ISO/IEC 27001:2022 + Amd 1:2024 Ledningssystem för informationssäkerhet (ISMS)

Informationssäkerhet, ISMS, certifierbar i hela världen

181 krav. Det går att certifiera sig mot denna standard hos ett ackrediterat certifieringsorgan. Utgåva 07/2026.

ISO/IEC 27001 fastställer kraven på ett ledningssystem för informationssäkerhet: riskbaserat, dokumenterat och med påvisad verkan. En prövning mot standarden är en ackrediterad certifieringsrevision i två steg (dokumentgranskning och därefter prövning av verkan på plats), följd av årliga uppföljningsrevisioner och omcertifiering efter tre år.

Företag	Datum	Upprättad av

4 Organisationens kontext 8

4.1-1 **De externa och interna frågor som påverkar organisationens förmåga att uppnå de avsedda resultaten av ISMS är fastställda och hålls aktuella.**

Vad som styrker det: Belagt genom en kontextanalys, antingen som ett eget dokument eller som ett avsnitt i ISMS-handboken: marknadsläge, kunder och avtal, rättslig ram (GDPR, NIS2), teknikplattform, personalstyrka, beroende av molnleverantörer. För en liten verksamhet räcker en tabell på en sida med datum och en cykel för genomgång, förutsatt att ledningens genomgång visar att den verkligen uppdateras.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.1-2 **Organisationen har fastställt om klimatförändringar är en relevant fråga för den. Slutsatsen är motiverad, oavsett om svaret är ja eller nej.**

Vad som styrker det: Kravet infördes genom Amd 1:2024 och revisorer frågar särskilt efter det. Håll en egen rad i kontextanalysen: värmeperioder som påverkar serverrum och tillgänglighet, extremväder som påverkar molnleverantörernas datacenter, elnätets stabilitet. Ett motiverat resultat som lyder inte relevant är godtagbart, en saknad post är det inte.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.2-1 **De intressenter som är relevanta för ISMS är fastställda.**

Vad som styrker det: Intressentlista med kunder, personal, personuppgiftsbiträden och underbiträden, tillsynsmyndigheter, försäkringsgivare, certifieringsorganet och ägare. I en liten verksamhet räcker en tabell med part, förväntan och källa till förväntan.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.2-2 **De relevanta kraven från dessa intressenter är fastställda, inklusive eventuella krav som rör klimatförändringar.**

Vad som styrker det: Ange den konkreta källan för varje part: avtalsklausul, personuppgiftsbiträdesavtal, kundfrågeformulär, rättslig skyldighet. Amd 1:2024 lägger till en anmärkning om att intressenter kan ha krav som rör klimatförändringar. Det är inget eget tvingande krav, men revisorer tar regelmässigt upp det, till exempel hållbarhetsfrågor i en stor kunds leverantörsrevision. En rad i intressenttabellen med resultatet, även om resultatet är inga sådana krav, räcker.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.2-3 **Det är beslutat och spårbart vilka av dessa krav som hanteras genom ISMS.**

Vad som styrker det: Lägg till en kolumn i intressenttabellen som pekar på den regel som hanterar kravet (policy, säkerhetsåtgärd, avtalsbilaga). Det visar att kraven inte bara samlats in utan också behandlats.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.3-1 **Omfattningen av ISMS är fastställd och tar hänsyn till frågorna i 4.1, kraven i 4.2 samt gränssnitt och beroenden till verksamhet som utförs av tredje part.**

Vad som styrker det: Omfattningen anger orter, organisatoriska enheter, produkter, system och nätverksgränser. Utlagda delar (drift, betalleverantörer, support) beskrivs som gränssnitt med en tydlig ansvarsgräns. En konstlat snäv omfattning som skär bort kärnprocesser underkänns av certifieringsorganen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.3-2 **Omfattningen finns tillgänglig som dokumenterad information och anger gränserna för ISMS entydigt.** Dokument

Vad som styrker det: Ett godkänt omfattningsdokument med version, datum och underskrift av högsta ledningen. Dess exakta ordalydelse hamnar senare på certifikatet, så formulera den precist och så att den tål att citeras offentligt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

4.4-1 **ISMS, inklusive de processer som behövs och deras samspel, är upprättat, infört, underhållet och ständigt förbättrat.**

Vad som styrker det: En processkarta eller processlista som kopplar samman riskhantering, incidenthantering, ändringshantering, revision och ledningens genomgång med ansvariga och frekvens. Levande bevis väger tyngre än diagrammet: ärenden, protokoll, kalenderposter.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5 Ledarskap 8

5.1-1 **Högsta ledningen tar ansvar för verkan hos ISMS och säkerställer att policyn och målen är fastställda och förenliga med den strategiska inriktningen.**

Vad som styrker det: Bevis är bland annat undertecknade godkännanden av policyn, omfattningen och uttalandet om tillämplighet, protokoll från ledningens genomgång och dokumenterade budgetbeslut. I en mycket liten verksamhet är högsta ledningen ofta samma person som den ansvarige för ISMS, vilket är godtagbart men måste anges öppet i rollbeskrivningen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.1-2 **Kraven i ISMS är integrerade i verksamhetsprocesserna och betydelsen av verkningsfull informationssäkerhet kommuniceras.**

Vad som styrker det: Visas bäst där säkerheten inte är en egen pärm: ett säkerhetskriterium i definition of done, en säkerhetskontroll i försäljningsprocessen eller inköpsprocessen, en återkommande säkerhetspunkt i protokoll från teammöten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.1-3 **Ledningen tillhandahåller nödvändiga resurser, stöder de personer som bidrar till verkan hos ISMS och främjar ständig förbättring.**

Vad som styrker det: Godkänd säkerhetsbudget, avsatt tid för utbildning, anlitande av externa revisorer eller penetrationstestare. Ett förbättringsregister eller åtgärdsregister med poster över flera kvartal visar kontinuitet i stället för en engångsinsats.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.2-1 **En informationssäkerhetspolicy är fastställd som passar organisationens syfte och ger ett ramverk för målen för informationssäkerhet.** Dokument

Vad som styrker det: Ett kort godkänt policydokument, två till tre sidor räcker. Det anger skyddsmålen, omfattningen, ansvaret och principen om ett riskbaserat arbetssätt. Generisk malltext utan koppling till den verkliga verksamheten sticker ut i revisionen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.2-2 **Policyn innehåller ett åtagande att uppfylla tillämpliga krav och ett åtagande om ständig förbättring av ISMS.** Dokument

Vad som styrker det: Båda åtagandena måste finnas som uttryckliga meningar i policyn, och de läses ord för ord i revisionens steg 1. Hänvisa dessutom till de bakomliggande processerna (lagregister, förbättringsregister).

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.2-3 **Policyn är kommunicerad inom organisationen och finns tillgänglig för intressenter i den utsträckning det är lämpligt.** Dokument

Vad som styrker det: Bevis genom en post på intranät eller wiki med läskrav, en introduktionschecklista med bekräftelse eller en publicerad sammanfattning på webbplatsen. En sändlista med kvitterade mottagningar är det enklaste hållbara beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.3-1 **Ansvar och befogenheter för säkerhetsrelevanta roller är fördelade och kommunicerade inom organisationen.**

Vad som styrker det: En rollmatris (RACI) som täcker den ansvarige för ISMS, riskägare, tillgångsägare, incidentsamordnaren och kontaktpersonen för dataskydd. I enmansverksamheter och mycket små team fördelas varje roll till en namngiven person och den ansamling av roller som blir följden dokumenteras öppet i stället för att döljas.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.3-2 **Befogenheten att säkerställa att ISMS uppfyller standarden och att rapportera om prestandan hos ISMS till högsta ledningen är fördelad till en roll.**

Vad som styrker det: Ett utnämningsbrev eller en rollbeskrivning för den ansvarige för ISMS med en uttrycklig rapporteringsväg till ledningen. Rapporteringsvägen måste verkligen kunna beläggas med protokoll från ledningens genomgång.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6 Planering 21

6.1.1-1 **Med utgångspunkt i frågorna i 4.1 och kraven i 4.2 är de risker och möjligheter som behöver hanteras fastställda, så att ISMS uppnår sina avsedda resultat och oönskade effekter förebyggs.**

Vad som styrker det: Ett register som kopplar kontextfrågor till risker och möjligheter, fört antingen separat eller inne i riskregistret. Det viktiga är spårbarheten: varje fråga från kontextanalysen leder synligt till en bedömning eller till ett motiverat beslut att inte beakta den.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.1-2 **Åtgärderna för att hantera dessa risker och möjligheter är planerade, integrerade i processerna i ISMS, och deras verkan utvärderas.**

Vad som styrker det: Åtgärdsplan med ansvarig, slutdatum och kriterium för verkan. Håll utvärderingen av verkan som en egen kolumn, annars saknar revisionen bevis för att åtgärden inte bara genomfördes utan också verifierades.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-1 **En process för riskbedömning av informationssäkerhet är fastställd och tillämpad; den innehåller kriterier för riskacceptans och kriterier för när riskbedömningar genomförs.** Dokument

Vad som styrker det: En policy för riskhantering med skalor för sannolikhet och konsekvens, en fastställd riskmatris och en tydlig acceptansnivå. Nivån måste vara ett tal eller en zon, inte en formulering som efter eget omdöme.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-2 **Processen ger vid upprepade riskbedömningar resultat som är samstämmiga, giltiga och jämförbara.**

Vad som styrker det: Belagt genom en fast metodik med fastställda skalor och genom jämförelse av två versioner av bedömningen: samma risker, samma bedömningslogik, förklarbara skillnader. En daterad version av förra årets riskregister är det starkaste beviset här.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-3 **Riskerna för informationssäkerheten är identifierade för att upptäcka förlust av konfidentialitet, riktighet och tillgänglighet inom omfattningen, och varje risk har en tilldelad riskägare.**

Vad som styrker det: Riskregister med hänvisning till tillgångar eller processer, de tre skyddsmålen och en namngiven riskägare. Riskägaren måste ha befogenhet att acceptera risken; i en liten verksamhet är det normalt den verkställande direktören.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-4 **De identifierade riskerna är analyserade: möjliga konsekvenser, realistisk sannolikhet och den risknivå som följer av dem är fastställda.**

Vad som styrker det: Kolumner för konsekvens, sannolikhet och resulterande risknivå, var och en med en kort motivering. En mening med resonemang per risk förhindrar det vanligaste revisionsresultatet, nämligen siffror utan härledning.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-5 **Riskerna är jämförda mot acceptanskriterierna och prioriterade för behandling.**

Vad som styrker det: Riskregistret måste visa vilka risker som ligger över acceptansnivån och i vilken ordning de behandlas. En sorterad vy eller en prioritetskolumn räcker.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.2-6 **Processen för riskbedömning finns tillgänglig som dokumenterad information.** Dokument

Vad som styrker det: Metodiken i sig är ett obligatoriskt dokument, inte bara dess resultat. En godkänd policy med version och godkännandedatum, länkad från dokumentförteckningen för ISMS.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-1 **För varje risk över acceptansnivån är ett lämpligt behandlingsalternativ valt (minska, undvika, överföra eller acceptera).**

Vad som styrker det: En kolumn för behandlingsalternativ i riskregistret. Där en risk accepteras dokumenteras motiveringen och riskägarens formella godkännande; där den överförs anges avtalet eller försäkringen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-2 **Alla säkerhetsåtgärder som behövs för att genomföra de valda alternativen för riskbehandling är fastställda.**

Vad som styrker det: Formulera säkerhetsåtgärderna konkret och verifierbart, med ansvarig och slutdatum. Att hänvisa till tekniskt arbete som redan pågår (införande av MFA, test av säkerhetskopiering) går bra så länge det pekar på ett ärende eller en konfigurationsartefakt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-3 **De fastställda säkerhetsåtgärderna är jämförda med säkerhetsåtgärderna i bilaga A för att verifiera att ingen nödvändig åtgärd har förbisetts.**

Vad som styrker det: Jämförelsen är ett eget spårbart steg, inte en biprodukt. Belagt genom en mappningskolumn i riskregistret som hänvisar till numren i bilaga A, plus daterat protokoll från jämförelsen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-4 **Ett uttalande om tillämplighet (SoA) finns. Det bedömer alla 93 säkerhetsåtgärder i bilaga A var för sig, anger tillämplighet med motivering för varje åtgärd, status för införandet och motiveringen till varje undantag.** Dokument

