.

Annexe B (contrôles «L»): contrôles pour les opérateurs de loteries

L.1	**Tickets à gratter physiques**	
L.1.1	**Fonctionnement des jeux de grattage**	
Objectif:	S'assurer que les éléments conceptuels du jeu, ainsi que sa production, sont conformes aux obligations légales et réglementaires, et s'assurer de l'intégrité du jeu et de prévenir la fraude.	
L.1.1.1	Sélection des imprimeurs/fournisseurs	*Contrôle* Il existe un processus d'approbation formel dans lequel participe la fonction de sécurité.
L.1.1.2	Exigences d'intégrité et tests	*Contrôle* L'organisation doit mettre en place une procédure documentée, en spécifiant les exigences d'intégrité pour chaque jeu de grattage pendant tout son cycle de vie, dès sa conception jusqu'à sa destruction. Les exigences d'intégrité doivent inclure, au moins, les visuels et les textes finaux, le tableau de lots, la protection des fichiers de validation/gagnants, les contrôles de la qualité, l'inventaire auditable à des fins de distribution, la localisation des livrets, ainsi que les tests appropriés des exigences avant l'acceptation du jeu, entre autres.
L.1.1.3	Intégrité des données de jeux	*Contrôle* Des contrôles sont mis en place pour permettre d'assurer l'intégrité des données de jeux. Ces contrôles incluent, sans s'y limiter, l'importation des données de jeux dans le système de jeu ainsi que le transfert des données de validation entre le fournisseur, l'opérateur et les détaillants.
L.1.1.4	Confidentialité des tickets gagnants	*Contrôle* Des contrôles sont mis en place pour s'assurer que, avant la réclamation des prix, personne dans l'organisation n'a accès ni connaissance de quel ticket à gratter est un ticket gagnant et lequel ne l'est pas. Il ne sera pas non plus possible d'identifier la localisation du ticket gagnant ni à quel détaillant il a été attribué.

L.2	Tirages de loterie	
L.2.1	**Gestion du tirage de loterie**	
Objectif :	S'assurer que les tirages sont effectués au moment spécifié par la réglementation et conformément aux règles du jeu de la loterie concernée.	
L.2.1.1	Tirage	*Contrôle* Une politique est rédigée pour garantir que les tirages sont effectués de manière planifiée et contrôlée, et conformément à des instructions précises.
L.2.1.2	Instructions du tirage	*Contrôle* L'organisation doit diffuser avant chaque tirage des instructions, notamment les instructions spécifiques relatives à ce tirage.
L.2.1.3	Membres de l'équipe de tirage	*Contrôle* Les instructions doivent comprendre la liste des membres de l'équipe de tirage et leurs numéros de téléphone.
L.2.1.4	Rôles des membres de l'équipe de tirage	*Contrôle* Les instructions doivent comprendre le descriptif des rôles de chaque membre de l'équipe.
L.2.1.5	Équipe de tirage suppléante	*Contrôle* Les instructions doivent comprendre les noms des suppléants ainsi que les modalités de leur intervention.
L.2.1.6	Déroulement du tirage	*Contrôle* Les instructions doivent comprendre le déroulement précis du tirage, de l'ouverture du site de tirage à sa fermeture.
L.2.1.7	Observateurs présents lors du tirage	*Contrôle* Les instructions doivent comprendre les exigences (issues de la réglementation des loteries) concernant la participation d'observateurs indépendants lors du tirage.

