Mars, 2026

IT-säkerhet i kommunal upphandling 2026

Från kravställning till uppföljning – vad blir avgörande framåt?

SOKIGO
PART OF ADDNODE GROUP

Innehåll

Inledning

IT-säkerhet i kommunal upphandling har blivit en strategisk fråga. Kraven ökar, hotbilden förändras och regelverk som NIS2 skärper förväntningarna på struktur, dokumentation och leverantörsansvar. Samtidigt blir systemen fler, leveranskedjorna mer komplexa och beroendet av externa driftmiljöer större.

I den här miljön räcker det inte att formulera rätt krav i upphandlingsfasen. Säkerhetsarbetet behöver fungera över tid – i dialogen med leverantörer, i uppföljningen av avtal och i de interna processerna.

För att få en bild av hur kommuner hanterar dessa frågor i praktiken har vi tagit del av hur ett hundratal svenska kommuner beskriver sitt arbete med IT-säkerhet vid offentlig upphandling och efter införande av digitala system. Denna sammanställning lyfter de mönster som framträder och pekar på vad som verkar bli avgörande framåt.

Syftet är att bidra med en aktuell nulägesbild och ge underlag för reflektion i det egna arbetet.

Kravställning är inte längre den svåra delen

De flesta kommuner har i dag en etablerad struktur för upphandling. Ramverk som KLASSA och ISO 27001 används som grund. Kraven är ofta genomarbetade men utmaningen ligger inte i att formulera rätt krav. Den ligger i att följa upp dem konsekvent över tid och det är här skillnaderna blir tydliga.

Uppföljningen är nästa steg

När systemen är införda varierar graden av systematisk uppföljning. Dialog finns ofta, men formaliserade kontroller är mindre vanliga. Det innebär att säkerhetsarbetet riskerar att bli starkt i upphandlingsfasen – och svagare i förvaltningsfasen.

För kommuner blir frågan därför inte bara:

Vad ställde vi för krav?

utan snarare:

Hur säkerställer vi att de fortsatt efterlevs?

ISO 27001 är en baslinje, inte ett mål

ISO 27001 spelar en viktig roll i kommunernas bedömning av leverantörer. Certifiering signalerar struktur, kunskap och extern granskning. I en tid där NIS2 ställer ökade krav på dokumentation och systematik blir detta en tydlig startpunkt. Ett certifikat ersätter dock inte behovet av transparens och löpande dialog.

Leveranskedjan har blivit synlig

Kommunerna tittar inte längre enbart på den direkta leverantören. Frågor om underleverantörer, driftmiljöer och beroenden är i dag en del av riskbedömningen.

Säkerhet är inte isolerad till ett system, den är en fråga om hela ekosystemet.

Driftvalen är strategiska

Molntjänster erbjuder skalbarhet och kompetens. Egen drift kan ge rådighet och kontroll. Båda alternativen innebär avvägningar.

Det finns ingen entydig riktning. Men det finns ett gemensamt behov av tydlighet kring ansvar och uppföljning, oavsett driftmodell.

Vad blir avgörande framåt?

Utifrån nulägesbilden är tre saker centrala:

1. Säkerhetskrav måste följas upp strukturerat över tid.
2. Leverantörer behöver arbeta transparent med sin leveranskedja.
3. NIS2 kräver processförändring – inte bara teknik.

Det är här samverkan mellan kommun och leverantör blir avgörande.

Hur kan vi bidra?

Som leverantör behöver vi kunna erbjuda mer än funktionalitet. Det handlar om:

- Tydlig dokumentation av vårt säkerhetsarbete
- Strukturerad dialog kring uppföljning
- Transparens i leveranskedjan
- Förmåga att stödja kommuner i NIS2-arbetet

Om underlaget

Den här sammanställningen bygger på en undersökning som genomfördes av EB Affärspartner AB på uppdrag av Sokigo under hösten 2025. Syftet var att få en tydligare bild av hur kommuner i praktiken arbetar med IT-säkerhet vid offentlig upphandling och efter att systemen är införda.

Underlaget baseras på samtal och telefonintervjuer med representanter från omkring 100 svenska kommuner, främst inom IT, informationssäkerhet och digitalisering.

Intervjuerna har utgått från gemensamma frågeområden, med utrymme för fördjupning där det behövts. Svaren har anonymiserats och analyserats tematiskt för att synliggöra återkommande mönster.

Frågeområden

1. Upphandling och kravställning

- Använder ni SKR:s verktyg KLASSA eller motsvarande metodstöd vid upphandling av digitala system?
- Hur ser era rutiner ut om ni inte använder KLASSA?
- Hur kravställer ni kring IT-säkerhet vid upphandling?

2. Uppföljning efter införande

- Kontrollerar ni i efterhand att leverantörens lösning motsvarar de krav som ställdes i upphandlingen?
- Hur sker uppföljningen i praktiken?
- Har ni en struktur för löpande leverantörsuppföljning?

3. ISO 27001

- Hur väl känner ni till ISO 27001 och vad certifieringen innebär?
- Hur viktigt är det för er att leverantörer är ISO 27001-certifierade?

- Hur säkerställer ni säkerhetsarbete om leverantören inte är certifierad?

4. Leverantörsdialog och ansvar

- Diskuterar ni regelbundet IT-säkerhet med era leverantörer?
- Hur ser dialogen ut kring leverantörens eget säkerhetsarbete?
- Hur arbetar ni för att säkerställa ansvar i leveranskedjan?

5. NIS2 och framtida krav

- Hur väl känner ni till NIS2 och dess påverkan på kommuner?
- Hur bedömer ni att NIS2 kommer att förändra er kravställning?
- Har ni en strategi för att säkerställa att leverantörer lever upp till kommande krav?

6. Riskmedvetenhet och beredskap

- Hur ser ni på risken för cyberangrepp mot den egna organisationen?
- Vad gör ni för att minska risk och sårbarhet?
- Hur arbetar ni med kontinuitet och återställning?

7. Driftmodeller och framtidsperspektiv

- Hur ser ni på drift hos leverantör jämfört med egen drift?
- Tror ni att ni om fem år har fler eller färre system driftade hos leverantör?
- Vad påverkar era vägval framåt?