



Dokumentnamn: Försäkrings AB Göta Lejons rutin för riskbedömning av äldre IKT-system

Beslutad av:
VD

Gäller för:
Försäkrings AB Göta Lejon

Diarienummer:

**Datum och paragraf för
beslutet:**
[Text]

Dokumentsort:
Rutin

Giltighetstid:
Tills vidare

Senast reviderad:
2026-01-08

Dokumentansvarig:
Säkerhetschef

Bilagor:

Bilaga 1 Riskbedömningsmall

Försäkrings AB Göta Lejons rutin för riskbedömning av äldre IKT-system

Syftet med denna rutin

Syftet med denna rutin är att säkerställa att Göta Lejon uppfyller kravet i Dora artikel 8.7 att regelbundet genomföra särskilda IKT-riskbedömningar av äldre IKT-system, minst årligen och i samband med förändringar.

Rutinen kompletterar bolagets övergripande ramverk för IKT-riskhantering.

Vem omfattas av rutinen

Denna rutin gäller tills vidare för Försäkrings AB Göta Lejon

Koppling till andra styrande dokument

Denna rutin har koppling till nedanstående styrande dokument.

Styrande dokument	Koppling till denna anvisning
Försäkrings AB Göta Lejons riktlinje för säkerhet	Fastställer avsikt och krav inom risktagande och beskriver bolagets riskhantering och interna styrning och kontroll
Försäkrings AB Göta Lejons anvisning för riskhantering	Tydliggör hur bolaget arbetar med riskhantering

Stödjande dokument

Denna rutin har koppling till nedanstående stödjande dokument.

Styrande dokument	Koppling till denna anvisning
Försäkrings AB Göta Lejons handbok för systematiskt informationssäkerhetsarbete	Förtydligar hur arbetet med informationssäkerhet bedrivs i bolagets styrning, inklusive årshjul för informationssäkerhetsarbetet.

Rutin

Rutinen omfattar:

- Alla äldre IKT-system som används av bolaget, oavsett om de drifas av Intraservice eller extern IKT-tredjepartsleverantör.
- Alla bolagets processer, inklusive kritiska och viktiga funktioner, som är beroende av sådana system.

Rutinen ska tillämpas

- Minst en gång per år för varje identifierat äldre IKT-system.
- Alltid före och efter att ny teknik, applikationer eller system kopplas till ett äldre IKT-system, t ex med nya gränssnitt, integrationer eller länkar.

Definitioner

Med **äldre IKT-system** avses system som används av Göta Lejon och som stödjer bolagets verksamhet eller processer men som

- nått slutet av sin livscykel (end-of-life) och inte längre är lämpligt för uppgraderingar eller korrigeringar, eller
- inte längre stöds av leverantör eller tredjepartsleverantör.

I praktiken innebär detta t ex:

- Operativsystem eller databaser som är ”end-of-support” från Intraservice eller annan leverantör.
- Applikationer där säkerhetsuppdateringar inte längre släpps.
- Hårdvara eller plattformar där leverantören avisat slut på support men där systemet fortfarande används i produktion.

Med **specifik IKT-riskbedömning av äldre IKT-system** avses en fördjupad riskanalys som:

- Fokuserar på systemets tekniska och säkerhetsmässiga svagheter.
- Beaktar beroenden, integrationer och eventuella nya anslutningar.
- Leder till beslut om kompensatoriska kontroller, begränsningar eller avvecklingsplan.

Roller och ansvar

IT-strateg säkerställer att riskbedömningar genomförs och dokumenteras enligt denna rutin. IT-strateg ansvarar även för att säkerställa att förteckning över äldre IKT-system upprätthålls.

Arbetsgång

Steg 1 – Identifiering och klassificering av äldre IKT-system

Vid den årliga genomgången av IKT-system besvaras följande:

- Är systemet end-of-life/ end-of-support?
- Släpps fortfarande säkerhetspatchar och uppdateringar?
- Finns aktiv leverantörssupport?

De system som uppfyller någon av ovanstående frågor markeras som **äldre IKT-system** i systemförteckningen.

Steg 2 – Genomför specifik IKT-riskbedömning

Genomför riskbedömning genomförs i enlighet med mall i Bilaga 1.

Steg 3 – Uppföljning

Efter genomförd förändring ska en uppföljning genomföras som verifierar:

- Att planerade kontroller är implementerade.
- Att eventuell integration följer plan.
- Att bedömd risknivå kvarstår.

Dokumentation och uppföljning

Specifika riskbedömningar bevaras enligt dokumenthanteringsplan med tydlig referens till bolagets systemförteckning.

Systemförteckning uppdateras med datum för senaste specifika riskbedömning samt datum för nästa planerade bedömning.

Åtgärder från riskbedömningar följs upp i bolagets informationssäkerhetsarbete.

Eventuella höga risker införs i bolagets riskregister.

Bilaga 1

Riskbedömningsmall

Systemets namn:

Leverantör:

Berörda processer och eventuella kritiska/viktiga funktioner:

Driftmiljö:

Teknisk status:

Kända sårbarheter:

Avsaknad av säkerhetsfunktioner (kryptering, loggning, autentisering etc):

Befintliga integrationer:

Beskrivning av kommande tekniska förändringar och bedömning av förändrad hot/sårbarhet:

Konsekvensbedömning (Konfidentialitet, Riktighet, Tillgänglighet):

Bedömning av påverkan på regelefterlevnad:

Bedömning av sannolikhet för ovan konsekvens:

Beskrivning av kompensatoriska åtgärder och/eller kontroller:

Samlad bedömning (acceptabel risk/acceptabel med åtgärdsplan /oacceptabel risk)

Förslag till bedömning (använd, begränsa, avveckla):