Vad som styrker det: SoA är det centrala obligatoriska dokumentet och kartan över hela revisionen. Det måste vara fullständigt: säkerhetsåtgärder som inte är tillämpliga finns också med, med en motivering, aldrig som en tom rad. Rekommenderade kolumner: åtgärdens nummer, titel, tillämplig ja eller nej, motivering, status för införandet, hänvisning till policy eller bevis, koppling till risken. Version och ledningens godkännande är obligatoriska, eftersom SoA stäms av mot verkligheten vid varje uppföljningsrevision.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-5 **En plan för riskbehandling är framtagen som samlar säkerhetsåtgärder, ansvar, slutdatum och nödvändiga resurser.** Dokument

Vad som styrker det: Det kan vara en flik i riskkalkylen eller en projekttavla. Det som räknas är att datumen är realistiska och att missade datum synligt planerades om, eftersom det är precis vad revisorn kontrollerar.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-6 **Planen för riskbehandling är godkänd av riskägarna och de kvarvarande restriskerna är formellt accepterade av dem.** Dokument

Vad som styrker det: Underskrift, elektroniskt godkännande eller ett daterat beslut i protokoll. En rad i protokollet från ledningens genomgång med hänvisning till registrets version räcker, förutsatt att versionen är entydig.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.1.3-7 **Processen för riskbehandling finns tillgänglig som dokumenterad information.** Dokument

Vad som styrker det: Täcks vanligen i samma policydokument som riskbedömningen. Flödet från bedömning via val av alternativ till acceptans av restrisk måste vara beskrivet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.2-1 **Mål för informationssäkerhet är fastställda för relevanta funktioner och nivåer, är förenliga med policyn och är mätbara där det är praktiskt möjligt.**

Vad som styrker det: Ett målblad med tre till sex mål, vart och ett med ett nyckeltal, en baslinje, ett målvärde och ett slutdatum. Exempel: andelen system med MFA höjd från 80 till 100 procent till kvartalets slut. Mål utan ett tal räknas som inte mätbara.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.2-2 **Målen tar hänsyn till de tillämpliga kraven på informationssäkerhet samt till resultaten av riskbedömning och riskbehandling.**

Vad som styrker det: Lägg till en ursprungskolumn i målbladet: vilken risk, vilket kundkrav eller vilket lagkrav målet kommer från. Det förhindrar mål som ser godtyckliga ut.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.2-3 **Målen övervakas, kommuniceras och uppdateras vid behov.**

Vad som styrker det: Kvartalsvis uppföljning i målbladet plus kommunikation till teamet, till exempel en kort notis i wikin eller en punkt på dagordningen för teammötet. Historiska versioner visar att uppdateringar sker.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.2-4 **Målen för informationssäkerhet finns tillgängliga som dokumenterad information.** Dokument

Vad som styrker det: Ett godkänt måldokument med datum räcker. Det får ingå i ledningens genomgång, men det måste finnas där som ett eget avsnitt som går att hitta.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.2-5 **För varje mål är det planerat vad som görs, vilka resurser som krävs, vem som är ansvarig, när det är klart och hur resultaten utvärderas.**

Vad som styrker det: Dessa fem punkter är verifierbara var för sig och efterfrågas var för sig i revisionen. Lägg upp dem som fem kolumner i målbladet, då syns överensstämmelsen med en blick.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

6.3-1 **Där organisationen fastställer att ändringar i ISMS behövs, genomförs dessa ändringar på ett planerat sätt.**

Vad som styrker det: Belagt genom ändringsbegäran, protokoll eller ärenden som visar orsaken, konsekvensbedömningen, godkännandet och införandet. Typiska orsaker i en liten verksamhet: byte av molnleverantör, nya orter, den första anställningen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7 Stöd 15

7.1-1 **De resurser som behövs för att upprätta, införa, underhålla och ständigt förbättra ISMS är fastställda och tillhandahållna.**

Vad som styrker det: En budgetpost för säkerhet, verktygslicenser (lösenordshanterare, MDM, loggplattform), planerade persondagar för att sköta ISMS och externa revisionstjänster. En faktura eller ett budgetgodkännande visar detta snabbare än någon text.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.2-1 **Den nödvändiga kompetensen hos de personer vars arbete påverkar prestandan inom informationssäkerhet är fastställd.**

Vad som styrker det: Kompetensmatris eller rollprofiler som anger vilken kunskap som krävs per roll, till exempel säker utveckling för utvecklare, incidenthantering för samordnaren. I mycket små team räcker en rad per person.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.2-2 **Kompetensen är säkerställd genom lämplig utbildning, träning eller erfarenhet.**

Vad som styrker det: Certifikat, kursintyg, meritförteckningar eller dokumenterad praktisk erfarenhet. Självstudier är godtagbara om de är belagda, till exempel med intyg om genomförda nätkurser eller med godkända interna kunskapstester.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.2-3 **Där kompetensbrister finns har åtgärder vidtagits för att täcka dem och verkan av dessa åtgärder har utvärderats.**

Vad som styrker det: Utbildningsplan med jämförelse mellan mål och utfall och en kontroll av verkan, till exempel ett testresultat, klickfrekvensen i en nätfiskesimulering eller observation i arbetet. Kontrollen av verkan glöms ofta bort och är en klassisk mindre avvikelse.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.2-4 **Lämplig dokumenterad information finns tillgänglig som bevis på kompetens.** Dokument

Vad som styrker det: En mapp för kompetens och utbildning per person med bevis och datum. I en liten verksamhet räcker en katalog med sparade PDF-dokument plus en översiktstabell.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.3-1 **De personer som arbetar inom omfattningen är medvetna om informationssäkerhetspolicyn.**

Vad som styrker det: Bekräftelse vid introduktion och efter varje ändring av policyn, med datum och version. En läskvittensfunktion i wikin eller en undertecknad lista räcker.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.3-2 **Personerna känner till sitt eget bidrag till verkan hos ISMS och nyttan med förbättrad prestanda inom informationssäkerhet.**

Vad som styrker det: Utbildningsmaterial och närvarolistor där kopplingen till det egna arbetet syns. Revisorer intervjuar personalen direkt, så utbilda med konkreta vardagsexempel i stället för abstrakta citat ur standarden.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.3-3 **Personerna känner till följderna av att inte uppfylla kraven i ISMS.**

Vad som styrker det: Ange följderna i utbildningsmaterial och arbetsinstruktioner och koppla dem till processen under A.6.4. Även verksamheter utan anställda måste täcka detta för uppdragstagare och frilansare genom deras avtal.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.4-1 **Intern och extern kommunikation som är relevant för ISMS är fastställd: vad som kommuniceras, när, med vem och på vilket sätt.**

Vad som styrker det: En kommunikationsmatris med rader som säkerhetsincident till kunder, anmälan till tillsynsmyndigheten inom 72 timmar, månatlig statusrapport till ledningen. Den är grunden för kriskommunikationen och ses över efter varje incident.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.5.1-1 **ISMS omfattar den dokumenterade information som standarden kräver samt den dokumenterade information som organisationen har fastställt som nödvändig för verkan hos ISMS.** Dokument

Vad som styrker det: En dokumentförteckning som listar varje ISMS-dokument med syfte, ansvarig, version och lagringsplats. Den visar att de obligatoriska dokumenten är fullständiga och är den snabbaste ingången för revisorn.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.5.2-1 **Vid framtagning och uppdatering av dokument är lämplig identifiering, lämpligt format och lämpligt medium säkerställda, och dokumenten är granskade och godkända som lämpliga.**

Vad som styrker det: Ett enhetligt dokumenthuvud med titel, version, datum, författare och godkännare. I Git-baserade miljöer uppfyller granskade pull requests med godkännande kravet på granskning och godkännande, förutsatt att historiken inte går att ändra.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.5.3-1 **Den dokumenterade informationen finns tillgänglig och är användbar där och när den behövs.**

Vad som styrker det: En central lagringsplats som alla behöriga når, med sökfunktion. Går att pröva med stickprov: vilken arbetsinstruktion som helst måste gå att hitta på under en minut.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

7.5.3-2 **Den dokumenterade informationen är tillräckligt skyddad, särskilt mot förlust av konfidentialitet, felaktig användning och förlust av riktighet.**

Vad som styrker det: Rollbaserade behörigheter till ISMS-dokumenten, versionshantering med historik, skrivskydd för godkända versioner och säkerhetskopiering av dokumentarkivet. Beviset för säkerhetskopieringen är den del som oftast glöms bort.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

7.5.3-3 **Distribution, åtkomst, återsökning, lagring, ändringsstyrning samt bevarande och gallring av dokumenterad information är styrda.**

Vad som styrker det: En kort regel för dokumentstyrning med bevarandetider och gallringsregler. Den måste stämmas av mot rättsliga skyldigheter (bokföringslagen, skattelagstiftningen, GDPR) och är grunden för A.5.33 och A.8.10.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

7.5.3-4 **Extern dokumenterad information som är nödvändig för att planera och driva ISMS är identifierad och styrd.**

Vad som styrker det: En lista över externa dokument med version och källa: standarder, författningstexter, härdningsguider från tillverkare, dokumentation om molnsäkerhet, personuppgiftsbiträdesavtal. Utan versionshänvisning går styrningen inte att visa.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8 Verksamhet 8

8.1-1 **De processer som behövs för att uppfylla kraven på informationssäkerhet och för att genomföra åtgärderna från avsnitt 6 är planerade, införda och styrda, och kriterier för dessa processer är fastställda.**

Vad som styrker det: En drifthandbok eller runbooks med tydliga kriterier, till exempel längsta tid för att installera kritiska säkerhetsuppdateringar, kriterier för release vid driftsättning, larmtrösklar. Kriterier utan tal är värdelösa i revisionen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8.1-2 **Det finns dokumenterad information i den omfattning som behövs för att ge förtroende för att processerna har genomförts som planerat.** Dokument

Vad som styrker det: Redovisande dokument från driften som bevis: ärendehistorik, körningar i CI-kedjan, rapporter om säkerhetsuppdateringar, loggar från säkerhetskopiering, genomgångar av behörigheter. Dessa redovisande dokument är det egentliga beviset för verkan i revisionens steg 2.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8.1-3 **Planerade ändringar är styrda och följderna av oavsiktliga ändringar ses över; där det behövs mildras negativa effekter.**

Vad som styrker det: En ändringsprocess med godkännande och en väg tillbaka, kopplad till A.8.32. För oavsiktliga ändringar (felkonfiguration, oavsiktlig utökning av behörighet) dokumenteras händelsen och rättelsen beläggs.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8.1-4 **Externt tillhandahållna processer, produkter och tjänster som är relevanta för ISMS är fastställda och styrda.**

Vad som styrker det: En lista över leverantörerna med kritikalitet, avtalshänvisning och läget för bevisen (leverantörens certifikat enligt ISO 27001, SOC 2-rapport, personuppgiftsbiträdesavtal). För en liten verksamhet är detta den största hävstången, eftersom merparten av tekniken ändå drivs externt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

8.2-1 **Riskbedömningar genomförs med planerade intervall och när betydande ändringar eller incidenter inträffar, med hänsyn till de fastställda kriterierna.**

Vad som styrker det: En rytm (vanligen årlig) plus fastställda utlösande händelser för bedömningar utanför planen. Belagt genom daterade versioner av riskregistret och poster i kalendern eller ärendesystemet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.2-2 **Resultaten av riskbedömningarna sparas som dokumenterad information.** Dokument

Vad som styrker det: Historiska versioner av riskregistret med datum, inte bara det aktuella läget. Att skriva över filen gör utvecklingen omöjlig att visa; versionshantering i filsystemet eller i Git löser det.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.3-1 **Planen för riskbehandling är genomförd.**

Vad som styrker det: Jämför plan mot verklighet: avslutade åtgärder med införandedatum och en konkret artefakt (konfiguration, policy, avtal). Öppna åtgärder behöver en dokumenterad motivering och ett nytt måldatum.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.3-2 **Resultaten av riskbehandlingen sparas som dokumenterad information.** Dokument

Vad som styrker det: Statusrapporter eller avslutade åtgärdsposter med hänvisning till beviset. Registret ensamt räcker om varje rad bär ett avslutsdatum och en länk till beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9 Utvärdering av prestanda 21

9.1-1 **Det är fastställt vad som behöver övervakas och mätas, inklusive processerna och säkerhetsåtgärderna för informationssäkerhet.**

Vad som styrker det: Ett nyckeltalsblad med ett hanterbart antal stabila mått: eftersläpning i säkerhetsuppdateringar, täckning för MFA, tid för att lösa incidenter, resultatet av det senaste återläsningstestet, öppna avvikelser. Några få nyckeltal som verkligen samlas in slår en lång önskelista.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.1-2 **Metoderna för övervakning, mätning, analys och utvärdering är fastställda och ger giltiga resultat.**

