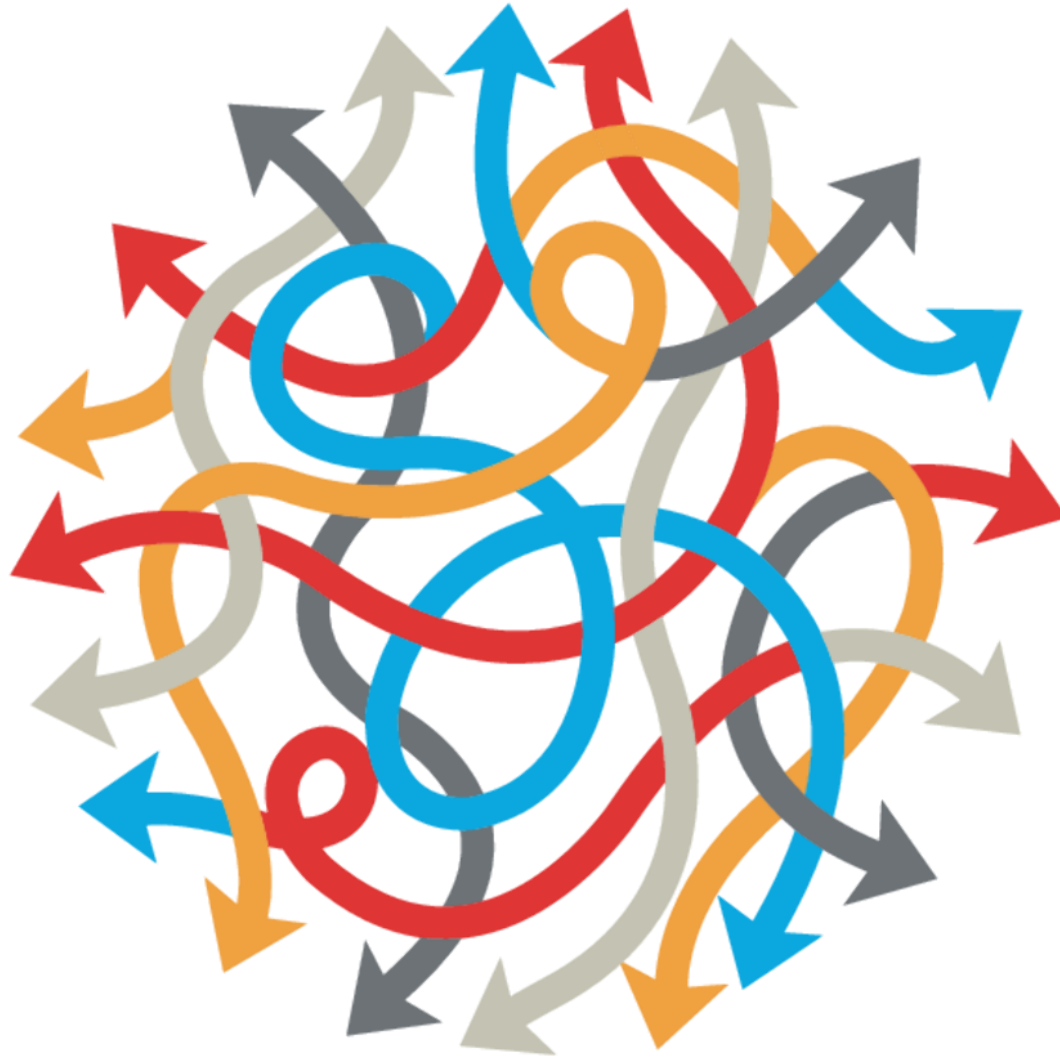




Strætó

Innri endurskoðun 2021

Greinargerð til endurskoðunarnefndar og stjórnar

12. nóvember 2021 TRÚNAÐARMÁL

Innri endurskoðun Strætó 2021



Strætó bs.
b.t. framkvæmdastjóra
Hestháli 14
110 Reykjavík

Áhætturáðgjöf Deloitte hefur lokið innri endurskoðun hjá Strætó bs. vegna ársins 2021. Hjálagt er greinargerð til endurskoðunarnefndar og stjórnar Strætó bs. sem er úrdráttur úr niðurstöðum vinnuskýrslu innri endurskoðunar til stjórnenda Strætó bs. um innri endurskoðun 2021.