L.2.2	**Modalités du tirage**	
Objectif :	S'assurer que la procédure de tirage respecte les exigences réglementaires et les règles du jeu de la loterie concernée.	
L.2.2.1	Procédure de tirage	*Contrôle* L'organisation doit établir une procédure détaillant toutes les étapes du tirage, permettant de s'assurer qu'elles sont conformes aux règles du jeu de la loterie concernée et à la réglementation.
L.2.2.2	Guide étape par étape du tirage	*Contrôle* La procédure de tirage doit comprendre un guide étape par étape du processus de tirage.
L.2.2.3	Lieu du tirage	*Contrôle* La procédure de tirage doit comprendre le lieu du tirage.
L.2.2.4	Participants au tirage et responsabilités	*Contrôle* La procédure de tirage doit comprendre la liste des participants au tirage ainsi que leurs rôles et responsabilités.
L.2.2.5	Surveillance du tirage	*Contrôle* La procédure de tirage doit comprendre les modalités de participation d'un tiers indépendant (ex. : huissier) ou d'un auditeur indépendant.
L.2.2.6	Sécurité des opérations de tirage	*Contrôle* La procédure de tirage doit comprendre les mesures de sécurité applicables aux opérations de tirage et à l'ensemble des équipements utilisés lors du tirage.
L.2.2.7	Urgence durant le tirage	*Contrôle* La procédure de tirage doit comprendre les actions à mener en cas d'urgence intervenant durant le déroulement du tirage.
L.2.2.8	Intégrité du tirage, alerte et communication	*Contrôle* L'opérateur de loteries doit mettre en place un système ou un processus permettant de s'assurer qu'aucune personne ou aucun groupe de personnes ayant accès au système central de jeu ne manipule les transactions avant, durant ou après le tirage. Ce système ou ce processus permet également d'établir une piste de vérification détaillée de l'accès de l'utilisateur ainsi qu'un audit des transactions.

L.2.3	**Équipement de tirage et jeux de boules**	
Objectif :	S'assurer que les équipements de tirage et les jeux de boules respectent les normes de sécurité définies ou les spécifications réglementaires.	
L.2.3.1	Procédure d'inspection	*Contrôle* L'équipement de tirage (comprenant les jeux de boules) doit être inspecté lors de sa livraison puis à intervalles réguliers par un organisme indépendant attestant de sa conformité technique et du respect des normes. Une procédure est rédigée en ce sens.
L.2.3.2	Inspection et entretien réguliers	*Contrôle* Des interventions d'entretien et de vérification doivent être effectuées régulièrement (minimum une fois par an) sur l'équipement de tirage, afin de s'assurer du respect des normes tout au long de la vie de l'équipement.
L.2.3.3	Jeux de boules compatibles	*Contrôle* L'organisation doit s'assurer que les jeux de boules utilisés respectent les critères de dimension et de poids compatibles avec l'équipement de tirage. Une procédure est rédigée en ce sens.
L.2.3.4	Remplacement de l'équipement de tirage	*Contrôle* Dans le cas où les tirages sont retransmis en direct, l'organisation doit s'assurer qu'il existe un équipement ainsi qu'un jeu de boules de secours utilisables en cas de problème mécanique ou autre. Une procédure est rédigée en ce sens.
L.2.3.5	Transport, entreposage et manipulation de l'équipement de tirage et des jeux de boules	*Contrôle* L'organisation doit s'assurer que l'équipement de tirage et les jeux de boules sont transportés, entreposés et manipulés dans de bonnes conditions de sécurité. Une procédure est rédigée en ce sens.
L.2.3.6	Retransmission/diffusion en direct du tirage	*Contrôle* Lorsque les tirages sont retransmis ou diffusés en direct sur Internet, une procédure doit être appliquée afin de réduire les risques associés à la corruption des données, au retard de l'audio ou de la vidéo, aux erreurs dans la génération graphique ou autres similaires qui pourraient miner la confiance du public envers l'intégrité du tirage.

L.2.4	**Tirages de loterie et jeux de grattage électroniques**	
Objectif :	Garantir l'intégrité du système de tirage électronique au moyen d'une protection physique et logique. Cette section couvre les jeux à tirage et à grattage électroniques.	
L.2.4.1	Protection physique et logique du système technique	*Contrôle* Les mesures nécessaires doivent être prises pour garantir d'une part la protection logique du générateur de nombres aléatoires (source entropique) et de l'algorithme de tirage et d'autre part que seules les personnes autorisées en disposent d'un accès physique, afin d'empêcher toute modification des paramètres de l'algorithme de tirage et de la source entropique. Le ou les systèmes physiques doivent être protégés contre le vol, les modifications non autorisées et les interférences.
L.2.4.2	Transmissions sécurisées	*Contrôle* Des mesures doivent être prises afin d'assurer l'intégrité et l'authenticité des données transmises entre le générateur de nombres aléatoires (source entropique) et l'algorithme de tirage.
L.2.4.3	Caractère aléatoire du tirage électronique et vérification de l'intégrité	*Contrôle* Avant le déploiement, des tests et des vérifications doivent être effectués par des tierces parties indépendantes afin de vérifier que le système de tirage électronique est bien aléatoire. L'organisation doit documenter sa politique relativement aux tests et aux vérifications après le déploiement afin de vérifier que le générateur de nombres aléatoires et l'algorithme de tirage fonctionnent adéquatement.
L.2.4.4	Séparation des tâches	*Contrôle* Outre le contrôle G.2.1.7, une procédure spécifique doit être mise en place concernant la séparation des tâches impliquées dans un tirage électronique, afin de prévenir toute fraude interne. Notamment, personne ne doit être autorisé à effectuer plusieurs des types de tâches suivants : maintenance, surveillance ou réalisation des tirages sur un équipement de jeu électronique.