Vad som styrker det: Dokumentera datakällan och beräkningen för varje nyckeltal, till exempel en export från sårbarhetsskannern eller från identitetsleverantörens rapport. Spårbarheten till källan är kärnan i giltigheten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.1-3 **Det är fastställt när och av vem övervakning och mätning genomförs och när resultaten analyseras och utvärderas.**

Vad som styrker det: Lägg till kolumner för frekvens och ansvarig i nyckeltalsbladet. En återkommande kalenderbokning för utvärderingen visar regelbundenheten bättre än någon beskrivning.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.1-4 **Resultaten av övervakning och mätning sparas som dokumenterad information.** Dokument

Vad som styrker det: Arkiverade utvärderingar, exporterade instrumentpaneler eller ett nyckeltalsblad som förs som en tidsserie. En livevy utan historik uppfyller inte kravet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.1-5 **Prestandan inom informationssäkerhet och verkan hos ISMS utvärderas utifrån mätresultaten.**

Vad som styrker det: En skriftlig utvärdering, inte bara siffror: trend, orsaker, åtgärdsbehov. Denna utvärderingstext är samtidigt ett underlag till ledningens genomgång.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.1-1 **Internrevisioner genomförs med planerade intervall och ger information om huruvida ISMS uppfyller organisationens egna krav och kraven i standarden och är infört på ett verkningsfullt sätt.**

Vad som styrker det: Före certifieringsrevisionen måste minst en fullständig cykel av internrevision som täcker hela omfattningen vara avslutad. Utan den är certifiering utom räckhåll; det är ett av de vanligaste hindren vid en första certifiering.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.2-1 **Ett revisionsprogram är planerat, upprättat och underhållet; det fastställer frekvens, metoder, ansvar, planeringskrav och rapportering, och det beaktar betydelsen av berörda processer och resultaten från tidigare revisioner.**

Vad som styrker det: Ett flerårigt revisionsprogram som täcker alla avsnitt och alla tillämpliga säkerhetsåtgärder över certifieringscykeln, med högre frekvens för kritiska områden. En enkel tabell över tre år räcker gott.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.2-2 **Revisionskriterier och revisionens omfattning är fastställda för varje revision.**

Vad som styrker det: En revisionsplan per datum med kriterierna (standarden, interna policyer, avtal) och en tydlig omfattning. En revisionsplan på en sida per revision räcker och fungerar samtidigt som underlag för rapporten.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.2-3 **Revisorer är utsedda och revisioner genomförs på ett sätt som säkerställer objektivitet och opartiskhet. Ingen reviderar sitt eget arbete.**

Vad som styrker det: Oberoendet är den svåra tröskeln här: den som skrivit policyerna och konfigurerat systemen får inte revidera dem. I en mycket liten verksamhet betyder det nästan alltid en extern internrevisor, till exempel en anlitad konsult eller en kollega från ett partnerföretag; ett revisionsavtal plus revisorns försäkran om oberoende är beviset. Bara i tillräckligt stora team kan rollen roteras internt till en person utan ansvar för det område som revideras, och det måste då framgå av rollmatrisen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.2-4 **Revisionsresultaten rapporteras till berörd ledning.**

Vad som styrker det: En revisionsrapport med revisionsresultat, avvikelser, rekommendationer och en sändlista, plus bevis på överlämnandet till ledningen, till exempel en protokollförd punkt eller ett daterat överlämnande via e-post.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.2.2-5 **Revisionsprogrammet och revisionsresultaten sparas som dokumenterad information.** Dokument

Vad som styrker det: Håll revisionsprogrammet, revisionsplanerna, revisionsrapporterna och de åtgärder som följer på ett ställe. Kopplingen från ett revisionsresultat till en korrigerande åtgärd (avsnitt 10.2) måste synas hela vägen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.1-1 **Högsta ledningen går igenom ISMS med planerade intervall för att säkerställa dess fortsatta lämplighet, tillräcklighet och verkan.**

Vad som styrker det: Minst en gång per år och inplanerat före den externa revisionen. Även i en mycket liten verksamhet måste det finnas daterade och undertecknade protokoll, även när ledningen och den ansvarige för ISMS är samma person.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-1 **Ledningens genomgång beaktar status för åtgärder från tidigare genomgångar.**

Vad som styrker det: Protokollet inleds med en uppföljningstabell över förra årets beslut och deras aktuella status. Utan denna återkoppling räknas genomgången som ofullständig.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-2 **Ledningens genomgång beaktar ändringar i de externa och interna frågor som är relevanta för ISMS, inklusive relevanta aspekter av klimatförändringar.**

Vad som styrker det: En egen punkt på dagordningen som hänvisar till den uppdaterade kontextanalysen. Klimatförändringar nämns inte uttryckligen i texten till detta avsnitt (Amd 1:2024 ändrar bara 4.1 och 4.2), men de kommer in här genom ändringar i frågorna under 4.1 och revisorer förväntar sig det. Även ett resultat som lyder inte relevant, oförändrat hör hemma i protokollet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-3 **Ledningens genomgång beaktar ändringar i intressenternas behov och förväntningar som är relevanta för ISMS.**

Vad som styrker det: Nya kundkrav från avtal och säkerhetsfrågeformulär, nya rättsliga skyldigheter, krav från certifieringsorganet. Dokumentera dem som en lista med källor i protokollet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-4 **Ledningens genomgång beaktar återkoppling om prestandan inom informationssäkerhet, inklusive avvikelser och korrigerande åtgärder, resultat från övervakning och mätning, revisionsresultat och uppfyllelsen av målen för informationssäkerhet.**

Vad som styrker det: Behandla dessa fyra block som egna punkter på dagordningen, annars saknas något av dem i protokollet i efterhand. Bifoga nyckeltalsbladet, revisionsrapporten och målbladet som bilagor.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-5 **Ledningens genomgång beaktar återkoppling från intressenter.**

Vad som styrker det: Kundklagomål med säkerhetsvinkel, resultat från kundrevisioner, rapporter från visselblåsarkanalen, återkoppling från leverantörer. Dokumentera det i protokollet även när resultatet är att inget inkommit.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

9.3.2-6 **Ledningens genomgång beaktar resultaten av riskbedömningen och status för planen för riskbehandling.**

Vad som styrker det: Bifoga det aktuella riskregistret och status för införandet av behandlingsplanen, med uttrycklig bekräftelse på riskägarnas acceptans av restrisk.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

9.3.2-7 **Ledningens genomgång beaktar möjligheter till ständig förbättring.**

Vad som styrker det: En punkt på dagordningen med konkreta förbättringsidéer och ett beslut om var och en. Antagna idéer förs in i förbättringsregistret som poster med slutdatum.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

9.3.3-1 **Resultaten från ledningens genomgång omfattar beslut om möjligheter till ständig förbättring och om eventuella behov av ändringar i ISMS.**

Vad som styrker det: Protokollet avslutas med ett beslutsavsnitt: beslut, ansvarig, slutdatum. Protokoll utan beslut är ett revisionsresultat, eftersom ledningseffekten då saknas.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

9.3.3-2 **Bevis för resultaten från ledningens genomgång sparas som dokumenterad information.** Dokument

Vad som styrker det: Undertecknat protokoll med datum, deltagare, underlag, utvärdering och beslut. Det är ett av de första dokument som ett certifieringsorgan efterfrågar i steg 1.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

10 Förbättring 7

10.1-1 **Lämpligheten, tillräckligheten och verkan hos ISMS förbättras ständigt.**

Vad som styrker det: Ett förbättringsregister som matas från flera källor (revisioner, incidenter, idéer, avvikande nyckeltal) med synliga framsteg över tid. Kontinuiteten över flera månader är beviset, inte antalet poster.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

10.2-1 **När en avvikelse inträffar reagerar organisationen på den: den styr och korrigerar avvikelsen och hanterar följderna.**

Vad som styrker det: En avvikelserapport med en omedelbar åtgärd och ett datum. Källorna är internrevisioner, externa revisioner, incidenter och observationer i den dagliga driften; alla matar samma register.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

10.2-2 **Det är utvärderat om åtgärder behövs för att undanröja orsakerna så att avvikelsen inte återkommer eller uppstår någon annanstans; detta omfattar en kontroll av om liknande avvikelser finns eller kan uppstå.**

Vad som styrker det: Dokumentera grundorsaksanalysen, till exempel med 5 varför eller Ishikawa, plus ett uttryckligt uttalande om överförbarheten till andra system eller processer. Steget om överförbarhet är det som oftast hoppas över.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

10.2-3 **Nödvändiga korrigerande åtgärder är genomförda och deras verkan ses över.**

Vad som styrker det: Dokumentera för varje åtgärd införandedatumet, bevisartefakten och en senare kontroll av verkan med eget datum. Två datumfält per rad är det enklaste sättet att inte tappa bort kontrollen av verkan.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

10.2-4 **Där det behövs görs ändringar i ISMS till följd av avvikelsen.**

Vad som styrker det: Om en avvikelse går tillbaka på en lucka i en policy, i riskregistret eller i SoA måste ändringen bli synlig där. En hänvisning från avvikelsen till den uppdaterade dokumentversionen sluter kedjan.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

10.2-5 **Korrigerande åtgärder står i proportion till effekterna av de avvikelser som uppstått.**

Vad som styrker det: En allvarlighetsgradering i registret som gör åtgärdens proportionalitet tydlig. Varken småsaker som drivs som projekt eller allvarliga avvikelser som besvaras med enbart ett påminnelsemejl.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

10.2-6 **Avvikelsernas art, de åtgärder som vidtagits och resultaten av de korrigerande åtgärderna sparas som dokumenterad information.** Dokument

Vad som styrker det: Ett register över avvikelser och korrigerande åtgärder med kolumner för art, orsak, åtgärd, ansvarig, slutdatum och resultatet av kontrollen av verkan. Det är ett obligatoriskt bevis och tas fram vid varje uppföljningsrevision.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5 Bilaga A: Organisatoriska säkerhetsåtgärder 37

A.5.1 **Policyer för informationssäkerhet: En övergripande informationssäkerhetspolicy och ämnesspecifika policyer är fastställda, godkända av ledningen, kommunicerade och ses över med planerade intervall och när betydande ändringar inträffar.** Dokument

Vad som styrker det: En uppsättning policyer med version, godkännandedatum och datum för nästa genomgång, plus bevis på bekräftelse. För en liten verksamhet räcker en ramverkspolicy och en handfull ämnespolicyer (behörigheter, kryptografi, distansarbete, incidenter).

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.2 **Roller och ansvar för informationssäkerhet: Roller och ansvar för informationssäkerhet är fastställda och fördelade efter organisationens behov.**

Vad som styrker det: En rollmatris med namn, ersättare och uppgifter. I en mycket liten verksamhet anges öppet var flera roller samlas hos en person, och detta kopplas till de kompenserande säkerhetsåtgärderna under A.5.3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.3 **Uppdelning av arbetsuppgifter: Uppgifter och ansvarsområden som är avsedda att kontrollera varandra ligger inte hos en enda person. Målet är att ingen på egen hand kan initiera, godkänna och dölja en ändring.**

Vad som styrker det: I en liten verksamhet är full uppdelning strukturellt omöjlig; ett svepande påstående om att kravet är uppfyllt faller genast i revisionsintervjun. Det som håller är en ärlig analys: vilka kombinationer av uppgifter som är kritiska (utveckla och släppa, tilldela behörigheter och använda dem, initiera och godkänna betalningar), vilka av dem som ligger hos en person, och vilka kompenserande säkerhetsåtgärder som gäller. Beprövade grepp är oföränderliga revisionsloggar som en tredje part kommer åt, MFA på privilegierade konton, automatiska grindar i CI och skyddade grenar i stället för granskning enligt fyraögonsprincipen, en periodisk genomgång av loggar av en extern person, och separat godkännande av betalningar. Håll analysen och de kompenserande säkerhetsåtgärderna som ett eget daterat dokument och länka det från SoA.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.4 **Ledningens ansvar: Ledningen kräver att all personal tillämpar informationssäkerhet i linje med fastställda policyer och rutiner.**

Vad som styrker det: Ett åtagande i anställningsavtal och uppdragsavtal, bekräftelse av policyerna vid introduktion och regelbundna påminnelser från ledningen. Bevis: undertecknade åtaganden och mötesprotokoll.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.5 **Kontakt med myndigheter: Lämpliga kontakter med berörda myndigheter upprätthålls och går att nå vid behov.**

Vad som styrker det: En kontaktlista med behörig dataskyddsmyndighet, polis eller enhet för it-brottslighet, den nationella mottagningspunkten för rapportering om cybersäkerhet och, där det ligger inom omfattningen, rapporteringskanaler enligt NIS2. Notera tidsfristerna (som de 72 timmarna enligt GDPR) direkt i listan.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.6 **Kontakt med särskilda intressegrupper: Kontakter med särskilda intressegrupper, säkerhetsforum och branschföreningar upprätthålls.**

