Gäller för: Västra Götalandsregionen
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2024-12-20
Giltig till: 2029-12-20

Uppföljning och rapportering

Regional rutin 2025 – 2029

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

1 Inledning

Mål: *Informationssäkerheten och informationssäkerhetsarbetet ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag*.

Syftet med rutinen är att fastställa hur, när och av vem uppföljning, internrevision och rapportering av informationssäkerhet, cybersäkerhet, IT-säkerhet och dataskydd ska göras. Rutinen utgår från riktlinje Informationssäkerhet och dataskydd 2023 - 2027.

Rutinen är styrande för alla förvaltningar och bolag i Västra Götalandsregionen (VGR) och ingår som en del i ledningssystemet för informationssäkerhet och dataskydd (ledningssystemet).

När begreppet informationssäkerhet används i rutinen omfattar det även cybersäkerhet och IT-säkerhet.

Anledningen till att kontinuerlig uppföljning, internrevision och rapportering behövs är krav från:

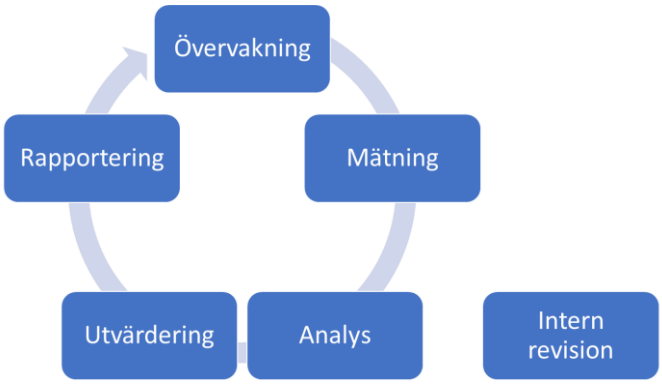
- Standarden[1],
- Kommunallagen,
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster,
- Socialstyrelsens föreskrifter, och
- Dataskyddsförordningen.

Utöver dessa finns även krav på VGR genom anslutning till IS/IT-tjänster från exempelvis:

- Inera,
- Internetstiftelsen, och
- E-hälsomyndigheten.

[1] SS-EN ISO/IEC 27001:2023 samt ISO/IEC 27701:2021

Rutinen beskriver ett antal aktiviteter för området. Dessa hänger ihop genom att övervakning och mätning ger underlag till analys som sedan utvärderas och rapporteras. Internrevision av ledningssystemet ses som en isolerad aktivitet eftersom oberoende och opartiskhet behöver särskilt säkerställas.



Figur: Samband mellan aktiviteterna

2 Termer och begrepp

Internrevision (förstapartsrevision), systematisk, oberoende och dokumenterad process som syftar till att skaffa revisionsbelägg och utvärdera objektivt för att avgöra i vilken utsträckning revisionskriterierna har uppfyllts. En internrevision utförs av organisationen själv eller för dess räkning av en extern part.

Lämplighet innebär att informationssäkerheten och dess styrning står i samklang med VGR:s övergripande mål.

Tillräcklighet innebär att den styrning som beslutats om och ger uttryck för i styrdokument fortfarande räcker till för att hantera VGR:s informationssäkerhets- och integritetsrisker.

Verkan innebär att beslutade säkerhetsåtgärder har implementerats, det vill säga att de existerar, och fungerar tillfredsställande och därmed minskar riskerna.

3 Ansvar och roller

Säkerhets- och beredskapschef

- Ansvarar regionalt för att följa upp att ledningssystemet är tillräckligt för att hantera VGR:s informationssäkerhets- och integritetsrisker.
- Ansvarar regionalt för att styrningen av informationssäkerheten och dataskyddet står i samklang med VGR:s övergripande mål.
- Ansvarar övergripande för rapportering till högsta ledning.

Informationssäkerhetschef

- Ansvarar för uppföljning av ledningssystemets lämplighet, tillräcklighet och verkan.
- Ansvarar för internrevision av ledningssystemet.
- Ansvarar för att rapportera resultat av uppföljning till säkerhets- och beredskapschef och andra berörda.
- Ansvarar för att rapportera allvarliga brister i verksamhetens tillämpning och efterlevnad av ledningssystemet till högsta tjänstemanna- och/eller politisk ledning.