L.3	Sécurité chez les détaillants	
L.3.1	**Opérations chez les détaillants**	
Objectif :	S'assurer que les opérations chez les détaillants, en ligne ou en magasin, respectent les exigences organisationnelles de sécurité.	
L.3.1.1	Sécurité chez les détaillants	*Contrôle* Afin de s'assurer que les détaillants respectent les exigences organisationnelles de sécurité, l'organisation doit définir dans un contrat les obligations des détaillants et les conditions de sécurité qu'ils doivent respecter dans leur fonctionnement.

L.3.2	**Sécurité des terminaux de jeux**	
Objectif :	S'assurer de la bonne sécurité des terminaux de jeux	
L.3.2.1	Sécurité des transactions	*Contrôle* Les échanges de données entre les terminaux de jeux et le système central de jeu doivent être protégés. Des mesures sont mises en place afin d'assurer l'intégrité des transactions. Lorsqu'un dispositif du point de vente du détaillant est utilisé au lieu d'un terminal de loterie dédié, la transmission de données depuis l'application de loterie sur ce dispositif du point de vente au système central de jeu doit être protégée. On ne se fiera pas à la sécurité du dispositif du point de vente du détaillant pour l'intégrité des jeux de loterie.

L.4	Paiement des gains	
L.4.1	**Validation et paiement des gains**	
Objectif :	S'assurer que l'organisation a mis en place les contrôles nécessaires à la validation et au paiement des gains et prévenir la fraude liée aux gains non réclamés.	
L.4.1.1	Processus de validation	*Contrôle* L'organisation doit définir et mettre en œuvre des procédures afin d'assurer la validité des transactions gagnantes, des réclamations ou des tickets pour les différents niveaux de gains et les différents types de jeux, et de traiter les paiements des gains correspondants.
L.4.1.2	Référence unique sur le ticket	*Contrôle* Chaque ticket pour chaque jeu doit disposer d'un numéro de référence unique.
L.4.1.3	Sécurité des données des gains non réclamés	*Contrôle* L'organisation doit mettre en place des contrôles techniques et des procédures pour assurer la confidentialité, l'intégrité et la disponibilité des données des gains non réclamés. Ceci comprend au moins, les fichiers contenant des informations sur des transactions déterminées non encore réclamées, ainsi que tout fichier de validation, entre autres. Une considération spéciale doit être accordée au contrôle d'accès afin de restreindre l'accès aux données et contrôler l'interaction de l'utilisateur avec elles. Un processus doit être mis en place pour traiter les accès non autorisés et l'exportation des données.
L.4.1.4	Procédure pour le paiement des gains	*Contrôle* Il doit exister une procédure pour le paiement des gains, qui établit une période maximale de réclamation des gains ; cela comprend un processus pour auditer les derniers transferts à la clôture du jeu ; cela détaille les règlements et la diligence appropriée nécessaire avant de prendre une décision sur le paiement des tickets perdus, volés ou abîmés ; cela explique la procédure relative aux vérifications sur la validité des réclamations. Il doit exister également une procédure pour les paiements en retard ou à la dernière minute.
L.4.1.5	Détection de la fraude	*Contrôle* Des registres d'audit adéquats doivent être maintenus et révisés dans le cadre de la procédure de paiement des gains afin d'identifier les séquences inhabituelles de paiement de dernière minute et toute réclamation faite par les détaillants ou le personnel qui pourrait nécessiter une enquête.