Strætó bs. („Strætó“ eða „fyrirtækið“) og Deloitte ehf. (Deloitte“ eða „við“) gerðu með sér samkomulag um innri endurskoðun frá árinu 2016, síðast framlengt til ársins 2021.

Í viðskiptaskilmálum Deloitte sem eru hluti af ráðningarbréfi við Strætó kemur m.a. fram að Deloitte er eigandi höfundarréttar alls efnis sem útbúið er við framkvæmd verkefnisins og að fyrirtækinu er kunnugt um að það álit og sú ráðgjöf sem því er veitt í tengslum við verkefnið er eingöngu ætluð fyrirtækinu sjálfu í tengslum við innri endurskoðun þess. Ráðgjöfina skal ekki nota í öðrum tilgangi nema að gerðu skriflegu samþykki Deloitte, undir slíka takmörkun fellur umfjöllun eða tilvísun í niðurstöður innri endurskoðunar Deloitte. Fyrirtækinu er heimilt að veita ytri endurskoðanda aðgang að greinargerð Deloitte ásamt fylgigögnum að fenginni skaðleysisyfirlýsingu þeirra gagnvart Deloitte. Aðilum er kunnugt um að efni það sem kynnt er og lagt er fram varðar viðkvæmar trúnaðarupplýsingar sem óheimilt er að hagnýta hvort sem er einstakar upplýsingar er fram koma eða í heild. Samningsaðilar eru ábyrgir fyrir því að einstakir efnispættir eða upplýsingarnar í heild sinni verði ekki notuð á óheimilan hátt.

Eftirfarandi starfsmenn Deloitte unnu við gerð skýrslunnar í stafrófsröð: Eygló Sigfúsdóttir verkefnastjóri, Sara Fönn Jóhannesdóttir verkefnastjóri, Sif Einarsdóttir eigandi, Sigurður Dagur Sturluson sérfræðingur, Úlfar Andri Jónasson verkefnastjóri og Veronica Sjöfn Garcia aðstoðarmaður.

Við viljum færa öllum starfsmönnum Strætó þakkar fyrir gott samstarf og góðar móttökur. Starfsfólk veitti okkur alla þá aðstoð sem við óskuðum eftir og brást vel við ábendingum okkar og athugasemdum.

Kópavogur, 12.11.2021

Deloitte, áhætturáðgjöf

Umfang og afmörkun

Innri endurskoðun hitti framkvæmdastjóra Strætó í tengslum við undirbúning áhættumats innri endurskoðunar. Endurskoðunarnefnd samþykkti innri endurskoðunaráætlun fyrir árið 2021 þann 2. júní 2021. Innri endurskoðunaráætlunin skiptist í eftirfarandi liði og greinist tímafjöldi þannig:

2021

Eftirlitsumhverfi – Staða gæðamála. Reikningshaldsferill. Fundargerðir stjórnar. Sviksemismál 2021, viðbrögð og úrbætur	30
Staða persónuverndar – Fylgni við kröfur persónuverndar og netöryggismál því tengd	40
Rekstrarkostnaður – Samþykktarferli reikninga	10
Upplýsinga- og netöryggi – Aðgangsmál, afritun, netöryggi og valin mikilvæg atriði	50
Eftirfylgni athugasemda frá fyrra ári	20
Samtals klst	150

Yfirferð innri endurskoðunar 2021 takmarkast við ofangreinda liði og markast af því umfangi sem fram kemur í töflunni hér fyrir ofan. Gerð var eftirfylgni á öllum rauðum, appelsínugulum og gulum athugasemdum fyrra árs auk valinna ábendinga.