Vad som styrker det: Medlemskap, prenumererade säkerhetsmeddelanden (nationell CERT, meddelanden från tillverkare), deltagande i intressegrupper. Ett enkelt bevis: en lista över prenumerationer plus ett exempel på hur ett säkerhetsmeddelande ledde till en åtgärd.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.7 **Hotunderrättelser: Information om hot mot informationssäkerheten samlas in och analyseras för att lämpliga åtgärder ska kunna härledas ur den.**

Vad som styrker det: Nytt i 2022 års version. Genomförbart för en liten verksamhet: prenumerera på säkerhetsmeddelanden från nationell CERT och från tillverkare, och gör sedan en kort månatlig genomgång med ett relevansbeslut och ärenden som följer av det. Beviset är analysen, inte prenumerationen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.8 **Informationssäkerhet i projektledning: Informationssäkerhet är integrerad i projektledningen, oavsett typ av projekt.**

Vad som styrker det: Säkerhetspunkter i projektchecklistan: skyddsbehov, riskgenomgång, dataskyddskontroll, säkerhetsgodkännande före driftsättning. I agila team förankras de som fasta punkter i definition of ready och definition of done.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.9 **Förteckning över information och andra tillhörande tillgångar: En förteckning över information och andra tillhörande tillgångar med namngivna ägare är upprättad och underhållen.**

Vad som styrker det: En tillgångsförteckning som täcker maskinvara, programvara, molntjänster, datalager, domäner och konton, var och en med en ägare och sitt skyddsbehov. I en liten verksamhet kan den sättas ihop automatiskt från en MDM-export, en licenslista och molnkonsolen; ett aktuellt datum är obligatoriskt.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.10 **Godtagbar användning av information och andra tillhörande tillgångar: Regler för godtagbar användning och hantering av information och andra tillhörande tillgångar är identifierade, dokumenterade och införda.** Dokument

Vad som styrker det: En policy för godtagbar användning av enheter, nätverk, molnkonton och AI-verktyg, med bekräftelse. Privata enheter och externa AI-tjänster bör täckas uttryckligen, eftersom det är där merparten av läckaget uppstår.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.11 **Återlämning av tillgångar: När ett anställnings- eller uppdragsförhållande upphör eller ändras är det styrt och skriftligen bekräftat att alla utlämnade enheter, nycklar, konton och dokument återlämnas.**

Vad som styrker det: En checklista för avslut med kvitto på återlämning av bärbar dator, tokens, nycklar, certifikat och lagringsmedier, plus avstängning av konton samma dag. Detta gäller frilansare och praktikanter i lika hög grad.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.12 **Klassificering av information: Information är klassificerad efter sitt skyddsbehov när det gäller konfidentialitet, riktighet, tillgänglighet och lagkrav.**

Vad som styrker det: Ett enkelt schema med tre eller fyra nivåer (offentlig, intern, konfidentiell, strängt konfidentiell) och konkreta hanteringsregler per nivå. Dokumentera tilldelningen i tillgångsförteckningen eller i registret över behandling av personuppgifter.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.13 **Märkning av information: Klassificeringsnivån är synlig på dokumentet, filen eller meddelandet självt, så att mottagarna vet hur de ska hantera det utan att behöva fråga.**

Vad som styrker det: Märkning i dokumenthuvudet, i filnamnet, i ämnesraden för e-post eller via känslighetsetiketter i molnkontorssviten. Bevis genom stickprov på dokument som verkligen är märkta, inte bara genom regeln.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.14 **Informationsöverföring: Regler, rutiner och avtal för att överföra information inom organisationen och med externa parter finns på plats.**

Vad som styrker det: En regel som anger vilken kanal som är tillåten för vilken klassificeringsnivå: krypterad e-post eller ett datarum för konfidentiellt innehåll, ingen sändning via privata meddelandetjänster. Backa upp konfidentiella överföringar med sekretessavtal.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.15 **Behörighetsstyrning: Regler för att styra fysisk och logisk åtkomst till information och andra tillhörande tillgångar är fastställda och införda utifrån verksamhetens och säkerhetens krav.**

Vad som styrker det: En policy för behörighetsstyrning enligt behovsprincipen och minsta möjliga behörighet, med en koppling från roll till behörighet. Bevis genom den faktiska behörighetskonfigurationen hos identitetsleverantören, inte genom policyn ensam.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.16 **Identitetshantering: Hela livscykeln för identiteter är styrd.**

Vad som styrker det: En process från skapande via ändring till avstängning, helst samlad hos en identitetsleverantör med enkel inloggning. Inga delade gruppkonton; där det tekniskt inte går att undvika namnges kontot, motiveras och dess användning loggas.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.17 **Autentiseringsinformation: Tilldelning och hantering av autentiseringsinformation styrs av en hanteringsprocess som kräver att personerna hanterar den på rätt sätt.**

Vad som styrker det: En lösenordshanterare som obligatoriskt verktyg, en policy om lösenordskvalitet och MFA, säker första inloggning och en återställningsrutin med identitetskontroll. Bevis genom skärmbilder av konfigurationen och rapporten från lösenordshanteraren.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.18 **Behörigheter: Behörigheter tilldelas, ses över, ändras och tas bort i enlighet med policyn för behörighetsstyrning.**

Vad som styrker det: En periodisk genomgång av behörigheter, minst en gång per år, med ett dokumenterat resultat per konto och bevis på behörigheter som togs bort. Borttagning samma dag som någon slutar är en punkt som revisorer gärna följer genom ett konkret fall.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.19 **Informationssäkerhet i leverantörsrelationer: Processer och rutiner är fastställda och införda för att hantera de säkerhetsrisker som uppstår genom användning av produkter och tjänster från tredje part.**

Vad som styrker det: En lista över leverantörerna med kritikalitetsnivå och djupet i bedömningen. För kritiska leverantörer inhämtas bevis (certifikat enligt ISO 27001, SOC 2-rapport) i stället för egna revisioner, vilket är den enda realistiska vägen för en liten verksamhet.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.20 **Informationssäkerhet i leverantörsavtal: Relevanta säkerhetskrav är överenskomna med varje leverantör och nedtecknade i avtalen.**

Vad som styrker det: En avtalsbilaga om informationssäkerhet med skyldighet att anmäla incidenter, regler om underleverantörer, raderingsskyldigheter och revisionsrätt. För standardtjänster räcker leverantörens villkor plus ett personuppgiftsbiträdesavtal, förutsatt att innehållet har granskats och dokumenterats.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.21 **Hantering av informationssäkerhet i leveranskedjan för teknik: Processer för att hantera säkerhetsriskerna i leveranskedjan för informationsteknik och kommunikationsteknik är fastställda och införda.**

Vad som styrker det: Detta omfattar programvaruberoenden och leverantörernas egna underleverantörer. I praktiken: en innehållsförteckning för programvaran (SBOM) eller en beroendelista, automatiska kontroller av sårbara paket i CI, och programvara enbart från signerade eller officiella kanaler.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.22 **Övervakning, genomgång och ändringshantering av leverantörstjänster: Ändringar i leverantörstjänster övervakas, ses över och hanteras regelbundet.**

Vad som styrker det: En årlig genomgång av leverantörerna som ser på incidenter, tillgänglighetsrapporter och certifikatens giltighet, plus en kanal för leverantörens meddelanden om ändringar. Dokumentera resultatet som en kort notis per leverantör.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.23 **Informationssäkerhet vid användning av molntjänster: Processer för att anskaffa, använda, hantera och avveckla molntjänster är fastställda i linje med säkerhetskraven.**

Vad som styrker det: Nytt i 2022 års version och den centrala säkerhetsåtgärden för en liten molnbaserad verksamhet. Bevis genom en molnpolicy med en godkännandeprocess för nya tjänster, en dokumenterad modell för delat ansvar per tjänst, härdningsinställningar, och en avvecklingsstrategi som omfattar återlämning av data och bekräftelse på radering.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.24 **Planering och förberedelse för incidenthantering: Processer, roller och ansvar för hantering av informationssäkerhetsincidenter är planerade och fastställda.** Dokument

Vad som styrker det: En incidenthanteringsplan med rapporteringsväg, roller, eskaleringsnivåer, kontakter utanför kontorstid och kommunikationsmallar. Realistiskt för små team: en sida, men övad.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.5.25 **Bedömning och beslut om informationssäkerhetshändelser: Säkerhetshändelser bedöms och beslut fattas om huruvida de ska klassas som informationssäkerhetsincidenter.**

Vad som styrker det: Triagekriterier med en allvarlighetsmatris och ett händelseregister där även avfärdade händelser finns med, med en motivering. Skillnaden mellan händelse och incident måste synas i registret.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.26 **Åtgärder vid informationssäkerhetsincidenter: Incidenter hanteras i enlighet med de dokumenterade rutinerna.**

Vad som styrker det: Incidentakter med tidslinje, vidtagna åtgärder, involverade personer och avslutsbeslutet. Om ingen verklig incident har inträffat ännu är en dokumenterad skrivbordsövning det bästa tillgängliga beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.27 **Lärdomar från informationssäkerhetsincidenter: Kunskap från incidenter används för att stärka säkerhetsåtgärderna.**

Vad som styrker det: En skuldfri genomgång efter incidenten med grundorsaksanalys och härledda åtgärder, kopplad till förbättringsregistret och vid behov till riskregistret.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.28 **Insamling av bevis: Det är styrt hur spår som rör en säkerhetshändelse identifieras, säkras och bevaras så att de förblir användbara senare.**

Vad som styrker det: En kort rutin för bevissäkring: bygg inte om system för tidigt, säkra avbilder och loggar, dokumentera bevisets hanteringskedja. För en liten verksamhet räcker det att fastställa från vilken allvarlighetsnivå en extern forensikleverantör kallas in, tillsammans med kontaktuppgifterna.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.29 **Informationssäkerhet vid störningar: Organisationen planerar hur informationssäkerheten upprätthålls på en lämplig nivå under en störning.**

Vad som styrker det: Nödlägesarrangemang får inte stänga av säkerheten. Dokumentera att MFA, loggning och åtkomstbegränsningar också gäller i reservdrift, och att nödkonton (break-glass-konton) är förseglade, dokumenterade och granskade i efterhand.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.30 **Teknikberedskap för kontinuitetshantering: Beredskapen i informationstekniken och kommunikationstekniken är planerad, införd, underhållen och testad utifrån målen för kontinuitetshantering och kraven på teknisk kontinuitet.**

Vad som styrker det: Nytt i 2022 års version. Bevis genom fastställda mål för återställningstid (RTO) och för återställningspunkt (RPO) per kritiskt system, en återställningsrutin och minst ett dokumenterat test per år. Ett lyckat återläsningstest med datum och varaktighet är det starkaste enskilda beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.31 **Lagkrav, författningskrav, myndighetskrav och avtalskrav: De relevanta kraven och sättet att uppfylla dem är identifierade, dokumenterade och hålls aktuella.** Dokument

Vad som styrker det: Ett lagregister som täcker GDPR, telelagstiftning, bokföringslagen och skattelagstiftningen, och där det är tillämpligt NIS2 eller branschspecifika regler, var och en med den regel som genomför kravet och datum för genomgång. En årlig genomgång räcker, men den måste vara daterad.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.32 **Immateriella rättigheter: Lämpliga rutiner för att skydda immateriella rättigheter är införda.**

Vad som styrker det: En licensförteckning för den programvara som används, en kontroll av licenser för öppen källkod i produkten (en licensskanner i CI) och en regel för hantering av kod från tredje part och genererad kod. Bevis: licensrapporten från bygget.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.33 **Skydd av redovisande dokument: Verksamhetens redovisande dokument och bevisdokument lagras så att de inte kan gå förlorade, inte kan ändras obemärkt och inte kan hamna i fel händer, och detta gäller under hela bevarandetiden.**

Vad som styrker det: En bevarandeplan med de lagstadgade tiderna, manipulationssäker lagring, begränsad åtkomst och säkerhetskopiering. För skatterelevanta dokument anges de lagstadgade bevarandetiderna uttryckligen, eftersom revisorer gärna kontrollerar just det.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.34 **Integritetsskydd och skydd av personuppgifter: Kraven på integritet och skydd av personuppgifter (PII) är identifierade och uppfyllda i enlighet med tillämplig lag.**

Vad som styrker det: Register över behandling av personuppgifter, personuppgiftsbiträdesavtal, ett raderingskoncept, en process för de registrerades rättigheter och, där det krävs, en konsekvensbedömning avseende dataskydd. Att koppla detta till ISMS genom en gemensam tillgångsförteckning gör att inget behöver skötas dubbelt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.35 **Oberoende genomgång av informationssäkerheten: Organisationens sätt att styra informationssäkerheten ses över oberoende med planerade intervall och när betydande ändringar inträffar.**

Vad som styrker det: Belagt genom internrevisionen utförd av en oberoende revisor, genom externa penetrationstester eller genom certifieringsrevisionen i sig. Oberoende betyder att den inte utförs av den person som ansvarar för det område som ses över.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.36 **Efterlevnad av policyer, regler och standarder för informationssäkerhet: Efterlevnaden av organisationens egna säkerhetspolicyer och de tillämpliga reglerna ses över regelbundet.**

Vad som styrker det: Efterlevnadskontroller med datum och resultat, till exempel en konfigurationskontroll mot den egna härdningsbaslinjen, stickprov på dokumentmärkning, automatiska policykontroller i molnet. Avvikelser förs in i registret över korrigerande åtgärder.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5.37 **Driftrutiner i dokumenterad form: Rutiner för drift av anläggningar för informationsbehandling är dokumenterade och tillgängliga för de personer som behöver dem.** Dokument

Vad som styrker det: Runbooks för säkerhetskopiering och återläsning, driftsättning, användaradministration, installation av säkerhetsuppdateringar och incidenthantering. Kort och aktuellt slår omfattande och föråldrat; ett datum för senaste ändring per runbook är obligatoriskt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6 Bilaga A: Personrelaterade säkerhetsåtgärder 8

A.6.1 Bakgrundskontroll: Kandidater som ska arbeta för organisationen kontrolleras i förväg, inom lagens gränser och i proportion till skyddsbehovet; för känsliga roller upprepas kontrollen under anställningen.