L.5	Canaux de vente numériques et services interactifs	
L.5.1	**Systèmes de jeu numériques**	
Objectif :	Assurer la confidentialité, l'intégrité et la disponibilité des systèmes de jeu numériques, afin de protéger les données de jeu et les informations relatives aux joueurs.	
L.5.1.1	Systèmes à architecture multicouches	*Contrôle* L'organisation doit définir une architecture multicouche de la sécurité au sein de l'architecture des systèmes de jeu numériques de façon à garantir la sécurité du stockage et du traitement des informations.
L.5.1.2	Attaques actives et passives	*Contrôle* Des mesures appropriées doivent être mises en place pour détecter, prévenir, atténuer et répondre aux attaques techniques actives et passives les plus courantes. L'organisation doit également disposer de politiques convenues au sujet des correctifs des systèmes de jeu numériques, qu'ils soient développés et pris en charge en interne ou par une tierce partie.
L.5.1.3	Séparation des réseaux	*Contrôle* Les bases de données de production qui contiennent des informations relatives aux joueurs ou aux transactions doivent être stockées sur des réseaux distincts des serveurs qui hébergent les pages Web.
L.5.1.4	Information sur les sessions	*Contrôle* L'identifiant sur les sessions des utilisateurs doivent toujours être créées en mémoire selon une méthode aléatoire, puis être supprimées une fois les sessions correspondantes achevées.
L.5.1.5	Identification des points d'entrée et de sortie	*Contrôle* Tous les points d'entrée et de sortie vers les systèmes des réseaux publics doivent être identifiés, gérés, surveillés et contrôlés. L'organisation doit surveiller tous ses systèmes de jeu numériques afin de prévenir, détecter, atténuer et répondre aux cyberattaques.
L.5.1.6	Génération et stockage des fichiers journaux	*Contrôle* Des fichiers journaux de sécurité prédéfinis doivent être générés, et maintenus pour une durée déterminée, sur chaque composant du système sensible afin de surveiller et de rectifier les anomalies, les défauts et les alertes.
L.5.1.7	Tests de sécurité	*Contrôle* Il doit y avoir des tests de sécurité appropriés lors des changements majeurs dans le système. Des tests réguliers d'intrusion, qui tentent de trouver et d'exploiter les vulnérabilités ou d'autres faiblesses du système, doivent être effectués au moins une fois par année.
L.5.1.8	Divulgation responsable	*Contrôle* L'opérateur de loteries doit avoir mis en place une politique de divulgation responsable permettant que le public signale les vulnérabilités de sécurité à la loterie.

L.5.2	Compte de joueur	
Objectif :	Protéger le joueur et gérer le risque de fraude et de blanchiment d'argent.	
L.5.2.1	Compte de joueur	*Contrôle* Il existe un processus formel d'identification, d'authentification et d'autorisation du joueur. Les données du joueur et leur portefeuille doivent être considérés comme des actifs majeurs à des fins d'évaluation des risques.
L.5.2.2	Comptes de joueurs multiples	*Contrôle* Des mesures raisonnables sont mises en place pour assurer que chaque joueur n'a qu'un seul compte actif.
L.5.2.3	Exclusion de joueurs	*Contrôle* Un processus est établi pour exclure des joueurs conformément à la législation locale en vigueur ou aux procédures internes.
L.5.2.4	Détenteur de plusieurs moyens de paiement	*Contrôle* Une procédure doit être établie, conformément à la législation locale en vigueur, pour assurer la correspondance entre le détenteur d'un moyen de paiement avec le détenteur d'un compte de joueur afin d'éviter la fraude et le blanchiment d'argent.

L.5.3	Conception et approbation des jeux	
Objectif :	S'assurer que la conception des jeux répond aux exigences légales et réglementaires et que ceux-ci sont autorisés au niveau approprié avant leur lancement.	
L.5.3.1	Procédures documentées des jeux	*Contrôle* Les règles établies doivent couvrir la conception et le développement. De plus, les joueurs doivent pouvoir consulter les règles des jeux.
L.5.3.2	Approbation et modification des jeux	*Contrôle* Une procédure d'approbation doit être établie pour valider que chaque nouveau jeu ainsi que les modifications importantes dans le système de jeu numérique sont contrôlés. La conception finale des jeux doit être formellement approuvée au moyen d'un processus où la fonction de sécurité est impliquée.