Innri endurskoðun Strætó 2021



Gögn og gagnaöflun

Skýrsla okkar er unnin í samræmi við gögn og upplýsingar frá Strætó. Við höfðum aðgang að gögnum og upplýsingum í samræmi við samning um innri endurskoðun. Við yfirferð okkar tókum við viðtöl við stjórnendur og starfsmenn Strætó, skoðuðum gögn og fórum yfir samræmi við lög og reglur, verklagsreglur- og ferla. Innri endurskoðunarvinnan fór fram frá júní til október 2021.

Niðurstaða kannana

Við vinnu okkar var miðað við eftirlitslíkan COSO (Committee of Sponsoring Organizations of the Treadway Commission). Í skýrslunni er lögð áhersla á að benda á atriði þar sem við sjáum tækifæri til úrbóta og er það von okkar að athugasemdir og ábendingar okkar verði skoðaðar með það í huga. Ábendingar okkar og athugasemdir er að finna í einstökum köflum, merktar með litum og flokkaðar eftir mikilvægi, byggt á mati okkar, sjá áhættuflokkunarkerfi útskýrt á bls. 8.

Framsetning niðurstaðna

Í skýrslunni er lögð áhersla á að benda á tækifæri til úrbóta í innra eftirliti, áhættustýringu og stjórnarháttum. Er það von okkar að athugasemdir og ábendingar okkar verði skoðaðar með það í huga. Stjórnendur hafa lesið yfir drög að skýrslunni og staðfest að rétt sé haft eftir þeim og að umfjöllunin endurspeglar gögn sem til skoðunar komu. Einnig að þeim sé ekki kunnugt um að neinar mikilvægar upplýsingar sem varða efni skýrslunnar vanti.

Viðbrögð stjórnenda

Gerð verður tímasett áætlun til að fylgja athugasemdum og tillögum eftir. Viðeigandi stjórnendur bera ábyrgð á einstökum úrbótaatriðum. Æskilegt er að stjórn fylgi sérstaklega eftir eldri úrbótaatriðum svo hægt sé að loka þeim tímanlega.

Fjöldi athugasemda og ábendinga

Alvarlegt frávik	Mikil frávik	Miðlungs frávik	Lítill frávik	Samtals
0	2	10	12	24

Athugasemdir og ábendingar flokkaðar

Flokkur	Fjöldi	Áhætta
Eftirlitsumhverfið og rekstrarkostn.	1	
Persónuvernd	8	
Upplýsinga- og netöryggi	3	
Eftirfylgni athugasemda frá fyrra ári	12	
Samtals	24	



