Trúnaðarmál

Kópavogsbær

Viðauki II – Ábendingar og athugasemdir vegna upplýsingatækni, endurskoðun ársreiknings 2025

Davíð Arnar Einarsson
Eigandi
david.einarsson@is.gt.com

Sif Jónsdóttir
Eigandi
sif.jonsdottir@is.gt.com

Sigurjón Oddsson
Verkefnastjóri
sigurjon.oddsson@is.gt.com

Skjal sótt af '0000000000' dags. 11.11.2026

Skjal sótt af '0000000000' dags: 11.11 2026

12. maí 2026

Bæjarstjórn Kópavogsbæjar
Digranesvegi 1
200 Kópavogi

Grant Thornton endurskoðun ehf.
Suðurlandsbraut 20
108 Reykjavík
Sími: 520-7000
www.grantthornton.is

Endurskoðun ársreiknings 2025

Við höfum framkvæmt prófanir á innra eftirliti sem hluta af endurskoðun okkar á ársreikningi Kópavogsbæjar árið 2025.

Í skýrslu þessari er gerð grein fyrir niðurstöðum úttekta er snýr að upplýsingatækniumhverfi Kópavogsbæjar sem framkvæmdar hafa verið samhliða endurskoðun ársreiknings 2025.

Markmið skýrslunnar er að veita stjórnendum bæjarins upplýsingar sem nýtast geta við að bæta og styrkja innra eftirlit og upplýsingatækni.

Í skýrslu þessari eru athugasemdir og ábendingar flokkaðar eftir alvarleika:

- Ef alvarleiki er mikill (rautt) er um athugasemd að ræða sem æskilegt er að stjórnendur bregðist sem fyrst við, enda um verulegan veikleika í innra eftirliti að ræða að okkar mati.
- Ef alvarleiki er í meðallagi (appelsínugult) er um athugasemd að ræða sem æskilegt er að okkar mati að stjórnendur bregðist sem fyrst við.
- Ef alvarleiki er lítill (grænt) er um ábendingu að ræða sem æskilegt er að stjórnendur taki til skoðunar og leggi mat á hvort aðgerða sé þörf.

Virðingarfyllst,
Grant Thornton endurskoðun ehf.

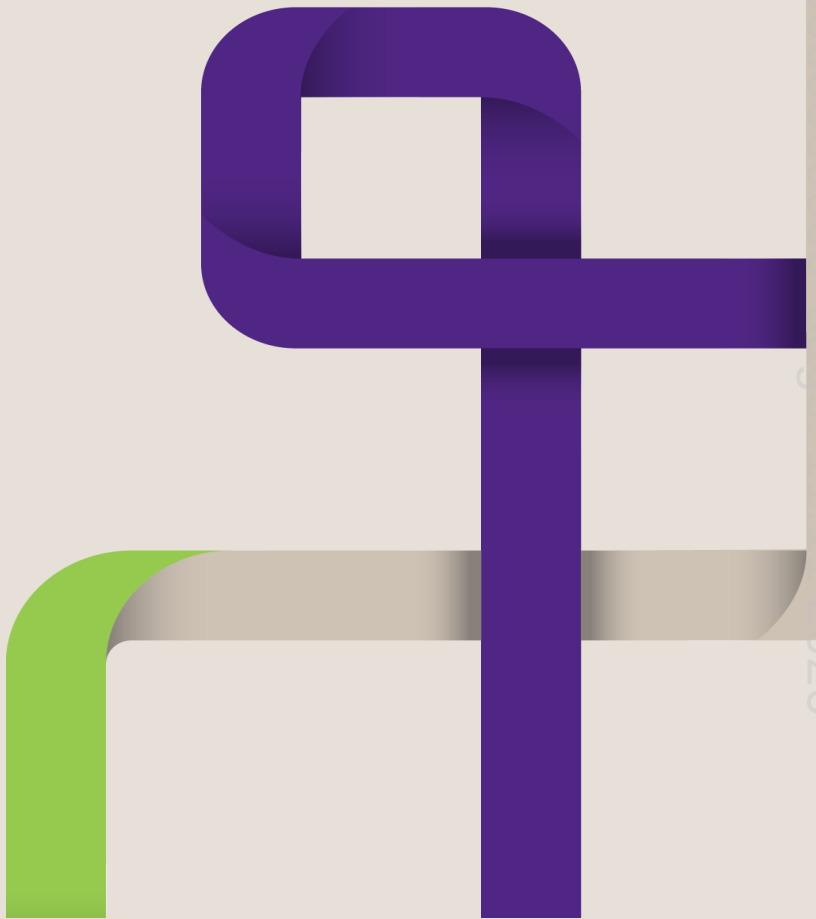
Davíð A. Einarsson
Löggiltur endurskoðandi

