



# Öruggur.

„Secure“

Að vera öruggur þýðir að forgangsraða áhættum og setja upp varnir til að verjast þekktum og hugsanlegum ógnum.

# Vakandi.

„Vigilant“

Að vera vakandi þýðir að nota vitræna upplýsingaöflun og að vera meðvitaður um hugsanlegar ógnir til að greina skaðleg hegðun.

# Seigur.

„Resilient“

Að vera seigur þýðir að vera úrræðagóður, hafa getu til að endurbyggja eftir áföll, og draga úr áhrifum þeirra.

## Af hverju að velja Deloitte

Samstarf við framkvæmd áhættu- og öryggisstefnu í netumhverfi yrdi byggt á djúpri reynslu sem Deloitte hefur af vinnu við áhættumat, öryggisáætlanir og tölvutækni. Það mun hjálpa þér að –

**Stöðugt viðhalda "Öruggur, Vakandi, Seigur" stefnunni hjá þínu fyrirtæki**, óháð því hvar þú ert staddur í ferlinu, skapa sveigjanlegan grunn að framtíðar-getu.

**Tengja saman kröfur og tækniáhættu** sem hjálpar þér að takast á við kröfur sem reglugerðir og aðrar væntingar krefst af þér, án þess að missa sjónar á annarri viðskiptaáhættu..

**Ná hraðar stjórn á grundvallaratriðum**, með öflugri þátttöku okkar, sem byggir á vídtækri reynslu á þessu sviði, og yfirgripsmikilli þekkingu á áhættum í netumhverfi.

**Leggja áherslu á það sem skiptir máli** með hópvinnu sem forgangsraðar áhættum fyrirtækisins, byggt á ítarlegu áhættumati.

**Stuðningur við viðskiptastefnu** með samþættum aðgerðum sem takast á við áhættur í netumhverfi.



## Stefnumótun og stjórnarhættir

**Niðurstöður verkefna við stefnumótun og) áhættumat** eru notaðar til að varða leiðir (roadmap) sem styðja við þróun, sem síðan leiðir af sér öryggisstefnu byggða á "**Öruggur, Vakandi, Seigur**" nálguninni.

**Hönnun á öryggisstefnu** skilgreinir næstu kynslóð stjórnarháttanna sem styður nýsköpun og dregur úr vaxandi ógnum sem steðjar að fyrirtækinu.

**Gott stjórnskipulag** ásamt vinnu við áhættumat og öryggisstefnu veita stjórnendum gagnsæi í þá áhættu sem að steðjar.

**Áhættumat á þriðja aðila** aðstoðar fyrirtækið að meta heildar rekstraráhættu fyrirtækisins.

*Það að ná og viðhalda takmarkinu, sem er að vera „Öruggur, Vakandi, Seigur“ (Secure.Vigilant.Resilient.™) krefst stöðugar viðleitni í að skilgreina og endurskilgreina áhættustefnu vegna netumhverfis. Áhættustefna verður að vera rekin er af æðstu stjórnendum. Það þarf að fylgjast með þróun í tækniumhverfi og stöðugt aðlagða öryggisstefnuna að breytilegri viðskiptastefnu og breytingum á áhættum í netumhverfi.*

**Auðkennis- og aðgangsstýringar** hjálpa til við ört vaxandi þörf fyrir rafræn auðkenni og veitingu viðeigandi aðgangs að mikilvægum upplýsingum.

**Kerfi sem halda utanum gagnavernd** eru notuð til að vernda viðkvæmar persónu-upplýsingar og að vernda önnur viðkvæm gögn.

**Eftirlitslausnir** eru notaðar til að hafa eftirliti með heilum kerfum og viðskiptaferlum.

**Tölvuendurskoðun** er notuð til að tryggja réttleika viðskiptaupplýsinga sem finnast í tæknivistkerfi félagsins, frá borðtölvu til netþjóna, hvort sem eru staðsettir í húsnæði fyrirtækisins eða hjá þriðja aðila.

**Raunlægt öryggi** er notað til að tryggja grunnleggjandi vernd fyrir kjarnakerfi og útbúnað.

**Við endurskoðun og hagræðingu rekstraröryggis** eru hannaðar öryggis- og eftirlitsaðgerðir, sem bæta greiningu á ógnum og reglubrotum, ásamt því að gerðar eru viðbragðsáætlanir við áföllum.

**Áhættumiðuð kerfisvöktun** bætir sýn inn í þá áhættu sem ógnar kerfum og viðskiptaferlum og bæta öryggi í breytinga-stjórnun..

**Þekking og greining** á áhættum eykur skilning á núverandi ógnum í tækniumhverfinu og bætir eftirlit og meðhöndlun ógna.

**Veikleikastjórnun** hjálpar til við að draga úr möguleikum sem hægt er að misnota vegna kerfisgalla eða veikleika í vélbúnaði.

**Áfallaaðstoð vegna áfalla** í netumhverfi er þjónusta sem aðstoðar við gerð viðbragðsáætlana, sem á að tryggja rétt viðbrögð til að stöðva og jafna sig á áföllum sem hafa í för með sér meiri eða minni þjónusturof, fjárhagsskaða eða jafnvel skaðað orðspor sem getur haft skaðleg áhrif á verðmæti hlutabréfa.

**"Cyber Wargaming"** er gagnvirk tækni sem greinir hugsanlegar ógnir í netumhverfi með því að skapa atburðarrás í sýndarumhverfi sem nota má til að hanna mótvægis-aðgerðir og viðbúnaðaráætlanir.

**Tæknimiðaður viðnámsþróttur** er markmið sem unnið er í sem hluti af öryggisáætlun og leggur áherslu á að auka getu fyrirtækisins til að jafna sig á tækniáföllum með tæknilausnum.

## Láttu okkur sjá um framkvæmdina

*Deloitte býður vandaða stjórnunarþjónusta sem er aðlöguð að þínu fyrirtæki. Við hjálpum þér að auka skilvirkni og gæði vegna áhættu í netumhverfi þínu og vinnum með þér svo þú getur náð háleittum markmiðum um vandaða áhættu- og öryggisstefnu án þess að þurfa að byggja upp krefjandi hátækniþekkingu innanhúss.*

- Stjórnarhættir, áhætta og viðmið

- Eftirlit með kerfum
- Auðkennis- og aðgangsstýringar
- Gagnavernd

- Öryggisstefna
- Greining á ógnum og áhættum
- Kerfisvöktun og þekking
- Veikleikastjórnun

- Viðbragðsáætlanir
- Úrræði sem þjónusta

Deloitte býður upp á fjölbreyttar lausnir við mótun á ferlum og góðum stjórnarháttum til að byggja upp áhættustefnu, meta ásættanlega áhættu, hönnun og framkvæmd áhættustefnu sem byggir á því að verða "Öruggur, Vakandi, Seigur"™  
Við aðstoðum einnig við áframhaldandi stjórnun, viðhald og aðlögun á áhættustefnunni samhliða þeim breytingum sem verða í umhverfinu.