Algemene Rekenkamer Curaçao


**Status van de beheersmaatregelen van de geautomatiseerde omgeving**

**Doelmatigheid**

# Landsloterij

# -

# Geautomatiseerde omgeving

**December**

**2020**

www.rekenkamercuracao.cw

# Inhoudsopgave

## Lijst van afkortingen en begrippen

| Afkorting/Begrip | Omschrijving |
|---|---|
| AC | Application controls<br>De beheersingsmaatregelen in de geautomatiseerde processen |
| Automated controls | Een mechanisme binnen een applicatie of een interface dat een regelset of validatie op een of meer voorwaarden binnen een proces afdwingt of controleert |
| COBIT | Control Objectives for Information and related Technology |
| CTO | Chief Technology Officer |
| IT | Informatie Technologie |
| ITGC | Information Technology General Controls<br>De randvoorwaardelijke beheersingsmaatregelen voor het functioneren van een informatiesysteem |
| ISO-standaarden | Standaarden uitgebracht door de International Standards Organization |
| ISSAI | International Standards for Supreme Audit Institutions |
| Lotenregistratiesysteem | Geautomatiseerd systeem voor het registreren van de loten |
| Rekenkamer | Algemene Rekenkamer Curaçao |
| RvTA | Raad van Toezicht en Advies van de Landsloterij |

# Rapport in het kort

## Samenvatting

De Rekenkamer is wettelijk aangewezen om de rekening van ontvangsten en uitgaven van de Landsloterij goed te keuren alvorens deze aan de Staten ter goedkeuring aan te bieden. Als voorbereiding op de controle van de rekeningen van de Landsloterij heeft de Rekenkamer een onderzoek uitgevoerd op de geautomatiseerde systemen die de bedrijfsvoering van de organisatie ondersteunen. Het gaat hierbij om het geautomatiseerd lotenregistratiesysteem en financieel systeem. Volledigheidshalve wordt vermeld dat geen onderzoek is gedaan naar de trekkingen. Het onderzoek behelst de periode 2010 tot en met 2017. Gekozen is voor deze periode omdat de jaarrekening 2017 de laatst gecontroleerde jaarrekening van de Landsloterij betreft.
Het lotenregistratiesysteem wordt door de Landsloterij gebruikt voor de registratie van met name de verkoop van de loten. De Landsloterij organiseert de verkoop van loten op Curaçao, Aruba, Sint Maarten en de BES-eilanden. De financiële administratie van de organisatie wordt in een geautomatiseerd financieel systeem bijgehouden. Vanuit dit systeem wordt informatie aangeleverd voor de financiële verslaglegging en de jaarlijks op te stellen rekening van ontvangsten en uitgaven.

De betrouwbaarheid van de inrichting en werking van deze twee bovenvermelde systemen zijn door de Rekenkamer beoordeeld ten einde een volledig risicobeeld te krijgen van de betrouwbaarheid van de informatie uit deze systemen.

Als centrale vraag voor dit onderzoek heeft de Rekenkamer de volgende twee vragen geformuleerd:

1. ***Waren de beheersingsmaatregelen rondom het lotenregistratie- en financieel systeem die de bedrijfs- en informatieprocessen van de Landsloterij gedurende 2010 tot en met 2017 hebben ondersteund van voldoende kwaliteit zodat zekerheid kan worden verkregen over de betrouwbaarheid van de informatie voortvloeiende uit deze systemen?***

2. ***Heeft de Landsloterij de aanbevelingen uit de diverse IT rapporten van de controlerende accountant inzake de te treffen beheersmaatregelen rond en binnen het***

***lotenregistratiesysteem geïmplementeerd zodat de tekortkomingen kunnen worden weggewerkt?***

Voor het onderzoeken van de betrouwbaarheid van de bovenvermelde systemen is door de Rekenkamer nagegaan of de 'automated controls' in deze applicaties, zijnde de ITGC en de AC, toereikend zijn.

Om de centrale vraag te beantwoorden heeft de Rekenkamer interviews gehouden met de directeur, de ontwikkelaar/beheerder van het lotenregistratiesysteem en de leden van het team dat verantwoordelijk was voor de implementatie van de beheersmaatregelen. Daarnaast heeft de Rekenkamer onderliggende documenten verzameld en beoordeeld en een waarneming ter plaatse gedaan van de trekking van 5 maart 2020.

Uit het onderzoek is gebleken dat de Landsloterij gedurende de periode 2010 tot en met 2017 niet over een vastgesteld informatiebeveiligingsbeleid beschikte. Daarnaast zijn er diverse tekortkomingen geconstateerd die een effectieve werking van het lotenregistratiesysteem konden belemmeren. Hierdoor bestond er geen zekerheid over de betrouwbaarheid van de informatie uit dit systeem in de onderzoeksperiode en waren aanvullende werkzaamheden nodig om de jaarrekeningen te controleren. In 2019 heeft de Landsloterij diverse acties ondernomen om de geconstateerde tekortkomingen weg te werken. Een belangrijke stap was het introduceren van een informatiebeveiligingsbeleid met de bijbehorende werkwijzen. De beheersmaatregelen die de kwaliteit van de informatieverwerking in het financieel systeem moeten waarborgen zijn in maart 2020 door de Rekenkamer onderzocht en toereikend bevonden.

Op basis van deze bevindingen is de Rekenkamer tot de hierna vermelde conclusies gekomen en zijn de volgende aanbevelingen door de Rekenkamer gegeven.

## Conclusies

Uit het onderzoek concludeert de Rekenkamer dat:

1. de beheersmaatregelen die betrekking hebben op het lotenregistratiesysteem, te weten de ITGC, gedurende de periode 2010-2017 niet toereikend waren. Ondanks dat er geconcludeerd is dat de AC in het lotenregistratiesysteem

gedurende 2010-2017 over het algemeen toereikend waren, kon de ongestoorde werking van de AC niet worden gewaarborgd, omdat de randvoorwaardelijke beheersingsmaatregelen niet toereikend waren. Hierdoor was er een onzekerheid of de gegevens juist, volledig en tijdig in het lotenregistratiesysteem waren verwerkt;

2. de maatregelen van de Landsloterij rond het beheer van de toegangen in het financieel systeem en de controles ingebouwd in dit systeem niet beoordeeld zijn voor de periode 2010 tot en met 2017. Gezien het verloop van tijd en het ontbreken van relevante vastleggingen was deze controle achteraf niet meer mogelijk. Per maart 2020 is geconstateerd dat deze maatregelen toereikend zijn om de juiste werking van deze applicatie te waarborgen;
3. de Landsloterij alle zestien aanbevelingen uit de rapporten van de controlerende accountant heeft opgevolgd. De Landsloterij dient, waar nodig, de procedures uit te schrijven;
4. de acties die de Landsloterij heeft uitgevoerd de geïdentificeerde tekortkomingen zullen verhelpen;
5. de huidige status van de ITGC en AC in opzet en bestaan voldoende zijn. De werking hiervan dient in een volgend onderzoek te worden onderzocht.

## Aanbevelingen

De Rekenkamer beveelt de Staten aan om de minister van Financiën te vragen erop toe te zien dat de Landsloterij:

a. uitvoering geeft aan het vastgestelde informatiebeveiligingsbeleid en bijbehorende procedures, zodat de juiste werking van de beheersingsmaatregelen (de ITGC en de AC) rondom en in de geautomatiseerde systemen gewaarborgd worden. Met de juiste werking van deze maatregelen wordt de betrouwbaarheid van de informatie in de systemen gegarandeerd, zodat vertrouwen wordt behouden in de loterij;
b. de implementatie van alle aanbevelingen uit de diverse rapporten van de controlerende accountant afrondt door de nog uit te werken richtlijnen in concrete procedures te voltooien;
c. tweejaarlijks verantwoording aan hem aflegt over de kwaliteit van de beheersmaatregelen in de geautomatiseerde omgeving.

# Rapòrt resumí

## Resúmen

Kontraloria ta apuntá pa lei pa aprobá e kuenta di entrada i gastu di Landsloterij promé ku esaki wòrdu entregá na Parlamento pa su aprobashon. Komo preparashon pa kòntròl di e kuentanan di Landsloterij, Kontraloria a hasi un investigashon di e sistemanan outomatisá ku ta sostené e maneho operashonal. Ta trata aki di e sistema outomatisá di registrashon di brièchi i e sistema finansiero. No a investigá e sorteonan. E investigashon ta kubri e periodo di 2010 te ku 2017. A skohe pa e periodo akí pa motibu ku e kuenta anual di 2017 ta e último kuenta anual ouditá di Landsloterij.
Landsloterij ta usa e sistema di loteria prinsipalmente pa registrashon di benta di brièchi. Landsloterij ta organisá benta di loteria pa Kòrsou, Aruba, Sint Maarten i e islanan BES. E atministrashon finansiero di e organisashon ta wòrdu tené den un sistema finansiero outomatisá. E sistema akí ta suministrá informashon pa e relato finansiero i pa e kuenta anual di entrada i gastu.

Kontraloria a evaluá kon e dos sistemanan ariba menshoná ta funshoná i kon konfiabel nan diseño ta, pa por haña un bista kompleto di e riesgo di konfiabilidat di e informashon ku e sistemanan akí ta produsí.

Komo pregunta sentral pa e investigashon akí Kontraloria a formulá e siguiente dos preguntanan:

1. ***E medidanan di maneho ròmt di e sistemanan di registrashon di brièchi i finansiero ku a sostené e prosesonan di maneho i informashon di Landsloterij durante 2010 te ku 2017 tabata di sufisiente kalidat pa por tin sigur ku e informashon ku e sistemanan akí ta produsí ta konfiabel?***

2. ***Landsloterij a implementá e rekomendashonnan di e diferente rapòrtnan di IT di e akountent enkuanto e medidanan di maneho ku mester ehekutá ròmt di i dentro di e sistema di registrashon di brièchi pa asina e fayonan por wòrdu eliminá?***

Pa investigá konfiabilidat di e sistemanan ariba menshoná, Kontraloria a chèk si e 'automated controls' den e aplikashonnan akí, esta, e ITGC i AC, ta adekuado.