Sif Jónsdóttir
Löggiltur endurskoðandi

Grant Thornton International Ltd
VAT reg 888 0195 82. Registered in England. Company number 05523714
Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered independently by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

grantthornton.global

Ábendingar og athugasemdir



Upplýsingatækniumhverfi

Nr.	Ferill	Ábendingar	Áhrif	Tillögur að úrbótum	Viðbrögð stjórnenda	Stig alvarleika	Staða
1.	Upplýsinga tækni	**Greining á aðgreiningu hlutverka í upplýsingakerfum:** Ekki fékkst tímanlega aðgangur að lykilkerfum sem tengjast reikningsskilum eða fjárhagsupplýsingagerð til að taka út lista yfir notendur eða heimildir. Ekki fengust slíkir listar frá starfsmönnum Kópavogsbæjar heldur til að hægt væri að meta veikileika í aðgreiningu hlutverka. Teljum nauðsynlegt að notendur sem koma nálægt reikningsskilum og fjárhagsupplýsingagerð. Hafi aðeins þau réttindi sem þeir þurfa á að halda til að sinna sínu starfi og uppfylla sína ábyrgð.	Verulegur veikleiki í aðgreiningu hlutverka og heimildastjórnun er tengist fjárhagskerfinu BC. Getur leitt til verulegrar öryggisáhættu, svo sem aðgang óviðkomandi að viðkvæmum gögnum eða möguleika á að breyta stillingum í kerfinu. Sem gæti leitt til mistaka eða sviksemi. Mikilvægt að takmarka þessa heimild við kerfisstjóra. Þar sem hún gerir notendum kleift að stýra mikilvægum aðgerðum í kerfinu, þar á meðal breyta kerfisstillingum og notendaheimildum.	Aðeins þeir sem þurfa kerfisstjórnunarréttindi hafi slíkt. Heimildir annara notenda takmarkist við þær heimildir sem taldar eru nauðsynlegar. Skilgreindir ábyrgðaraðilar meti hvaða notendur þurfi að vera með svo víðtæk réttindi. Ráðlegt er að takmarka úthlutun víðtækra heimilda eins og kostur er og fylgjast náið með aðgerðum þeirra sem hafa slíkar heimildir. Til að tryggja réttleika og öryggi kerfisins.	SAP hefur verið útleitt og Kjarni innleitt í staðinn. Rýni var framkvæmd samhliða innleiðingu. Aðgangur hefur að miklu leyti verið rýndur, samanber næstu athugasemd. Að öðru leyti er ábending réttmæt og hefur verið tekin til greina, unnið er að umbótum í samræmi við forgangsröðun og áhættumat. Ferli verður skilgreint og innleitt. Stig lækkað úr **Hátt** í **Meðal**	Meðal	**Í vinnslu**
2.	Upplýsinga tækni	**Eftirlit með aðgang og heimildum notenda að upplýsingakerfum:** Samkvæmt verklagsreglu um aðgangsheimildir skulu stjórnendur skila skýrslu árlega um að þeir hafi tekið út að aðgangur sinna starfsmanna sé réttur og staðfesti það. Samkvæmt sömu verklagsreglu skulu eigendur (security group managers) aðgangshópa í Active Directory (AD) skila skýrslu minnst árlega um að þeir hafi farið yfir aðgang og staðfesta að hann er réttur. Samkvæmt reglum um kerfiseiganda skal hann rýna aðgang notenda að lausninni á þriggja til sex mánaða fresti, lágmarki árlega. Ekki fékkst staðfesting frá starfsmönnum Kópavogsbæjar að þetta eftirlit væri virkt. VLS-0025 Aðgangsheimildir Kerfiseigandi (Application Owner)	Að óviðkomandi séu með aðgang eða of víðtækar heimildir að mikilvægum kerfum sem Kópavogsbær notar.	Að farið sé eftir skjalfestu verklagi til að tryggja öryggi kerfa og gagna. Mikilvægt að reglulega sé farið yfir notendur og lokað á þá aðila sem ekki eigi að vera með aðgang að neti eða kerfum. Jafnframt að heimildir samræmist hlutverki og ábyrgð notenda.	Rýni á aðgangi hefur verið framkvæmd en ekki skjalað. Rýni á aðgangi að Kjarna var framkvæmd þegar kerfi var innleitt. Að öðru leyti er ábending réttmæt og hefur verið tekin til greina, unnið er að umbótum í samræmi við forgangsröðun og áhættumat. Ferli verður skilgreint og innleitt. Með innleiðingu Kjarna tekur við sjálfvirkt "offboarding" á notendum þegar þeir fara af launaskrá, og þar með missa þeir aðgang að innra kerfi Kópavogsbæjar. Stig lækkað úr **Hátt** í **Meðal**	Meðal	**Í vinnslu**

