

Bilaga 5 – Klassning av information som lagras i IT-system

All information som hanteras av regionen ska klassas för att kunna ges nödvändigt skydd. Informationen skyddas för:

- att alltid finnas när vi behöver den (**tillgänglighet**)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (**riktighet**)
- att endast behöriga personer får ta del av den (**konfidentialitet**)
- att vi ska veta vem som har ändrat den eller använt den (**spårbarhet**)

Om inte klassningen är fullständig riskeras att informationen inte fått rätt skydd och inte är tillgänglig när den behövs.

Det är verksamheterna som ansvarar för att klassa sin information. Verksamheten måste sedan se till att rätt krav ställs mot intern IT-organisation, leverantör och den egna verksamheten. En intern överenskommelse mellan verksamheten och IT dokumenteras i en förvaltningsplan. Där ska tydligt framgå IT:s uppdrag gällande teknisk förvaltning av IT-systemet.

Kontrollmoment

Denna kontroll tittar på om RSF:s informationsmängder som lagras i IT-system är fullständigt klassade. Vidare kontrolleras om överensstämmelse finns mellan klassning för tillgänglighet på allvarlig eller betydande nivå och bedömning för kontinuitetskrav.

Kontrollmetod

Kontroll genom rapporter i LISa (vårt IT-stöd för klassning, risk- och sårbarhetsanalyser, incidenthantering, GDPR-hantering och förvaltningsplaner).

Resultat

Förvaltningen har 168 informationsmängder som lagras i IT-system och som ska klassas. Av dessa är det fem som saknar fullständig klassning.

I en jämförelse om överensstämmelse finns mellan tillgänglighet och kontinuitetskrav ses en viss diskrepans. 32 ärenden har klassat tillgänglighetsperspektivet på allvarlig eller betydande nivå. Detta att jämföra med att 43 ärenden har bedömt maximala tiden för bortfall för informationstillgången innan det får allvarliga konsekvenser för verksamheten till 1 dygn.

Analys/slutsats

De flesta av regionstyrelsens ärenden är fullständigt klassade i LISa. Vilken ger förutsättning för arbetet med att säkerställa rätt skyddsnivå.

Däremot när klassningsresultat för tillgänglighetsperspektivet jämförs med bedömning av kontinuitet så ses behov att utveckla analysdelen för kontinuitet. Detta är ett generellt problem. Digitaliseringsavdelningen behöver ta fram en tydlig instruktion för hur man bedömer kontinuitetskrav kopplat till informationssystem.

Åtgärd

Digitaliseringsavdelningen kommer att kontakta de som inte har fullständiga klassningar för åtgärd under 2026.

Digitaliseringsavdelningen tar fram mall och instruktion för verksamheter med kritiska beroenden till informationssystem.

Kontinuitetsplan för IT-system som en kritisk resurs behöver skapas.

Utökad information om kontinuitetsplanering kommer realiseras i nytt systemstöd för LIS (ledningssystem för informationssäkerhet) under 2027.

Kontroll utförd av:

Madeleine Johansson, digitaliseringsavdelningen

Kontrollansvarig:

Antonios Arvanitidis, digitaliseringsdirektör