Förvaltningschef/VD

- Ansvarar för uppföljning inom egna förvaltningen/bolaget.
- Ansvarar för att rapportera till den egna nämnden/styrelsen och informationssäkerhetschef med hjälp av informationssäkerhetssamordnare och dataskyddsamordnare.

Informationssäkerhetssamordnare och dataskyddssamordnare

- Följer upp den egna förvaltningens informationssäkerhets- och dataskyddsarbete, på eget initiativ efter verksamhetens behov samt som ett led i regional uppföljning.
- Övervakar informationssäkerhetsarbetet hos den egna verksamheten.
- Rapporterar resultat av uppföljning och övervakning till förvaltningschef/VD och informationssäkerhetschef.

Ägare av IS/IT-tjänst

- Ansvarar för att rapportera informationssäkerhets- och dataskyddsarbete inom sin IS/IT-tjänst till informationssäkerhetschef.
- Ansvarar för att rapportera hur IS/IT-tjänsten uppfyller informationssäkerhets- och dataskyddskrav till informationssäkerhetschef.

Övriga ansvar och roller

- Dataskyddsombudens kontroller ger ett underlag som används i uppföljningsarbetet och används i informationssäkerhetschefs analys och utvärdering av ledningssystemet.
- Regionstyrelsens internkontroll och revisionsenhetens kontroller utgör underlag i uppföljningsarbetet och internrevision.

4 Uppföljning

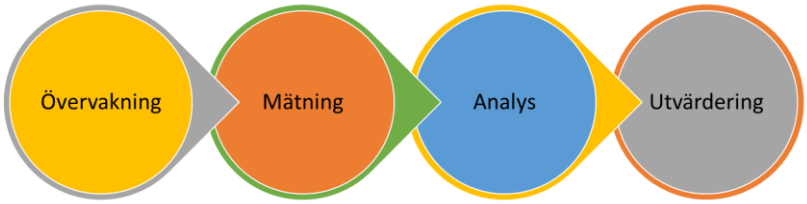
Syftet med uppföljning är att utvärdera informationssäkerheten och dataskyddet, inklusive styrningens lämplighet, tillräcklighet och verkan.

Uppföljningen ligger till grund för ledningens inriktning och ständiga förbättringar.

Metoden för uppföljning är övervakning, mätning, analys och utvärdering.

Informationssäkerhetschef ska följa upp ledningssystemet, hur effektivt och resurssnålt målen med ledningssystemet nås. informationssäkerhetschef ska även utvärdera arbetets och styrningens lämplighet, tillräcklighet och verkan som är en väsentlig del i ett systematiskt och riskbaserat informationssäkerhets- och dataskyddsarbete.

Övervakning ska göras kontinuerligt medan mätning, analys och utvärdering av resultatet från analys sker enligt bestämd frekvens. Informationssäkerhetschef ska identifiera nyckeltal där det är relevant för mätning av respektive uppföljningsområde.



Figur: Metod för uppföljning

4.1 Uppföljningsområden

Tillämpning och efterlevnad

Tillämpning och efterlevnad av ledningssystemet följs av informationssäkerhetschef genom rapportering från det operativa informationssäkerhets- och dataskyddsarbetet på förvaltningar/bolag.

Om informationssäkerhetschef identifierar allvarliga brister rapporterar informationssäkerhetschef dessa till högsta tjänstemanna- och/eller politisk ledning.

Exempel på nyckeltal för mätning av uppföljningsområdet:

- Användningsgrad av avsedda verktyg för informationssäkerhets och/eller dataskyddsarbetet.
- Andel informationstillgångar som är informationsklassade.
- Andel informationstillgångar i respektive informationsklass

Informationen som samlas in analyseras och utvärderas årligen av informationssäkerhetschef. Analysen syftar till att titta på om ledningssystemet är känt i organisationen och om styrningen tillämpas och efterlevs.