Skjal sótt af '0000000000' dags: 11.11 2026

Upplýsingatækniumhverfi

Nr.	Ferill	Ábendingar	Áhrif	Tillögur að úrbótum	Viðbrögð stjórnenda	Stig alvarleika	Staða
3.	Upplýsinga tækni	**Eftirlit með aðgerðum notenda með víðtæk réttindi:** Ekki hægt að sjá skráningu á að farið sé yfir aðgerðir notenda, að lágmarki með víðtæk réttindi (admin), í mikilvægum kerfum reglulega. Teljum mikilvægt að vöktun sé með aðgerðum aðila með víðtæk réttindi í mikilvægum kerfum. Hægt að rekja aðgerðir notenda samkvæmt upplýsingum frá stjórnendum. Ekki fékkst staðfesting frá starfsmönnum Kópavogsbæjar að eftirlit sé virkt.	Verið sé að framkvæma óviðeigandi aðgerðir í kerfum án þess að það uppgötvist. Þessar óviðeigandi aðgerðir geta t.d. tengst sviksemi.	Rýna aðgerðir notenda með víðtæk réttindi að mikilvægum kerfum reglulega samkvæmt skráðu ferli. Tryggja að ekki sé hægt að eiga við breytinga skrár (e.logs) og aðgreiningu hlutverka við yfirferð á aðgerðum notenda með víðtækar heimildir.	Allar aðgerðir í kerfunum BC og Kjarna eru skráðar (e. log). SOC vöktun fylgist með öllum breytingum á "viðkvæmum" öryggishópum í AD og öryggisatvik er skráð sem þörf er á að loka sérstaklega. Auk þess er skráning í ManageEngine AD audit sem heldur utan um allar breytingar í AD. Að öðru leyti er ábending réttmæt og hefur verið tekin til greina, unnið er að umbótum í samræmi við forgangsröðun og áhættumat. Ferli verður skilgreint og innleitt.	Hátt	Í vinnslu
4.	Upplýsinga tækni	**Útvistunarsamningar vegna úthýstrar þjónustu og eftirlit með þjónustu:** Kölluðum eftir samningum frá bænum vegna þeirrar þjónustu sem er úthýst til þjónustuaðila fyrir upplýsingatækniumhverfið og mikilvæg kerfi bæjarins. Ekki fengust samningar bakvið þjónustu fyrir helstu kerfi sem tengjast reikningskilum og helstu viðskiptaferlum bæjarins. Því er ekki hægt að meta hvort samningar séu orðnir gamlir, hvort þeir séu endurskoðaðir reglulega eða þeir séu í samræmi við bestu framkvæmd. Eða hvort búið sé að gera viðeigandi vinnslusamninga þar sem persónugreinanleg gögn geta legið til grundvallar. Sú þjónusta sem bærinn útvistar er á endanum á ábyrgð bæjarins því er mikilvægt að reglulega sé tekin út sú þjónusta sem þjónustuaðilar eru að sjá um fyrir bæinn.	Bærinn sé ekki að uppfylla ábyrgðarhlutverk sitt með að fylgjast með þjónustu sem er útvistuð. Varðandi kröfur til eftirlits með útvistaðri þjónustu, vöktun þeirra og öryggisstjórnun kerfa og gagna í hýsingum.	Setja upp stefnu eða reglur varðandi útvistun. Innleiða skjalfest ferli fyrir reglulega endurskoðun á samningum við þjónustuaðila sem sjá um útvistaða þjónustu. Teljum mikilvægt bærinn leiti upplýsinga reglulega um að þjónusta sem framkvæmd er sé í samræmi samninga og þjónustuaðilar hafi viðeigandi innra eftirlit til staðar.	Nýtt kerfi Kjarni hefur verið innleitt í staðinn fyrir SAP og gerður nýr viðaukasamningur við Origo vegna innleiðingar og þjónustu við Kjarna. Notkun á eldra kerfi SAP hefur verið hætt. Ábending er réttmæt og hefur verið tekin til greina, unnið er að umbótum í samræmi við forgangsröðun og áhættumat. Ferli verður skilgreint og innleitt.	Meðal	Í vinnslu