L.5.4	**Sécurité des méthodes de paiement**	
Objectif :	Protéger les méthodes de paiement contre les usages frauduleux.	
L.5.4.1	Collecte de données	*Contrôle* La collecte de données sensibles directement liées au paiement doit être limitée uniquement aux données strictement nécessaires pour la transaction.
L.5.4.2	Protection de la méthode de paiement	*Contrôle* Des mesures adéquates doivent être prises pour protéger tout moyen de paiement utilisé dans le système contre une utilisation frauduleuse.
L.5.4.3	Validation du service de paiement	*Contrôle* L'organisation doit vérifier que le service de paiement garantit la protection des données des joueurs, y compris toute information personnelle identifiable fournie par le joueur ou les données liées au paiement.
L.5.4.4	Enregistrements des transactions portant sur les paiements	*Contrôle* L'organisation doit générer tous les enregistrements des transactions sur les comptes des joueurs. Les données enregistrées doivent permettre à l'organisation de tracer chaque opération financière d'un joueur indépendamment des autres.

L.6	Paris sportifs	
L.6.1	**Sélection de l'offre**	
Objectif :	Garantir l'intégrité de l'offre de paris.	
L.6.1.1	Encadrement de l'offre	*Contrôle* Le cadre dans lequel l'organisation propose des paris sportifs ainsi que les règles correspondantes doivent être définis, maintenus et publiés, y compris, sans toutefois s'y limiter, tous les types d'évènements sportifs et tous les types de paris autorisés pour chaque sport.

L.6.2	**Gestion des évènements, des cotes et des résultats**	
Objectif :	Garantir l'intégrité des évènements et leurs cotes correspondantes.	
L.6.2.1	Gestion des évènements, des cotes et des résultats	*Contrôle* Des procédures doivent être établies pour sélectionner les évènements, fixer et mettre à jour les cotes, la marge des paris ou le blocage des évènements, ainsi que pour recevoir les résultats de sources fiables. Un processus doit exister pour valider l'exactitude des données et prévenir les activités frauduleuses. Les procédures doivent se baser sur le respect de l'intégrité, le jeu responsable, et la garantie de transparence.
L.6.2.2	Paris en direct	*Contrôle* Il doit exister des procédures documentées pour garantir et surveiller l'intégrité de l'offre de paris en direct, de la gestion des résultats et de la protection de parieurs. À titre indicatif, les domaines à prendre en compte pour la procédure de gestion de résultats doivent comprendre, sans s'y limiter, les retards, les sources des résultats et l'annulation des résultats. Les procédures doivent également tenir compte des mécanismes de prévention contre la pratique de relayer des informations à des parieurs ou de placer des paris directement à partir d'un évènement (courtsiding), notamment, sans toutefois s'y limiter, le délai de transmission des images en direct.
L.6.2.3	Respect des limites de paiement	*Contrôle* L'organisation doit établir un ensemble de mesures pour garantir que les limites de paiements autorisées ne sont pas dépassées.

L.6.3	**Contrôle des fraudes et du blanchiment d'argent**	
Objectif :	Garantir des actions pour minimiser le risque de fraude ou de blanchiment d'argent.	
L.6.3.1	Contrôle des activités de paris sportifs	*Contrôle* Des procédures doivent être établies pour contrôler tous les changements de cotes ou bloquer un évènement sportif; suivre le marché, les évènements et les transactions des clients afin de détecter des irrégularités et pour surveiller les gagnants au-delà d'un certain montant de gains et les versements supérieurs à un montant déterminé. Les procédures doivent également spécifier les seuils et les méthodes de paiement des gains. Les procédures doivent s'établir conformément aux lois de la juridiction dans laquelle le membre certifié réside.

L.7	Appareils de loterie vidéo interactifs	
L.7.1	**Appareils de loterie vidéo (ALV)**	
Objectif :	Garantir le fonctionnement sécurisé de tous les ALV, quels que soient la conception du système et les modèles d'exploitation.	
L.7.1.1	ALV	*Contrôle* Les ALV doivent être surveillés en matière de sécurité et de pourcentage de paiement des gains.
L.7.1.2	Jeux ALV	*Contrôle* Les règles du jeu et le pourcentage total de paiement des gains doivent être à la disposition des clients.
L.7.1.3	Certificat de jeu ALV	*Contrôle* Les jeux dédiés aux ALV doivent être testés et un certificat attestant de l'intégrité et du pourcentage total de paiement des gains doit être émis et renouvelé.
L.7.1.4	Incidents ALV	*Contrôle* Il doit exister des procédures documentées pour gérer les litiges ou réclamations des clients concernant les gains ou les pertes.
L.7.1.5	Architecture du système des ALV	*Contrôle* L'organisation doit maintenir une description de l'architecture générale du système des ALV, y compris les mesures de sécurité, afin d'assurer l'intégrité des jeux ALV, ainsi que le traitement et le stockage sécurisé des données.

