Bevittning Certifiering av ledningssystem-Informationssäkerhet

Bakgrund

Ackreditering av certifieringsorgan för certifiering av ledningssystem för informationssäkerhet ISO/IEC 27001:2022 (SS-EN ISO/IEC 27001:2023) bygger på STAFS 2020:1, SS-EN ISO/IEC 17021-1:2015, SS-EN ISO/IEC 27006-1:2024 samt relevanta IAF MD-dokument.

Swedac använder sig av en branschindelning i ackrediteringens omfattning för att beskriva områden där kompetens granskas hos certifieringsorganen, och bevittning planeras utifrån denna indelning.

Branschindelning enligt Swedac definition:

- Produktion
- Samhällskritisk verksamhet
- Tjänster
- Telekommunikation, IT- och datatjänster
- Bank, finans och försäkring
- Offentlig förvaltning och utbildning
- Hälso- & sjukvård, sociala tjänster
- Spel- & vadhållning
- Kärnkraft

Beskrivning av bevittningsplanering

Bevittning planeras för varje kluster med minst en bevittning över två ackrediteringscykler. Dock ska minst en bevittning per ackrediteringscykel ske. Under den första ackrediteringscykeln ska samtliga kluster bevittnas.

Frekvensen planeras utifrån riskbedömning kopplat till respektive certifieringsorgan där parametrar som antal revisorer (och andel nya revisorer), antal certifierade företag (och förändringar i antal), förändringar i organisation och processer, utfall av tidigare bedömningar etc vägs in.

Bevittning av någon av branscherna i respektive kluster täcker hela klustret.

Kluster A-B-C kräver bevittning, kluster D kan undantas om det finns ackreditering inom de andra klustren.

Vid initial ackreditering och utökningar gäller:

En bevittning inom ett kluster anses visa kompetens för hela klustret (i kombination med granskning av organets kompetenskriterier och kvalificering för samtliga ansökta branscher i klustret).

Kluster D kan undantas om det finns ackreditering inom de andra klustren.

Certifieringsorganen är inte ålagda att kategorisera sina kunder enligt Swedacs indelning, men behöver visa på korrelationen mellan denna indelning och sin egen kategorisering.

Klusterindelning

Kluster	Ingående branscher enligt Swedacs befintliga definition
A	Telekommunikation, IT- och datatjänster Spel- & vadhållning
B	Samhällskritisk verksamhet Kärnkraft
C	Hälso- & sjukvård, sociala tjänster
D	Produktion Tjänster Bank, finans och försäkring Offentlig förvaltning och utbildning