Kansspelautoriteit

IT-audit programma loterijen

Het IT-audit programma loterijen is bestemd voor de beoordeling van de betrouwbaarheid van de geautomatiseerde processen die onderdeel zijn van het kansspel van de vergunninghouder voor niet-incidentele artikel 3 loterijen, lotto, en staatsloterij. Aan de hand van de in dit document genoemde uitgangspunten en een 'framework' kunt u verantwoorden wat de scope is van het onderzoek en welke aspecten van geautomatiseerde processen van het kansspel in de beoordeling zijn betrokken.

In het IT-audit programma geeft u ook de benodigde aard en de diepgang van het onderzoek aan, en de daarbij behorende mate van zekerheid die op grond van het onderzoek kan worden verkregen.

Als u als vergunninghouder ISO 27001 gecertificeerd bent kunt u onderdelen van de rapportages gebruiken om de beoordeling van de betrouwbaarheid van de geautomatiseerde processen te verantwoorden.

Vaststelling scope en audit aspecten

De oordeelsvorming over de betrouwbaarheid (integriteit, vertrouwelijkheid en beschikbaarheid) van de door of namens de vergunninghouder gebruikte technologie behoort tot de expertise van de IT-auditor.

De IT-auditor moet op de hoogte zijn van de doelstellingen, regels en juridische grondslag voor het kansspel. Ook moet hij vaststellen met welke (technische) informatiesystemen en op welke wijze er invulling is gegeven aan de informatie-verwerking en de wijze waarop vaststelling van de uitslag van het kansspel plaatsvindt. De IT-auditor maakt een inventarisatie op van de relevante informatiesystemen, technische systemen en processystemen. De volgende geautomatiseerde processen zijn hierbij onderwerp van onderzoek:

- Vaststellen, samenstellen en gebruik van het prijzenschema.
- Vaststellen, samenstellen en gebruik van de lijst van deelnemers.
- Aanwijzing winnend(e) lot(en) en/of aanwijzing winnaar(s) (spelresultaat).
- Uitbetaling van prijzen aan de winnaar(s)..

Bij de toepassing en werking van geavanceerde telecommunicatie- en/of internet-technologie is het oordeel van de IT-auditor van groot belang. Het beveiligingsniveau van deze technologie is bepalend om het risico op onrechtmatige beïnvloeding van de uitslag en verwerking van informatie van het kansspel te verkleinen.

Wettelijke voorschrift t.a.v. geautomatiseerde processen bij prijsbepaling

Indien mechanische, elektrische of elektronische processen onderdeel uitmaken van de geautomatiseerde processen van prijsbepaling, en bij niet-incidentele artikel 3 loterijen de prijzen en premies gezamenlijk een grotere waarde hebben dan € 45.000, is *de methode* van prijsbepaling onderworpen aan een voorafgaande goedkeuring door een door de Minister van Justitie en Veiligheid aangewezen onafhankelijke deskundige of keuringsinstelling, als bedoeld in artikel 4, derde lid, van het Kansspelenbesluit.

De IT-auditor stelt vast dat er een goedkeuring van de methode van prijsbepaling is.

Reikwijdte van de IT-audit

De reikwijdte van de IT-audit betreft minimaal de 12 voorgaande maanden.

Eisen aan de IT-auditor

De Kansspelautoriteit vindt een IT-auditor in ieder geval geschikt als hij voldoet aan alle van de volgende eisen:

1. De IT-auditor is ingeschreven bij een beroepsorganisatie voor IT-auditors.
2. De IT- auditor is minimaal in het bezit van een RE-titel of CISA-titel.
3. De IT-auditor is werkzaam bij een onafhankelijke auditorganisatie.

Eisen auditrapportage

De IT-auditor moet in lijn met richtlijn ISAE 3000 type 1 rapporteren. Hoewel de rapportage geen formele ISAE 3000 rapportage hoeft te zijn, dient per onderdeel van beheersobject 1 en 2 en 3 te worden gerapporteerd. Indien er sprake is van een geldig ISO 27001 certificering, dient er een mapping gemaakt te worden naar beheersobject 1 , 2 en 3 met toevoeging van een Verklaring van Toepasselijkheid.
Per bevinding dient de IT Auditor toe te lichten op welke wijze invulling is gegeven aan een voorgeschreven beheersmaatregel.