Pa kontestá e pregunta sentral, Kontraloria a tene entrevista ku e direktor, e desaroyadó/atministradó di e sistema di loteria i e miembronan di e tim responsabel pa implementashon di e medidanan di maneho. Banda di esei, Kontraloria a buska i evaluá e dokumentonan konserní i a tuma parti na e opservashon di e rifa di 5 di mart 2020.

For di e investigashon a sali na kla ku durante e periodo di 2010 te ku 2017, Landsloterij no tabata disponé di un maneho fihá di protekshon di informashon. Ademas, a konstatá diferente fayo ku por a difikultá funshonamentu efektivo di e sistema di registrashon di brièchi. Pa e motibu aki, no a eksistí garantia tokante konfiabilidat di e informashon ku a sali for di e sistema akí den e periodo di investigashon i mester a hasi mas trabou pa kontrolá e kuentanan di entrada i gastu. Den 2019, Landsloterij a tuma vários akshon pa eliminá e fayonan konstatá. Un paso importante tabata introdukshon di un maneho di protekshon di informashon huntu ku e prosedurenan korespondiente. Na mart 2020, Kontraloria a investigá e medidanan di maneho ku mester garantisá kalidat di e prosesamentu di informashon den e sistema finansiero, i a yega na e konklushon ku nan ta adekuá.

A base di e resultadonan akí, Kontraloria a yega na e siguiente konklushonnan i ta duna e siguiente rekomendashonnan.

## Konklushon

For di e investigashon Kontraloria ta konkluí ku:

1. e medidanan di maneho relashoná ku e sistema di registrashon di brièchi, esta e ITGC, no tabata adekuado. Aunke a konkluí ku e AC den e sistema di loteria durante 2010 – 2017 en general tabata adekuado, no por a garantisá funshonamentu sin interupshon di e AC, pasobra den práktika e medidanan indispensabel di maneho no tabata funshoná adekuadamente. Pa e motibu akí tabatin inseguridat si e datonan a wòrdu prosesá korektamente, kompleto i na tempu;
2. e medidanan di Landsloterij ròmt di e maneho di akseso den e sistema finansiero i e kontrolnan inkorporá den e sistema akí no a wòrdu evaluá pa e periodo 2010 te ku 2017. Mirando ku tempu a pasa i ku tabata falta dokumentashon relevante, e kontrol akí despues no tabata posibel mas. Pa mart 2020, a konstatá ku e

medidanan akí tabata adekuado pa garantisá funshonamentu korekto di e aplikashon akí;

3. Landsloterij a sigui tur e dieseis rekomendashonnan di e rapòrt di e akountent kontroladó. Unda ta nesesario, Landsloterij tin ku kaba di pone e proseduranan por eskrito;
4. e akshonnan ku Landsloterij a tuma lo remediá e fayonan identifiká;
5. e státus aktual di e ITCC i AC manera nan ta diseñá i e manera ku nan ta den realidat ta wòrdu konsiderá adekuado. Nan funshonamentu lo tin di wòrdu evaluá den un siguiente investigashon.

## Rekomendashonnan

Kontraloria ta rekomendá Parlamento pa puntra minister di Finansa pa laga sòru ku Landsloterij:

a. ta duna ehekushon na e maneho establesí di protekshon di informashon i proseduranan korespondiente pa asina e funshonamentu korekto di e medidanan di maneho (ITGC i AC) ròmt di i den e sistemanan outomatisá ta wòrdu garantisá. Un funshonamentu korekto di e medidanan akí lo garantisá e konfiabilidat di e informashon den e sistemanan pa asina e konfiansa den e loteria por keda mantené;
b. ta finalisá implementashon di tur e rekomendashonnan di e diferente rapòrtnan di e akountent kontroladó dor di kaba di elaborá e indikashonnan den prosedura konkreto;
c. ta duna kuenta i rason na e minister kada dos aña tokante kalidat di e medidanan di maneho den e ambiente outomatisá.

# 1. Inleiding

De Rekenkamer is bij wet[1] aangewezen om de rekening van ontvangsten en uitgaven[2] van de Landsloterij goed te keuren. In dit kader heeft de Landsloterij de jaarrekeningen van de jaren 2010 tot en met 2017 aan de Rekenkamer ter controle aangeboden. Deze jaarrekeningen zijn voorzien van een accountantsverklaring van de controlerende accountant. De verklaringen bij de voornoemde jaarrekeningen vermelden allen dat de jaarrekeningen een getrouw beeld geven van de grootte en samenstelling van het vermogen van de Landsloterij per einde van het betreffende jaar en eveneens van het resultaat over dat jaar.

Aangezien de lotenregistratie door de Landsloterij hoofdzakelijk digitaal gebeurt is het van belang dat de Rekenkamer, alvorens de rekeningen van de Landsloterij te controleren, eerst de betrouwbaarheid van de beheersmaatregelen van de geautomatiseerde systemen onderzoekt. De Landsloterij maakt gebruik van een geautomatiseerd systeem voor het organiseren van de loterij. In dit lotenregistratiesysteem wordt de volgende informatie geregistreerd:

a. trekking gegevens;
b. verkochte loten;
c. geretourneerde loten;
d. loten geblokkeerd voor uitbetaling;
e. winnende lotnummers per trekking;
f. verzilverde loten.

Naast het lotenregistratiesysteem maakt de Landsloterij gebruik van een financieel systeem voor de registratie van de financiële transacties rondom de lotenverkoop en de overige operationele transacties. Deze twee systemen zijn niet met elkaar verbonden. De financiële gegevens uit het lotenregistratiesysteem worden handmatig in het grootboek in het financieel systeem geboekt. De informatie die jaarlijks in de jaarrekening wordt opgenomen is afkomstig uit dit systeem.

Voor beide applicaties is gekeken naar de kwaliteit van de beheersmaatregelen voor de

[1] P.B. 1965, no. 122 tot wijziging van de Landsverordening van de 15de oktober 1949 betreffende de Landsloterij.
[2] Inmiddels stelt de Landsloterij geen staat van ontvangsten en uitgaven meer op. Door de overgang naar dubbelboekhouding wordt tegenwoordig een jaarrekening opgesteld.

geautomatiseerde omgeving. Beide geautomatiseerde registraties zijn belangrijk om zekerheid te verkrijgen over het verloop van de lotenverkoop en voor de getrouwheid van de informatie die voortvloeit uit deze systemen. Op basis hiervan kunnen de risico's van een materiële afwijking in de jaarrekeningen worden onderkend.

Voor de controle van de betrouwbaarheid van het lotenregistratiesysteem alsook het financieel systeem, is de Rekenkamer nagegaan of de 'automated controls' in deze applicaties, zijnde de ITGC en de AC, toereikend zijn. De ITGC zijn noodzakelijk om de ongestoorde werking van de AC te garanderen. De AC zorgen voor gerichte vergelijkingen van gegevens binnen de applicatie, zodat zekerheid kan bestaan dat de gegevens juist, volledig en tijdig binnen de applicatie worden verwerkt.

De Rekenkamer heeft voor haar onderzoek waar mogelijk gebruik gemaakt van de onderzoeken uitgevoerd door de controlerend accountant. Gezien het tijdsverloop is de Rekenkamer ook nagegaan of de tekortkomingen die de accountant heeft geconstateerd in de controlejaren 2010 tot en met 2017, door de Landsloterij zijn weggewerkt door de maatregelen, die in de rapporten van de controlerend accountant zijn aanbevolen, te implementeren.

In dit rapport gaan wij in op onze bevindingen.

# 2. Opzet onderzoek

## 2.1 Achtergrond onderzoek

De Landsloterij organiseert de staatsloterij op Curaçao middels gewone en bijzondere loterijen. Tot en met december 2018 werden er per jaar totaal 24 trekkingen [3] georganiseerd:

- 20 kleine trekkingen met een hoofdprijs van NAf. 200.000,-
- 2 middelgrote trekkingen met een hoofdprijs van NAf. 500.000,-
- 2 grote trekkingen met een hoofdprijs van NAf. 1.000.000,-

De opbrengsten van de Landsloterij zijn afhankelijk van het aantal verkochte loten. Uit de jaarrekeningen over de jaren 2010 tot en met 2017 blijkt dat in die jaren de jaarlijkse opbrengsten tussen de 24 miljoen en 26 miljoen fluctueerden. De jaarlijkse opbrengsten zijn in onderstaande tabel opgenomen.

*Tabel 1: Kengetallen 2010-2017.*

| Jaar | Totaal aantal verkochte loten | Totaal opbrengst verkoop loten (NAf) | Totaal uitgekeerd aan prijzen en premies (NAf) | Prijzen en premies in % v/d opbrengst | Totaal betaald aan vergunnings-recht (NAf) | Totaal betaald aan zegelbelasting (NAf) | Totaal betaald aan omzetbelasting (NAf) | Provisie aan de wederver-kopers (NAf) |
|---|---|---|---|---|---|---|---|---|
| **2010** | 495,194.5 | 26,082,250 | 11,436,645 | 44% | 2,422,141 | 1,863,127 | 1,050,085 | 4,489,252 |
| **2011** | 507,447.5 | 26,533,415 | 12,200,258 | 46% | 2,465,893 | 1,896,782 | 1,069,030 | 4,577,633 |
| **2012** | 516,070 | 27,076,113 | 12,631,565 | 47% | 2,514,435 | 1,934,121 | 1,298,211 | 4,664,241 |
| **2013** | 509,566 | 26,788,193 | 11,469,265 | 43% | 2,487,698 | 1,913,554 | 1,599,488 | 4,612,697 |
| **2014** | 490,277.5 | 25,833,758 | 11,176,865 | 43% | 2,399,065 | 1,845,377 | 1,817,654 | 4,445,745 |
| **2015** | 475,027.5 | 24,944,770 | 11,237,805 | 45% | 2,316,508 | 1,781,873 | 1,755,901 | 4,296,265 |
| **2016** | 477,407.5 | 25,182,043 | 11,849,005 | 47% | 2,338,543 | 1,798,823 | 1,772,409 | 4,332,824 |
| **2017** | 471,598 | 24,760,780 | 10,440,445 | 42% | 2,299,421 | 1,768,730 | 1,742,819 | 4,264,794 |
| **Totaal** | **3,942,588.5** | **207,201,322** | **92,441,853** | **45%** | **19,243,704** | **14,802,387** | **12,105,597** | **35,683,451** |

Uit de tabel blijkt ook welk aandeel van de opbrengsten uitgegeven is aan prijzen en premies (zijnde extra prijzen). Dat komt neer op gemiddeld 45% per jaar. Ook blijkt hieruit welk deel van de opbrengst is betaald aan vergunningsrecht, zegelbelasting, omzetbelasting en provisie aan de wederverkopers.

[3] Vanaf 2019 worden totaal 22 trekkingen per jaar georganiseerd:
- 11 kleine trekkingen;
- 7 middelgrote trekkingen;
- 4 grote trekkingen.

De Landsloterij gebruikt het aantal verkochte en onverkochte loten, zoals in het lotenregistratiesysteem vastgelegd, voor hun verantwoording van de ontvangsten, betaalde prijzen, afdrachten van belastingen en voor de financiële verslaglegging. Hierdoor is het van belang dat zekerheid bestaat dat de informatie uit deze systemen betrouwbaar is zodat de juistheid en volledigheid van de afdrachten gegarandeerd kan worden alsook dat de financiële verslaggeving getrouwe informatie weergeeft.

## 2.2 Doel van het onderzoek

Met dit onderzoek beoogt de Rekenkamer na te gaan of de beheersmaatregelen in de geautomatiseerde systemen toereikend zijn. Hiermee kunnen de Rekenkamer en andere belanghebbenden zekerheid hebben in de betrouwbaarheid van de gegevens voortvloeiende uit deze systemen.

Daarnaast beoogt de Rekenkamer, zoals reeds vermeld, vast te stellen of de geconstateerde tekortkomingen in de voorgaande jaren zijn weggewerkt.
Gelet op het bovenstaande heeft de Rekenkamer de centrale vraag voor dit onderzoek tweeledig geformuleerd en luidt deze als volgt:

***Waren de beheersingsmaatregelen rondom het lotenregistratie- en financieel systeem die de bedrijfs- en informatieprocessen van de Landsloterij gedurende 2010 tot en met 2017 hebben ondersteund van voldoende kwaliteit, zodat zekerheid kan worden verkregen over de betrouwbaarheid van de informatie voortvloeiende uit deze systemen?***

***Heeft de Landsloterij de aanbevelingen uit de diverse IT auditrapporten van de controlerend accountant inzake de te treffen beheersmaatregelen rond en binnen het lotenregistratiesysteem geïmplementeerd, zodat de tekortkomingen kunnen worden weggewerkt?***

De onderzoeksvraag is door de Rekenkamer onderverdeeld in de onderstaande drie deelvragen:

1. Waren de beheersmaatregelen te weten de ITGC en AC in de geautomatiseerde systemen gedurende de periode 2010-2017 toereikend?
2. In hoeverre zijn de aanbevelingen die in het verleden gegeven zijn door de controlerende accountant voor het wegwerken van de tekortkomingen in de

beheersingsmaatregelen in het geautomatiseerd lotenregistratiesysteem door de Landsloterij doorgevoerd?

3. Voor zover de aanbevelingen zijn doorgevoerd, wat is de huidige status van de beheersingsmaatregelen?

## 2.3 Aard en reikwijdte van het onderzoek

In dit onderzoek wordt de betrouwbaarheid van de beheersmaatregelen in en rondom de geautomatiseerde systemen van de Landsloterij onderzocht. Dit onderzoek beperkt zich tot de boekjaren 2010 tot en met 2017. Dit, aangezien de jaarrekeningen over de jaren 2018 en 2019 nog niet gereed zijn en er geen controle door de controlerende accountant op de geautomatiseerde systemen is uitgevoerd over deze twee jaren. Gezien de verstreken periode is ook gekeken naar de status van de beheersmaatregelen per 2020. Het onderzoek beperkt zich tot uitsluitend de beheersingsmaatregelen rondom de vermelde systemen. Dit houdt in dat de Rekenkamer geen onderzoek heeft gedaan naar:

- de IT governance[4] van de Landsloterij;
- de IT strategie, -organisatie en -structuur van de Landsloterij;
- de maatregelen rondom de acquisitie danwel ontwikkeling van de systemen;
- de 'environmental controls' ter bescherming van de IT componenten van de Landsloterij.

Volledigheidshalve wordt vermeld dat geen onderzoek is gedaan naar de trekkingen gehouden in deze onderzoeksperiode.

## 2.4 Aanpak van het onderzoek

Voor het uitvoeren van het onderzoek heeft de Rekenkamer de volgende werkzaamheden verricht:

- Het identificeren van de benodigde beheersmaatregelen ter beoordeling van de ITGC en AC binnen de geautomatiseerde systemen.
- Het verzamelen van bewijsmateriaal ter beoordeling van de geïdentificeerde beheersmaatregelen binnen de geautomatiseerde systemen. Hiervoor is, gezien de reeds verstreken periode en de beperkingen om deze controles alsnog uit te voeren, zoveel mogelijk gebruik gemaakt van de reeds door de controlerend

[4] IT governance zijn de processen die zorgen voor een effectief en efficiënt gebruik van IT om een organisatie in staat te stellen haar doelen te bereiken.

accountant uitgevoerde onderzoeken naar deze beheersingsmaatregelen.

- Het interviewen van de directeur van de Landsloterij tezamen met de projectleden[5] over de ondernomen stappen om de aanbevelingen vermeld in de diverse IT audit rapporten te implementeren om zodoende de geconstateerde tekortkomingen uit deze rapporten weg te werken.
- Het nagaan van de huidige beheersingsmaatregelen (in het jaar 2020) binnen het lotenregistratiesysteem om het bestaan van deze maatregelen per heden vast te stellen. Hiertoe heeft de Rekenkamer ook de trekking van 5 maart 2020 bijgewoond.
- Het vaststellen van de status van de implementatie van de aanbevelingen door de Landsloterij voor zover nog niet alle aanbevelingen zijn doorgevoerd. Hiertoe is de planning, uitvoering en voortgang van de activiteiten inzichtelijk gemaakt en beoordeeld.
- Het vaststellen of met de genomen maatregelen en gevoerde acties de Landsloterij de aanbevelingen uit de eerdere IT audits daadwerkelijk heeft opgevolgd.

## 2.5 Normenkader

Om de onderzoeksvragen te beantwoorden heeft de Rekenkamer criteria geformuleerd om de maatregelen te toetsen. Hierbij is de Rekenkamer uitgegaan van de ISSAI-richtlijnen zoals vastgelegd in ISSAI 5310[6] en erkende internationale standaarden opgenomen in de COBIT- en ISO-standaarden. Ook de relevante bepalingen uit de Landsloterijverordening zijn gehanteerd als normen voor het toetsen van de beheersingsmaatregelen.
In bijlage 1 zijn de criteria opgenomen waaraan de beheersingsmaatregelen rond ITGC en AC rondom en binnen de geautomatiseerde systemen zijn getoetst.

## 2.6 Leeswijzer

In hoofdstuk 3 worden de bevindingen met betrekking tot het geautomatiseerd lotenregistratiesysteem gepresenteerd alsook de huidige status van de beheersingsmaatregelen nadat de aanbevelingen zijn geïmplementeerd. Hierna wordt in

[5] De projectleden waren naast de directeur de externe IT consultant (projectleider), de beheerder van het geautomatiseerd lotenregistratiesysteem, hoofd van de afdeling Financiën, hoofd van de afdeling Interne Controle en de assistent van de directeur.
[6] 'Information System Security Review Methodology' uitgegeven door 'EDP Audit Committee International Organization of Supreme Audit Institutions' in October 1995.

hoofdstuk 4 ingegaan op de bevindingen betrekking hebbende op het financieel systeem. Op basis van de bevindingen in de eerdere hoofdstukken wordt in hoofdstuk 5 een algehele conclusie getrokken gevolgd door onze aanbevelingen. De ambtelijke en bestuurlijke reacties in het kader van 'hoor en wederhoor' worden in hoofdstuk 6 weergegeven. Het rapport wordt met hoofdstuk 7 afgesloten met het nawoord van de Rekenkamer.

# 3. Bevindingen lotenregistratiesysteem

De Rekenkamer heeft op basis van haar onderzoek geconstateerd dat er niet voldoende beheersmaatregelen zijn ingebouwd rondom en in het lotenregistratiesysteem om de betrouwbaarheid van de informatie te garanderen. Deze constateringen zijn mede gebaseerd op de bevindingen van de controlerend accountant die in de periode 2010 tot en met 2017 drie verschillende IT audits heeft verricht op dit systeem. Deze audits bestrijken de periodes 2010-2013[7], 2014-2015[8] en 2015-2017[9]. Uit het onderzoek van de Rekenkamer blijkt dat de ITGC en de AC binnen het lotenregistratiesysteem voor de periode 2010 tot en met 2017 niet toereikend waren. Hierdoor waren aanvullende werkzaamheden noodzakelijk om de jaarrekeningen te controleren.