Vad som styrker det: Utan anställda kan denna säkerhetsåtgärd motiveras som för närvarande inte tillämplig, men rutinen för det fall att någon anställs bör ändå vara fastställd och dokumenterad i uttalandet om tillämplighet som planerad. En genomförbar omfattning: kontroll av identitet, meritförteckning och referenser, plus certifikat; ett utdrag ur belastningsregistret bara där skyddsbehovet motiverar det och lagen tillåter det. Kräv samma nivå av frilansare och uppdragstagare genom deras avtal, annars öppnar sig luckan just där.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.2 Anställningsvillkor: De avtalsmässiga överenskommelserna anger personalens och organisationens ansvar för informationssäkerhet.

Vad som styrker det: En säkerhetsklausul i anställningsavtalet eller uppdragsavtalet som hänvisar till de tillämpliga policyerna. För frilansare samma klausul i uppdragsavtalet, plus ett sekretessavtal.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.3 Medvetenhet, utbildning och träning inom informationssäkerhet: Personal och relevanta externa parter får lämplig medvetenhet och utbildning samt regelbunden uppdatering om organisationens policyer.

Vad som styrker det: Årlig utbildning med närvarobevis och datum, kompletterad med nätfiskesimuleringar med utvärderad klickfrekvens. Även ensamföretagare behöver bevis på sin egen fortbildning, till exempel kursintyg.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.4 Disciplinär process: En formell och kommunicerad process finns för att vidta åtgärder mot personer som har brutit mot säkerhetspolicyerna.

Vad som styrker det: Utan anställda kan detta motiveras som för närvarande inte tillämpligt, men processen måste ändå vara fastställd för det fall att någon anställs; bara tillämpningen bortfaller, inte regeln. Det som krävs är en trappa av kommunicerade reaktioner (samtal, tillrättavisning, formell varning, uppsägning) i linje med arbetsrätt och regler om facklig samverkan. För uppdragstagare speglas sanktionsnivån i avtalet, till exempel ett vite eller en rätt att häva.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.5 Ansvar efter avslutad eller ändrad anställning: Säkerhetsansvar och skyldigheter som gäller även efter att anställningen upphört eller rollen ändrats är fastställda, upprätthållna och kommunicerade till de berörda.

Vad som styrker det: En checklista för avslut med borttagning av behörigheter, återlämning av tillgångar, överlämning och en uttrycklig påminnelse om den fortsatta sekretesskyldigheten. Ett undertecknat protokoll från avslutssamtalet är det enklaste beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.6 Sekretessavtal: Det är fastställt vem som måste underteckna ett sekretessavtal. Innehållet motsvarar informationens skyddsbehov, avtalen är undertecknade, arkiverade och ses över regelbundet så att de hålls aktuella.

Vad som styrker det: Undertecknade sekretessavtal för anställda, frilansare, leverantörer och praktikanter, med en efterverkanstid. En översiktstabell med motpart, datum och giltighet gör beståndet möjligt att revidera.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.7 **Distansarbete: Säkerhetsåtgärder är införda där personer arbetar utanför organisationens lokaler och därvid kommer åt organisationens information.**

Vad som styrker det: En policy för hemarbete och distansarbete med krav på diskkryptering, skärmlås, säkert trådlöst nät, användning av VPN eller åtkomst enligt zero trust, insynsskydd och ett förbud mot att använda privata enheter utan godkännande. Bevis genom efterlevnadsrapporten från MDM för slutpunkterna.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.8 **Rapportering av informationssäkerhetshändelser: Det finns en mekanism genom vilken personer i tid kan rapportera iakttagna eller misstänkta säkerhetshändelser.**

Vad som styrker det: En tydligt kommunicerad rapporteringskanal (brevlåda, chattkanal, telefonnummer) med en försäkran om inga sanktioner för rapporter i god tro. Bevis: antalet rapporter i händelseregistret; ett ständigt tomt register är ett varningstecken i revisionen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7 Bilaga A: Fysiska säkerhetsåtgärder 14

A.7.1 **Fysiska säkerhetszoner: Säkerhetszoner är fastställda och används för att skydda utrymmen som innehåller information och anläggningar för informationsbehandling.**

Vad som styrker det: En beskrivning av zonerna med en skiss eller foton: byggnad, kontor, serverskåp. I ett hemmakontor är zonen det låsbara arbetsrummet eller, om det saknas, ett låsbart skåp; beskriv det hellre än att utelämna det.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.2 **Fysiskt tillträde: Säkra utrymmen skyddas av lämpliga tillträdeskontroller och passagepunkter.**

Vad som styrker det: Ett register över nycklar och passerkort med utlämning och återlämning, och en besöksregel med eskort och loggning. Om ett kontorshotell eller ett datacenter används tas operatörens tillträdeskontroller som bevis och säkras avtalsmässigt.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.3 **Skydd av kontor, rum och lokaler: Fysisk säkerhet för kontor, rum och lokaler är utformad och införd.**

Vad som styrker det: Låsbara dörrar, fönsterskydd i markplan, inga konfidentiella skärmar synliga utifrån, ingen företagsskylt på känsliga utrymmen. En kort beskrivning plus ett foto räcker som bevis.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.4 **Fysisk säkerhetsövervakning: Lokalerna övervakas fortlöpande med avseende på obehörigt fysiskt tillträde.**

Vad som styrker det: Nytt i 2022 års version. Alternativen är larmsystem, rörelsedetektorer, kamerabevakning eller tillträdesloggar. Kamerabevakning måste kontrolleras mot dataskyddsreglerna; i ett hemmakontor är det motiverade alternativet en kombination av larmsystem, ett låst rum och konstaterandet att inga känsliga servrar förvaras där.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.5 **Skydd mot fysiska hot och miljöhot: Skydd finns mot fysiska hot och miljöhot som naturkatastrofer och avsiktlig eller oavsiktlig skada.**

Vad som styrker det: En genomgång av brand, vatten, värme, strömavbrott och inbrott, tillsammans med de åtgärder som finns (brandvarnare, brandsläckare, ingen utrustning under vattenledningar, säkerhetskopia lagrad på annan plats). Det är här slutsatsen om klimatförändringar från 4.1 hakar i.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.6 **Arbete i säkra utrymmen: Åtgärder för arbete i säkra utrymmen är utformade och införda.**

Vad som styrker det: Regler för serverrummet eller utrymmen med hög konfidentialitet: inget oövervakat tillträde för tredje part, ingen inspelning med kameror eller mobila enheter, loggning av utfört arbete. Om det inte finns några säkra utrymmen kan det motiveras med hänvisning till ren molndrift.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.7 **Rent skrivbord och tom skärm: Regler för ett rent skrivbord när det gäller papper och flyttbara medier och för låsta skärmar är fastställda och följs.**

Vad som styrker det: Detta gäller fullt ut även i hemmakontoret och får därför inte förklaras inte tillämpligt. Belagt genom en kort regel (lås in dokument, skärmlås efter fem minuter, inga klisterlappar med inloggningsuppgifter) plus det tekniskt framtvingade låset via enhetspolicy, vars konfiguration går att exportera.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.8 **Placering och skydd av utrustning: Utrustning är säkert placerad och skyddad.**

Vad som styrker det: Placering bort från genomgångsstråk och publika ytor, ingen insyn utifrån, skydd mot värme och fukt, kabellås för mobila enheter. En kort beskrivning i policyn för hemmakontor eller kontor räcker.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.9 **Säkerhet för tillgångar utanför lokalerna: Tillgångar som befinner sig utanför lokalerna är skyddade.**

Vad som styrker det: I en liten verksamhet handlar det främst om den bärbara datorn, mobiltelefonen och externa medier, och det går inte att argumentera bort. Bevis: framtvingad diskkryptering, fjärradering aktiverad genom MDM, en regel mot att lämna enheter i fordon och mot att använda publika nät utan VPN, plus en väg för att anmäla förlust. Efterlevnadsrapporten från MDM som visar krypteringsstatus per enhet är det stabilaste enskilda beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.10 **Lagringsmedier: Lagringsmedier hanteras under hela sin livscykel i linje med klassificeringsschemat och hanteringskraven, från anskaffning via användning och transport till kassering.**

Vad som styrker det: Detta gäller även vid rent mobilt arbete, eftersom USB-minnen, externa diskar och medier för säkerhetskopiering finns. Bevis: ett medieregister, krypterade medier, ett tekniskt framtvingat förbud mot icke godkända flyttbara medier, säker förvaring på ett låsbart ställe, och överlämning till A.7.14 vid livslängdens slut.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.11 **Stödjande försörjningssystem: Anläggningar för informationsbehandling är skyddade mot avbrott i de stödjande försörjningssystemen, särskilt strömförsörjningen.**

Vad som styrker det: Där servrar drivs i egen regi, en avbrottsfri kraftförsörjning med ett dokumenterat test. I en ren molnuppsättning är beviset hänvisningen till leverantörens åtaganden plus en regel för hur arbetet fortsätter vid ett lokalt avbrott i ström eller internet (mobil delning, reservplats).

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.12 **Kabelsäkerhet: Kablage för ström, data och kommunikation är skyddat mot avlyssning, störning och skada.**

Vad som styrker det: Där kablaget ägs av verksamheten, skydd mot skada och mot obehörig åtkomst till kopplingspaneler. I små kontor och hemmakontor är motiveringen kortfattad, men den måste ges: router och nätverksuttag är inte publikt åtkomliga, oanvända portar är avstängda.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.13 **Underhåll av utrustning: Utrustning underhålls korrekt för att säkerställa informationens tillgänglighet, riktighet och konfidentialitet.**

Vad som styrker det: En underhållsplan eller status för tillverkarstöd per enhet, och en regel för reparationer som utförs av tredje part (ta först ut lagringsenheten eller radera data, och ingå ett sekretessavtal med leverantören). Följ upp datumen för när stödet upphör i tillgångsförteckningen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7.14 **Säker kassering eller återanvändning av utrustning: Innan en enhet med lagring lämnas vidare, säljs eller skrotas är det kontrollerat och dokumenterat att inga skyddade data och ingen licensierad programvara går att återskapa på den.**

Vad som styrker det: Detta gäller även i hemmakontoret och för utrangerade privata enheter som använts i arbetet. Bevis: ett raderingsprotokoll per enhet med serienummer, datum och metod (kryptoradering på krypterade SSD-diskar, överskrivning, fysisk förstöring), eller ett intyg om förstöring från en leverantör. För krypterade enheter räcker den dokumenterade förstöringen av nyckeln, förutsatt att förfarandet är beskrivet.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8 Bilaga A: Tekniska säkerhetsåtgärder 34

A.8.1 **Användarnas slutpunktsenheter: Information som lagras på, behandlas av eller är åtkomlig via användarnas slutpunktsenheter är skyddad.**

Vad som styrker det: En härdningsbaslinje per operativsystem, central hantering via MDM, diskkryptering, automatiska uppdateringar och skärmlås. Efterlevnadsrapporten från MDM med status per enhet belägger allt detta på en gång.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.2 **Privilegierade behörigheter: Tilldelning och användning av privilegierade behörigheter är begränsade och styrda.**