Onderzoek IT-auditor

De IT-auditwerkzaamheden vinden plaats op basis van het IT-audit framework dat bestaat uit drie beheers objecten. U rapporteert op beheersobject 1 en 2 of beheers-object 1, 2 en 3. Waarop u rapporteert is gebaseerd op de omvang van de door de loterij jaarlijks beschikbaar gestelde prijzen:

Omvang	IT-audit framework van toepassing	Voorgeschreven
Minder dan 5 miljoen euro	Beheersobject 1 en 2	Beperkte mate van zekerheid
Meer dan 5 miljoen euro	Beheersobject 1, 2 en 3*	Redelijke mate van zekerheid

* Onderdeel 3 past u alleen toe als de ICT-omgeving en kritische systemen via een publiek toegankelijk netwerk (v.b. het internet) ''van buitenaf'' bereikbaar zijn.

Het volgende overzicht geeft met betrekking tot de aanpak en de te verwachten resultaten van de werkzaamheden van een IT-auditor een indruk:

Werkzaamheden IT-auditor:

- Analyse van het spelreglement en de op basis daarvan opgestelde procedurebeschrijving;
- Inventarisatie en analyse van de relevante technologie;
- Opstellen van een normenkader dat als werkplan en bijlage bij het auditrapport kan dienen;
- Uitvoering van eventuele systeemtesten;
- Vaststellen dat de IT-controls zijn ingericht, periodiek zijn gecontroleerd en issues zijn opgevolgd door de vergunninghouder;
- Vaststellen dat er goedkeuring als bedoeld in artikel 4, derde lid, van het Kansspelenbesluit, is afgegeven op de methode van prijsbepaling;
- Opstellen van een verklaring omtrent de uitvoering;
- Afronding van de eindrapportage, blijkens een oordeel over de mate van zekerheid en betrouwbaarheid van het proces.

Niveau van zekerheid:

- Redelijke mate van zekerheid - De uitdrukking “redelijke mate van zekerheid” verwijst naar de situatie waarin de auditor toereikende informatie heeft verkregen om te kunnen concluderen dat het object van onderzoek in alle van materieel belang zijnde opzichten voldoet aan bepaalde van toepassing zijnde criteria. Slechts in uitzonderingsgevallen kan de auditor “absolute” zekerheid verschaffen, bijvoorbeeld wanneer het beschikbare bewijsmateriaal volkomen sluitend en betrouwbaar is omdat het object van onderzoek en de te hanteren criteria volkomen eenduidig zijn en het toegepaste proces van aanvaarding en uitvoering van de opdracht allesomvattend kan zijn. Vanwege de beperkingen in het proces van aanvaarding en uitvoering van de opdracht is een “absolute” zekerheid echter in de regel niet haalbaar en kan maximaal een “redelijke” mate van zekerheid bereikt worden. De auditor richt het proces van aanvaarding en uitvoering van de opdracht in dit geval zodanig in dat het risico tot een laag niveau wordt gereduceerd dat de auditor ten onrechte zou concluderen dat het object van onderzoek in alle van materieel belang zijnde opzichten voldoet aan bepaalde van toepassing zijnde criteria.
- Beperkte mate van zekerheid - Bij een opdracht verschaft de auditor een (relatief) hoge maar niet absolute mate van zekerheid, dat de gecontroleerde informatie geen onjuistheden van materieel belang bevat.

De onderzoeksinspanning om een redelijke mate van zekerheid te verkrijgen is extra kostbaar ten opzichte van een onderzoek dat dient om een beperkte mate van zekerheid te verkrijgen. De vereiste mate van zekerheid is daarom afhankelijk van de omvang van de jaarlijkse beschikbare prijzen.