Op basis van de tekortkomingen die in deze audits zijn geconstateerd, heeft de accountant diverse aanbevelingen gedaan aan de organisatie. De Rekenkamer constateert dat tot mei 2019 deze aanbevelingen niet zijn opgevolgd. Pas in juni 2019 heeft de nieuw aangetreden directeur opdracht gegeven aan een IT consultancy bedrijf om samen met de ontwikkelaar en de beheerder te zorgen dat voornoemde aanbevelingen worden geïmplementeerd. Tijdens het onderzoek van de Rekenkamer bleek dat diverse van de aanbevelingen zijn doorgevoerd. In onderstaande tabel is een samenvatting van de status van de aanbevelingen per object van de geautomatiseerde gegevensverwerking opgenomen.

*Tabel 2: Samenvatting status van aanbevelingen op het lotenregistratiesysteem*

| | Aantal aanbevelingen | | |
|---|---|---|---|
| | **voortvloeiende uit de diverse rapporten** | die zijn opgevolgd | waarvan de implementatie niet geheel is afgerond* |
| Incidenten beheer | 5 | 5 | - |
| Wijzigingen beheer | 1 | 1 | - |
| Logische toegangsbeheer | 6 | 3 | 3 |
| Back-up beheer | 4 | 4 | - |
| Fysieke beveiliging | - | - | - |
| **Totaal aantal** | **16** | **13** | **3** |
| *** De Landsloterij dient nog enkele richtlijnen uit te werken in concrete procedures.** | | | |

[7] Rapport van bevindingen met kenmerk 13/1344C/JH d.d. 12 december 2013
[8] Rapport van bevindingen met kenmerk 15/1072C/SF d.d. 2 december 2015
[9] Rapport van bevindingen met kenmerk 18/0280C/JH d.d. 5 april 2018

In dit hoofdstuk wordt ingegaan op de bevindingen met betrekking tot de geconstateerde tekortkomingen en de huidige status van de beheersingsmaatregelen nadat de aanbevelingen zijn doorgevoerd. De huidige status is cursief vermeld aan het einde van iedere paragraaf.

De tekortkomingen zijn als volgt ingedeeld:

1. ITGC:
    a. incidentenbeheer;
    b. wijzigingenbeheer;
    c. logische toegangsbeheer;
    d. back-upbeheer;
    e. fysieke beveiliging.
2. AC

De resultaten met betrekking tot de tekortkomingen zijn in bijlage 1 per criterium overzichtelijk weergegeven, terwijl de aanbevelingen van de controlerend accountant[10] en de status na implementatie van de aanbevelingen in bijlage 2 zijn weergegeven.

## 3.1 General IT controls

### 3.1.1. Incidenten beheer

Incidenten doen zich voor als een afwijking van het normaal functioneren van apparatuur, systeemsoftware en toepassingen is geconstateerd. De afwijking kan dusdanig zijn dat de betrouwbaarheid van de informatie in het lotenregistratiesysteem niet gegarandeerd kan worden. De procedures voor incidentenbeheer zorgen voor het afhandelen van verstoringen en het tijdig herstellen van geconstateerde afwijkingen in de informatievoorziening.

De Landsloterij beschikte gedurende de onderzoeksperiode niet over een formele incidentenprocedure waarin eenduidig was vastgelegd hoe incidenten moesten worden gemeld. Ook was niet beschreven dat gemelde incidenten centraal moesten worden vastgelegd en dat geanalyseerd moest worden wat de impact van het incident is op de bedrijfsvoering. De richtlijnen voor de bewaking van de doorlooptijden van de oplossingen

[10] gedateerd 5 april 2018

en de wijze van afhandeling van de incidenten waren ook niet beschreven. Daarnaast werd achteraf ook niet geëvalueerd of het incident adequaat is opgelost.

Er bestond slechts een informele werkafspraak met de beheerder van het lotenregistratiesysteem voor slechts één type incident. Uit de rapporten over de onderzoeksperiode blijkt dat deze informele werkafspraak niet altijd werd gevolgd aangezien de incidenten niet altijd formeel werden gemeld.

***Huidige status***

*Nadat de aanbevelingen zijn doorgevoerd blijkt dat de gebruikers de mogelijkheid hebben om incidenten te registreren. Daarnaast heeft de Landsloterij de richtlijnen voor het afhandelen en periodiek analyseren van incidenten beschreven, vastgesteld en intern gecommuniceerd met het personeel.*

### 3.1.2. Wijzigingen beheer

Het beheren van wijzigingen is het proces van evalueren, plannen en coördineren van de implementatie van wijzigingen in hardware of software. Goed wijzigingsbeheer waarborgt de ongestoorde werking van het lotenregistratiesysteem. Gedurende de onderzochte periode heeft de Landsloterij onvoldoende maatregelen getroffen om te zorgen dat wijzigingen die betrekking hebben op het lotenregistratiesysteem, beheerst werden doorgevoerd. Wijzigingen kunnen in de productieomgeving[11] worden genomen alleen als deze wijzigingen door de directie geaccordeerd zijn nadat deze succesvol in een aparte omgeving zijn getest. De Landsloterij had geen formeel wijzigingsbeleid geformuleerd voor wijzigingen aan het lotenregistratiesysteem. Hierdoor ontbraken richtlijnen voor het doorvoeren van de wijzigingen en zijn de verschillende verantwoordelijkheden van de betrokkenen niet bekend gemaakt binnen de organisatie. Uit de onderzoeken gedaan in de controleperiode bleek dat, ondanks dat de beheerder van het lotenregistratiesysteem over een ontwikkelomgeving beschikte, er geen actuele registratie was van de wijzigingen doorgevoerd in het geautomatiseerd lotenregistratiesysteem. Er waren enkel e-mailberichten beschikbaar over deze wijzigingen. Ook bleek dat er geen testdossiers waren waaruit kon blijken:

- wat de impact van de wijzigingen was op de bestaande functionaliteit van het

[11] De productieomgeving is de omgeving waarin de nieuwe softwareproducten functioneel en actief moeten zijn.

geautomatiseerd lotenregistratiesysteem;

- op welke omgeving de tests van de wijzigingen zijn uitgevoerd;
- of de wijzigingen positief zijn getest voor de implementatie in productie;
- hoe en wie van de Landsloterij akkoord heeft gegeven voor het doorvoeren van de wijzigingen in de productieomgeving.

Hierdoor blijkt dat het proces dat werd toegepast voor het doorvoeren van deze wijzigingen, niet toereikend was ingericht.

***Huidige status***

*In de maand mei 2020 heeft de Landsloterij een wijziging in het lotenregistratiesysteem doorgevoerd. Wij constateren dat deze wijziging procedureel goed is verlopen aangezien uit de ontvangen documentatie blijkt dat:*

- *een verzoek is gedaan (door de directeur van de Landsloterij) om deze wijziging door de voeren;*
- *de impact van de wijziging voor het doorvoeren van de wijziging geanalyseerd is;*
- *de wijziging getest is in een testomgeving, de testresultaten zijn vastgelegd en ondertekend voor akkoord door de daartoe bevoegde.*

### 3.1.3. Logische toegangsbeheer

Logische toegangsbeveiliging heeft betrekking op alle organisatorische en software matige maatregelen die erop gericht zijn de toegang tot het lotenregistratiesysteem te beschermen tegen benadering door ongeautoriseerde personen. Hieronder vallen:

- Het vastleggen van de organisatorische functiescheiding binnen het systeem via autorisatiematrix/competentietabel.
- Het beheren van inlognaam en wachtwoord van gebruikers.
- Beveiliging van de toegang tot de database.

**Autorisatiematrix/competentietabel**

Geconstateerd is dat gedurende de onderzoeksperiode de Landsloterij geen autorisatiematrix had. Daarnaast werd gebruik gemaakt van bepaalde accounts die risico's met zich meebrachten.

De risico's betreffen het volgende:

- De uitgegeven rechten waren mogelijkerwijs niet beperkt tot alleen die rechten noodzakelijk voor het uitoefenen van een functie.

- De vereiste functiescheidingen konden doorbroken worden met de 'administrator' rechten.
- De acties uitgevoerd in het lotenregistratiesysteem waren hierdoor niet traceerbaar naar personen.

**Inlognaam en wachtwoord**

De gebruikers maakten gebruik van een combinatie van inlognaam en wachtwoord om toegang te krijgen tot het lotenregistratiesysteem. Hoewel de Landsloterij interne afspraken had over hoe de inlognamen aangemaakt moesten worden, bleek dat deze afspraken niet consequent werden toegepast. Bovendien waren er ook geen eisen gesteld aan de complexiteit van het wachtwoord.

Ook is gebleken dat accounts die niet meer in gebruik waren niet (tijdig) geblokkeerd werden. Door het ontbreken van geformaliseerde werkwijzen voor het aanmaken, wijzigen, beëindigen en periodiek controleren van de uitgegeven bevoegdheden, heeft de Landsloterij het proces voor het beperken van ongeautoriseerde toegang tot het lotenregistratiesysteem niet toereikend ingericht.

**Beveiliging toegang tot de database**

Door het ontbreken van de nodige bewijzen kon de Rekenkamer niet vaststellen of de database van het lotenregistratiesysteem adequaat was beveiligd gedurende 2010 tot en met 2017. Aangezien de server van het lotenregistratiesysteem en de bijbehorende database door een extern bedrijf worden gehost was het noch voor de controlerend accountant noch voor de Rekenkamer mogelijk om de beveiliging van de database van het systeem te toetsen.