Vad som styrker det: En lista över alla administratörskonton med en motivering, separata administratörskonton som inte används i det dagliga arbetet, framtvingad MFA, tidsbegränsad höjning av behörighet där det går, och periodisk genomgång. I en liten verksamhet är detta den viktigaste kompenserande säkerhetsåtgärden för A.5.3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.3 **Begränsning av åtkomst till information: Åtkomst till information och andra tillhörande tillgångar är begränsad i enlighet med den fastställda policyn för behörighetsstyrning.**

Vad som styrker det: Ett behörighetskoncept som bygger på roller och grupper i stället för enskilda tilldelningar, belagt genom en export av gruppmedlemskap. Se över publika delningslänkar i molnlagringen regelbundet och låt dem löpa ut.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.4 **Åtkomst till källkod: Läsåtkomst och skrivåtkomst till källkod, utvecklingsverktyg och programbibliotek är styrda på ett lämpligt sätt.**

Vad som styrker det: Behörigheter i kodförrådet efter roll, skyddade huvudgrenar, framtvingade granskningar eller framtvingade statuskontroller, ingen direkt push till huvudgrenen. Bevis genom konfigurationen av grenskyddet och organisationens medlemslista.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.5 **Säker autentisering: Tekniker och rutiner för säker autentisering är införda utifrån åtkomstbegränsningarna och den ämnesspecifika policyn.**

Vad som styrker det: MFA för all extern åtkomst och alla administratörskonton, nätfiskeresistenta metoder (passkeys, FIDO2) där det går, och utelåsning efter misslyckade försök. Bevis genom identitetsleverantörens rapport om MFA-täckning.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.6 **Kapacitetshantering: Lagring, beräkningskraft, bandbredd och licenser övervakas, och behovet justeras tillräckligt tidigt för att flaskhalsar aldrig ska hota tillgängligheten.**

Vad som styrker det: Övervakning av lagring, beräkningsbelastning, licenskvoter och molnbudgetar med tröskellarm. I en liten verksamhet räcker ett larm på diskutnyttjande och på kostnadsgränser plus en årlig kapacitetsöversyn.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.7 **Skydd mot skadlig kod: Tekniska försvar mot skadlig kod är aktiva och aktuella, och de personer som använder enheterna är tillräckligt utbildade för att inte underminera dessa försvar.**

Vad som styrker det: Aktivt slutpunktsskydd med en central statusöversikt, ett e-postfilter som granskar bilagor och länkar, och en regel mot att köra icke godkänd programvara. Den daterade statusrapporten från skyddslösningen är det direkta beviset.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.8 **Hantering av tekniska sårbarheter: Organisationen håller sig aktivt underrättad om sårbarheter i den teknik den använder, avgör för varje fynd hur exponerad den är, och sluter luckan inom fastställda tidsfrister eller motiverar ett annat svar.**

Vad som styrker det: Sårbarhetshantering med en källa (skanner, beroendekontroll i CI, meddelanden från tillverkare), en allvarlighetsgradering och fastställda tidsfrister per nivå, till exempel kritisk inom 7 dagar. Bevis: skanningsrapporter från flera tidpunkter som visar att antalet öppna fynd sjunker.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.9 **Konfigurationsstyrning: Konfigurationer av maskinvara, programvara, tjänster och nätverk, inklusive säkerhetskonfigurationer, är fastställda, dokumenterade, införda, övervakade och granskade.**

Vad som styrker det: Nytt i 2022 års version. Bevis genom dokumenterade baslinjekonfigurationer (härdningsbaslinjer) och deras upprätthållande, helst som infrastruktur som kod i versionshantering eller genom MDM-profiler. Upptäckt av avdrift och en periodisk konfigurationsjämförelse rundar av det.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.10 **Radering av information: Information som lagras i informationssystem, på enheter och på lagringsmedier raderas när den inte längre behövs.**

Vad som styrker det: Nytt i 2022 års version och nära knutet till GDPR. Bevis genom ett raderingskoncept med bevarandetider per datakategori, tekniskt införda bevaranderegler i molntjänster och databaser, och raderingsloggar. Även säkerhetskopior och loggarkiv behöver en bevarandetid.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.11 **Datamaskering: Datamaskering tillämpas i enlighet med den ämnesspecifika policyn för behörighetsstyrning och med verksamhetens och lagens krav.**

Vad som styrker det: Nytt i 2022 års version. I praktiken: inga produktionsdata i testmiljöer och utvecklingsmiljöer, utan anonymiserade eller syntetiska data i stället; pseudonymisering i analys; maskering av kontonummer och inloggningsuppgifter i loggar och supportgränssnitt. Bevis genom det skript eller det förfarande som skapar testdata.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.12 **Förhindrande av dataläckage: Åtgärder för att förhindra dataläckage tillämpas på system, nätverk och enheter som behandlar, lagrar eller överför känslig information.**

Vad som styrker det: Nytt i 2022 års version. Realistiskt i en liten verksamhet: styrning av delningslänkar i molnlagringen, blockering av icke godkända flyttbara medier, regler mot vidarebefordran till privata brevlådor, kontroller av om konfidentiella uppgifter matas in i externa AI-tjänster, och sökning efter hemligheter i källkoden. Bevis genom konfigurationen och genom genomgångar av träffarna.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.13 **Säkerhetskopiering av information: Säkerhetskopior av data, programvara och system finns enligt en fastställd regel (omfattning, frekvens, bevarande, plats), och återläsning från dem testas verkligen med regelbundna intervall.**

Vad som styrker det: En policy för säkerhetskopiering med frekvens, bevarande och en kopia på annan plats enligt principen 3-2-1, kryptering av säkerhetskopiorna, och skydd mot överskrivning av utpressningsprogram (oföränderliga säkerhetskopior). Avgörande är det dokumenterade återläsningstestet med datum och resultat, eftersom en otestad säkerhetskopia räknas som obefintlig i revisionen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.14 **Redundans i anläggningar för informationsbehandling: Anläggningar för informationsbehandling är införda med tillräcklig redundans för att uppfylla kraven på tillgänglighet.**

Vad som styrker det: Redundansen måste matcha målen för tillgänglighet, inte det högsta möjliga. Bevis genom en arkitekturbeskrivning med redundanta instanser eller zoner, reservenheter, och ett motiverat beslut om var redundans avsiktligt saknas.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.15 **Loggning: Säkerhetsrelevanta aktiviteter lämnar spår. Loggar skapas, bevaras, skyddas mot ändring och analyseras verkligen, inte bara samlas in.**

Vad som styrker det: Logga som ett minimum inloggningar och misslyckade försök, ändringar av behörigheter, administrativa åtgärder och åtkomst till konfidentiella uppgifter. Loggarna är skyddade mot ändring och bär en fastställd bevarandetid; i en liten verksamhet är oföränderliga loggar samtidigt kompensationen för den uteblivna uppdelningen av arbetsuppgifter enligt A.5.3.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.16 **Övervakningsaktiviteter: Nätverk, system och applikationer övervakas med avseende på avvikande beteende och lämpliga åtgärder vidtas för att utvärdera möjliga säkerhetsincidenter.**

Vad som styrker det: Nytt i 2022 års version. Genomförbart utan ett eget säkerhetsteam: larm från identitetsleverantören om omöjliga resor och om serier av misslyckade försök, larm från molnplattformen om ovanliga kostnader eller ändrade behörigheter, vidarebefordrade till en bevakad brevlåda med en fastställd svarstid. Bevis genom larmreglerna plus exempel på larm som hanterats.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.17 **Klocksynkronisering: Alla system som skriver loggar hämtar sin tid från en fastställd, betrodd källa, så att händelser kan ordnas i rätt följd över systemgränserna.**

Vad som styrker det: NTP-konfiguration på servrar och slutpunkter, och en enhetlig tidszon i loggarna (helst UTC). Utan synkroniserad tid håller inte en rekonstruktion av en incident enligt A.5.28; ett konfigurationsutdrag räcker som bevis.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.18 **Användning av privilegierade systemverktyg: Användningen av systemverktyg som kan sätta systemskydd ur spel är begränsad och noga styrd.**

Vad som styrker det: En lista över godkända administrationsverktyg, begränsning av lokala administratörsrättigheter, applikationsstyrning (tillåtlistning) där det går, och loggning av användningen. Bevis: policyn plus konfigurationen av behörighetshanteringen.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.19 **Installation av programvara i driftsatta system: Rutiner och åtgärder för att säkert hantera installation av programvara i driftsatta system är införda.**

Vad som styrker det: Endast godkänd programvara från betrodda källor, installation genom central distribution eller en pakethanterare, en väg tillbaka och bevarande av den föregående versionen. Bevis genom godkännandelistan och driftsättningsloggarna.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.20 **Nätverkssäkerhet: Nätverk och aktiva nätverksenheter har en namngiven ägare, en härdad konfiguration och en spårbar regeluppsättning som anger vilken trafik som över huvud taget är tillåten.**

Vad som styrker det: En brandväggsregeluppsättning enligt principen neka som standard, dokumenterade öppna portar med en motivering, en säker konfiguration av det trådlösa nätet, och ändrade fabrikslösenord på nätverksenheter. Bevis genom en export av regeluppsättningen och en extern portskanning.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.21 **Säkerhet i nättjänster: Säkerhetsmekanismer, tjänstenivåer och hanteringskrav för nättjänster är identifierade, införda och övervakade.**

Vad som styrker det: Dokumentera för varje nättjänst som används (VPN, DNS, e-post, CDN) säkerhetsåtagandena och den egna konfigurationen, inklusive kryptering under överföring och leverantörens åtaganden om tjänstenivå. Bevis: en konfigurationsöversikt plus avtalet eller tjänstebeskrivningen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.22 **Uppdelning av nätverk: Nätverket är indelat i zoner så att tjänster, användargrupper och system med olika skyddsbehov inte når varandra ofiltrerat.**

Vad som styrker det: Separata nätverkssegment eller VLAN för gäster, administration och produktion; i molnet separata konton eller virtuella nätverk med säkerhetsgrupper. I ett hemmakontor är den genomförbara lösningen ett separat nätverk eller VLAN för arbetsenheterna, hållet åtskilt från privata enheter och smarta hemprodukter.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.23 **Webbfiltrering: Åtkomsten till externa webbplatser är styrd för att minska exponeringen för skadligt innehåll.**

Vad som styrker det: Nytt i 2022 års version. Går att nå med liten insats genom en filtrerande DNS-tjänst eller den webbfiltrering som ingår i slutpunktsskyddet, med blockerade kategorier och loggning av blockerade anrop. Bevis genom filterkonfigurationen och ett rapportutdrag.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.24 **Användning av kryptografi: Det är bindande fastställt var kryptering tillämpas, med vilka algoritmer, och hur nycklar skapas, lagras, byts och förstörs under hela sin livscykel.** Dokument

Vad som styrker det: En kryptografipolicy med godkända algoritmer och minsta nyckellängder, kryptering under överföring (TLS) och i vila, plus en rutin för nyckelhantering som täcker skapande, lagring, byte och förstöring. Bevis genom policyn plus konfigurationen av nyckeltjänsten eller valvet.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.25 **Säker utvecklingslivscykel: Regler för säker utveckling av programvara och system är fastställda och tillämpade.**

Vad som styrker det: En beskrivning av utvecklingsprocessen med säkerhetspunkter per fas: krav, konstruktion, implementation, test, release, drift. För små team räcker en sida som hänvisar till de konkreta grindarna i CI och till granskningsplikten.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.26 **Säkerhetskrav för applikationer: Säkerhetskrav för applikationer är identifierade, specificerade och godkända under utveckling och anskaffning.**

Vad som styrker det: Säkerhetskrav som uttryckliga punkter i kravlistan eller som en återanvändbar checklista, med utgångspunkt till exempel i gängse standarder för verifiering av applikationssäkerhet. Bevis genom ärenden eller kravdokument med säkerhetsvinkel.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.27 **Principer för säker systemarkitektur och systemkonstruktion: Principer för säker systemkonstruktion är fastställda, dokumenterade och tillämpade på utvecklingsarbetet.**

Vad som styrker det: Dokumenterade principer som minsta möjliga behörighet, djupförsvar, säkra grundinställningar, dataminimering och ett arbetssätt enligt zero trust, tillsammans med synlig tillämpning av dem i arkitekturskisser eller beslutsdokument.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.28 **Säker kodning: Principer för säker kodning tillämpas i programvaruutvecklingen.**

Vad som styrker det: Nytt i 2022 års version. Bevis genom bindande kodregler, statisk kodanalys och sökning efter hemligheter som obligatoriska grindar i CI, användning av granskade bibliotek, och dokumenterade kodgranskningar. Där uppdelning av arbetsuppgifter är omöjlig träder framtvingade automatiska grindar i stället för granskning enligt fyraögonsprincipen; motivera detta och belägg det med konfigurationen av kedjan.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.29 **Säkerhetstestning vid utveckling och godkännande: Processer för säkerhetstestning är fastställda och införda inom utvecklingens livscykel.**

Vad som styrker det: Automatiska säkerhetstester i kedjan (beroendekontroller, statisk och dynamisk analys) plus ett periodiskt penetrationstest där skyddsbehovet är förhöjt. Bevis genom daterade testrapporter och uppföljningen av fynden.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.30 **Utlagd utveckling: Utlagd utvecklingsverksamhet styrs, övervakas och ses över.**

Vad som styrker det: Där utveckling läggs ut fastställs säkerhetskraven i avtalet, äganderätten till koden och rätten att granska säkras, och kodgranskningar och säkerhetstester genomförs före godkännande. Utan utlagd utveckling måste den bristande tillämpligheten motiveras sammanhängande i SoA.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.31 **Åtskillnad mellan utvecklingsmiljö, testmiljö och produktionsmiljö: Utvecklingsmiljöer, testmiljöer och produktionsmiljöer är åtskilda och skyddade.**

Vad som styrker det: Separata konton, projekt eller namnrymder, separata inloggningsuppgifter och separata datamängder. I kombination med A.8.11 säkras att inga produktionsdata hamnar i miljöer utanför produktionen. Bevis genom miljööversikten och behörighetstilldelningen.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.32 **Ändringshantering: Ändringar i anläggningar för informationsbehandling och i informationssystem omfattas av rutiner för ändringshantering.**

Vad som styrker det: En ändringsprocess med begäran, konsekvensbedömning, test, godkännande, införande och en väg tillbaka. I utvecklingsteam uppfyller en kedja med pull requests med framtvingade kontroller och loggade driftsättningar denna punkt, förutsatt att historiken inte går att ändra.

◯ Öppet ◯ Pågår ◯ Uppfyllt ◯ Ej tillämpligt

Bevis / motivering

A.8.33 **Testinformation: Testinformation är lämpligt utvald, skyddad och hanterad.**

Vad som styrker det: Principen: inga verkliga personuppgifter i testsystem. Där det inte går att undvika dokumenteras godkännandet, maskeringen, åtkomstbegränsningen och raderingen efter testet. Bevis genom testdatakonceptet och raderingsloggarna.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8.34 **Skydd av informationssystem vid revisionstester: Revisionstester som innebär åtkomst till driftsatta system är planerade och överenskomna med ledningen för att undvika störningar i driften.**

Vad som styrker det: En revisionsöverenskommelse med tidsfönster, omfattning, endast läsande åtkomst där det går, loggning av revisionsåtkomsten och godkännande av ledningen. Detta gäller även penetrationstester: ett skriftligt testtillstånd med tidsfönster och en nödkontakt är beviset.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

ISO/IEC 27018:2025, Informationssäkerhet, cybersäkerhet och skydd av personlig integritet: Vägledning för skydd av personuppgifter (PII) i publika moln i rollen som personuppgiftsbiträde (3:e utgåvan, 2025-08)

Skydd av personuppgifter i publika moln

36 krav. För denna standard finns inget ackrediterat certifikat. Utgåva 07/2026.

ISO/IEC 27018 är ingen standard för ledningssystem utan en vägledning med utökade säkerhetsåtgärder utöver ISO/IEC 27002:2022. Det finns inget fristående ackrediterat certifikat mot ISO/IEC 27018. Säkerhetsåtgärderna tas in i uttalandet om tillämplighet för ett system enligt ISO/IEC 27001, och certifikatet utfärdas därefter mot ISO/IEC 27001 med hänvisning till ISO/IEC 27018. Standarden riktar sig till leverantören av en publik molntjänst som behandlar personuppgifter för sina molnkunders räkning. En organisation som enbart använder molntjänster har inte den rollen och bedömer med fördel kraven mot sina leverantörer, inte mot sig själv. För Leanshift är denna checklista därför framför allt ett bedömningsraster för leverantörer. Varje punkt kan ställas som en fråga till leverantören och säkras genom personuppgiftsbiträdesavtalet enligt artikel 28 i dataskyddsförordningen (GDPR). Resultatet av en sådan bedömning är ett internt redovisande dokument om överensstämmelse eller en bedömningsprofil för leverantören, inte ett certifikat. Om numreringen: Avsnitt A.2 till A.12 följer dataskyddsprinciperna i bilaga A till standarden, punkter med nummer som A.11.6 är de ytterligare säkerhetsåtgärder som anges där. Punkter med nummer som 8.10 eller 5.34 hänvisar till säkerhetsåtgärder ur ISO/IEC 27002:2022 som standarden gör specifika för molnet. Punkter med tillägget (Grundsatz), alltså princip, härleds ur avsnittets egen princip i de fall bilaga A inte har någon egen ytterligare säkerhetsåtgärd.

Företag	Datum	Upprättad av

A.2 Samtycke och valmöjlighet 2

A.2.1 **Molnleverantören stödjer molnkunden i att uppfylla de registrerades rättigheter, till exempel tillgång, rättelse, radering och invändning. Ansvar och tidsfrister är reglerade i avtal.** Dokument

Vad som styrker det: Beviset är personuppgiftsbiträdesavtalet enligt artikel 28 i dataskyddsförordningen med en klausul om stöd vid de registrerades rättigheter, tillsammans med de tekniska medlen i själva tjänsten: funktioner för export, rättelse och radering eller en dokumenterad supportrutin med svarsfrist. Fråga till leverantören: Vilken funktion eller vilken process erbjuder ni så att vi kan hantera en begäran om tillgång eller radering inom en månad?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.2 (Grundsatz) **Molnkundernas personuppgifter behandlas uteslutande enligt kundens dokumenterade instruktioner. Att inhämta samtycke från de registrerade är fortsatt kundens uppgift i rollen som personuppgiftsansvarig, och leverantören föregriper inte det.**

Vad som styrker det: Beviset är instruktionsklausulen i personuppgiftsbiträdesavtalet plus ett bevis på att leverantören inte gör någon egen sekundäranvändning av uppgifterna, till exempel tjänstens integritetspolicy och produktdokumentationen. Fråga till leverantören: Behandlar ni våra kunduppgifter på något sätt utanför våra instruktioner, till exempel för produktförbättring eller modellträning?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.3 Ändamålets laglighet och angivande 2

A.3.1 **Ändamålet med leverantörens behandling av personuppgifter är begränsat till att leverera den avtalade tjänsten och är angivet i avtalet. Någon behandling för leverantörens egna ändamål sker inte.** Dokument

Vad som styrker det: Beviset är personuppgiftsbiträdesavtalet med föremål, art, ändamål och varaktighet för behandlingen samt kategorierna av registrerade enligt artikel 28.3 i dataskyddsförordningen. Fråga till leverantören: Lämna den avtalsbilaga som beskriver ändamålet med behandlingen uttömmande. För en liten verksamhet räcker leverantörens standardbilaga för personuppgiftsbehandling, förutsatt att den innehåller dessa uppgifter.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.3.2 **Personuppgifter som anförtrotts leverantören används inte för reklam, marknadsföring eller andra kommersiella ändamål hos leverantören utan föregående uttryckligt samtycke. Leveransen av tjänsten görs inte beroende av ett sådant samtycke.**

Vad som styrker det: Beviset är en uttrycklig avtalsklausul som utesluter kommersiell sekundäranvändning, tillsammans med användarvillkoren. Fråga till leverantören: Bekräfta skriftligt att kunduppgifter inte används för reklam, profilering eller träning av AI-modeller. Saknas det åtagandet är tjänsten olämplig för personuppgifter.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.4 Begränsad insamling 1

A.4 (Grundskydd) **Utöver de uppgifter som kunden lägger in i tjänsten samlar leverantören inte in ytterligare personuppgifter för egna ändamål, till exempel telemetri, användningsprofiler eller innehållsanalys. Driftdata och metadata som samlas in är angivna och motiverade.**

Vad som styrker det: Beviset är en lista över de uppgifter som tjänsten dokumenterar vid sidan av innehållsdata (åtkomstloggar, telemetri, diagnostikdata) med ändamål och lagringstid, plus en skärmbild av den inställning som stänger av valfri telemetri. Fråga till leverantören: Vilka data om användning, telemetri och diagnostik samlar ni in därutöver, vad använder ni dem till och kan vi stänga av insamlingen?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.5 Uppgiftsminimering 2

A.5.1 **Tillfälliga filer som skapas vid behandling av personuppgifter, till exempel arbetslagring, cachar eller återställningsjournaler, raderas säkert inom en fastställd tid.**

Vad som styrker det: Beviset är en rutin för drift eller radering med angiven lagringstid för tillfälliga data, styrkt av systemkonfigurationen, till exempel en cachetid (TTL) eller ett schemalagt rensningsjobb med sin körningslogg. Fråga till leverantören: Efter vilken tid raderas cachar, tillfälliga filer och mellanliggande tillstånd och hur övervakas det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.11 **Där drift, test eller support inte kräver skarpa data är personuppgifter maskerade, pseudonymiserade eller anonymiserade. Mängden behandlade uppgifter är begränsad till det som tjänsten faktiskt behöver.**

Vad som styrker det: Beviset är en regel om vilka miljöer som får se skarpa data, plus skärmbilder eller skript för den maskering som används i system för test och utveckling. Fråga till leverantören: Arbetar era team för support och utveckling med produktionsdata och i så fall under vilka skyddsåtgärder? För en liten verksamhet räcker en regel om att testsystem uteslutande körs på genererade exempeldata.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6 Begränsad användning, lagring och utlämning 3

A.6.1 **Om leverantören får en rättsligt bindande begäran om att lämna ut personuppgifter, till exempel från en myndighet, informerar leverantören molnkunden i förväg så långt lagen tillåter.**

Vad som styrker det: Beviset är en avtalad underrättelseklausul och en intern process för myndighetsförfrågningar med utpekad ansvarig. Fråga till leverantören: Underrättar ni oss innan uppgifter lämnas ut och publicerar ni en transparensrapport om förfrågningar från myndigheter? En aktuell transparensrapport är ett starkt bevis.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.6.2 **Om leverantören lämnar ut personuppgifter till tredje part dokumenterar leverantören händelsen så att den kan spåras: vem som tog emot uppgifterna, när det skedde, vilka uppgifter det gällde och på vilken grund utlämningen vilar.** Dokument

Vad som styrker det: Beviset är ett register över utlämningar eller en ärendehistorik med dessa fält, även om det inte innehåller några poster. Ett tomt men underhållet register är godtagbart och är den praktiska vägen för en liten verksamhet. Fråga till leverantören: För ni ett register över utlämningar och kan vi få utdrag ur det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.10 **Personuppgifter raderas när den avtalade lagringstiden löper ut eller avtalet upphör, inklusive kopior i säkerhetskopiorna efter deras rotationscykel.**

Vad som styrker det: Beviset är ett raderingskoncept med lagringstider per datakategori, lagringstiden för säkerhetskopior och en raderingslogg eller en raderingsbekräftelse. Fråga till leverantören: Hur länge lever våra uppgifter kvar i era säkerhetskopior efter uppsägning och får vi en skriftlig bekräftelse på raderingen?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.7 Riktighet och kvalitet 2

A.7 (Grundskydd) **Leverantören ändrar inte de personuppgifter som anförtrotts den på eget initiativ. Rättelser och uppdateringar sker uteslutande på molnkundens instruktion eller genom funktioner som kunden själv använder.**

Vad som styrker det: Beviset är tjänstens redigeringsfunktioner tillsammans med deras ändringshistorik, plus instruktionsklausulen i personuppgiftsbiträdesavtalet. Fråga till leverantören: Kan vi rätta poster själva och loggas varje ändring så att den kan spåras?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

8.13 **Personuppgifternas riktighet är skyddad vid lagring, vid överföring och vid återställning. Säkerhetskopior finns och deras återställbarhet är testad.**

Vad som styrker det: Beviset är konfigurationen för säkerhetskopiering, kontrollsummor eller mekanismer för riktighet och minst ett dokumenterat återställningstest per år med datum och resultat. Fråga till leverantören: Hur ofta testar ni återställningar och vilken återställningstid åtar ni er i servicenivån?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8 Öppenhet, transparens och information 2

A.8.1 **Anlitandet av underleverantörer som behandlar personuppgifter redovisas innan avtalet ingås. Ändringar i listan meddelas kunden i god tid, så att kunden kan invända eller säga upp avtalet.** Dokument

Vad som styrker det: Beviset är en aktuell lista över underbiträden, publicerad eller tillgängliggjord genom avtal, med namn, land och ändamål med behandlingen, plus en regel om underrättelse enligt artikel 28.2 i dataskyddsförordningen. Fråga till leverantören: Var hittar vi er lista över underbiträden, hur lång tid i förväg meddelar ni ändringar och hur kan vi invända?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.8 (Grundskydd) **Innan avtalet ingås tillhandahåller leverantören begriplig information om hur personuppgifter behandlas, vilka skyddsåtgärder som finns och i vilka jurisdiktioner behandlingen sker.**

Vad som styrker det: Beviset är integritetspolicyn, ett publicerat säkerhetsdokument, en sida med förtroendeinformation och personuppgiftsbiträdesavtalet inklusive de tekniska och organisatoriska åtgärderna som bilaga. Fråga till leverantören: Lämna den aktuella listan över tekniska och organisatoriska åtgärder som avtalsbilaga, inte bara marknadsföringsmaterial.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.9 Den enskildes medverkan och tillgång 2

A.9 (Grundskydd) **Tjänsten ger molnkunden de tekniska medlen att på egen hand hantera de registrerades begäran om tillgång, rättelse och radering, till exempel genom funktioner för export, sökning och radering.**

Vad som styrker det: Beviset är produktdokumentationen för funktionerna för export och radering, styrkt av en intern provkörning: En begäran om tillgång genomförs från början till slut och tidsåtgången dokumenteras. Fråga till leverantören: Kan vi hitta, exportera och radera alla uppgifter om en enskild person utan ert stöd?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.34 **Om kunden inte själv kan hantera en begäran från en registrerad bistår leverantören inom en avtalad tid. Begäran som registrerade skickar direkt till leverantören vidarebefordras till kunden i stället för att besvaras av leverantören.**

Vad som styrker det: Beviset är motsvarande klausul i personuppgiftsbiträdesavtalet med en konkret svarsfrist, plus en ärendehistorik från supporten som ett verkligt exempel. Fråga till leverantören: Vilken svarsfrist åtar ni er för stöd vid de registrerades rättigheter och vad kostar det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.10 Ansvarsskyldighet 4

A.10.1 **Personuppgiftsincidenter rapporteras till molnkunden utan onödigt dröjsmål med uppgift om omfattning, berörda uppgifter, orsak och vidtagna åtgärder. En process för underrättelse med ansvar och tidsfrister är fastställd.** Dokument

Vad som styrker det: Beviset är planen för incidenthantering med sin eskaleringskedja, den avtalade underrättelsefristen (24 till 48 timmar fungerar i praktiken, så att kunden fortfarande hinner med fristen på 72 timmar enligt artikel 33 i dataskyddsförordningen) och redovisande dokument om tidigare incidenter eller om en övning. Fråga till leverantören: Inom vilken tid rapporterar ni en incident, genom vilken kanal och vilken information lämnar ni med den?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.10.2 **Säkerhetspolicyer, driftrutiner och tillhörande redovisande dokument bevaras under en fastställd tid, så att behandlingen kan rekonstrueras i efterhand.** Dokument

Vad som styrker det: Beviset är en bevaranderegel med versionshistoriken för policyerna, till exempel genom ett dokumentregister eller ett versionshanteringssystem med datum för godkännande. Fråga till leverantören: Hur länge bevarar ni policyversioner och tillhörande redovisande dokument och får vi tillgång till dem vid en revision?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.10.3 **En fastställd reglering finns för återlämnande, överföring och förstöring av personuppgifter när avtalet upphör, med angivna format, tidsfrister och hantering av kopior.** Dokument

Vad som styrker det: Beviset är avslutsklausulen i personuppgiftsbiträdesavtalet plus en raderingsbekräftelse efter att avtalet upphört. Fråga till leverantören: I vilket format och inom vilken tid får vi tillbaka våra uppgifter, när förstörs alla kopior och får vi en skriftlig bekräftelse?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.35 **Skyddsåtgärdernas verkan ses över oberoende med regelbundna intervall, till exempel genom internrevisioner, penetrationstester eller granskningsrapporter från tredje part. Resultaten görs tillgängliga för molnkunden i lämplig form.**

Vad som styrker det: Beviset är ett certifikat enligt ISO/IEC 27001 med ett uttalande om tillämplighet som omfattar säkerhetsåtgärderna i ISO/IEC 27018, eller en SOC 2-rapport, tillsammans med aktuella sammanfattningar av penetrationstester. Fråga till leverantören: Lämna certifikatet, dess omfattning och en bekräftelse på att ISO/IEC 27018 återspeglas i uttalandet om tillämplighet. Det är värt att kontrollera om omfattningen verkligen täcker den tjänst som används.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11 Informationssäkerhet 13

A.11.1 **Alla med åtkomst till personuppgifter är bundna av sekretess, oavsett om de är direkt anställda eller anlitade externt.** Dokument

Vad som styrker det: Beviset är undertecknade sekretessavtal eller sekretessförbindelser som gäller även efter att uppdraget upphört. Fråga till leverantören: Är alla medarbetare och leverantörer med åtkomst till uppgifter skriftligen bundna av sekretess?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.2 **Utskrifter och andra papperskopior med personuppgifter skapas endast där det är strikt nödvändigt. Den tillåtna omfattningen styrs av en fastställd regel.**

Vad som styrker det: Beviset är en regel för hantering av utskrifter, som i datacenter vanligen är ett generellt förbud mot utskrift i utrymmen med kunddata. Fråga till leverantören: Skrivs kunddata över huvud taget ut i er verksamhet och i så fall under vilka villkor?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.3 **Återställningar från säkerhetskopior godkänns i förväg och loggas, inklusive den person som utlöste återställningen och de berörda uppgifterna.** Dokument

Vad som styrker det: Beviset är återställningsloggen med tidsstämpel, uppgift om vem som utlöste återställningen och omfattning, som vanligen skapas automatiskt av verktyget för säkerhetskopiering. Fråga till leverantören: Loggar ni varje återställning och kan vi granska loggarna vid en revision?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.4 **Lagringsmedier med personuppgifter som lämnar lokalerna är skyddade mot obehörig åtkomst och förlust, som regel genom kryptering och ett redovisande dokument för transporten.**

Vad som styrker det: Beviset är ett bevis på kryptering (fullständig kryptering av mediet), redovisande dokument för transport och överlämning samt en förteckning över medier. Fråga till leverantören: Lämnar medier med kunddata någonsin era anläggningar, till exempel för säkerhetskopiering, och hur skyddas de under transporten?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.5 **Användning av okrypterade bärbara medier och enheter för personuppgifter är förbjuden eller begränsad till motiverade undantag med dokumenterat godkännande.**

Vad som styrker det: Beviset är en policy för flyttbara medier plus tekniska spärrar som tvingar fram regeln, till exempel påtvingad kryptering av enheter eller USB-portar som blockeras genom enhetshantering. Fråga till leverantören: Kan medarbetare kopiera kunddata till okrypterade enheter och vad hindrar det tekniskt?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.6 **Personuppgifter som överförs via publika nät är krypterade. De mekanismer som används motsvarar aktuell teknisk nivå.**

Vad som styrker det: Beviset är TLS-konfigurationen (aktuell protokollversion, inga föråldrade krypteringssviter) och ett externt konfigurationstest som rapport. Praktiskt för en liten verksamhet: en kostnadsfri TLS-skanning en gång per år och det sparade resultatet. Fråga till leverantören: Vilken transportkryptering kräver ni och är kryptering av lagrade uppgifter aktiv?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.7 **Pappersdokument med personuppgifter förstörs på ett sätt som utesluter rekonstruktion.**

Vad som styrker det: Beviset är dokumentförstörare med tillräcklig säkerhetsnivå eller intyg om förstöring från en leverantör som arbetar enligt DIN 66399 eller en likvärdig standard. Fråga till leverantören: Hur förstör ni pappersdokument som rör kunder och finns intyg om förstöring sparade?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.8 **Användaridentiteter är entydigt kopplade till en person och varken återanvänds eller delas. Delade konton finns endast i motiverade undantagsfall och med ytterligare spårbarhet.**

Vad som styrker det: Beviset är en användarlista från identitetssystemet utan gruppkonton, tillsammans med regeln att administrativt arbete utförs under ett personligt konto. Fråga till leverantören: Arbetar er driftpersonal med personliga konton och är flerfaktorsautentisering obligatorisk?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.9 **Leverantören kan när som helst ange vilka personer eller roller som får åtkomst till personuppgifter och håller den översikten aktuell.** Dokument

Vad som styrker det: Beviset är en översikt över behörigheter per roll, styrkt av en återkommande genomgång av behörigheter med datum och resultat. För en liten verksamhet räcker en export av användarlistan varje halvår, godkänd med underskrift. Fråga till leverantören: Hur många av era medarbetare kan komma åt våra uppgifter och hur ofta ser ni över det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.10 **Användarkonton hanteras över hela sin livscykel: skapande, ändring och snabb avaktivering när någon slutar eller byter roll.**

Vad som styrker det: Beviset är en rutin för introduktion och avslut med en checklista, plus loggar över avaktiverade konton med tidsstämplar. Fråga till leverantören: Inom vilken tid drar ni in åtkomsten för medarbetare som slutar och hur styrker ni det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.11 **Leverantörens skyldigheter för säkerhet och dataskydd är fastställda i avtal, inklusive de tekniska och organisatoriska åtgärderna, att kundens instruktioner är bindande och att kunden har rätt till revision.** Dokument

Vad som styrker det: Beviset är det undertecknade personuppgiftsbiträdesavtalet enligt artikel 28 i dataskyddsförordningen med bilagan över åtgärder och en rätt till revision eller information. Fråga till leverantören: Lämna det undertecknade personuppgiftsbiträdesavtalet inklusive bilagor, inte enbart en hänvisning till allmänna användarvillkor.

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.12 **Underleverantörer som behandlar personuppgifter omfattas av minst samma skyldigheter som leverantören själv. Urvalet av dem och den löpande övervakningen styrs av en fastställd process.**

Vad som styrker det: Beviset är vidareförda skyldigheter i avtalen med underleverantörer (artikel 28.4 i dataskyddsförordningen) och en leverantörsbedömning med datum. Fråga till leverantören: Hur bedömer ni era underleverantörer och vilka bevis kräver ni av dem?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.11.13 **Innan lagringsutrymme återanvänds är det säkerställt att inga uppgifter från tidigare användare förblir åtkomliga, varken på fysiska medier eller i virtualiserade miljöer.**

Vad som styrker det: Beviset är rutinen för rensning eller överskrivning när lagring frigörs, redovisande dokument om förstöring av medier och den separation mellan kunder som beskrivs i arkitekturdokumentet. Fråga till leverantören: Hur säkerställer ni att återanvänd lagring inte innehåller restdata från andra kunder?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.12 Efterlevnad av dataskydd 3

A.12.1 **De länder där personuppgifter lagras och behandlas är angivna och kända för molnkunden. Ändringar av lagringsplatserna meddelas.** Dokument

Vad som styrker det: Beviset är leverantörens översikt över anläggningar och regioner, i avtalet eller i dokumentationen, plus en skärmbild av regioninställningen för den tjänst som används. Fråga till leverantören: I vilka länder ligger våra uppgifter lagrade, från vilka länder sker åtkomsten, till exempel i supporten, och kan vi låsa regionen?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

A.12.2 **Överföringar av personuppgifter till tredjeland är kända, motiverade och täckta av lämpliga skyddsåtgärder.** Dokument

Vad som styrker det: Beviset är standardavtalsklausuler eller ett beslut om adekvat skyddsnivå, styrkt av en konsekvensbedömning av överföringen, som för en liten verksamhet får vara kort: berörda datakategorier, mottagarland, risk, vidtagna kompletterande åtgärder. Fråga till leverantören: På vilken rättslig grund överför ni uppgifter till tredjeland och vilka kompletterande åtgärder tillämpar ni?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering

5.31 **De lagkrav och avtalskrav som gäller för behandling av personuppgifter är kartlagda och hålls aktuella när rättsläget ändras. Motstridiga jurisdiktioner är bedömda.**

Vad som styrker det: Beviset är en översikt över de tillämpliga kraven (dataskyddsförordningen, nationella regler, branschspecifika skyldigheter) med ansvarig och datum för genomgång. I en liten verksamhet räcker en lista på en sida som ses över en gång per år. Fråga till leverantören: Omfattas ni eller era underleverantörer av jurisdiktioner som ger myndigheter åtkomst till våra uppgifter och hur hanterar ni det?

○ Öppet ○ Pågår ○ Uppfyllt ○ Ej tillämpligt

Bevis / motivering