Annexe C (contrôles «S»): contrôles pour les opérateurs et les fournisseurs des systèmes de jeu

Les contrôles «S» s'appliquent aux systèmes de jeu (tel que définis dans cette norme) et doivent être inclus dans le périmètre de certification de l'organisation qui développe et/ou gère le système de jeu, qu'il s'agisse d'un fournisseur de technologie ou des développeurs chez l'opérateur.

S.1	**Assurance de la sécurité des systèmes de loteries**	
S.1.1	**Intégration de la sécurité dans le développement des applications des systèmes de jeu**	
Objectif:	Garantir la sécurité dans la conception des systèmes de jeu.	
S.1.1.1	Politique de sécurité pour le développement des applications	*Contrôle* Le fournisseur de technologie de loterie doit disposer d'une politique sur la sécurité des applications tout au long du cycle de vie du développement du logiciel.
S.1.1.2	Analyse statique et dynamique de code	*Contrôle* Le fournisseur de technologie de loterie doit effectuer des analyses statiques et dynamiques de code et transmettre un résumé de leurs résultats à l'opérateur conjointement avec les notes de mise à jour de son produit, depuis la première version et toutes les versions intermédiaires importantes, dans l'environnement de production.
S.1.1.3	Tests de sécurité	*Contrôle* Le fournisseur de technologie de loterie doit effectuer des tests de sécurité de leurs produits et/ou services, hébergés et configurés de manière à ce qu'ils montrent comment ils seront déployés par l'opérateur dans un environnement de production. Un résumé des résultats de ces tests doit être transmis à l'opérateur conjointement avec les notes de mise à jour de son produit, depuis la première version et toutes les versions intermédiaires importantes, dans l'environnement de production.
S.1.1.4	Pratiques de développement sécurisé	*Contrôle* Le fournisseur de technologie de loterie doit définir et demander à ses développeurs de suivre un ensemble de pratiques de développement sécurisé. Il doit également mettre en place des mesures lui permettant de vérifier l'efficacité et la conformité avec ces pratiques.
S.1.1.5	Formation et sensibilisation au développement sécurisé	*Contrôle* Le fournisseur de loterie doit disposer d'un programme de formation et sensibilisation aux pratiques de développement sécurisé pour tous les développeurs de code pour les systèmes de jeu (tel que définis dans cette norme).

S.1.2	**Mesures d'intégrité relatives au développement du matériel, du logiciel et du micrologiciel des systèmes de jeu**	
Objectif :	Garantir l'intégrité des technologies de loterie	
S.1.2.1	Contrôles d'intégrité lors du processus de développement/déploiement	*Contrôle* Le fournisseur de technologie de loterie doit garantir l'intégrité des matériels/micrologiciels qu'il a développés dans chaque étape du processus de développement, y compris au moins, sans s'y limiter, pendant le processus de contrôle de la qualité et lorsque le logiciel/micrologiciel est déployé dans un environnement de production.
S.1.2.2	Journalisation de sécurité	*Contrôle* Le fournisseur de technologie de loterie doit s'assurer de fournir les traces de sécurité appropriées des logiciels/micrologiciels qu'il a développés à l'équipe de sécurité de l'opérateur de loteries pour qu'elle puisse l'intégrer dans les outils de sécurité de l'organisation afin d'assurer l'intégrité de ses logiciels/micrologiciels. Le fournisseur de technologie de loterie doit fournir à l'équipe de sécurité un document détaillant les fonctionnalités des traces de sécurité.
S.1.2.3	Intégrité des fichiers	*Contrôle* Le fournisseur de technologie de loterie doit identifier et documenter les fichiers cruciaux dans leur produit afin que l'opérateur de loteries puisse vérifier l'intégrité de l'environnement de production.
S.1.2.4	Intégrité du matériel informatique	*Contrôle* Le fournisseur de technologie de loterie doit mettre en place des mesures permettant de découvrir les tentatives d'ajouts ou de modifications non autorisées du matériel du système de jeu qui pourraient affecter l'intégrité du système de loterie. Dans ce contexte, le matériel comprend au moins les appareils de loterie vidéo, les équipements de loterie dans les points de vente et les générateurs de nombres aléatoires, entre autres. La liste exhaustive du matériel auquel ce contrôle s'applique doit être déterminée par une évaluation des risques. Le matériel fourni et hébergé par un fournisseur d'infrastructure en tant que service sera dispensé de se conformer aux obligations de ce contrôle.
S.1.2.5	Gestion des vulnérabilités et des correctifs	*Contrôle* Le fournisseur de technologie de loterie doit garantir l'existence d'un processus pour la mise à jour en temps opportun du logiciel/micrologiciel et des bibliothèques de code d'une tierce partie employés. Une évaluation des risques permet de décider de l'application ou non des correctifs sur les systèmes de production de jeux, tout en considérant la politique de gestion des vulnérabilités et des correctifs de l'opérateur de loteries, ainsi que toute considération commerciale.
S.1.2.6	Divulgation responsable	*Contrôle* Le fournisseur de technologie de loterie doit mettre à la disposition des clients ayant acheté ses produits et services une politique de divulgation responsable permettant la divulgation des vulnérabilités de sécurité dans leurs produits de systèmes de jeu.

S.1.3	**Mesures d'intégrité liées à l'impression des tickets à gratter physiques**
Objectif :	Garantir l'intégrité des tickets à gratter physiques.

S.1.3.1	Exigences pour les jeux de grattage sur support physique	
Objectif :	Aligner les spécifications du fournisseur sur les exigences de l'opérateur de loteries.	
S.1.3.1.1	Exigences pour les jeux de grattage	*Contrôle* Le fournisseur doit valider formellement les exigences avec l'opérateur de loteries et les traduire en spécifications ; toute modification des spécifications doit suivre les processus de gestion des changements de l'opérateur de loteries et du fournisseur.

S.1.3.2	Création et validation des données	
Objectif :	Assurer la sécurité et la conformité aux exigences de la programmation des jeux de grattage.	
S.1.3.2.1	Génération de données pour les jeux de grattage	*Contrôle* Le processus de randomisation employé pour la génération des données de jeux de grattage est soumis à l'application des contrôles établis dans la section L.2.4 de la norme WLA-SCS relativement aux tirages de loterie et aux jeux de grattage électroniques, et aux exigences convenues entre l'opérateur et le fournisseur.
S.1.3.2.2	Validation des données de jeux	*Contrôle* Le fournisseur doit assurer qu'une équipe indépendante certifie que les données logiques du jeu sont conformes aux exigences de l'opérateur de loteries. Les rapports contenant les résultats doivent être mis à la disposition de l'opérateur de loteries.
S.1.3.2.3	Confidentialité des données	*Contrôle* Le fournisseur doit garantir que l'accès aux données de validation est en tout temps restreint, même après la livraison du jeu de grattage, conformément au principe de privilège minimal.

S.1.3.3	Impression	
Objectif :	Assurer l'intégrité du processus d'impression.	
S.1.3.3.1	Validation avant l'impression	*Contrôle* Le fournisseur doit valider formellement avec l'opérateur de loteries les visuels et les textes finaux des tickets avant leur impression.
S.1.3.3.2	Contrôles d'intégrité	*Contrôle* Le fournisseur doit effectuer régulièrement des vérifications d'intégrité sur les tickets.

S.1.3.4	Finition	
Objectif:	Assurer la conformité avec le tableau de lots et garantir l'intégrité des tickets lors de l'acheminement.	
S.1.3.4.1	Numéro de référence unique sur le ticket	*Contrôle* Des mesures doivent être prises pour que chaque ticket livré ait un numéro de référence unique.
S.1.3.4.2	Conformité avec le tableau de lots	*Contrôle* Le fournisseur doit prouver qu'il a fourni le bon nombre des tickets dans chaque lot d'impression, conformément au tableau de lots requis.
S.1.3.4.3	Tickets mis au rebut	*Contrôle* Il doit exister une procédure documentée pour assurer la destruction sécuritaire des tickets imprimés non délivrés.
S.1.3.4.4	Sécurité du transport	*Contrôle* Le fournisseur doit garantir la sécurité dans le transport des tickets entre le fournisseur et l'opérateur de loteries.

Annexe D (contrôles «M»): contrôles pour les jeux multijuridictionnels

M.1	**Exigences pour participer dans des jeux administrés par la Multi-State Lottery Association (MUSL)**	
M.1.1	**Sécurité, intégrité et disponibilité des transactions**	
Objectif:	Assurer la sécurité et l'enregistrement appropriés des transactions.	
M.1.1.1	Validation des réclamations	*Contrôle* En plus de se conformer aux contrôles établis dans la section L.4.1 du présent document, l'organisation devra respecter les normes minimales de sécurité du jeu de la MUSL.
M.1.1.2	Redondance des données de transaction	*Contrôle* Les enregistrements des données des transactions effectuées dans le système informatique de jeu doivent exister dans au moins deux emplacements différents du centre de données, suffisamment séparés de manière à ce qu'ils ne fassent pas l'objet de la même catastrophe informatique.
M.1.1.3	Accusé de réception de transaction	*Contrôle* Chaque emplacement doit recevoir et accuser réception des données de transaction avant l'autorisation d'impression des reçus.
M.1.1.4	Copie de sécurité des données du jeu	*Contrôle* Les données du jeu doivent être sauvegardées quotidiennement et stockées hors ligne et hors site.
M.1.1.5	Intégrité des transactions avant et après un tirage	*Contrôle* Une fonction de hachage cryptographique approuvée par la MUSL doit être appliquée à l'ensemble complet de transactions stockées par le système de contrôle interne avant chaque tirage afin de créer un condensé du hash. La même fonction de hachage cryptographique devra être appliquée à nouveau à l'ensemble complet de transactions une fois créé le rapport des gagnants par niveaux immédiatement après le tirage.

M.1.2	Sécurité du dispositif du point de vente du détaillant	
Objectif :	Assurer la sécurité des dispositifs du point de vente qui ne sont pas des terminaux de loterie dédiés.	
M.1.2.1	Dispositif du point de vente	*Contrôle* Lorsqu'un dispositif du point de vente du détaillant est utilisé au lieu d'un terminal de loterie dédié, le dispositif du point de vente doit se conformer aux exigences de l'Association nord-américaine de loteries d'État et provinciales (NASPL).
M.1.2.2	Terminaux de loterie non conçus pour émettre des tickets sur place	*Contrôle* Les terminaux qui n'ont pas été conçus pour émettre des tickets sur place, et auxquels ont accès les opérateurs du système de contrôle interne et du système informatique de jeu, doivent être modifiés de manière à ce qu'il soit clair que les tickets émis par ces terminaux ne sont pas valides. Ni les opérations *in situ* ni le personnel TI pourront se soustraire aux modifications.

M.1.3	Mises-éclair (Quick Picks)	
Objectif :	Assurer la sélection aléatoire des mises-éclair.	
M.1.3.1	Caractère aléatoire des mises-éclair	*Contrôle* Les logiciels employés pour générer les nombres aléatoires pour les mises-éclair doivent se conformer aux exigences établies dans la section L.2.4.3 de la norme WLA-SCS « Caractère aléatoire du tirage électronique et vérification de l'intégrité ».

M.1.4	Séparation entre le système de contrôle interne et le système informatique de jeu	
Objectif :	Assurer la séparation entre le système de contrôle interne et le système informatique de jeu (ICS et CGS, respectivement.)	
M.1.4.1	Séparation entre le système de contrôle interne et le système informatique de jeu	*Contrôle* En ce qui concerne le contrôle L.2.2.8 de la norme WLA-SCS « Intégrité du tirage, alerte et communication », si un fournisseur externe gère le système informatique de jeu, le ICS devra être géré par une autre organisation. Dans tous les cas, la responsabilité de ces deux systèmes doit être bien séparée ; personne n'aura accès total ou partiel aux deux systèmes : le ICS et le CGS.

M.1.5	Processus de tirage	
Objectif :	Assurer la continuité et l'intégrité entre le traitement des nombres gagnants et le traitement des transactions de vente.	
M.1.5.1	Utilisation du même personnel et du même système de contrôle interne	*Contrôle* L'opérateur de loteries, ou une autre organisation désignée par lui, doit utiliser le même personnel et le même système de contrôle interne pour traiter les transactions de vente et les nombres gagnants.

M.1.6	**Système de détection d'intrusion**	
Objectif :	Gérer les risques de cyberattaques aux systèmes ICS et CGS.	
M.1.6.1	Système de détection d'intrusion sur les réseaux des systèmes ICS et CGS	*Contrôle* Un système de détection d'intrusion et communication ou un système de prévention d'intrusion doit être en place sur les réseaux des deux systèmes, le ICS et le CGS, et doit être configuré activement pour qu'il notifie les administrateurs locaux.