Säkerhetsåtgärder existerar och fungerar tillfredställande

Säkerhetsåtgärder följs av informationssäkerhetschef genom rapportering från det operativa informationssäkerhets- och dataskyddsarbetet samt genom stickprov. Rapportering ska göras löpande både lokalt inom den egna verksamheten, av ägare IS/IT-tjänst till informationssäkerhetschef samt från informationssäkerhetschef till säkerhets- och beredskapschef.

Exempel på nyckeltal för mätning av uppföljningsområdet:

- Antal identifierade risker över riskacceptansnivå
- Antal informationssäkerhets- och dataskyddsincidenter

Informationen som samlas in analyseras och utvärderas årligen av informationssäkerhetschef. Analysen syftar till att titta på om säkerhetsåtgärden finns och ger förväntat skydd. Uppföljningen omfattar organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder.

Mognadsnivå

Mognadsnivå följs upp för att följa informationssäkerhets- och dataskyddsarbetets utveckling samt för att jämföra organisationens utveckling gentemot andra organisationer.

VGR:s mognadsnivå ska mätas av informationssäkerhetschef på förvaltnings/bolags-nivå årligen med hjälp av nationellt tillhandahållna verktyg för att öka möjligheten till jämförelse av resultat över tid samt mellan organisationer.

Nyckeltal för mätningen ska omfatta men inte begränsas till följande områden:

- Informationsklassning,
- riskhantering,
- incidenthantering,
- upphandling,
- kompetens, och
- uppföljning

Informationen ska analyseras och utvärderas förvaltnings-/bolagsvis årligen av informationssäkerhetschef. Vartannat år sammanställer informationssäkerhetschef en organisationsövergripande mognadsnivå.

Måluppfyllnad

Uppföljning av mål är en väsentlig del i att säkerställa att arbetet utvecklas och ger önskad effekt. Informationssäkerhetschef ska övervaka informationssäkerhets- och dataskyddsmål, analysera och utvärdera måluppfyllnad mot målens kriterier utifrån det samlade uppföljningsarbetet årligen.

Eventuella förslag på ändrade målformuleringar och kriterier identifieras och föreslås av informationssäkerhetschef till säkerhets- och beredskapschefen som i sin tur föreslår dessa till tjänstemanna- och/eller politisk ledning.

Organisationsgemensam riskbild

Syftet med ledningssystemet är att hantera de informations- och integritetsrisker som organisationen utsätts för. En organisationsgemensam riskbild ger en grov bild av vilka risker som VGR i stort bedöms ha.

En organisationsgemensam riskbild ger:

- Medvetenhet gällande risker och nyckelroller i organisationen och därmed kan bidra till ledningens engagemang för området.
- Stöd till riskidentifiering och riskanalys.
- Utgör underlag till utformning och förbättring av organisationens systematiska arbete med informationssäkerhet och dataskydd.
- Utför underlag för val av säkerhetsåtgärder på en övergripande nivå.

Informationssäkerhetschef ansvarar för att årsvis sammanställa en organisationsgemensam riskbild utifrån aktuella hot.

Specifikt för dataskydd

För att undvika dubbelarbete och ökad belastning för VGR:s verksamheter ska informationssäkerhetschef analysera och utvärdera dataskyddsarbetet med stöd av dataskyddsombudens kontroller.

5 Internrevision

Internrevision görs i syfte att inhämta information om huruvida ledningssystemet uppfyller egna och standardens krav samt har implementerats och underhålls på ett verkningsfullt sätt.

Informationssäkerhetschef ska själv eller via extern part genomföra internrevision för att inhämta information om ledningssystemet enligt ett dokumenterat revisionsprogram som sträcker sig över tre år.

Revisionen ska kontrollera:

- Ledningssystemets uppfyllnad mot egna och regulatoriska krav,
- Ledningssystemets uppfyllnad mot krav i standarden SS-EN ISO/IEC 27001:2023
- Ledningssystemets uppfyllnad mot krav i standarden SS-EN ISO/IEC 27701:2021

Informationssäkerhetschef ska dokumentera ett revisionsprogram som ska ta hänsyn till de berörda processerna och säkerhetsåtgärderna i ledningssystemet och innefatta intervall, metoder, ansvar, planeringskrav och rapportering.

