ISO	Krav	Nuläge	Kommentar	Handlingsplan	Ansvarig	Åtgärdsbehov	Datum
4.1	Organisationen avgör vilka externa och interna frågor som är relevanta för dess syfte och som påverkar dess förmåga att nå de avsedda resultaten med ledningssystemet för informationssäkerhet (LIS).	Ja	Centralt ledningssystem bör ses som tillräckligt. Ses över i övrigt med det här dokumentet.				
4.2	Organisationen fastställer vilka intressenter som är relevanta för ledningssystem för informationssäkerhet (LIS) och vilka av deras krav som är relevanta för informationssäkerheten.	Delvis	Lagar har definierats, ingår i kvalitetsfrågorna och getts ansvarig chef. Intressenter i övrigt i analysarbete utgår dock från individ, verksamhet, ekonomi och samhälle.	Intressenter utifrån kategorier av intressenter skulle kunna hjälpa organisationen ytterligare att förstå informationssäkerheten. Vilken relation olika delar av allmänhet har till förvaltningen utifrån kundrelation, myndighetsutövning/ servicegivare m.m. En sådan lista skulle lättare kunna användas i riskanalysarbete och informationssäkerhetsarbete. Det skulle också kunna underlätta och skapa större förståelse för att hämta in synpunkter vid t.ex. konsekvensbedömningar så att företrädare för intressenter kan ge input. Förslag till handlingsplan är att skapa ett dokument som bilaga till nästa års uppdaterade rutin.	ISAM	Låg	Februari

4.3	Organisationen fastställer gränserna och tillämpligheten för ledningssystemet för informationssäkerhet (LIS) för att bestämma dess omfattning.	Ja	Lokala anvisningar kompletterar stadens centrala och innehåller även begränsningar och omfattning. Övrigt för denna är frågan irrelevant.			Ingen	
4.4	Organisationen upprättar, inför, underhåller och förbättrar ständigt sitt ledningssystem förinformationssäkerhet (LIS).	Ja	Finns i årshjul				
5.1	Högsta ledningen visar ledarskap och engagemang i fråga om ledningssystem för informationssäkerhet (LIS).	ja	Ledningen har aktivt engagerat sig i fråan och informationssäkerhetsarbetet finns tydligt med , med egna årshjul och i verksamhetsplanen. Ledningen deltar i ledningens genomgång och beslutar om tilsättning av objektägare.			Ingen	
5.2	Högsta ledningen fastställer en informationssäkerhetspolicy.	Ja	Riktlinje tas av staden centralt. För organisationen lokalt finns lokala anvisningar. Lokala tillämpningsanvisningarna är anpassade efter stadens centrala riktlinje och centrala tillämpningsanvisningar.			Ingen	

5.3	Högsta ledningen säkerställer att roller som är relevanta för informationssäkerhet tilldelas ansvar och befogenheter och att dessa kommuniceras inom organisationen.	Delvis	Nya lokala tillämpningsanvisningar har tagits fram, och PM3-modellen implementeras samt kompletteras med dataskyddshandläggare. Roller har utsett till stora delar men är inte helt klart. Tilldelade uppgifter och avgränsningar har gjorts med nya rutiner. Implementeringen och förståelse för ansvar är inte fullt klart i organisationen.	Ökad utbildning för dataskyddshandläggare och objektledare. Behov av enklare "steg för steg"-dokumentation för nya objektledare. