World Lottery Association

WLA-SCS:2020

WLA Standard für Sicherheits-maßnahmen

Informations-, Betriebssicherheits- und Integritäts-anforderungen an Lotterie- und Sportwettenbetreiber und an deren Zulieferer

Veröffentlichung: Oktober 2020,
Version 1.1
(Revidiert: 10. Dezember 2020)

Inhalt

Vorwort

Die World Lottery Association (WLA) hat die Notwendigkeit angemessener Sicherheits- und Integritätsstandards für Lotterie- und Sportwettenbetreiber bereits bei ihrer Gründung erkannt und deshalb die von ihren Vorgängerorganisationen in diesem Bereich begonnene Arbeit weiter fortgesetzt.

Lotterie- und Sportwettenbetreiber müssen für ihre Geschäftstätigkeit eine transparente und dokumentierte, auf Sicherheit und Integrität ausgerichtete Umgebung aufbauen, die ihnen das Vertrauen der Spielteilnehmer und anderer Stakeholder dauerhaft sichert. Der WLA Standard für Sicherheitsmaßnahmen (WLA Security Control Standard, kurz WLA-SCS) unterstützt Lotterie- und Sportwettenbetreiber auf der ganzen Welt, ebenso wie deren Zulieferer, damit sie Maßnahmen auf einem Niveau erreichen, das den allgemein anerkannten Informationssicherheits- und Qualitätssicherungspraktiken wie auch den branchenspezifischen Anforderungen entspricht. Dies gibt den Lotterie- und Sportwettenbetreibern mehr Sicherheit in Bezug auf die Integrität ihrer Geschäftstätigkeit. Die Zertifizierung nach WLA-SCS ist ein objektiver Leistungsnachweis für die Sicherheitsmaßnahmen und das Risikomanagement eines Lotterie- und Sportwettenbetreibers.

Der WLA-SCS wurde vom WLA Ausschuss für Sicherheit und Risikomanagement (WLA Security and Risk Management Committee, kurz WLA SRMC) erarbeitet. Ihm gehören Vertreter und Sicherheitsexperten von Lotterie- und Sportwettenbetreibern aus der ganzen Welt an. Durch den Vergleich branchenüblicher Sicherheits- und Integritätspraktiken mit den von internationalen Lotterieexperten anerkannten Praktiken wurde ein solider Sicherheits- und Risikomanagementrahmen für Lotterie- und Sportwettenbetreiber und deren Zulieferer geschaffen.

Der WLA SRMC überprüft alle in der Lotterie- und Sportwettenbranche verwendeten Standards für Sicherheitsmaßnahmen und dient als Anlaufstelle für die Branche bei Fragen zu Sicherheit und Risikomanagement. Er überwacht die Zertifizierung nach WLA-SCS, mit der WLA Mitgliedern und assoziierten Mitgliedern die Erfüllung des Standards bescheinigt wird.

Alle vom WLA SRMC neu erarbeiteten oder aktualisierten Standards müssen vom WLA Exekutivkomitee (Executive Committee) gebilligt und freigegeben und von den Delegierten an der alle zwei Jahre stattfindenden Generalversammlung genehmigt werden, um formell gültig zu sein.

Die Struktur des WLA-SCS orientiert sich an derjenigen der International Standards Organization (ISO). Die WLA ist verpflichtet, ihn entsprechend der Norm ISO/IEC 27001 laufend zu aktualisieren und anzupassen.

Einleitung

Der WLA-SCS ist der Standard für Sicherheit, Integrität und Risikomanagement im Lotterie- und Sportwettensektor. Er ist für die Branche in Sachen Sicherheit und Integrität von zentraler Bedeutung. Der Standard beinhaltet einen Sicherheitsmanagement-Prozess, der sowohl international anerkannte Standards als auch die gängigen Sicherheitspraktiken der Lotterie- und Sportwettenbetreiber berücksichtigt. Er umfasst eine Vielzahl von Maßnahmen und Anforderungen, die Lotterie- und Sportwettenbetreiber und deren Zulieferer erfüllen müssen.

Der WLA-SCS dient als Grundlage für den Aufbau von Vertrauensverhältnissen mit Branchen-Stakeholdern und Aufsichtsbehörden im Rahmen der Durchführung von Lotterien und Sportwetten sowie grenzüberschreitenden Glücksspielen. Er unterstützt auch das Top-Management, indem er eine unabhängige Prüfung vorsieht, die das Vertrauen in die Sicherheit des Lotterie- und Sportwettenbetriebs erhöht.

Mit der neusten Fassung des Standards, WLA-SCS:2020, wird ein neuer zweistufiger Zertifizierungsrahmen eingeführt.

Die Erfüllung von WLA-SCS Stufe 1 stellt die Informationssicherheit von Lotterie- und Sportwettenbetreibern auf einem grundlegenden, aber entscheidenden Niveau sicher, mit dem Ziel, auch die WLA-SCS Stufe 2, die höchste Zertifizierungsstufe, zu erreichen. Die Zertifizierung nach WLA-SCS Stufe 1 eignet sich für solche WLA Mitglieder, welche die Zertifizierung eher Schritt für Schritt angehen wollen.

Durch die Erfüllung von WLA-SCS Stufe 2 gewährleisten WLA Mitglieder die Integrität, Verfügbarkeit und Vertraulichkeit der Dienstleistungen und Informationen, die für einen sicheren Betrieb entscheidend sind. Die Begutachtung der Maßnahmen der Lotterie- und Sportwettenbetreiber wird zudem mit der Erfüllung der Norm ISO/IEC 27001 für Informationssicherheits-Managementsysteme verbunden. Damit stellt die WLA-SCS Stufe 2 den komplettesten und umfassendsten Zertifizierungsstandard für Lotterie- und Sportwettenbetreiber und deren Zulieferer dar.

Die Einführung des WLA-SCS ist eine strategische Entscheidung. Die Entwicklung und Umsetzung der Sicherheits- und Integritätsmanagementsysteme einer Organisation hängt von ihren spezifischen Bedürfnissen, Zielen, Risiken, Sicherheitsanforderungen, verwendeten Prozessen, ihrer Größe und ihrer Struktur ab. Diese Faktoren und die ihnen zugrunde liegenden Systeme können sich im Laufe der Zeit ändern. Außerdem ist davon auszugehen, dass ein Managementsystem jeweils entsprechend den Bedürfnissen der Organisation ausgelegt wird, d. h. eine einfache Organisation erfordert nur ein einfaches System.

Die Einhaltung des WLA-SCS kann von interessierten internen und externen Parteien zur Beurteilung der Sicherheit und Integrität der Systeme eines Lotterie- und Sportwettenbetreibers und seiner Zulieferer herangezogen werden.

Neben ISO/IEC 27001 entspricht der WLA-SCS auch ISO 9001. Er ermöglicht somit eine einheitliche und integrierte Einführung und Umsetzung zusammen mit den entsprechenden Managementstandards.

1. Geltungsbereich

Der WLA-SCS gilt für alle Arten von Lotterie- und Sportwettenbetreibern, einschließlich kommerzieller Unternehmen, staatlicher Institutionen und gemeinnütziger Organisationen.

Der WLA-SCS spezifiziert die Anforderungen an Aufbau, Implementierung, Betrieb, Überwachung, Überprüfung, Unterhalt und Optimierung eines dokumentierten Sicherheits- und Integritätssystems im Rahmen der gesamten Risiken einer Organisation.

Die im WLA-SCS dargelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, unabhängig von ihrer Art, Größe und Beschaffenheit, anwendbar sein. Wenn sich eine Organisation auf die Einhaltung des WLA-SCS beruft, dürfen keine in den Anhängen A, B, C oder D dargelegten Anforderungen ausgeschlossen werden.

Jegliche Ausschlüsse von Maßnahmen der Anhänge A, B, C oder D, die sich als notwendig erweisen, müssen formell begründet werden, und es muss der Nachweis erbracht werden, dass die Ausschlüsse von den Verantwortlichen genehmigt wurden. Wenn Maßnahmen ausgeschlossen werden, kann die Einhaltung von WLA-SCS nur dann geltend gemacht werden, wenn die betreffenden Ausschlüsse keinen Einfluss auf die Fähigkeit und/oder Pflicht der Organisation zur Gewährleistung der Sicherheit und Integrität entsprechend den Anforderungen der Risikobewertung und entsprechend den geltenden gesetzlichen oder regulatorischen Anforderungen haben. Alle in den Anhängen A, B, C oder D ausgeschlossenen Schutzmaßnahmen werden im WLA-SCS-Zertifikat hinsichtlich des Anwendungsbereichs der Zertifizierung vermerkt.

Hinweis: Wenn eine Organisation bereits ein Geschäftsprozess-Managementsystem (z. B. gemäß ISO 9001 oder ISO 14001) in Betrieb hat, empfiehlt es sich in den meisten Fällen, die Erfüllung der Anforderungen nach WLA-SCS in das bestehende Managementsystem einzubeziehen.

Wichtiger Hinweis: Der WLA-SCS erhebt nicht den Anspruch, alle notwendigen Bedingungen eines Vertrags zu enthalten. WLA Mitglieder, die den WLA-SCS einführen, sind

für dessen korrekte Anwendung verantwortlich. Die Erfüllung eines Standards enthebt per se niemanden seiner rechtlichen Verpflichtungen.

2. Normative Verweise

In diesem Dokument wird normativ auf die folgenden Dokumente verwiesen; sie sind für dessen Anwendung unerlässlich. Bei datierten Verweisen gilt nur die angegebene Ausgabe. Bei undatierten Verweisen gilt die neuste Ausgabe des betreffenden Dokuments (einschließlich Änderungen).

ISO/IEC 27001 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen.

ISO/IEC 27017 Informationstechnik – IT-Sicherheitsverfahren – Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud-Dienste.

WLA-SCS:2020 Code of Practice (Anwendungsleitfaden) – Best-Practices-Richtlinien für die Sicherheits- und Integritätsmaßnahmen und -anforderungen nach WLA-SCS.

Zertifizierungsanleitung für den WLA-SCS.

3. Begriffe und Definitionen

3.1 Abkürzungen

WLA: World Lottery Association

WLA-SCS: WLA Security Control Standard (Standard für Sicherheitsmaßnahmen)

WLA SRMC: WLA Security and Risk Management Committee (Ausschuss für Sicherheit und Risikomanagement)

3.2 Definitionen

Dieser Abschnitt enthält nur Begriffe, die in diesem Standard in einer besonderen Weise verwendet werden. Die meisten Begriffe werden in diesem Standard entweder gemäß ihrer allgemein anerkannten lexikalischen Bedeutung verwendet oder entsprechend den allgemein anerkannten Definitionen, die in den ISO-Sicherheitsglossaren oder anderen bekannten Sammlungen sicherheitsrelevanter Begriffe zu finden sind.

Vermögenswert: Durch Gegenmaßnahmen zu schützende Information oder Ressource.

Personal: Jede Person, die für den Lotteriebetreiber oder Lotterietechnologiezulieferer im Angestellten- oder Auftragsverhältnis oder als unabhängige Partei tätig ist und aufgrund ihrer Funktion oder ihres Zugangs Einfluss auf die Vertraulichkeit, Verfügbarkeit oder Integrität einer Lotterie nehmen könnte.

Spielesystem: Ein System, das für den Betrieb von Spielen benötigt wird. Dazu gehören das zentrale Spielesystem und dessen Peripheriekomponenten, die für den Betrieb der betreffenden Spiele notwendig sind.

Digitales Spielesystem: Jede Technologie, die das Anbieten von Spielen über digitale Vertriebskanäle ermöglicht.

4. Übersicht

Hauptziel des Sicherheits- und Integritätsansatzes für WLA Mitglieder ist es, einen geeigneten Betrieb sicherzustellen und Vertrauen zu schaffen.

Das Vertrauen in den Lotterie- und Sportwettenbetrieb ist für die Bindung der Spieler und anderer Stakeholder von entscheidender Bedeutung. WLA Mitglieder müssen deshalb eine transparente und dokumentierte Sicherheits- und Integritätsumgebung aufbauen und unterhalten.

Der WLA SRMC hat im WLA-SCS die Anforderungen, Kontrollziele und Maßnahmen dargelegt, die als bewährte Verfahren (Best Practices) gelten. Ein Lotterie- und Sportwettenbetreiber muss ein Informationssicherheits-Managementsystem betreiben, das allen Anforderungen der Norm ISO/IEC 27001 genügt und die obligatorischen Anforderungen und Maßnahmen des WLA-SCS umsetzt.

Der WLA-SCS beinhaltet grundlegende Anforderungen und Maßnahmen für den gesamten Sicherheits-, Integritäts- und Risikomanagementprozess eines Lotterie- und Sportwettenbetreibers und vermeidet Überschneidungen mit eher allgemeineren Sicherheitsrahmenwerken. Er bietet Sicherheits- und Integritätsfachleuten der Lotterie- und Sportwettenbetreiber einen Prozess, mit dem sie ihre Schutzmaßnahmen formal verwalten, aktualisieren und laufend optimieren können. Daher müssen die Fachleute eine transparente und dokumentierte Sicherheitsumgebung aufbauen und unterhalten.

Der WLA-SCS umfasst vier Teile, in denen die erforderlichen Mindestschutzmaßnahmen für ein effektives Sicherheits- und Integritätsmanagement von Lotterie- und Sportwettenbetreibern und Branchenzulieferern dargelegt sind.

Der erste Teil (Anhang A – G-Maßnahmen: Maßnahmen für alle Organisationen) umfasst die ISO/IEC 27001-Konformitätspflicht mit globalem Anwendungsbereich sowie weitere 24 ergänzende WLA Basis-Schutzmaßnahmen.

Der zweite Teil (Anhang B – L-Maßnahmen: Maßnahmen für Lotteriebetreiber) umfasst weitere 64 lotterie- und spielspezifische Sicherheits- und Integritätsmaßnahmen, die den aktuellen Best Practices entsprechen.

Der dritte Teil (Anhang C – S-Maßnahmen: Maßnahmen für Zulieferer und Betreiber von Spielesystemen) umfasst 21 Maßnahmen bezüglich Produkten und Dienstleistungen, die von Lotterie- und Sportwettenzulieferern angeboten werden.

Der vierte Teil (Anhang D – M-Maßnahmen: Maßnahmen für Mehrstaaten-Spiele) umfasst 11 Maßnahmen für die Beteiligung an Spielen, die von der Multi State Lottery Association (MUSL) in den USA durchgeführt werden.

5. Allgemeine Anforderungen an das Sicherheits- und Integritätsmanagement

5.1 Informationssicherheits-Managementsystem (ISMS)

Organisationen, die sich nach WLA-SCS:2020 Stufe 2 zertifizieren lassen wollen, müssen ein Informationssicherheits-Managementsystem (Information Security Management System, kurz ISMS) betreiben, das die Anforderungen nach der Norm ISO/IEC 27001 erfüllt.

5.2 Geltungsbereich des ISMS

Der Geltungsbereich des ISMS einer Organisation umfasst deren sämtliche Lotterie- und Glücksspielaktivitäten, einschließlich aller damit verbundener Vermögenswerte und Informationssysteme. Nur Tätigkeiten der Organisation, die sich nicht auf Lotterie- und Glücksspielaktivitäten beziehen, können vom Geltungsbereich ausgeschlossen werden. Ausgeschlossene Geschäftstätigkeiten sind in vollem Umfang auszuweisen, und die Gründe für den Ausschluss sind ausführlich darzulegen. Allgemeine organisatorische Funktionen (z. B. Personalwesen, Planung, Finanzen usw.), die für den Betrieb von Lotterien und Sportwetten benötigt werden, gehören zum Anwendungsbereich.

5.3 Anwendbarkeitserklärung

Die ISMS-Anwendbarkeitserklärung (ISMS Statement of Applicability) der Organisation schließt ausdrücklich sämtliche Maßnahmen der Anhänge A, B, C und D des WLA-SCS ein. Es darf keine Maßnahme ausgeschlossen werden, jedoch sind möglicherweise einige Maßnahmen der Anhänge B und C nicht anwendbar. Die Geltendmachung der Nicht-Anwendbarkeit muss detailliert begründet werden.

Der Ausschluss einer der im voranstehenden Absatz genannten Anforderungen oder einer Schutzmaßnahme aus Anhang A, B, C und D ist nicht zulässig, wenn eine Organisation WLA-SCS-Konformität erklären möchte.

Jede Nicht-Anwendbarkeit von Maßnahmen aus Anhang B und C, die für notwendig erachtet wird, muss formell begründet werden, und es muss der Nachweis erbracht werden, dass die Nicht-Anwendbarkeit von den Verantwortlichen der Organisation gutgeheißen wurde. Wenn Maßnahmen für nicht anwendbar erklärt werden, kann dies nur unter der Voraussetzung geltend gemacht werden, dass die Ausschlüsse keinen Einfluss auf die Fähigkeit und/oder Pflicht der Organisation zur Gewährleistung von Sicherheit und Integrität entsprechend den Anforderungen der Risikobewertung und entsprechend den geltenden gesetzlichen oder regulatorischen Anforderungen haben.

Anhang A (G-Maßnahmen): Maßnahmen für alle Organisationen

G.1	Organisation der Sicherheit	
G.1.1	**Zuweisung von Sicherheitspflichten**	
Ziel:	Gewährleistung, dass die Zuständigkeiten für die Sicherheitsfunktionen wirksam umgesetzt sind.	
G.1.1.1	Sicherheitsforum	*Maßnahme* Es wird ein aus Führungskräften bestehendes Sicherheitsforum oder eine andere organisatorische Struktur formell eingerichtet. Das Sicherheitsforum überwacht und überprüft das ISMS, um dessen weitere Eignung, Angemessenheit und Effektivität sicherzustellen, führt formelle Sitzungsprotokolle und kommt mindestens alle sechs Monate zusammen.
G.1.1.2	Sicherheitsfunktion	*Maßnahme* Es ist eine Sicherheitsfunktion vorhanden, die für die Erarbeitung einer Sicherheitsstrategie im Einklang mit dem Gesamtgeschäft zuständig ist. Die Sicherheitsfunktion arbeitet in der Folge mit den übrigen Geschäftsbereichen zusammen, um entsprechende Aktionspläne umzusetzen. Sie befasst sich mit der Überprüfung aller Aufgaben und Prozesse, die aus der Sicherheitsperspektive für die Organisation benötigt werden. Dies beinhaltet unter anderem den Schutz von Informationen und Daten, Kommunikation, physischer, virtueller, personeller sowie allgemeiner Betriebssicherheit
G.1.1.3	Berichterstattung der Sicherheitsfunktion	*Maßnahme* Die Sicherheitsfunktion berichtet mindestens an das geschäftsführende Management und ist in Bezug auf die Handhabung von Sicherheitsrisiken von der Technologiefunktion unabhängig.
G.1.1.4	Stellung der Sicherheitsfunktion	*Maßnahme* Die Sicherheitsfunktion verfügt über die Kompetenzen, ausreichenden Befugnisse und den Zugang zu allen Ressourcen, die nötig sind, um eine angemessene Einschätzung, Handhabung und Minderung der Risiken zu gewährleisten.
G.1.1.5	Zuständigkeit der Sicherheitsfunktion	*Maßnahme* Der Leiter der Sicherheitsfunktion gehört dem Sicherheitsforum als ordentliches Mitglied an. Er empfiehlt Sicherheitsrichtlinien und Änderungen.

G.2	Personalsicherheit	
G.2.1	**Einführung eines Verhaltenskodex**	
Ziel:	Sicherstellung, dass ein geeigneter Verhaltenskodex wirksam umgesetzt wird.	
G.2.1.1	Verhaltenskodex	*Maßnahme* Allen Mitarbeitern wird bei ihrer Einstellung ein Verhaltenskodex ausgehändigt. Sie müssen diesem Verhaltenskodex formell zustimmen.
G.2.1.2	Einhaltung und Disziplinarmaßnahmen	*Maßnahme* Der Verhaltenskodex hält fest, dass sämtliche Richtlinien und Verfahren einzuhalten sind und dass Zuwiderhandlungen oder Verstöße zu Disziplinarmaßnahmen führen können.
G.2.1.3	Interessenkonflikte	*Maßnahme* Der Verhaltenskodex hält fest, dass Mitarbeiter verpflichtet sind, Interessenkonflikte hinsichtlich ihrer Beschäftigung zu melden, falls bzw. sobald sie auftreten. Konkrete Beispiele für Interessenkonflikte sind im Verhaltenskodex erwähnt.
G.2.1.4	Bewirtung und Geschenke	*Maßnahme* Der Verhaltenskodex enthält Vorschriften zur Bekämpfung von Bestechung. Dies betrifft unter anderem Bewirtung und Geschenke, die von Personen oder Unternehmen, mit denen die Organisation Geschäfte tätigt, bereitgestellt oder von ihnen entgegengenommen werden.
G.2.1.5	Spielteilnahmerichtlinie für in der Organisation Beschäftigte	*Maßnahme* Es besteht eine interne Richtlinie, die den gesetzlichen und regulatorischen Anforderungen entspricht und das Recht von Mitarbeitern und Personen, die von ihnen finanziell abhängig sind, auf eine Teilnahme an Spielen regelt. Personen in Funktionen, die, ohne Absprachen, Einfluss auf die Integrität der Spiele haben könnten, dürfen nicht an den Spielen teilnehmen. Wenn die Richtlinie ein Spielverbot vorsieht, sind die davon betroffenen Funktionen ausdrücklich festzulegen, und das Verbot ist mit den Mitarbeitern oder deren Arbeitgeber (sofern dies nicht der Lotteriebetreiber selber ist) vertraglich festzuhalten.
G.2.1.6	Mitarbeitersicherheit	*Maßnahme* Es bestehen eine Richtlinie und ein Prozess, um durch Sicherheitsüberprüfungen das Vertrauen in Personen zu festigen, die Einfluss auf die Integrität der Spiele haben könnten. Weiter bestehen eine entsprechende Richtlinie und ein Prozess zur Überwachung der Systemaktivität der Mitarbeiter, um Aktivitäten, die Einfluss auf die Integrität der Spiele haben könnten, zu erkennen und zu untersuchen. Diese Richtlinien müssen zwischen dem persönlichen Recht auf Privatsphäre und der Verpflichtung des Lotteriebetreibers zum Schutz der Integrität der Spiele abwägen.

G.2.1.7	Aufgabentrennung	*Maßnahme* Es besteht eine Richtlinie, die eine Aufgabentrennung festlegt. Darin sind die Aufgaben und Pflichten der Personen enthalten, die für entscheidende Prozesse verantwortlich sind, welche Einfluss auf die Integrität eines Spiels haben könnten, beispielsweise die Ziehungsverarbeitung und die Gewinnauszahlung. Damit soll die Möglichkeit von Absprachen verhindert werden. Außerdem darf keine einzelne Gruppe und kein einzelnes Team die Gesamtkontrolle in solcher Weise innehaben, dass dies ohne Managementaufsicht einen Einfluss auf die Integrität des Spiels haben könnte. Bei einem Lotterietechnologiezulieferer bezieht sich diese Maßnahme auf entscheidende Codebereiche, die einen Einfluss auf die Integrität eines Spiels haben könnten, beispielsweise die Handhabung von Ein- und Ausgabe der Zufallszahlengenerierung, die zur Festlegung der Spielergebnisse dient.

G.2.2	**Mitarbeiterschutz**	
Ziel:	Sicherstellung, dass die Mitarbeiter einen angemessenen Schutz genießen.	
G.2.2.1	Richtlinie über Mitarbeiterschutz	*Maßnahme* Es besteht eine Richtlinie, die sicherstellt, dass Mitarbeiter, die allein, an abgesetzten Standorten außerhalb der Räumlichkeiten des Lotteriebetreibers oder in den Räumlichkeiten des Lotteriebetreibers in Bereichen mit Publikumszugang arbeiten, angemessen geschützt und abgesichert sind.

G.3 Physische und umgebungsbezogene Sicherheit

G.3.1	**Sichere Bereiche**	
Ziel:	Sicherstellung, dass der Zugang zu den Datenzentren des Spielbetriebs und zu anderen Systembereichen, die für den Spielbetrieb wichtig sind, angemessen abgesichert ist.	
G.3.1.1	Physische Zugangskontrollen	*Maßnahme* Der physische Zugang zu den Datenzentren des Spielbetriebs, Computerräumen, Netzwerkbetriebszentren und anderen als entscheidend geltenden Bereichen ist beschränkt und angemessen abgesichert oder wird von den Mitarbeitern jederzeit überwacht. Obwohl diese Maßnahme risikoabhängig ist, muss sie in der Praxis mindestens über einen prüffähigen Zwei-Faktor-Authentifizierungsprozess verfügen.

G.4	Zugangskontrollen für Spielesysteme	
G.4.1	**Handhabung des Nutzerzugangs**	
Ziel:	Sicherstellung eines autorisierten Nutzerzugangs und Verhinderung unberechtigter Zugriffe auf die Spielesysteme. Bei Technologiezulieferern beziehen sich die G.4-Maßnahmen auf die Code-Repositories, die zur Entwicklung von Spielesystemen verwendet werden.	
G.4.1.1	Den Nutzern zugängliche Funktionen	*Maßnahme* Der Umfang der Funktionen, die für die Nutzer zugänglich sind, wird zusammen mit dem Prozessverantwortlichen, der IT-Funktion und der Sicherheitsfunktion festgelegt.
G.4.1.2	Protokollierung des Nutzerzugangs	*Maßnahme* Alle Aktionen, die durch menschliches Handeln oder systembedingt in den Spielesystemen durchgeführt werden, werden protokolliert. Die entsprechenden Protokolle werden überwacht, regelmäßig überprüft und lösen bei Bedarf entsprechende Maßnahmen aus.

G.5	Pflege von Informationssystemen	
G.5.1	**Kryptografische Maßnahmen**	
Ziel:	Schutz der Vertraulichkeit, Authentizität und Integrität kryptografischer Schlüssel sowie wichtiger Spiel-, Lotterie- und Kundeninformationen durch kryptografische Mittel.	
G.5.1.1	Kryptografische Maßnahmen für die Vertraulichkeit und Integrität von Daten, die sich auf tragbaren Systemen und auf Lotterieterminals befinden	*Maßnahme* Die Vertraulichkeit und Integrität sensibler Informationen, die sich auf tragbaren Computersystemen (Endnutzergeräte wie Laptops, Wechseldatenträger, z. B. USB-Sticks usw.) oder auf Lotterieterminals befinden, werden mittels Verschlüsselung geschützt.
G.5.1.2	Kryptografische Maßnahmen für die Vertraulichkeit und Integrität von Daten, die über Netzwerke übertragen werden	*Maßnahme* Die Vertraulichkeit und Integrität sensibler Informationen, die über Netzwerke übertragen werden, deren Schutzniveau sich gemäß Risikoanalyse als unzureichend erwiesen hat, werden in geeigneter Weise mittels Verschlüsselung geschützt. Dies betrifft unter anderem Validierungs- und andere wichtige Spielinformationen, Kundendaten und Finanztransaktionen.
G.5.1.3	Kryptografische Maßnahmen für die Integrität sensibler Spielscheindaten	*Maßnahme* Die Integrität gespeicherter Spielscheindaten und Validierungsinformationen wird mittels Kryptografie geschützt. Diese Maßnahme gilt für alle Spieltypen.

G.5.2	Systemtests	
Ziel:	Einrichtung und Durchführung von Systemtests.	
G.5.2.1	Richtlinie für Testmethoden sowie Testdaten	*Maßnahme* Die Richtlinie für Testmethoden enthält Bestimmungen, die verhindern, dass Daten, die in einem Live-Produktionssystem für den aktuellen Ziehungszeitraum generiert wurden, oder personenbezogene Informationen von Spielteilnehmern, Annahmestellen oder Mitarbeitern verwendet werden. Als Ziehungszeitraum gilt in diesem Zusammenhang der Zeitraum, für den Gewinne immer noch beansprucht werden können.
G.5.2.2	Sicherheitstests für Spielesysteme	*Maßnahme* Die Sicherheitsfunktionen der Spielesysteme müssen vor Übernahme in die Produktion und bei jeder Änderung gründlich getestet werden.

G.5.3	Cloud-Sicherheit	
Ziel:	Gewährleistung der Informationssicherheit von Lotteriesystemen, die in einer Cloud gehostet werden.	
G.5.3.1	Cloud-Sicherheit	*Maßnahme* Cloud-Umgebungen, die Spielesysteme hosten, müssen ISO/IEC 27017 erfüllen. Eine Cloud-Umgebung wird definiert als eine vom Standort abgesetzte Drittplattform mit einer Reihe von Applikationen, welche die Organisation für Dienstleistungen wie folgende abonniert: „Infrastructure as a Service“, „Platform as a Service“, „Software as a Service“ usw., die für den Geschäftsbetrieb benötigt werden. Bei Technologiezulieferern beziehen sich die Maßnahmen nach WLA-SCS G.5.3 auf die Code-Repositories, die für die Entwicklung von Spielesystemen verwendet werden.

G.6 Systemverfügbarkeit und Geschäftskontinuität

G.6.1	Dienstverfügbarkeit und Geschäftskontinuität	
Ziel:	Schutz von Image und Ruf der Organisation sowie Verhinderung von Unterbrechungen der Geschäftstätigkeit.	
G.6.1.1	Anforderungen an Verfügbarkeit und Ausfallsicherheit	*Maßnahme* Die Organisation führt eine Liste über die entscheidenden Dienstleistungen für Spielteilnehmer (Annahmestellen und digitale Kanäle), die für den Weiterbetrieb der Lotterien erforderlich sind, und über die Anforderungen, die an die Verfügbarkeit und Ausfallsicherheit der entsprechenden Dienstleistungen gestellt werden. Die Systeme werden so konzipiert, dass diese Anforderungen erfüllt sind.
G.6.1.2	Geschäftskontinuität	*Maßnahme* Die Organisation erstellt einen dokumentierten Geschäftskontinuitätsplan, der mindestens den Weiterbetrieb der Lotterien und die Aufrechterhaltung des Vertrauens der Stakeholder in die Integrität des Lotteriebetriebs abdeckt. Außerdem plant die Organisation regelmäßige Geschäftskontinuitätsübungen, führt diese durch und wertet sie aus, um die Organisation auf Krisensituationen vorzubereiten. Die Übungen decken die im Geschäftskontinuitätsplan enthaltenen Elemente ab.

Anhang B (L-Maßnahmen): Maßnahmen für Lotteriebetreiber

L.1	**Physische Sofort-Lose**	
L.1.1	**Betrieb von Sofortspielen**	
Ziel:	Sicherstellung, dass die Gestaltung und Produktion der Spiele die gesetzlichen und regulatorischen Anforderungen erfüllen, sowie Gewährleistung der Spielintegrität und Betrugsbekämpfung.	
L.1.1.1	Auswahl von Druckereien/Lieferanten	*Maßnahme* Es besteht ein formelles Genehmigungsverfahren, das die Sicherheitsfunktion einbezieht.
L.1.1.2	Integritätsanforderungen und -tests	*Maßnahme* Die Organisation verfügt über ein dokumentiertes Verfahren, das den ganzen Lebenszyklus der Spiele von der Entwicklung bis zur Zerstörung abdeckt und für jedes Sofortspiel die geltenden Integritätsanforderungen spezifiziert. Die Integritätsanforderungen betreffen mindestens Folgendes: definitive Visualisierungen und Texte, Gewinnstruktur, Schutz von Validierungs-/Gewinnerdateien, Qualitätskontrollen, prüffähiges Inventar zum Nachweis der Verteilung, Aufbewahrungsorte der Pakete sowie geeignete Tests der Anforderungen, bevor das Spiel genehmigt wird.
L.1.1.3	Integrität der Spieldaten	*Maßnahme* Es bestehen Maßnahmen zur Sicherstellung der Integrität der Spieldaten, einschließlich unter anderem des Imports von Spieldaten in das Spielesystem und der Übertragung von Validierungsdaten zwischen Zulieferer, Betreiber und Annahmestellen.
L.1.1.4	Vertraulichkeit der Losgewinne	*Maßnahme* Es bestehen Maßnahmen, die sicherstellen, dass vor der Beanspruchung eines Gewinns niemand in der Organisation weiß oder herausfinden kann, welches Sofortlos ein Gewinnlos ist und welches nicht. Auch darf niemand in der Lage sein, den Ort eines Gewinnloses oder die Annahmestelle, der es zugeteilt wurde, zu identifizieren.

L.2	Lotterieziehungen	
L.2.1	**Handhabung von Lotterieziehungen**	
Ziel:	Sicherstellung, dass die Ziehungen zu den vorgeschriebenen Zeiten und gemäß den geltenden Regeln der betreffenden Lotterie durchgeführt werden.	
L.2.1.1	Ziehungsvorgang	*Maßnahme* Es besteht eine Richtlinie, die sicherstellt, dass Lotterieziehungen als geplanter und kontrollierter Vorgang und gemäß einer klaren Arbeitsanweisung durchgeführt werden.
L.2.1.2	Arbeitsanweisungen für Ziehungen	*Maßnahme* Die Organisation veröffentlicht vor jeder Ziehung eine Arbeitsanweisung, die spezielle Instruktionen für die betreffende Ziehung enthält.
L.2.1.3	Mitglieder des Ziehungsteams	*Maßnahme* Die Arbeitsanweisung enthält die Namen der Mitglieder des Ziehungsteams und deren Telefonnummern.
L.2.1.4	Pflichten des Ziehungsteams	*Maßnahme* Die Arbeitsanweisung enthält die Pflichten der namentlich bestimmten Mitglieder des Ziehungsteams.
L.2.1.5	Ersatz-Ziehungsteam	*Maßnahme* Die Arbeitsanweisung benennt Ersatzpersonen und beschreibt genau, unter welchen Bedingungen das Ersatzteam zum Einsatz kommt.
L.2.1.6	Zeitangaben für die Ziehung	*Maßnahme* Die Arbeitsanweisung enthält genaue Zeitangaben für die Ziehung, von der Öffnung des Ziehungsstandortes bis zu dessen Schließung.
L.2.1.7	Ziehungsbeobachter	*Maßnahme* Die Arbeitsanweisung enthält genaue Angaben zu unabhängigen Beobachtern, falls solche gemäß den Lotterieregeln während einer Ziehung anwesend sein müssen.

L.2.2	Durchführung der Ziehung	
Ziel:	Sicherstellung, dass die Ziehungen gemäß den aufsichtsrechtlichen Anforderungen und den Regeln der entsprechenden Lotterie durchgeführt werden.	
L.2.2.1	Ziehungsverfahren	*Maßnahme* Die Organisation legt ein detailliertes Verfahren für die Ziehungen fest, das sicherstellt, dass alle Ziehungsfunktionen gemäß den Regeln der entsprechenden Lotterie wie auch den aufsichtsrechtlichen Anforderungen ausgeführt werden.
L.2.2.2	Schrittweise Ziehungs-anleitung	*Maßnahme* Das Ziehungsverfahren enthält eine schrittweise Anleitung für die Ziehung.
L.2.2.3	Ziehungsort	*Maßnahme* Das Ziehungsverfahren legt den Ziehungsort fest.
L.2.2.4	Anwesenheit bei der Ziehung und Zuständig-keiten	*Maßnahme* Das Ziehungsverfahren legt fest, wer bei der Ziehung anwesend ist und welche Zuständigkeiten und Aufgaben alle Anwesenden innehaben.
L.2.2.5	Ziehungsaufsicht	*Maßnahme* Das Ziehungsverfahren legt die Richtlinie bezüglich der Anwesenheit eines (unabhängigen) Compliance-Verantwortlichen oder eines Prüfers fest.
L.2.2.6	Sicherheit beim Ziehungsablauf	*Maßnahme* Das Ziehungsverfahren enthält geeignete Sicherheitsvorkehrungen für den Ziehungsablauf und für die während der Ziehung benötigten Geräte.
L.2.2.7	Notfall während der Ziehung	*Maßnahme* Das Ziehungsverfahren enthält Maßnahmen für den Fall, dass während der Ziehung ein Notfall eintritt.
L.2.2.8	Integrität der Ziehung, Warnungen und Bericht-erstattung	*Maßnahme* Der Lotteriebetreiber richtet ein System oder einen Prozess ein, womit sicher-gestellt wird, dass niemand, der Zugriff auf das zentrale Spielesystem (Central Gaming System) hat, die Transaktionen vor, während oder nach der Ziehung manipulieren kann und dass eine klare Prüfpfadverfolgung der Benutzerzugriffe und eine Transaktionsprüfung vorhanden sind.

L.2.3	**Physische Ziehungsgeräte und Kugelsätze**	
Ziel:	Sicherstellung, dass die physischen Ziehungsgeräte und Kugelsätze die vereinbarten Sicherheitsanforderungen und/oder regulatorischen Spezifikationen erfüllen.	
L.2.3.1	Inspektionsverfahren	*Maßnahme* Es wird ein Verfahren für die regelmäßige Inspektion der Ziehungsgeräte und Kugelsätze, bei der Lieferung wie auch danach, in Abstimmung mit einer unabhängigen Instanz eingerichtet (um die Einhaltung der technischen Spezifikationen und Standards sicherzustellen).
L.2.3.2	Regelmäßige Inspektion und Wartung	*Maßnahme* Inspektion und Wartung der Ziehungsgeräte werden mindestens einmal jährlich durchgeführt und dokumentiert, um sicherzustellen, dass die spezifizierten Standards während der ganzen Betriebsdauer der Geräte eingehalten werden.
L.2.3.3	Passende Kugelsätze	*Maßnahme* Die Organisation legt ein Verfahren für den Gebrauch von Kugelsätzen fest, die nach den Maßen und Gewichtstoleranzen der einzusetzenden Ziehungsgeräte gefertigt wurden.
L.2.3.4	Ersatzziehungsgeräte	*Maßnahme* Die Organisation legt ein Verfahren für die Bereitstellung eines Ersatzes für das Ziehungsgerät und die Kugelsätze fest, der im Fall von mechanischen Problemen oder Störungen jeglicher Art eingesetzt werden kann, wenn Ziehungen live übertragen werden.
L.2.3.5	Bedienung, Lagerung und Transport von Ziehungsgeräten und Kugelsätzen	*Maßnahme* Die Organisation legt ein Verfahren fest, das die Sicherheit der Ziehungsgeräte und Kugelsätze bei Lagerung, Transport und Bedienung gewährleistet.
L.2.3.6	Übertragung/Streaming der Ziehung	*Maßnahme* Bei einer Ausstrahlung oder einem Live-Stream der Ziehung über das Internet besteht ein Verfahren zur Minimierung der Risiken im Zusammenhang mit einer Datenverfälschung, einer Zeitverzögerung von Ton und/oder Bild, von Fehlern in der Grafikgenerierung oder Ähnlichem, was in der Öffentlichkeit den Eindruck erwecken könnte, dass bezüglich der Integrität der Ziehung ein Problem bestünde.

L.2.4	Elektronische Lotterieziehungen und Sofortspiele	
Ziel:	Sicherstellung der Integrität elektronischer Ziehungssysteme durch physischen und logischen Schutz. L.2.4 deckt sowohl Spiele auf der Basis elektronischer Ziehungen als auch elektronische Sofortgewinnspiele ab.	
L.2.4.1	Physischer und logischer Schutz der technischen Systeme	*Maßnahme* Es werden Vorkehrungen getroffen, um den physischen Zugang ausschließlich befugter Personen und logischen Schutz sowohl des Zufallszahlengenerators (RNG) (Entropiequelle) als auch des Ziehungsalgorithmus sicherzustellen. Damit soll eine Modifizierung des Algorithmus und der Einstellungen der Entropiequelle verhindert werden. Die physischen Systeme werden vor Diebstahl, nicht autorisierten Modifikationen und Eingriffen geschützt.
L.2.4.2	Sichere Übermittlungen	*Maßnahme* Es werden Vorkehrungen getroffen, um die Integrität und Authentizität der Daten sicherzustellen, die zwischen dem Zufallsgenerator (Entropiequelle) und dem Ziehungsalgorithmus übermittelt werden.
L.2.4.3	Verifizierung der Zufälligkeit und Integrität bei elektronischen Ziehungen	*Maßnahme* Vor der Implementierung werden Tests und Überprüfungen durch unabhängige Parteien durchgeführt, um nachzuweisen, dass die Ziehungen mit dem elektronischen Ziehungssystem dem Zufall unterliegen. Die Organisation hat eine Richtlinie für Implementierungstests und Validierung, um zu verifizieren, dass Zufallsgenerator und Ziehungsalgorithmus den Vorgaben entsprechend funktionieren.
L.2.4.4	Aufgabentrennung	*Maßnahme* Neben der Maßnahme G.2.1.7 ist ein spezifisches Verfahren zur Aufgabentrennung bei elektronischen Ziehungen vorhanden, um internen Betrug zu verhindern. Insbesondere darf niemand mehr als eine der folgenden Arten von Aufgaben ausführen: Wartung, Überwachung oder Durchführung von Ziehungen mittels elektronischer Spielausrüstung.

L.3	Sicherheit der Annahmestellen	
L.3.1	**Betrieb der Annahmestellen**	
Ziel:	Sicherstellung, dass die Annahmestellen mit ihrem Betrieb, online wie offline, die Sicherheitsanforderungen der Organisation erfüllen.	
L.3.1.1	Sicherheit bei den Annahmestellen	*Maßnahme* Um sicherzustellen, dass die Annahmestellen die Sicherheitsanforderungen der Organisation erfüllen, regelt die Organisation die Verpflichtungen einer Annahmestelle sowie die Sicherheitsbedingungen, die sie zu gewährleisten hat, mittels Vertrag.

L.3.2	**Sicherheit der Spielterminals**	
Ziel:	Sicherstellung einer angemessenen Absicherung der Spielterminals.	
L.3.2.1	Transaktionssicherheit	*Maßnahme* Der Datenverkehr zwischen den Spielterminals und dem zentralen Spielesystem ist geschützt, und es sind Vorkehrungen vorhanden, welche die Integrität der Transaktionen sicherstellen. Wird anstelle eines ausgewiesenen Lotterieterminals ein Gerät der Annahmestelle verwendet, muss der Datenverkehr zwischen der Lotterieapplikation auf dem Gerät der Annahmestelle und dem zentralen Spielesystem geschützt sein und darf bezüglich der Integrität der Lotterien nicht von der Sicherheit des Geräts der Annahmestelle abhängig sein.

L.4	Gewinnauszahlungen	
L.4.1	**Validierung und Auszahlung von Gewinnen**	
Ziel:	Sicherstellung, dass die Organisation über die notwendigen Maßnahmen zur Validierung und Auszahlung von Gewinnen und zur Verhinderung von Betrug im Zusammenhang mit nicht beanspruchten Gewinnen verfügt.	
L.4.1.1	Validierungsprozess	*Maßnahme* Die Organisation legt Verfahren zur Sicherstellung der Gültigkeit der Gewinntransaktionen, Gewinnansprüche und/oder Spielscheine für verschiedene Gewinnklassen und Spielarten und zur Abwicklung der entsprechenden Gewinnauszahlungen fest und setzt diese Verfahren um.
L.4.1.2	Eindeutige Kennziffer für Spielscheine	*Maßnahme* Jeder Spielschein für jedes Spiel besitzt eine eindeutige Spielscheinnummer.
L.4.1.3	Sicherheit der Daten zu nicht beanspruchten Gewinnen	*Maßnahme* Die Organisation führt technische und verfahrensbezogene Maßnahmen durch, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu nicht beanspruchten Gewinnen sicherzustellen. Dies betrifft mindestens unter anderem Dateien, die Informationen über spezifische noch zu beanspruchende Transaktionen enthalten, und jegliche Validierungsdateien. Von besonderer Bedeutung sind dabei Zugangskontrollen zwecks Beschränkung des Zugriffs auf die Daten, die Überwachung der Nutzerinteraktionen mit den Daten sowie ein Prozess für den Umgang mit unberechtigten Zugriffen oder dem Export der Daten.
L.4.1.4	Gewinnauszahlungsverfahren	*Maßnahme* Es besteht ein Verfahren für die Gewinnauszahlungen, das Folgendes regelt: maximaler Zeitraum für die Beanspruchung eines Gewinns; ein Prozess zur Prüfung der abschließenden Überweisungen bei Beendigung des Spiels; genaue Regeln und Sorgfaltspflichten, die zu befolgen sind, bevor über Auszahlungen für verlorene, gestohlene oder beschädigte Spielscheine entschieden wird; genaues Vorgehen bei Anfragen zur Gültigkeit von Ansprüchen; sowie das Vorgehen bei späten Auszahlungen oder Auszahlungen in letzter Minute.
L.4.1.5	Betrugserkennung	*Maßnahme* Im Rahmen des Gewinnauszahlungsverfahrens werden geeignete Prüfprotokolle geführt und überprüft, um ungewöhnliche Muster von späten Auszahlungen oder geltend gemachte Ansprüche von Annahmestellen oder Mitarbeitern, die unter Umständen einer näheren Abklärung bedürfen, aufzudecken.

L.5	Digitale Vertriebskanäle und interaktive Dienste	
L.5.1	**Digitale Spielesysteme**	
Ziel:	Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit digitaler Spielesysteme, um Spiel- und Spielerdaten zu schützen.	
L.5.1.1	Mehrschichtige Systemarchitektur	*Maßnahme* Die Organisation verfolgt in Bezug auf die Sicherheit innerhalb der Architektur der digitalen Spielesysteme einen mehrschichtigen Ansatz, um eine sichere Datenspeicherung und -verarbeitung zu gewährleisten.
L.5.1.2	Aktive und passive Angriffe	*Maßnahme* Es werden geeignete Vorkehrungen getroffen, um die gewöhnlichen aktiven und passiven technischen Angriffe aufzudecken, zu verhindern, zu mindern und auf sie zu reagieren. Außerdem verfügt die Organisation über vereinbarte Patching-Richtlinien für digitale Spielesysteme, die entweder intern oder von Dritten entwickelt und unterstützt werden.
L.5.1.3	Netzwerktrennung	*Maßnahme* Die Produktionsdatenbanken, die Daten zu Spielern oder Transaktionen enthalten, sind in Netzwerke eingebunden, die von jenen Servern getrennt sind, auf denen sich die Webseiten befinden.
L.5.1.4	Session-Daten	*Maßnahme* Die Sitzungs-ID des Nutzers wird immer zufällig und im Hauptspeicher generiert und nach Beendigung der Nutzer-Session wieder entfernt.
L.5.1.5	Ermittlung der Ein- und Austrittspunkte (Ports)	*Maßnahme* Alle Eintritts- und Austrittspunkte (Ports) von offenen, öffentlichen Netzwerksystemen werden ermittelt, verwaltet, überwacht und kontrolliert. Die Organisation überwacht alle ihre digitalen Spielesysteme, um Cyberangriffe zu verhindern, aufzudecken, zu mindern und darauf zu reagieren.
L.5.1.6	Generierung und Speicherung von Protokollen	*Maßnahme* Zu jeder sensiblen Systemkomponente werden vordefinierte Sicherheitsprotokolle generiert und während einer vordefinierten Zeit gespeichert, um Anomalien, Fehler und Alarme zu überwachen und zu beheben.
L.5.1.7	Sicherheitstests	*Maßnahme* Wichtige Systemänderungen werden geeigneten Sicherheitstests unterzogen. Es werden regelmäßige, mindestens jährliche Angriffserkennungstests (Intrusion Testing) durchgeführt, um Schwachstellen oder andere Mängel im System zu ermitteln und zu beheben.
L.5.1.8	Verantwortungsvolle Offenlegung von Sicherheitslücken	*Maßnahme* Der Lotteriebetreiber verfügt über eine Richtlinie zur verantwortungsvollen Offenlegung von Sicherheitslücken (Responsible-Disclosure-Richtlinie). Sie regelt, wie die Öffentlichkeit dem Lotteriebetreiber Sicherheitsschwachstellen melden kann.

L.5.2	Spielerkonto	
Ziel:	Schutz der Spieler sowie Risikomanagement bezüglich Betrug und Geldwäsche.	
L.5.2.1	Spielerkonto	*Maßnahme* Es besteht ein formeller Prozess zur Identifikation, Authentifizierung und Autorisierung eines Spielers. Sowohl die Spielerdaten als auch die Bonität sind wesentliche Faktoren bei der Risikobewertung.
L.5.2.2	Mehrfachkonten	*Maßnahme* Es bestehen geeignete Vorkehrungen, die sicherstellen, dass jeder Spieler nur ein aktives Konto besitzt.
L.5.2.3	Spieleraussschluss	*Maßnahme* Für den Ausschluss von Spielern besteht ein etablierter Prozess, der mit den geltenden Gesetzen vor Ort und/oder internen Verfahren im Einklang steht.
L.5.2.4	Inhaber mehrerer Zahlungsmittel	*Maßnahme* Ein etabliertes Verfahren, das mit den geltenden Gesetzen vor Ort im Einklang steht, stellt sicher, dass der Eigentümer des Zahlungsmittels mit der Identität des Spielteilnehmers übereinstimmt. Damit sollen Betrug und Geldwäsche verhindert werden.

L.5.3	Spieldesign und Spielabnahme	
Ziel:	Sicherstellung, dass die Spieldesigns die rechtlichen und regulatorischen Anforderungen erfüllen und von der zuständigen Instanz genehmigt wurden, bevor sie in Betrieb genommen werden.	
L.5.3.1	Dokumentierte Spielverfahren	*Maßnahme* Die Gestaltung und Entwicklung von Spielen folgt festen Regeln. Die Spieler haben Zugriff auf die Spielregeln.
L.5.3.2	Spielabnahme und -änderung	*Maßnahme* Es wird ein Abnahmeverfahren festgelegt, das sicherstellt, dass jedes neue Spiel und wichtige Änderungen in den digitalen Spielesystemen überprüft werden. Das endgültige Spieldesign wird durch ein Verfahren, in das die Sicherheitsfunktion eingebunden ist, formell genehmigt.

L.5.4	**Absicherung der Zahlungsmethoden**	
Ziel:	Schutz der Zahlungsmethoden gegen Missbrauch.	
L.5.4.1	Datenerfassung	*Maßnahme* Die Erfassung sensibler Daten, die in direktem Zusammenhang zur Zahlung stehen, beschränkt sich auf die Daten, die für die Transaktion dringend benötigt werden.
L.5.4.2	Schutz der Zahlungsmethoden	*Maßnahme* Es bestehen geeignete Vorkehrungen, um alle im System genutzten Zahlungsarten vor Missbrauch zu schützen.
L.5.4.3	Genehmigung eines Zahlungsdienstes	*Maßnahme* Die Organisation stellt sicher, dass ein Zahlungsdienst den Schutz der Spielerdaten gewährleistet, einschließlich personenbezogener Daten, die vom Spieler erfasst werden, sowie Zahlungsdaten.
L.5.4.4	Transaktionsdatensätze zu den Zahlungen	*Maßnahme* Alle Transaktionsdatensätze der Spielerkonten werden von der Organisation generiert. Die erfassten Daten ermöglichen es der Organisation, eine einzelne Finanzaktivität eines Spielers zu einer anderen Transaktion rückzuverfolgen.

L.6	Sportwetten	
L.6.1	**Auswahl des Angebots**	
Ziel:	Sicherstellung der Integrität eines Wettangebots.	
L.6.1.1	Rahmenbedingungen für Wetten	*Maßnahme* Die Rahmenbedingungen, unter welchen die Organisation Sportwetten anbietet, und die entsprechenden Regeln werden festgelegt, gepflegt und veröffentlicht. Dazu gehört unter anderem, welche Arten von Sportveranstaltungen und welche Arten von Wetten für jeden Sport genehmigt werden.

L.6.2	**Sportveranstaltungen, Quotenregelung und Handhabung der Ergebnisse**	
Ziel:	Sicherstellung der Integrität von Sportveranstaltungen und der entsprechenden Quoten.	
L.6.2.1	Sportveranstaltungen, Quotenregelung und Handhabung der Ergebnisse	*Maßnahme* Es werden Verfahren eingerichtet, welche die Auswahl der Sportveranstaltungen, die Festlegung und Aktualisierung der Quoten und Wettmargen und/oder das Sperren von Sportveranstaltungen regeln und sicherstellen, dass die Ergebnisse aus zuverlässigen Quellen stammen. Es besteht ein Prozess zur Überprüfung der Richtigkeit und zur Verhinderung betrügerischer Aktivitäten. Diese Verfahren basieren auf der Sicherstellung von Integrität, verantwortungsvollen Spielen und Transparenz.
L.6.2.2	Live-Wetten	*Maßnahme* Es bestehen dokumentierte Verfahren, welche die Integrität des Live-Wettangebots, die Handhabung der Ergebnisse und den Kundenschutz sicherstellen und überwachen. Bei der Handhabung der Ergebnisse werden unter anderem Zeitverzögerungen, die den Ergebnissen zugrundeliegenden Informationsquellen und Korrekturen von Spielergebnissen berücksichtigt. Die Verfahren tragen auch Präventionsmechanismen rund ums Spielfeld Rechnung, beispielsweise der Zeitverzögerung von Live-Bildern.
L.6.2.3	Absicherung der Auszahlungshöhen	*Maßnahme* Die Organisation trifft Vorkehrungen, die sicherstellen, dass die genehmigten Auszahlungshöhen nicht überschritten werden.

L.6.3	**Überwachung bezüglich Betrug und Geldwäsche**	
Ziel:	Sicherstellung von Vorkehrungen zur Minimierung des Betrugs- und/oder Geldwäscherisikos.	
L.6.3.1	Überwachung der Sportwettaktivitäten	*Maßnahme* Es werden Verfahren eingerichtet, die alle Änderungen von Quoten und/oder Sperren während einer Sportveranstaltung überwachen, die den Markt, Sportveranstaltungen und Kundentransaktionen zwecks Aufdeckung von Unregelmäßigkeiten überwachen und die Gewinner ab einem bestimmten Gewinnbetrag und Einzahlungen ab einer bestimmten Höhe überwachen. Die Verfahren legen auch Grenzwerte für Zahlungen und Zahlungsmethoden fest. Sie müssen die gesetzlichen Vorschriften im Rechtsgebiet erfüllen, in dem das zertifizierte Mitglied seinen Sitz hat.

L.7	Interaktive Video-Lotterie-Terminals	
L.7.1	**Interaktive Video-Lotterie-Terminals (VLT)**	
Ziel:	Gewährleistung des sicheren Betriebs aller Video-Lotterie-Terminals, ungeachtet des Systemdesigns und der Betriebsmodelle.	
L.7.1.1	VL-Terminals	*Maßnahme* VL-Terminals werden hinsichtlich ihrer Sicherheit und ihrer Gewinnauszahlungsquote überwacht.
L.7.1.2	VLT-Spiele	*Maßnahme* Die Spielregeln und die Gesamt-Gewinnauszahlungsquote stehen dem Kunden zur Verfügung.
L.7.1.3	Zertifikat für VLT-Spiele	*Maßnahme* VLT-Spiele werden getestet, und es wird ein Zertifikat erstellt/herausgegeben, das die Integrität und die Gewinnauszahlung belegt.
L.7.1.4	VLT-Vorfälle	*Maßnahme* Es bestehen dokumentierte Verfahren für den Umgang mit Streitfällen und Kundenreklamationen hinsichtlich Gewinnen oder Verlusten.
L.7.1.5	VLT-Systemarchitektur	*Maßnahme* Die Organisation verfügt über eine Beschreibung der gesamten VLT-Systemarchitektur, einschließlich der Sicherheitsvorkehrungen, welche die Integrität der VLT-Spiele sowie die sichere Datenspeicherung und -verarbeitung gewährleisten.

Anhang C (S-Maßnahmen): Maßnahmen für Zulieferer und Betreiber von Spielesystemen

Die S-Maßnahmen beziehen sich auf Spielesysteme (gemäß Definition in diesem Standard) und gehören zum Anwendungsbereich der Zertifizierung derjenigen Organisation, die das Spielesystem entwickelt und/oder das Spielesystem verwaltet – ob es sich dabei um einen Technologiezulieferer oder um die eigenen internen Entwickler des Betreibers handelt.

S.1	**Gewährleistung der Sicherheit von Lotteriesystemen**	
S.1.1	**Entwicklung sicherer Spielesystemapplikationen**	
Ziel:	Gewährleistung, dass die Lotteriesysteme von ihrem Design her sicher sind.	
S.1.1.1	Richtlinie für die Entwicklung sicherer Applikationen	*Maßnahme* Der Lotterietechnologiezulieferer verfügt über eine Richtlinie für die Applikationssicherheit im ganzen Lebenszyklus der Softwareentwicklung.
S.1.1.2	Statische und dynamische Codeanalyse	*Maßnahme* Der Lotterietechnologiezulieferer führt eine statische und dynamische Codeanalyse durch und liefert dem Betreiber eine Zusammenfassung der Ergebnisse in Ergänzung der Release Notes zu seinem Produkt für das erste Release und für alle nachfolgenden wesentlichen Releases in der Produktionsumgebung.
S.1.1.3	Sicherheitstests	*Maßnahme* Der Lotterietechnologiezulieferer führt Sicherheitstests an seinen Produkten und/oder Dienstleistungen durch. Diese werden in einer Art und Weise gehostet und konfiguriert, die repräsentativ ist dafür, wie sie vom Betreiber in einer Produktionsumgebung eingesetzt werden sollen. Er liefert dem Betreiber eine Zusammenfassung der Ergebnisse in Ergänzung der Release Notes zu seinem Produkt für das erste Release und für alle nachfolgenden wesentlichen Releases in der Produktionsumgebung.
S.1.1.4	Secure-Coding-Praktiken	*Maßnahme* Der Lotterietechnologiezulieferer legt Secure-Coding-Praktiken fest und verlangt von seinen Entwicklern, dass sie diese befolgen. Außerdem werden Vorkehrungen getroffen, um die Wirksamkeit dieser Praktiken und deren Befolgung zu überprüfen.
S.1.1.5	Schulung und Sensibilisierung für Secure-Coding	*Maßnahme* Der Lotterietechnologiezulieferer verfügt über ein Schulungs- und Sensibilisierungsprogramm über Secure-Coding-Praktiken für alle Entwickler, die Code für Spielesysteme (gemäß Definition in diesem Standard) schreiben.

S.1.2	**Integritätsvorkehrungen im Zusammenhang mit der Entwicklung von Hardware, Software und Firmware für Spielesysteme**	
Ziel:	Sicherstellung der Integrität der Lotterietechnologien.	
S.1.2.1	Integritätsprüfungen für den Release-Prozess	*Maßnahme* Der Lotterietechnologiezulieferer gibt auf jeder Stufe im Entwicklungsprozess eine Zusicherung der Integrität der von ihm entwickelten Software/Firmware ab. Dies geschieht mindestens während des Qualitätssicherungsprozesses und auch, wenn die Software/Firmware in der Produktionsumgebung übernommen wird.
S.1.2.2	Sicherheitsprotokollierung	*Maßnahme* Der Lotterietechnologiezulieferer stellt eine geeignete Sicherheitsprotokollierung der von ihm entwickelten Software/Firmware zur Verfügung. Diese kann von einem Sicherheitsteam in dessen Sicherheitsinstrumentarium integriert werden, um die Integrität der Lotterie-Software/Firmware sicherzustellen. Der Lotterietechnologiezulieferer stellt dem Sicherheitsteam ein Dokument zu, in dem genau beschrieben wird, wie die Sicherheitsprotokollierung zu verstehen und zu interpretieren ist.
S.1.2.3	Datei-Integrität	*Maßnahme* Der Lotterietechnologiezulieferer identifiziert und dokumentiert kritische Dateien in seinem Produkt, damit der Lotteriebetreiber die Integrität der Produktionsumgebung überprüfen kann.
S.1.2.4	Hardware-Integrität	*Maßnahme* Der Lotterietechnologiezulieferer trifft Vorkehrungen, um unberechtigte Versuche eines Hinzufügens oder Modifizierens von Hardware im Spielesystem zu erkennen, die sich auf die Integrität des Lotteriesystems auswirken könnten. Als Hardware gelten in diesem Zusammenhang unter anderem Video-Lotterie-Terminals, Ausrüstung von Annahmestellen und Zufallszahlengeneratoren. Die genaue Liste der Hardware, auf die sich diese Maßnahme bezieht, wird durch die Risikobeurteilung festgelegt. Hardware, die von einem „Infrastructure as a Service“-Anbieter bereitgestellt und gehostet wird, ist von dieser Kontrollpflicht ausgenommen.
S.1.2.5	Schwachstellen und Patch-Management	*Maßnahme* Der Lotterietechnologiezulieferer stellt sicher, dass ein Prozess vorhanden ist, durch den Updates für Software/Firmware und verwendete Programmbibliotheken Dritter schnell eingesetzt werden können. Die Entscheidung darüber, ob Patches zu den Produktions-Spielesystemen gepusht werden sollen oder nicht, ist Sache der Risikobeurteilung. Dabei sind die Richtlinie des Lotteriebetreibers über Schwachstellen und Patch-Management zu befolgen und kommerzielle Überlegungen zu berücksichtigen.
S.1.2.6	Verantwortungsvolle Offenlegung von Sicherheitslücken	*Maßnahme* Der Lotterietechnologiezulieferer verfügt über eine Richtlinie zur verantwortungsvollen Offenlegung von Sicherheitslücken (Responsible-Disclosure-Richtlinie), die allen zur Verfügung steht, die seine Produkte oder Dienstleistungen erworben haben, damit sie Sicherheitsschwachstellen in ihren Spielesystemprodukten melden können.

S.1.3	**Integritätsvorkehrungen im Zusammenhang mit dem Drucken physischer Sofortlose**
Ziel:	Sicherstellung der Integrität physischer Sofortlose.

S.1.3.1	Anforderungen an physische Sofortspiele	
Ziel:	Anpassung der Anforderungen des Lotteriebetreibers an die Spezifikationen des Zulieferers.	
S.1.3.1.1	Anforderungen an Sofortspiele	*Maßnahme* Der Zulieferer hat die Anforderungen formell mit dem Lotteriebetreiber zu validieren und in Spezifikationen umzuwandeln. Für alle Änderungen der Spezifikationen ist der Change-Management-Prozess sowohl des Zulieferers als auch des Lotteriebetreibers zu befolgen.

S.1.3.2	Generierung und Validierung der Daten	
Ziel:	Sicherstellung, dass die Sofortspielprogrammierung die Anforderungen erfüllt und abgesichert wird.	
S.1.3.2.1	Generierung von Sofortspieldaten	*Maßnahme* Für den zur Generierung von Sofortspieldaten verwendeten Randomisierungsprozess gelten die Maßnahmen von WLA-SCS L.2.4, „Elektronische Lotterieziehungen und Sofortspiele“, sowie die Anforderungen, die zwischen dem Betreiber und dem Zulieferer vereinbart werden.
S.1.3.2.2	Validierung der Spieldaten	*Maßnahme* Der Zulieferer stellt sicher, dass ein unabhängiges Team die logischen Spieldaten im Hinblick auf die Anforderungen des Lotteriebetreibers validiert. Entsprechende Ergebnisberichte werden dem Lotteriebetreiber zur Verfügung gestellt.
S.1.3.2.3	Vertraulichkeit der Daten	*Maßnahme* Der Zulieferer stellt sicher, dass der Zugriff auf die Validierungsdaten jederzeit, auch nach der Lieferung des Sofortspiels, nach dem Prinzip der geringsten Privilegierung (Least-Privilege-Prinzip) beschränkt ist.

S.1.3.3	Druck	
Ziel:	Sicherstellung der Integrität im Druckprozess.	
S.1.3.3.1	Validierung vor dem Druck	*Maßnahme* Der Zulieferer validiert formell die definitiven Bilder und Texte mit dem Lotteriebetreiber, bevor er die Lose druckt.
S.1.3.3.2	Integritätsüberprüfungen	*Maßnahme* Der Zulieferer führt regelmäßige Überprüfungen der Integrität der Lose durch.

S.1.3.4	Endbearbeitung	
Ziel:	Sicherstellung der Übereinstimmung mit der Gewinnstruktur und Gewährleistung der Integrität der Lose während der Lieferung.	
S.1.3.4.1	Eindeutige Kennziffern der Lose	*Maßnahme* Es werden Vorkehrungen getroffen, damit jedes gelieferte Los eine einmalige Nummer erhält.
S.1.3.4.2	Übereinstimmung mit der Gewinnstruktur	*Maßnahme* Der Zulieferer weist nach, dass er in jeder gedruckten Charge die richtige Anzahl Lose entsprechend der vorgeschriebenen Gewinnstruktur geliefert hat.
S.1.3.4.3	Vernichtete Lose	*Maßnahme* Es besteht ein dokumentiertes Verfahren, das sicherstellt, dass gedruckte, aber nicht gelieferte Lose auf sichere Weise vernichtet werden.
S.1.3.4.4	Versandsicherheit	*Maßnahme* Der Zulieferer stellt sicher, dass die Lieferung der Lose vom Zulieferer zum Lotteriebetreiber abgesichert erfolgt.

Anhang D (M-Maßnahmen): Maßnahmen für Mehrstaaten-Spiele

M.1	**Anforderungen für die Beteiligung an Spielen der Multi-State Lottery Association (MUSL)**	
M.1.1	**Sicherheit, Integrität und Verfügbarkeit der Transaktionen**	
Ziel:	Sicherstellung, dass Transaktionen ordnungsgemäß erfasst und abgesichert werden.	
M.1.1.1	Validierung der Gewinnansprüche	*Maßnahme* Damit die Bedingungen gemäß den Maßnahmen im Abschnitt L.4.1 dieses Dokuments als erfüllt gelten, muss eine Organisation zusätzlich die Minimum Game Security Standards der Multi-State Lottery Association (MUSL) einhalten.
M.1.1.2	Redundanz der Transaktionsdaten	*Maßnahme* Die Datensätze der Verkaufstransaktionsdaten im Spielesystem werden in Rechenzentren an mindestens zwei gesonderten Standorten gespeichert. Sie sind ausreichend voneinander getrennt, um nicht vom selben Katastrophenereignis betroffen werden zu können.
M.1.1.3	Transaktionsbestätigung	*Maßnahme* Jeder Standort erhält und bestätigt die Transaktionsdaten, bevor ein Spielschein ausgedruckt werden darf.
M.1.1.4	Backup der Spieldaten	*Maßnahme* Die Spieldaten werden täglich mittels Backup gesichert sowie offline und offsite gespeichert.
M.1.1.5	Integrität der Transaktionen vor und nach einer Ziehung	*Maßnahme* Vor jeder Ziehung wird eine von der MUSL genehmigte kryptografische Hashfunktion auf die ganze Menge der Transaktionen angewendet, die im Vorfeld der Ziehung auf dem internen Kontrollsystem (ICS) gespeichert wurden, um einen Hashwert („Message Digest of Hash“) zu generieren. Dieselbe kryptografische Hashfunktion wird erneut auf die ganze Menge der Transaktionen angewendet. Dies geschieht mit der Erstellung eines Gewinnklassenberichtes („Tier Report“), der unmittelbar nach der Ziehung erstellt wird.

M.1.2	Sicherheit von Geräten der Annahmestellen	
Ziel:	Gewährleistung der Sicherheit von Geräten der Annahmestellen, bei denen es sich nicht um ausgewiesene Lotterieterminals handelt.	
M.1.2.1	Gerät einer Annahme-stelle	*Maßnahme* Wird anstelle eines ausgewiesenen Lotterieterminals ein Gerät der Annahmestelle verwendet, so muss dieses die Anforderungen der NASPL erfüllen.
M.1.2.2	Lotterieterminals, die nicht zur Ausgabe von Live-Spielscheinen bestimmt sind.	*Maßnahme* Terminals, die nicht zur Ausgabe von Live-Spielscheinen bestimmt sind und die für Betreiber von Computerspielesystemen oder internen Kontrollsystemen zugänglich sind, werden so modifiziert, dass klar ist, dass von den entsprechenden Terminals erstellte Spielscheine ungültig sind. Weder die Standortbetriebe noch die IT-Mitarbeiter dürfen in der Lage sein, die Modifizierungen zu umgehen.

M.1.3	Quick-Picks	
Ziel:	Sicherstellung, dass Quick-Picks zufällig ausgewählt werden.	
M.1.3.1	Zufälligkeit von Quick-Picks	*Maßnahme* Software, die zur Generierung von Zufallszahlen für Quick-Picks verwendet wird, muss die WLA-SCS-Maßnahme L.2.4.3 „Verifizierung der Zufälligkeit und Integrität bei elektronischen Ziehungen“ erfüllen.

M.1.4	Trennung zwischen ICS und CGS	
Ziel:	Sicherstellung der Trennung zwischen dem Computerspielesystem (Computer Gaming System, CGS) und dem internen Kontrollsystem (Internal Control System, ICS).	
M.1.4.1	Trennung zwischen dem Computerspielesystem und dem internen Kontrollsystem	*Maßnahme* Falls das Computerspielesystem von einem Drittanbieter betrieben wird, muss das ICS im Sinne der WLA-SCS-Maßnahme L.2.2.8, „Unabhängiges Kontrollsys-tem“, von einem gesonderten Unternehmen betrieben werden. Die Verantwortung für diese Systeme muss auf jeden Fall strikt getrennt sein, und niemand darf auch nur teilweise Zugriff auf sowohl das ICS als auch das CGS haben.

M.1.5	Ziehungsverfahren	
Ziel:	Sicherstellung der Kontinuität und Integrität zwischen der Verarbeitung der Gewinnzahlen und der Verarbeitung der Verkaufstransaktionen.	
M.1.5.1	Einsatz derselben Mitarbeiter und desselben internen Kontrollsystems	*Maßnahme* Der Lotteriebetreiber oder der von ihm Beauftragte setzt für die Verarbeitung der Gewinnzahlen dieselben Mitarbeiter und dasselbe ICS-System ein wie für die Verarbeitung der Verkaufstransaktionen.

M.1.6	**Angriffserkennungssystem**	
Ziel:	Risikomanagement bezüglich Cyberangriffen auf das ICS und CGS.	
M.1.6.1	Angriffserkennungssystem auf dem ICS- und dem CGS-Netzwerk	*Maßnahme* Sowohl auf dem ICS- als auch auf dem CGS-Netzwerk ist ein Angriffserkennungs- und -meldesystem oder ein Angriffsabwehrsystem vorhanden und aktiv konfiguriert, um die lokalen Administratoren zu benachrichtigen.