***Huidige status***

*Thans zijn de volgende beheersingsmaatregelen van kracht:*

- *Alle gebruikers moeten middels een persoonlijk account en een wachtwoord inloggen. De wachtwoorden voldoen aan de voorgeschreven lengte, samenstelling en geldigheidsduur.*
- *Er gelden interne richtlijnen voor het aanmaken van gebruikersnamen en de gebruikersnamen dienen hieraan te voldoen.*
- *De gebruikers beschikken slechts over de autorisaties die zij nodig hebben voor het uitvoeren van de aan hen toebedeelde werkzaamheden.*
- *De vereiste functionele functiescheidingen zijn in het lotenregistratiesysteem ingebouwd.*

*In geval een gebruiker conflicterende taken moet uitvoeren, wordt gebruik gemaakt van separate accounts.*

### 3.1.4. Back-up beheer

Wanneer organisaties afhankelijk zijn van geautomatiseerde systemen voor hun bedrijfsprocessen kan discontinuïteit van het geautomatiseerd systeem (enorme) gevolgen hebben voor de organisatie. Hierdoor is het van belang om maatregelen te treffen om discontinuïteit van de geautomatiseerde systemen te voorkomen, snel op te heffen of te compenseren.

De Landsloterij beschikte niet over een formele back-up en herstelprocedure waarin eenduidig was vastgelegd welke back-ups gemaakt moesten worden en met welke frequentie en regelmaat de back-ups getest moesten worden op herstel. In de praktijk werden er wel back-ups gemaakt van het lotenregistratiesysteem. Uit de rapporten van de onderzoeken die uitgevoerd waren over de onderzoeksperiode, bleek dat geprogrammeerde back-up schema's en logbestanden van de back-ups aanwezig waren. Daarnaast bleek een limiet te zijn ingesteld om de historie van de back-up logs te bewaren. Door het ontbreken van procedures kan niet worden getoetst of deze back-ups aan de richtlijnen voldoen.

De server van het lotenregistratiesysteem staat fysiek bij een ander bedrijf waar de back-ups ook gemaakt worden. Volgens de Landsloterij worden de back-ups voor een korte tijd intern bij de Landsloterij opgeslagen. Een bewijs van de afname en het opslaan van de back-ups hebben wij echter niet ontvangen. Er is verder niet vastgelegd hoe de back-up procedure moest verlopen.

***Huidige status***

*Op basis van de ontvangen documenten heeft de Rekenkamer vastgesteld dat de Landsloterij periodiek succesvolle back-ups van het geautomatiseerde lotenregistratiesysteem heeft gemaakt en bewaard conform de voorgeschreven richtlijnen. Ook de richtlijnen voor het succesvol terugzetten van een werkende kopie van het geautomatiseerde lotenregistratiesysteem in geval van een calamiteit zijn beschreven.*

### 3.1.5. Fysieke beveiliging

Fysieke beveiliging omvat alle maatregelen gericht op het selectief verschaffen van

toegang tot ruimten met apparatuur van de organisatie aan daartoe bevoegde personen. De server van het lotenregistratiesysteem staat in een datacenter op een externe locatie. Aangezien de Landsloterij gebruik maakt van een datacenter voor het beheren van een deel van haar infrastructuur, moeten afspraken over de beoordeling van de dienstverlening van dit bedrijf contractueel zijn vastgelegd. Zo kan de Landsloterij de risico's met betrekking tot fysieke beveiliging van de data in het lotenregistratiesysteem mitigeren. Gebleken is dat de Landsloterij geen overeenkomst met dit datacenter heeft afgesloten waarin afspraken zijn vastgelegd over de verwachte dienstverlening inclusief de verantwoordelijkheden van beide partijen. Door het ontbreken van deze afspraken, beschikte de Landsloterij niet over een verklaring van dit bedrijf waarin zij aangeven voldoende maatregelen te hebben genomen om de toegang tot de servers te beheersen. Ook was er geen afspraak die het voor de Landsloterij mogelijk maakte om zelf de processen voor het beheren van de toegang tot de servers te beoordelen of te laten beoordelen door daartoe deskundigen.

***Huidige status***

*De Rekenkamer heeft geconstateerd dat de Landsloterij nog geen certificaat heeft ontvangen van het datacenter dat de server van het lotenregistratiesysteem host[12]. Hierdoor kan de Rekenkamer geen zekerheid verkrijgen of:*

- *de toegangsdeuren tot de serverruimte beveiligd zijn tegen ongeautoriseerde toegang;*
- *alleen daartoe bevoegde medewerkers en bezoekers toegang hebben tot de serverruimte;*
- *een logboek wordt bijgehouden van alle toegelaten bezoekers met datum en tijdstip van aankomst en vertrek, inclusief de reden van het bezoek;*

*Het risico op ongeoorloofde toegang tot de servers met eventuele discontinuïteit tot gevolg is door de directie op basis van de locatie waar de server staat als laag ingeschat[13]. De Rekenkamer is van mening dat voor het kunnen garanderen van de continuïteit van het lotenregistratiesysteem het raadzaam is om de vermelde afspraken contractueel vast te leggen.*

[12] Het hosten van software of applicaties op een webserver, waardoor men overal toegang heeft tot de applicaties, data of documenten.
[13] Reactie gegeven door de directie in rapport van bevindingen met kenmerk 18/0280C/JH d.d. 5 april 2018.

## 3.2 Application controls

De AC zijn belangrijk om te garanderen dat alle in het systeem ingevoerde gegevens juist zijn en volledig worden verwerkt en gepresenteerd. De AC zorgen ervoor dat:

- de invoergegevens volledig, nauwkeurig en geldig zijn;
- de interne verwerking de gewenste taken uitvoert en de verwachte resultaten oplevert;
- de outputrapporten beschermd zijn tegen onterechte openbaarmaking (verspreiding informatie aan de onjuiste ontvanger).

Tot de AC behoren:

- invoerautorisatie, batchcontroles, online toegangscontrole en werkstation identificatie;
- de geprogrammeerde instructies, dus harde coding in de applicatieprogrammatuur en verwerkingscontroles;
- de geprogrammeerde instructies, de beslissingen en/of berekeningen die door het systeem gebruikt moeten worden;
- de applicatie controles binnen het systeem en de tolerantie voor gegevensverlies.

De AC zijn effectief indien de vereiste beheersingsmaatregelen in de applicatieprogrammatuur zijn vastgelegd zodat de controle consequent wordt uitgevoerd.

Voor het vaststellen of de beheersmaatregelen binnen het lotenregistratiesysteem effectief functioneerden, zijn de ingebouwde controles op basis van de geïdentificeerde risico's getoetst aan gemiddeld zestien geïdentificeerde normen. Deze normen hebben betrekking op de te houden loterij en zijn afgeleid van de relevante bepalingen uit de Landsloterijverordening[14]. Gekeken is of de aspecten voorgeschreven in de wet door het systeem worden gecontroleerd (in het systeem zijn controles hierop geprogrammeerd).
De resultaten van de toetsing van de AC zijn per onderzoeksperiode, per type controle samengevat in tabel 3 en in bijlage 3 zijn de resultaten per getoetste maatregel gepresenteerd.

[14] artikelen 20.1, 20.2, 21, 22, 27, 28, 29.3, 32.1, 32.2 en 32.4.

*Tabel 3: Resultaat toetsing 'application controls'*

| Periode | Totaal getoetste beheersings-maatregelen | Aantal beheersings-maatregelen dat voldoet aan de norm[15] | Aantal beheersings-maatregelen dat niet aan de norm voldoet[16] | Totaal niet getoetste beheersings-maatregelen* |
|---|---|---|---|---|
| **2010-2013** | **14** | **12** | **2** | **8** |
| Invoercontrole | 5 | 5 | - | 5 |
| Audit trail | 7 | 6 | 1 | 3 |
| Logging | 2 | 1 | 1 | - |
| | | | | |
| **2014-2015** | **21** | **18** | **3** | **1** |
| Invoercontrole | 9 | 9 | - | 1 |
| Audit trail | 10 | 8 | 2 | - |
| Logging | 2 | 1 | 1 | - |
| | | | | |
| **2015-2017** | **14** | **13** | **1** | **8** |
| Invoercontrole | 6 | 6 | - | 4 |
| Audit trail | 7 | 6 | 1 | 3 |
| Logging | 1 | 1 | - | 1 |

* Deze beheersingsmaatregelen zijn op basis van hun risico inschatting niet getoetst door de controlerend accountant

Uit de resultaten blijkt dat de maatregelen over het algemeen aan de normen voldeden. Slechts de volgende drie maatregelen voldeden niet aan de normen.

- Audit trail

  De rollen binnen het lotenregistratiesysteem waren niet in lijn met de betreffende gebruikersfunctie binnen de Landsloterij want de richtlijnen voor de toekenning van gebruikersrechten ontbraken. Hierdoor was er geen zekerheid dat de toegekende rechten overeenkwamen met de werkzaamheden van de medewerkers. Deze maatregel voldeed in geen van de onderzoeksperioden aan de norm.

  Het juist functioneren van de maatregel om loten dubbel te kunnen uitprinten, in geval van een systeemstoring, kon gedurende de onderzoekperiode 2014-2015 niet worden vastgesteld. Gedurende 2015-2017 voldeed deze maatregel wel aan de gestelde norm.

[15] Maatregel voldoet aan de gestelde norm voor beheersing van het lotenregistratiesysteem.
[16] Maatregel voldoet niet aan de gestelde norm voor beheersing van het lotenregistratiesysteem.

- Logging

  De gebruikers- en systeemactiviteiten op gebruikersaccounts werden in 2010-2013 en 2014-2015 niet gelogd. Dit aangezien er geen functionaliteit in het lotenregistratiesysteem was ingebouwd om de wijzigingen op de gebruikersaccounts bij te houden in een logbestand. Deze maatregel werd gedurende 2015-2017 niet getoetst waardoor geen zekerheid is over die periode.