Bijlage: IT-audit Framework

IT-audit Framework		
Beheers object 1	*Beheers doel*	*Beheersmaatregel*
Geautomatiseerde systemen ingezet voor de volgende processen: • Vaststellen, samenstellen en gebruik van het prijzenschema; • Vaststellen, samenstellen en gebruik van de lijst van deelnemers; • Aanwijzing winnend(e) lot(en) en/of aanwijzing winnaar(s) (spelresultaat). Uitbetaling van prijzen aan de winnaar(s).	De vergunninghouder draagt er voor zorg dat de geautomatiseerde systemen beheersbaar wordt toegepast t.b.v. een integere, vertrouwelijke en beschikbare verwerking van informatie.	De vergunninghouder heeft een beheercyclus voor informatiebeveiliging opgezet die voorziet in continue verbetering van de informatiebeveiliging.
		Het beheer van informatiebeveiliging is gebaseerd op identificatie en beperking van risico's. De vergunninghouder heeft als uitgangspunt voor zijn maatregelen een risicobeoordeling uitgevoerd.
		Procedures en beleid ten aanzien van informatiebeveiliging worden gedocumenteerd en onderhouden.
		De vergunninghouder heeft ten minste de volgende documentatie beschikbaar: • beleid ten aanzien van informatiebeveiliging; • reikwijdte van het informatiebeveiligingsbeheer; • risicobeoordeling; • verantwoordelijkheden met betrekking tot informatiebeveiliging; • beschrijving van beveiligingsmaatregelen; • beschrijving van uitvoering en resultaten van de beheercyclus.
		De vergunninghouder verricht regelmatige controles op de informatiebeheercyclus.
		De vergunninghouder heeft procedures voor het beheer van veiligheidsincidenten opgezet.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende de organisatie van de informatiebeveiliging, waaronder in ieder geval: • functies en verantwoordelijkheden; • scheiding van functies; • mobiele apparaten en telewerken.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende personele middelen en veiligheid, waaronder in ieder geval: • screening; • arbeidsvoorwaarden; • managementverantwoordelijkheden; • bewustzijn van en onderwijs en opleiding betreffende informatiebeveiliging; • disciplinaire procedures; • verantwoordelijkheden in verband met beëindiging of wijziging van dienstbetrekking.

IT-audit Framework		
Beheers object 1	*Beheers doel*	*Beheersmaatregel*
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende beheer van activa, waaronder in ieder geval: • verantwoordelijkheid voor activa; • classificatie van informatie; • het gebruik van gegevensdragers en andere media.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende toegangscontrole, waaronder in ieder geval: • vereisten van toegangscontrole; • beheer van gebruikerstoegang; • verantwoordelijkheden van gebruikers; • toegangscontrole voor systemen en applicaties.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende cryptografie, waaronder in ieder geval: • cryptografiebeleid; • sleutelbeheer.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende operationele beveiliging, waaronder in ieder geval: • operationele procedures en verantwoordelijkheden; • bescherming tegen malware; • reservekopieën of reservebestanden; • geautomatiseerde verslaglegging, registratie en bewaking; • beheer van bedrijfssoftware; • beheer van technische kwetsbaarheden; • configuraties voor de controle van informatiesystemen.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende communicatiebeveiliging, waaronder in ieder geval: • beheer van netwerkbeveiliging; • informatieoverdracht.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende de aanschaf, ontwikkeling en het onderhoud van systemen, waaronder in ieder geval: • beveiligingseisen voor informatiesystemen; • beveiliging bij ontwikkelen ondersteuningsprocessen; • testgegevens.

IT-audit Framework		
Beheers object 1	*Beheers doel*	*Beheersmaatregel*
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende betrekkingen met leveranciers, waaronder in ieder geval: • informatiebeveiliging; • beheer van de dienstverlening van leveranciers.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende de informatiebeveiligingsaspecten van bedrijfscontinuïteitsmanagement, waaronder in ieder geval: • continuïteit van informatiebeveiliging; • backup procedures en jaarlijks testen van het terugzetten van de backup. • terugvalopties ingeval van incidenten.
		De vergunninghouder heeft op basis van een eigen risicobeoordeling maatregelen gespecificeerd betreffende naleving, waaronder in ieder geval: • naleving van wettelijke en contractuele vereisten; • toetsing van informatiebeveiliging.