Skjal sótt af '000000000' dags: 11.11 2026

Upplýsingatækniumhverfi

Nr.	Ferill	Ábendingar	Áhrif	Tillögur að úrbótum	Viðbrögð stjórnenda	Stig alvarleika	Staða
5	**Upplýsinga tækni**	Áhætta að kerfisstjóri eða þjónustuaðili geti framkvæmt breytingar, uppfært og innleitt breytingar í kerfi án þess að þær fari í gegnum samþykktarferli (Breytingarstjórnun) Ekki sjáanlegt eftirlit með breytingarbeiðnum hjá Kópavogsbæ. Til staðar eru verklagsreglur og ferli um breytingastjórnun fyrir gæðastjórnunarkerfi (ISO 9001) og innleiðingu á nýjum hugbúnaði. Ekki hægt að sjá að það sé sérstakt breytingastjórnunarferli fyrir kerfi sem nú þegar eru í rekstri. Fengum ekki afhentar slíkar reglur ef þær eru til, né var unnt að rekja breytingar (e.log) í innsendar beiðnir. VER-0131: Breytingastjórnun FER-0050: Breytingastjórnunarferli VER-0039: Kaup á hugbúnaði sem þarfnast prófunar	Ef ekki er til staðar skýr rammi fyrir breytingar á upplýsingatækni hjá Kópavogsbæ sé hætta á að ósamþykktar breytingar séu framkvæmdar. Jafnframt að ekki sé viðunandi aðgreining hlutverka og umhverfa við hönnun, þróun, prófun og samþykki breytinga áður en þær eru færðar yfir í raunumhverfi. Hægt sé að fara fram hjá breytinga-stjórnunarferlinu með því að keyra uppfærslur eða breytingar í kerfinu án þess að þær séu samþykktar af viðeigandi aðila.	Eftirlit þar sem farið sé yfir skráningar (e. log) í kerfum Kópavogsbæjar og þær bornar saman við breytingastjórnunarbeiðnir. Aðgerð sem gæti komið auga á ósamþykktar breytingar.	Í tilvikum skýjaþjónusta, s.s. Kjarna, eru breytingar framkvæmdar af þjónustuaðila. Að öðru leyti er ábending réttmæt og hefur verið tekin til greina, unnið er að umbótum í samræmi við forgangsröðun og áhættumat. Ferli verður skilgreint og innleitt.	Meðal	**Í vinnslu**

Skjal sótt af '0000000000' dags: 11.11 2026

Skjal sótt af '0000000000' dags: 11.11 2026



© 2026 Grant Thornton International Ltd. All rights reserved.

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton International Ltd (GTIL) and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.