***Huidige status***

*Op het moment van de controle in het jaar 2020 blijken de volgende AC ingebouwd te zijn:*

- *Het lotenregistratiesysteem zorgt ervoor dat de input van de trekkingsgegevens volledig, juist en geldig geschiedt.*
- *Een nieuwe trekking kan niet worden aangemaakt voordat de voorafgaande trekking is afgesloten. De printopdrachten kunnen alleen via de server gestuurd worden naar geregistreerde printers.*
- *De gebruikers en systeemactiviteiten worden op gebruikersaccounts gelogd en de logfiles worden adequaat beveiligd.*
- *Het lotenregistratiesysteem laat het dubbel uitprinten van loten niet toe. Ook niet in geval dat een systeemstoring is ontstaan.*

***Door de geconstateerde tekortkomingen in de ITGC heeft de Landsloterij een verhoogd risico gelopen dat indien zich een calamiteit had voorgedaan, de informatie opgeslagen in het lotensysteem niet beschikbaar zou zijn geweest om de situatie te herstellen. Dit mede gezien de procedures voor het maken en herstellen van back ups ontbraken.***

***Ondanks dat er geconcludeerd kan worden dat de AC in het lotensysteem gedurende 2010-2017 over het algemeen toereikend waren kon de ongestoorde werking van de AC niet worden gewaarborgd. Immers, de ongestoorde werking van de AC kon alleen gewaarborgd zijn als de randvoorwaardelijke beheersingsmaatregelen (ITGC) ook toereikend waren.***

***Hierdoor was er een onzekerheid dat de gegevens juist, volledig en tijdig in het lotensysteem zijn verwerkt.***

# 4. Bevindingen financieel systeem

Met betrekking tot het financieel systeem van de Landsloterij is in de onderzoeksperiode geen onderzoek uitgevoerd naar de ITGC rond en de AC binnen het systeem. Gezien de verstreken periode en het ontbreken van de relevante vastleggingen is het niet meer mogelijk om de kwaliteit van deze beheersingsmaatregelen over eerder vermelde periode alsnog vast te stellen. Aangezien de informatie uit dit systeem gebruikt wordt bij het opstellen van de jaarrekeningen, heeft de Rekenkamer besloten om de kwaliteit van deze beheersingsmaatregelen op het huidig moment (in maart 2020) te toetsen.

De toetsing is beperkt tot het beoordelen van de maatregelen betreffende de aspecten die een grote negatieve impact kunnen hebben op de betrouwbaarheid van de gegevensverwerking indien zij niet effectief functioneren. Deze aspecten omvatten het beheer van de toegang tot het systeem (de ITGC) en het beoordelen van de AC. In bijlage 1 is een overzicht van de resultaten per criterium opgenomen. In de volgende twee paragrafen worden de tekortkomingen vermeld.

## 4.1 Logische toegangsbeheer

De Rekenkamer heeft aan de hand van de verkregen informatie uit het financieel systeem vastgesteld dat de nodige maatregelen zijn ingebouwd om te garanderen dat alleen bevoegde personen toegang hebben tot deze applicatie. Op basis van deze maatregelen hebben personen toegang tot alleen die onderdelen/modules van de applicatie die voor hun werkzaamheden noodzakelijk zijn. Ook is gebleken dat de nodige functiescheidingen in de applicatie zijn doorgevoerd.
Ondanks dat er toegangsrechten zijn uitgegeven blijkt dat deze rechten niet jaarlijks worden geëvalueerd. Volgens de directeur is er weinig verloop in de organisatie en treden geen wisselingen onder het personeel op voor onder andere de afdelingen Financiële Administratie en Interne Controle. Hierdoor wordt geen noodzaak gezien voor het jaarlijks evalueren van deze rechten. De evaluatie vindt volgens hem slechts naar behoefte plaats. Door de geringe personeelswijzigingen is er volgens hem ook weinig aanleiding voor aanpassing van de toegangen in het financieel systeem. Het risico dat ongepaste rechten ontstaan als gevolg van personeelswijzigingen is dan ook beperkt.

## 4.2 Ingebouwde invoercontroles

Ten aanzien van de ingebouwde invoercontroles constateert de Rekenkamer dat het financieel systeem als standaardapplicatie reeds voorzien is van diverse invoercontroles. Als gebruiker van deze standaard applicatie kan de Landsloterij zelf geen wijzigingen aan de controles in de applicatie doorvoeren. Alleen de leverancier kan de nodige wijzigingen aan de applicatie doorvoeren. Door deze standaard functionaliteit ingebouwd in de applicatie wordt het risico dat de betrouwbaarheid van de gegevensverwerking in het financieel systeem negatief beïnvloed kan worden als laag ingeschat.

***De maatregelen rond het beheer van de toegang tot het financieel systeem en de ingebouwde controles zijn toereikend om de juiste werking van deze applicatie te waarborgen.***

# 5. Conclusie en aanbevelingen

## 5.1 Conclusie

De Rekenkamer concludeert op basis van dit onderzoek dat de ITGC rond en de AC binnen het lotenregistratiesysteem en het financieel systeem per 2020 in opzet toereikend zijn. De Landsloterij heeft passende maatregelen genomen om de tekortkomingen die in voorgaande jaren geconstateerd zijn weg te werken. Niet voor alle geïmplementeerde maatregelen kan de werking tijdens dit onderzoek worden getoetst. Bij de controle van de jaarrekening 2020 zal de Rekenkamer de werking van de ITGC en AC van deze twee applicaties controleren.

## 5.2 Aanbeveling

De Rekenkamer beveelt de Staten aan om de minister van Financiën te vragen erop toe te zien dat de Landsloterij:

a. uitvoering geeft aan het vastgestelde informatiebeveiligingsbeleid en de bijbehorende procedures, zodat de juiste werking van de beheersingsmaatregelen (de ITGC en de AC) rondom en in de geautomatiseerde systemen gewaarborgd worden. Met de juiste werking van deze maatregelen wordt de betrouwbaarheid van de informatie in de systemen gegarandeerd, zodat vertrouwen wordt behouden in de loterij;
b. de implementatie van alle aanbevelingen van de controlerende accountant afrondt door de nog uit te werken richtlijnen in concrete procedures te voltooien;
c. tweejaarlijks verantwoording aan hem aflegt over de kwaliteit van de beheersmaatregelen in de geautomatiseerde omgeving.

# 6. Ambtelijke en bestuurlijke reactie

## 6.1 Ambtelijke reactie

Het rapport is in het kader van hoor en wederhoor op 7 oktober 2020 aangeboden aan de directeur van de Landsloterij voor zijn reactie. Op 23 oktober hebben wij een reactie van de directeur ontvangen. In zijn reactie geeft hij aan de volgende acties te zullen ondernemen:

- In november 2020 zal gestart worden met het testen van de back-ups van het lotenregistratiesysteem op herstel ('recovery testing').
- De Landsloterij is van plan om in het jaar 2021 een digitale toegangscontrole tot de serverruimte te implementeren, waarmee de risicogebieden met betrekking tot fysieke beveiliging kunnen worden aangepakt.
- De procedures voor periodieke evaluatie van gebruikersrechten voor het einde van dit jaar zullen worden opgesteld.
- De richtlijnen voor de te nemen maatregelen in geval van geconstateerde afwijkingen zullen tegen einde van dit jaar worden afgehandeld.

De directeur heeft verder aangegeven dat de autorisatiematrix voor de financiële applicatie gedurende het onderzoek is opgeleverd. Wij hebben een uitdraai uit het systeem ontvangen met de bevoegdheden toegekend aan bepaalde gebruikers. Een formele vastlegging van de bevoegdheden verbonden aan de functies ontbreekt. Hierdoor konden wij niet vaststellen of de bevoegdheden zoals opgenomen in het systeem inderdaad geaccordeerd zijn door de daartoe bevoegde en aansluiten bij de juiste functies.

## 6.2 Bestuurlijke reactie

In het kader van bestuurlijk hoor en wederhoor is het conceptrapport inclusief conclusies, aanbevelingen en de reactie van de directeur op 3 november 2020 aangeboden aan de minister van Financiën en de RvTA. Wij hebben echter tot op het moment van aanbieding van dit rapport aan de Staten geen reactie ontvangen van de minister.

Op 11 november heeft de RvTA uitstel verzocht. Na het verkregen uitstel heeft de RvTA

op 25 november jl. een reactie gegeven. In haar reactie is de RvTA ingegaan op twee formuleringen zijnde:

> "1. De Landsloterij gedurende de periode 2010 tot en met 2017 niet over een informatiebeveiligingsbeleid beschikte en
> 2. [...J daarnaast zijn er diverse tekortkomingen geconstateerd die een effectieve werking van het lotenregistratiesysteem hebben belemmerd, waardoor geen zekerheid bestond over de betrouwbaarheid van de informatie uit het lotenregistratiesysteem in de onderzoeksperiode."

Volgens de RvTA doen deze formuleringen het overkomen alsof er helemaal geen beveiliging van de gegevens plaats heeft gevonden in de hiervoor genoemde periode. Zij zijn van mening dat de Rekenkamer hiermee voorbij is gegaan aan de door de Landsloterij genomen beheersmaatregelen die destijds weldegelijk van toepassing zijn geweest. Het weglaten van deze relevante informatie c.q. het niet nuanceren van de bevindingen terzake schetst volgens hen onnodig een onvolledig en wellicht onjuist beeld van de informatiebeveiligingsmaatregelen in de periode tussen 2010 en 2017.

De Rekenkamer is van mening dat de geconstateerde tekortkomingen feiten zijn en van invloed konden zijn op de betrouwbaarheid van de gegevens voortvloeiende uit deze systemen. In de tekst is hierdoor het woord kon toegevoegd en aangegeven dat het gaat om een vastgesteld informatiebeveiliginsbeleid. Daarnaast heeft de Rekenkamer erbij vermeld dat de trekkingen geen onderdeel van dit onderzoek vormen. Aangezien de trekkingen geen onderdeel van het onderzoek zijn kan op basis van dit rapport geen twijfel ontstaan over de trekkingen gehouden in de onderzoeksperiode.