IT-audit Framework		
Beheers object 2	*Beheers doel*	*Beheersmaatregel*
Het IT-beheer van de geautomatiseerde systemen ingezet voor de volgende processen: • Vaststellen, samenstellen en gebruik van het prijzenschema; • Vaststellen, samenstellen en gebruik van de lijst van deelnemers; • Aanwijzing winnend(e) lot(en) en/of aanwijzing winnaar(s) (spelresultaat); • Uitbetaling van prijzen aan de winnaar(s).	De vergunninghouder beheert interne IT-processen opdat hij voorspelbare en betrouwbare diensten kan bieden.	De vergunninghouder hanteert een IT-beleid dat aansluit op de doelen van de organisatie en het informatiebeveiligingsbeleid.
		De vergunninghouder draagt er zorg voor dat de methode van prijsbepaling onderworpen is aan een voorafgaande goedkeuring door een door de Minister van Justitie en Veiligheid aangewezen onafhankelijke deskundige of keuringsinstelling.
		De vergunninghouder beschikt over gedocumenteerde procedures voor het beheer van incidenten en problemen.
		Daarbij legt de vergunninghouder de incidenten vast en de opvolging daarvan.
		Incidenten worden geregistreerd, geclassificeerd, geanalyseerd en opgelost. Deze stappen worden gedocumenteerd.
		Problemen worden geregistreerd, geclassificeerd, geanalyseerd en opgelost. Deze stappen worden gedocumenteerd. Onder problemen worden in ieder geval incidenten verstaan die structureel van aard zijn of geen duidelijke oorzaak hebben.
		De vergunninghouder beschikt over gedocumenteerde procedures voor veranderings- en releasemanagement.
		Wijzigingen aan IT-systemen worden geregistreerd en gaan vergezeld van een beschrijving en toelichting.
		Wijzigingen worden pas door een bevoegde medewerker goedgekeurd nadat hun effect is beoordeeld, en geregistreerd.
		De vergunninghouder heeft procedures gespecificeerd en gedocumenteerd waarin een beschrijving wordt gegeven van het onderhoud en de configuratie van systemen.
		De vergunninghouder heeft procedures gespecificeerd en gedocumenteerd voor het beheer van de beschikbaarheid en capaciteit van systemen en infrastructuren.
		De vergunninghouder heeft procedures gespecificeerd en gedocumenteerd voor het beheer van de IT-aspecten van het financiële management.
		De vergunninghouder heeft procedures gespecificeerd en gedocumenteerd voor het beheer van interne en externe serviceniveaus.

IT-audit Framework		
Beheers object 3	*Beheers doel*	*Beheersmaatregel*
Specifieke elementen t.b.v. bedreiging van buitenaf* op te vangen al onderdeel van de geautomatiseerde systemen ingezet voor de volgende processen: • Vaststellen, samenstellen en gebruik van het prijzenschema; • Vaststellen, samenstellen en gebruik van de lijst van deelnemers; • Aanwijzing winnend(e) lot(en) en/of aanwijzing winnaar(s) (spelresultaat); • Uitbetaling van prijzen aan de winnaar(s). Indien de IT- Infrastructuur en geautomatiseerde systemen via een publiek toegankelijk netwerk (het internet) “van buitenaf” bereikbaar is.	De vergunninghouder voert minimaal per jaar één full penetratietest uit op de geautomatiseerde systemen.	De vergunninghouder voert een penetratietest uit en volgt daarbij de bevindingen actief op dat binnen 6 maanden alle issues zijn gemitigeerd.
		De vergunninghouder richt voldoende controle maatregelen in en beheert deze actief om bedreigingen vanuit buitenaf af te vangen. De vergunning heeft minimaal een firewall, en netwerk controls geïntegreerd in het IT systeem. *N.B. de firewall en netwerk controls zijn up to date.*

Afzendgegevens

Kansspelautoriteit
Rijnstraat 50
2515 XP Den Haag
Postbus 298
2501 CG Den Haag
www.kansspelautoriteit.nl