Samantekt



Eftirlitsumhverfið



Staða persónuverndar



Upplýsinga- og netöryggi



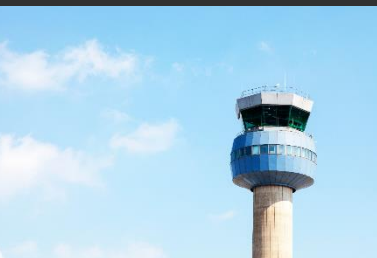
Eftirfylgni athugasemda frá fyrra ári



Viðauki



Greinargerð til endurskoðunarnefndar og stjórnar Strætó



Samantekt



Eftirlitsumhverfið



Staða persónuverndar



Upplýsinga- og netöryggi



Eftirfylgni athugasemda frá fyrra ári



Viðauki



Efni	Samantekt	Athugasemdir og tillögur
Eftirlits-umhverfi	Á árinu 2021 fór innri endurskoðun yfir nokkra þætti í kafla um eftirlitsumhverfi en það voru staða gæðamála hjá Strætó, farið var yfir fundargerðir stjórnar, farið var yfir reikningshaldsferil Strætó, stöðu sviksemismála og að lokum voru gerðar kannanir á samþykki rekstrarkostnaðar sem gerð var grein fyrir undir þessum lið.	Yfirferð innri endurskoðunar var án ábendinga og athugasemda fyrir utan að skerpa þarf á fylgni við verklagsreglu um heimildir og samþykktir reikninga.
Staða persónuverndar	Við innri endurskoðun 2021 fóru sérfræðingar innri endurskoðunar á sviði persónuverndar yfir atriði sem við teljum mikilvæg í tengslum við lög um persónuvernd og vinnslu persónuupplýsinga. Meðal annars var farið yfir hvort gætt væri að meginreglunni um lágmörkun gagna, skilgreiningu á viðeigandi vinnsluáðilum og gerð vinnslusamninga, verklagsreglur í tengslum við réttindi skráðra einstaklinga, gerð vinnsluskrár, persónuverndaryfirlýsingar, öryggisráðstafanir, þjálfun og fræðslu starfsfólks og hvort persónuupplýsingar séu í einhverjum tilvikum fluttar út fyrir EES svæðið og verlag því tengt.	Innri endurskoðun mælir með lokið verði við þær verklagsreglur og önnur skjöl sem eru í vinnslu. Komið var á framfæri við persónuverndarfulltrúa Strætó hvaða atriði skulu vera í reglum/skjölum eftir því sem við á.
Upplýsinga- og netöryggi	Umfang skoðunar beindist að nokkrum mikilvægum kerfum í starfsemi Strætó. Skoðaðar voru verklagsreglur, aðgangsstjórnun, aðgangsheimildir, breytingastjórnun, afritun og aðgreining starfa. Til staðar er ákveðinn skortur á starfaaðgreiningu sem bætt er upp að hluta til með öðrum eftirlitsaðgerðum, sem við fórum yfir og staðfestum með gögnum.	Innri endurskoðun gerði úrbótatillögur um að uppbætandi eftirlit fari fram ársfjórðungslega í stað árlega. Innri endurskoðun fékk upplýsingar um að nú þegar hafi verið bæt úr hluta athugasemda og ábendinga eftir að yfirferð innri endurskoðunar fór fram.



Eftirfylgni með athuga- semdum fyrra árs

Fylgt var eftir athugasemdum og ábendingum. Innri endurskoðun endurtók nokkrar athugasemdir þar sem ekki hafði verið brugðist við þeim þegar yfirferð okkar fór fram. Nokkrar athugasemdir varðandi netöryggi er enn verið að vinna að og bíða úrlausnar á næsta ári, samkvæmt stjórnendum. Ljúka þarf við heildstætt áhættumat upplýsingakerfa.

Athugasemdir og tillögur

Innri endurskoðun fékk upplýsingar um að bætt hefði verið úr hluta athugasemda og ábendinga eftir að yfirferð innri endurskoðunar fór fram. Í nokkrum tilfellum bregst Strætó við með uppþætandi eftirlitsaðgerðum sem innri endurskoðun hefur í hyggju að fylgja frekar eftir á næsta ári. Innri endurskoðun leggur áherslu á að Strætó bregðist við þeim athugasemdum sem fyrst sem eru áhættuflokkaðar sem gulmerktar.