# 7. Nawoord Rekenkamer

De Rekenkamer constateert op basis van het uitgevoerde onderzoek en de ontvangen reacties dat over de periode 2010 tot en met 2017 niet alle beheersingsmaatregelen rondom de geautomatiseerde systemen altijd voldoende waren om de betrouwbaarheid van de informatie te garanderen. Als gevolg hiervan zijn er aanvullende werkzaamheden uitgevoerd door de controlerende accountant om de getrouwheid van de jaarrekeningen vast te stellen.

In het jaar 2019 heeft de Landsloterij diverse acties ondernomen om de beheersingsmaatregelen te versterken en is hier nog mee bezig. De Rekenkamer juicht toe dat de Landsloterij concreet actie onderneemt om de betrouwbaarheid van hun informatievoorziening te blijven verhogen.

# Bijlagen

## Bijlage 1 Resultaat beoordeling van de beheersmaatregelen van de geautomatiseerde systemen

Maatregel voldoet aan de norm
Maatregel voldoet niet aan de norm
Maatregel is niet van toepassing
Niet gecontroleerd

| Object | Criteria | Resultaat toetsing | | |
|---|---|---|---|---|
| | | Lotenregistratie systeem in 2010-2017 | Lotenregistratie systeem in 2020 | Financieel systeem in 2020 |
| **ITGC** | | | | |
| Logische toegangsbeheer | De gebruikers beschikken alleen over autorisaties die zij nodig hebben voor het uitvoeren van de werkzaamheden conform hun functieomschrijving. | | | |
| | De functionele functiescheidingen zijn ook technisch doorgevoerd. | | | |
| | Er zijn aanvullende maatregelen ingevoerd in geval geen functiescheiding mogelijk is. | | | |
| | De gebruikers maken gebruik van persoonlijke accounts om in te loggen. | | | |
| | De toegangsrechten worden jaarlijks geëvalueerd. | | | |
| | De toegangsrechten worden alleen na goedkeuring van het management aangemaakt, gewijzigd of verwijderd. | | | |
| Wijzigingen beheer | Wijzigingen aan de functionaliteit van de applicatie worden in een ontwikkelomgeving geprogrammeerd. | | | |
| | Wijzigingen aan de functionaliteit van de applicatie worden positief getest in een testomgeving voordat ze in productie worden genomen. | | | |
| | Alleen door de directie geaccordeerde wijzigingen worden in productie doorgevoerd. | | | |
| | De implementatie naar productie gebeurt alleen door bevoegde personen die over de nodige rechten beschikken. | | | |
| Back-up beheer | De Landsloterij heeft een schema opgesteld voor het maken (minimaal eens per dag is raadzaam) en herstellen van de back-ups van het lotenregistratiesysteem (minimaal tweemaal per jaar is raadzaam). | | | |
| | Het lotenregistratiesysteem wordt volgens het opgestelde schema geback-upt. | | | |
| | De gemaakte back-ups worden geregistreerd en gecontroleerd. | | | |

| Object | Criteria | Resultaat toetsing | | |
|---|---|---|---|---|
| | | Lotenregistratie systeem in 2010-2017 | Lotenregistratie systeem in 2020 | Financieel systeem in 2020 |
| | De back-ups van het lotenregistratiesysteem worden tweemaal per jaar getest op herstel. | | | |
| | De Landsloterij bewaart kopieën van back-ups in een ander gebouw dan waar de server staat. | | | |
| Incidenten beheer | De incidenten gerelateerd aan het lotenregistratiesysteem worden geregistreerd. | | | |
| | De voortgang van de openstaande incidenten wordt bewaakt. | | | |
| | Incidenten worden in overleg met de melder afgesloten (issue is opgelost). | | | |
| Fysieke beveiliging | Alleen de gebruikers die uit hoofde van hun functie toegang nodig hebben tot de serverruimte hebben deze toegang. | | | |
| | De toegangsrechten tot de serverruimte worden twee maal per jaar geëvalueerd. | | | |
| | De toegangsrechten tot de serverruimte worden alleen na goedkeuring van het management gegeven. | | | |
| | Tijdelijk uitgegeven toegangsrechten tot de serverruimte wordt tijdig ingetrokken. | | | |
| **AC** | | | | |
| Application controls lotensysteem | Het lotenregistratiesysteem zorgt dat de invoer van trekkingsgegevens volledig, juist en geldig is. | | | |
| | Printopdrachten worden alleen via de server gestuurd naar geregistreerde printers. | | | |
| | Gebruikers en systeemactiviteiten op gebruikersaccounts worden gelogd en de logfiles zijn adequaat beveiligd. | | | |
| | Het lotenregistratiesysteem vermijdt het dubbel uitprinten van loten in geval een systeemstoring is ontstaan. | | | |
| | Nieuwe trekking kan niet worden aangemaakt voordat de voorafgaande trekking is afgesloten. | | | |
| Application controls financieel systeem | Het financieel systeem controleert of een ingevoerd factuurnummer reeds bestaat. | | | |
| | Het financieel systeem controleert of een ingevoerde datum van een factuur reeds bestaat, niet in de toekomst ligt en ook niet in het (verre) verleden. | | | |
| | Het financieel systeem controleert of een ingevoerd grootboekrekeningnummer reeds is aangemaakt. | | | |
| | Het financieel systeem controleert of een ingevoerd crediteurnummer reeds is aangemaakt. | | | |

| Object | Criteria | Resultaat toetsing | | |
|---|---|---|---|---|
| | | Lotenregistratie systeem in 2010-2017 | Lotenregistratie systeem in 2020 | Financieel systeem in 2020 |
| | Het financieel systeem controleert of een ingevoerde combinatie van crediteur en grootboek-rekening juist is. | | | |

## Bijlage 2 Status van de aanbevelingen op het lotenregistratiesysteem

In deze tabel wordt aangegeven in hoeverre de aanbevelingen die in het verleden door de controlerend accountant zijn gegeven, zijn doorgevoerd.

| Samenvatting van de aanbevelingen voor het lotensysteem uit het rapport d.d. 5 april 2018 van de controlerende accountant | Acties ondernomen door de Landsloterij | Beoordeling opvolging aanbeveling |
|---|---|---|
| **1. Logische toegangsbeveiliging - Informatiebeveiligingsbeleid en -plan**<br>Het opstellen van een informatiebeveiligingsbeleid waarin de richtlijnen en normen worden beschreven voor de implementatie van informatiebeveiliging binnen de Landsloterij, waaronder ook de maatregelen en procedures voor het beheren van de geautomatiseerde informatiesystemen (ITGC). Dit beleid dient door het management van de Landsloterij goedgekeurd te worden. | De Landsloterij heeft een informatiebeveiligingsbeleid opgesteld waarin de te implementeren richtlijnen en normen voor de beveiliging van de informatiesystemen zijn beschreven. Dit beleid bevat de procedures voor onder meer wijzigingsbeheer, back-up beheer, incidentenbeheer, wachtwoordbeheer, internetgebruik en een logisch toegangsbeheer. De directeur heeft het informatiebeleid op 10 februari 2020 geaccordeerd. Ook heeft de Landsloterij een externe consultant aangetrokken die als interim CTO ervoor moet zorgen dat de betreffende procedures werkelijk worden uitgevoerd door het personeel van de Landsloterij. | **Aanbeveling is opgevolgd en is in opzet toereikend.**<br>De werking hiervan moet nog worden getoetst. |
| **2. Logische toegangsbeveiliging - Autorisatiematrix**<br>Het opstellen van een autorisatiematrix waarin alle kritische applicaties zijn opgenomen. Deze matrix dient door de Landsloterij gebruikt te worden om gebruikers de juiste en rechtmatige autorisaties toe te kennen in lijn met hun functie. | In het informatiebeveiligingsbeleid is een onderdeel opgenomen dat voorschrijft dat er een autorisatiematrix moet komen om de toegang tot de verschillende informatiebronnen te beheren. | **De Landsloterij heeft deze aanbeveling deels opgevolgd.**<br><br>**Toelichting**<br>Er is een autorisatiematrix voor het lotenregistratiesysteem, maar voor de financiële applicatie is er nog geen matrix opgesteld. De Landsloterij heeft aangegeven hier nog aan te werken. |

| Samenvatting van de aanbevelingen voor het lotensysteem uit het rapport d.d. 5 april 2018 van de controlerende accountant | Acties ondernomen door de Landsloterij | Beoordeling opvolging aanbeveling |
|---|---|---|
| **3. Logische toegangsbeveiliging – Generieke gebruikersaccounts**<br>Het minimaliseren van het gebruik van generieke accounts op netwerk- en applicatieniveau zodat traceerbaarheid en aansprakelijkheid van gebruikersactiviteiten gewaarborgd kan worden. | In het informatiebeveiligingsbeleid is opgenomen dat alle gebruikers aparte accounts moeten hebben voor de toegang tot informatiebronnen. Ook is vermeld dat de beheerders van de systemen twee aparte accounts moeten hebben: één voor het uitvoeren van beheerderstaken en een als gebruiker.<br>Ook het delen van een wachtwoord wordt verboden. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>In een later stadium dient de Rekenkamer te toetsen of de ingevoerde richtlijnen effectief door de Landsloterij worden uitgevoerd. |
| **4. Logische toegangsbeveiliging – Gebruikersaccounts met speciale rechten**<br>Het intrekken van beheerdersrechten die aan niet-beheerders zijn toegekend. | De toegekende beheerdersrechten die aan niet-beheerders zijn toegekend zijn per 24 november 2019 ingetrokken. Sindsdien hebben drie beheerders van het lotenregistratiesysteem de beheerdersrechten. | **De Landsloterij heeft deze aanbeveling opgevolgd.** |
| **5. Logische toegangsbeveiliging - Periodieke evaluatie van gebruikersrechten**<br>Het inrichten van een proces voor de periodieke evaluatie van toegekende gebruikersrechten op onder meer geldigheid, rechtmatigheid en overeenkomst met de autorisatiematrix. | De Landsloterij heeft de evaluatie van de toegekende gebruiksrechten in november 2019 uitgevoerd. | **De Landsloterij heeft deze aanbeveling deels opgevolgd.**<br><br>**Toelichting**<br>Er moet nog een procedure voor de periodieke evaluatie door de CTO worden vastgesteld. |
| **6. Logische toegangsbeveiliging – Monitoren van logbestanden**<br>Het uitvoeren van een risicoanalyse om vast te stellen van welke systemen logbestanden gemaakt moeten worden en het periodiek bewaken van deze logbestanden door een onafhankelijke functionaris. | Er is een werkwijze beschreven voor het monitoren van de logbestanden van het netwerk en de servers. Vanwege de omvang van de IT afdeling zal de CTO de logbestanden monitoren | **De Landsloterij heeft deze aanbeveling deels opgevolgd.**<br><br>**Toelichting**<br>Naast de werkwijze voor het monitoren van het netwerk en de servers moeten de richtlijnen voor de te nemen maatregelen in geval van geconstateerde afwijkingen en de periodiciteit waarvoor de bewaking moet plaatsvinden nog uitgewerkt worden. |