Utöver det ska revisionsprogrammet:

- Fastställa mål, kriterier och omfattning för varje revision
- Säkerställa en oberoende och opartisk revisionsprocess
- Säkerställa att resultat från revisioner rapporteras till berörda ledningsfunktioner

6 Rapportering

Rapportering ska göras både som grund för analys och utvärdering av uppföljningsområden men också för att kommunicera resultat från uppföljning.

Syftet med rapportering att redovisa förmåga för ledning och medarbetare samt vara underlag för beslut om hur informationssäkerhets- och dataskyddsarbetet ska bedrivas fortsättningsvis.

Rapportering av informationssäkerhets- och dataskyddshändelser omfattas a separat rutin.

Till högsta tjänstemanna- och/eller politisk ledning

Säkerhets- och beredskapschef ska årligen rapportera följande till högsta tjänstemanna- och/eller politisk ledning. Rapporteringen utgör ledningens genomgång[2].

- Status för åtgärder som beslutats vid ledningens tidigare genomgångar
- Förändringar i externa och interna frågor som är relevanta för ledningssystemet
- Information om ledningssystemets prestanda
    - Avvikelser och korrigerande åtgärder
    - Resultat från uppföljning av tillämpning och efterlevnad av ledningssystemet, säkerhetsåtgärder, mål, mognadsnivå och organisationens riskbild
    - Revisionsresultat för perioden
    - Återkoppling på ledningssystemet från berörda parter, exempelvis kommuner, leverantörer, Sveriges Kommuner och Regioner (SKR) eller Inera
- Sammanställt övergripande resultat från riskbedömningar och status för riskbehandling

[2] SS-EN ISO/IEC 27001:2023 9.3

- Möjligheter till ständig förbättring
- Förslag på regional handlingsplan

Högsta tjänstemanna- och/eller politisk ledning ska fatta beslut som rör möjligheter till ständig förbättring samt eventuella behov av förändringar av ledningssystemet.

Till säkerhets- och beredskapschef

Rapportering till säkerhets- och beredskapschef görs av informationssäkerhetschef löpande. Rapporteringen utgår från analys och utvärdering av det underlag som förvaltningar, bolag och ägare av IS/IT-tjänst tillhandahåller samt utifrån egen övervakning och mätning.

Till Informationssäkerhetschef

Rapportering av förvaltnings/bolags och ägare av IS/IT-tjänsts informationssäkerhets- och dataskyddsarbete till informationssäkerhetschef görs löpande och i första hand genom:

- informationsdelning i gemensam IS/IT-tjänst för informationssäkerhets- och dataskyddsarbete eller,
- genom epost till informationssäkerhetschef utpekad funktionsbrevlåda.

Rapporteringen ska omfatta men är inte begränsad till:

- Resultat av informationsklassning,
- Riskregister (Informationssäkerhets- och integritetsrisker),
- Register över personuppgiftsbehandlingar,
- Konsekvensbedömningar avseende dataskyddsförordningen,
- Informationssäkerhets- och personuppgiftsincidenter,
- IT-säkerhetsspecifikationer för IS/IT-tjänster som förvaltningen/bolaget ansvarar för.

Till förvaltning och bolag

Informationssäkerhetschef rapporterar resultat av uppföljning och internrevision till informationssäkerhetssamordnare, dataskyddssamordnare och förvaltningschef/VD.

7 Relaterade dokument

- Riktlinje Informationssäkerhet och dataskydd - Regional riktlinje 2023 – 2027 (RS 2023–02811)
- Riskhantering för informationssäkerhet - Regional rutin 2024 – 2028
- Informationsklassning - Regional rutin 2024 - 2028
- Svensk standard SS-EN ISO/IEC 27001:2023 (Ledningssystem för informationssäkerhet – Krav)
- Svensk standard SS-EN ISO 27007:2022 (Vägledning för revision av ledningssystem för informationssäkerhet)
- Svensk standard SS-EN ISO 19011:2018 (Vägledning för revision av ledningssystem)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-269

Version: 1.0

Giltig från: 2024-12-20

Giltig till: 2029-12-20