Samantekt



Eftirlitsumhverfið



Staða
persónuverndar



Upplýsinga- og
netöryggi



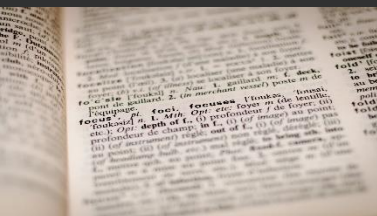
Eftirfylgni
athugasemda frá
fyrra ári



Viðauki



Viðaukar



Samantekt



Eftirlitsumhverfið



Staða
persónuverndar



Upplýsinga- og
netöryggi



Eftirfylgni
athugasemda frá
fyrra ári



Viðauki



Rauð	Appelsínugul	Gul	Græn
<i>Rauð athugasemd er vegna alvarlegra veikleika í innra eftirliti sem geta leitt af sér áhættur á einu eða fleiri eftirfarandi sviðum:</i>	<i>Appelsínugul athugasemd getur verið vegna verulegra veikleika í innra eftirliti sem geta leitt af sér áhættur á einu eða fleiri eftirfarandi sviðum:</i>	<i>Gul athugasemd er vegna veikleika í innra eftirliti sem geta leitt af sér áhættur á einu eða fleiri eftirfarandi sviðum:</i>	<i>Græn ábending þýðir að innra eftirlit er viðunandi en að umbótatækifæri geti verið til staðar.</i>
✓ Mikið fjárhagslegt tjón.	✓ Nokkurt fjárhagslegt tjón.	✓ Lítið fjárhagslegt tjón.	✓ Stjórnandi hefur möguleika á því að bæta innra eftirlit enn frekar.
✓ Brot á lögum eða ekki fylgni við aðrar kröfur ytri aðila.	✓ Ekki fylgni við kröfur ytri aðila.	✓ Fylgni við kröfur eða tilmæli ytri aðila ekki fullnægjandi.	
✓ Vöntun eða brot á siðareglum og/eða alvarlegt brot á innri reglum.	✓ Vöntun á innri reglum eða veruleg frávik í fylgni við þær.	✓ Uppbygging innri reglna eða fylgni við þær ekki fullnægjandi.	✓ Jafnframt getur græn ábending þýtt að brugðist hafi verið við ábendingu á vinnslutíma úttektar og að Innri endurskoðun hafi fengið staðfestingu á því að málinu sé lokið.
✓ Mikil orðsporsáhætta.	✓ Möguleg orðsporsáhætta.	✓ Litlar líkur á orðsporsáhættu.	
✓ Mikil sviksemisáhætta.	✓ Sviksemisáhætta.	✓ Litlar líkur á sviksemisáhættu.	
Tímafrestur viðbragða			
➤ Viðbrögð þurfa að vera tafarlaus.	➤ Úrbætur eigi sér stað innan sex mánaða.	➤ Úrbætur eigi sér stað innan árs.	

Umfjöllunarefni þessa skjals takmarkast við þau atriði sem athugun okkar beindist að við innri endurskoðunarvinnuna og er ekki ætlað að vera tæmandi yfirferð yfir alla mögulega veikleika sem eru til staðar hjá fyrirtæki því sem innri endurskoðunin beinist að og ekki tæmandi yfirferð yfir allar mögulegar úrbætur sem væri hægt að gera á þeim veikleikum. Fyrirtækið að leggja mat á tillögur innri endurskoðunar um úrbætur og áhrif þeirra áður en tillögurnar eru innleiddar hjá fyrirtækinu. Innri endurskoðun tekur ekki yfir ábyrgð stjórnar og stjórnenda á traustu innra eftirliti hjá fyrirtækinu.

Undir vörumerki „Deloitte“ sameinast kraftar þúsunda sérfræðinga sem starfa hjá sjálfstæðum félögum um allan heim við að veita viðskiptavinum þjónustu á sviði endurskoðunar, ráðgjafar, fjármála, áhættustjórnunar og skattamála. Þessi félög eru aðilar að Deloitte Touche Tohmatsu Limited (DTTL), sem er breskt einkahlutafélag (private company limited by guarantee). Hvert aðildarfélag veitir þjónustu á tilteknu landssvæði og er bundið þeim lögum og fagreglum sem þar gilda. Félagið DTTL innir ekki af hendi þjónustu til viðskiptavina. DTTL og aðildarfélög þess eru aðskildir og sérgreindir lögaðilar sem ekki geta skuldbundið hvert annað. DTTL og aðildarfélög þess bera eingöngu ábyrgð á eigin gjörðum eða vanrækslu en ekki á aðgerðum hvers annars. Hvert aðildarfélag DTTL er skipulagt í samræmi við innlend lög, reglugerðir, viðskiptavenju og aðra þætti, og getur veitt sérfræðiþjónustu á starfssvæði sínu í gegnum dótturfélög, tengd félög, og/eða önnur félög.

Deloitte veitir bæði opinberum aðilum og einkafyrirtækjum í fjölmörgum atvinnugreinum endurskoðunar-, skatta-, ráðgjafar- og fjármálaþjónustu. Alþjóðlegt sérfræðinet Deloitte tengir saman sérfræðinga í meira en 150 löndum þannig að saman fari ítarleg staðbundin þekking og alþjóðleg hæfni, viðskiptavinum til hagsbóta. Hjá Deloitte starfa um 286.000 sérfræðingar sem stefna saman að því að veita ávallt framúrskarandi þjónustu.