| Samenvatting van de aanbevelingen voor het lotensysteem uit het rapport d.d. 5 april 2018 van de controlerende accountant | Acties ondernomen door de Landsloterij | Beoordeling opvolging aanbeveling |
|---|---|---|
| **7. Wijzigingsbeheer - Analyse van wijzigingen**<br>Het analyseren van de impact van wijzigingen aan de IT-systemen van de Landsloterij om tijdig de mogelijke gevolgen van een wijziging op de (kritische) bedrijfsprocessen te bepalen en het beoordelen van de risico's verbonden aan de wijzigingen. | De Landsloterij heeft de volgende richtlijnen voor het beheren van wijzigingen geformuleerd in het informatiebeveiligingsbeleid:<br>- Alle wijzigingen moeten gepland, geëvalueerd, beoordeeld, geaccordeerd en gedocumenteerd worden.<br>- Alle wijzigingsverzoeken moeten vastgelegd en bijgehouden worden.<br>- Wijzigingen moeten gecategoriseerd en geprioriteerd worden.<br>- Wijzigingen moeten getest worden.<br>- Wijzigingen moeten door de 'business owners' geaccordeerd worden.<br>- Wijzigingen moeten een herstelplan hebben indien zij een grote impact kunnen hebben in geval de implementatie ervan mislukt. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **8. Back-up en herstel – Proces en procedures**<br>Het inrichten en formeel vastleggen van een (intern) back-up en recovery proces. | De Landsloterij heeft in het informatiebeveiligingsbeleid de richtlijnen voor back-up en recovery opgenomen. Conform de scope van dit beleid zijn de richtlijnen van toepassing op alle servers bij de Landsloterij. De richtlijnen betreffen:<br>- frequentie van de back-ups;<br>- bewaarperiode van back-ups;<br>- het bewaren van de back-ups op een andere locatie;<br>- het periodiek uitvoeren van volledige hersteltests van de back-ups.<br><br>De richtlijnen voor het maken en controleren van de back-ups en de procedures voor het herstellen van het lotenregistratiesysteem na een calamiteit zijn ook in maart 2020 vastgesteld. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **9. Back-up en herstel – Uitvoeren van back-up en hersteltests**<br>Het jaarlijks uitvoeren van back-up | De Landsloterij heeft de richtlijnen voor retentie en controle van back-ups beschreven. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.** |

| Samenvatting van de aanbevelingen voor het lotensysteem uit het rapport d.d. 5 april 2018 van de controlerende accountant | Acties ondernomen door de Landsloterij | Beoordeling opvolging aanbeveling |
|---|---|---|
| hersteltests. | | De werking van de maatregel moet nog worden getoetst. |
| **10. Back-up en herstel – Locatie voor het bewaren van back-ups**<br>Het bewaren van de back-ups op een veilige externe locatie. | In het informatiebeveiligingsbeleid is opgenomen dat de opslag van de back-ups op een externe locatie moet plaatsvinden. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **11. Back-up en herstel – Procedure continuïteitsmanagement**<br>Het vaststellen van de maximale tijd dat systemen niet beschikbaar mogen zijn en het uitvoeren van een volledige disaster recovery- en uitwijktest. | In het informatiebeveiligingsbeleid is opgenomen dat er jaarlijks een risicoanalyse uitgevoerd moet worden voor de systemen van de Landsloterij die gevoelige informatie bevatten. Verder zijn ook de procedures voor disaster recovery beschreven. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **12. Incident Management – Proces en procedure**<br>Het vaststellen van een gedocumenteerd proces voor Incident Management en het inrichten van een helpdesk conform 'Best Practices'. | De Landsloterij heeft richtlijnen vastgelegd voor het registreren, afhandelen en periodiek analyseren van incidenten. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **13. Incident Management – Bewaking van incidenten**<br>Het beoordelen van de doorlooptijd van de lopende incidenten tijdens periodieke overleggen. | De Landsloterij heeft de taak voor de bewaking van lopende incidenten aan de CTO toegekend. | **Aanbeveling is middels de toekenning van deze taak aan de CTO opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **14. Incident Management – Bewaking externe dienstverleners**<br>Het waarborgen dat externe dienstverleners op periodieke tijdstippen rapporteren over de geleverde diensten. | In het informatiebeveiligingsbeleid is opgenomen dat de Landsloterij een overeenkomst met de dienstverlenende partij moet afsluiten waarbij afspraken worden overeengekomen over het gewenste dienstverleningsniveau. Verder is ook opgenomen dat de Landsloterij vooraf audits moet plannen waarbij de Landsloterij de afgesproken serviceafspraken en -niveaus beoordeelt of laat beoordelen. | **Aanbeveling is middels hetgeen geregeld in het informatiebeveiligingsbeleid opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **15. Incident Management – Analyse van** | De Landsloterij heeft de taak voor het periodiek | **Aanbeveling is middels de toekenning van** |

| Samenvatting van de aanbevelingen voor het lotensysteem uit het rapport d.d. 5 april 2018 van de controlerende accountant | Acties ondernomen door de Landsloterij | Beoordeling opvolging aanbeveling |
|---|---|---|
| **incidenten**<br>Het periodiek analyseren van de afgesloten incidenten zodat terugkerende incidenten geïdentificeerd kunnen worden. | analyseren van de afgesloten incidenten aan de CTO toegekend. | **deze taak aan de CTO opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |
| **16. Incident Management – Rapportage en trendanalyse**<br>Het analyseren van de meest voorkomende incidenten om de mogelijke terugkeer van het incident te mitigeren/voorkomen. | De Landsloterij heeft de taak voor het analyseren van de meest voorkomende incidenten aan de CTO toegekend. | **Aanbeveling is middels de toekenning van deze taak aan de CTO opgevolgd en is in opzet toereikend.**<br>De werking van de maatregel moet nog worden getoetst. |

## Bijlage 3 Resultaat beoordeling AC van het lotenregistratiesysteem

Maatregel voldoet aan de gestelde norm

Maatregel voldoet niet aan de gestelde norm

Maatregel is niet getoetst

| Type controle | Citeria | Onderzoeksperiode | | |
|---|---|---|---|---|
| | | 2010-2013 | 2014-2015 | 2015-2017 |
| **Invoercontrole:** | Het systeem zorgt dat de input van trekkingsgegevens volledig, juist en geldig is. | | | |
| | Het systeem zorgt dat de input van de lotnummers volledig, juist en geldig is. | | | |
| | Bij een winnend lot wordt het biljet gescand en wordt ook het correcte winnende nummer gevalideerd. Het systeem controleert het winnende nummer op verkocht of niet verkocht zijn. | | | |
| | Een lot kan niet worden verzilverd na zes maanden van de trekkingsdatum. | | | |
| | Gestolen/verloren loten kunnen niet worden verzilverd. | | | |
| | Het systeem voorkomt het dubbel invoeren van trekkingsnummers als deze opnieuw opgeladen moeten worden. | | | |
| | De loten kunnen slechts één keer worden verkocht in het lotenregistratiesysteem. | | | |
| | Een nieuwe trekking kan niet worden aangemaakt zonder dat de voorafgaande trekking wordt afgesloten. | | | |
| | De loten kunnen niet na zes maanden worden verzilverd. | | | |
| | Het retourneren van loten is alleen mogelijk voor halve of hele loten. | | | |
| **Audit trail:** | De trekkingslijst wordt volledig geïmporteerd in het lotenregistratiesysteem. | | | |
| | De loten worden tegen de correcte prijs verzilverd. | | | |
| | De onverkochte loten worden geregistreerd. | | | |
| | De printopdrachten worden alleen door de server gestuurd naar geregistreerde printers. | | | |
| | Het trekkingssysteem genereert een trekkingslijst met de correcte prijzen. | | | |
| | De rollen binnen het lotenregistratiesysteem zijn in lijn met de betreffende gebruikersfunctie binnen het Landsloterij. | | | |
| | Het totale verkoopbedrag wordt automatisch en correct door het systeem bijgewerkt. | | | |
| | Het lotenregistratiesysteem vermijdt het dubbel uitprinten van loten in geval dat een systeemstoring is ontstaan. | | | |
| | Het lotenregistratiesysteem gebruikt 'hash totals' bij het verzilveren van trekking nummers. | | | |
| | Een trekking wordt in het lotenregistratiesysteem afgesloten en kan niet worden heropend. | | | |

| Type controle | Citeria | Onderzoeksperiode | | |
|---|---|---|---|---|
| | | 2010-2013 | 2014-2015 | 2015-2017 |
| **Logging:** | Elk lot heeft een uniek barcodenummer. | | | |
| | De gebruikers en systeemactiviteiten worden gelogd. De logfiles zijn adequaat beveiligd. | | | |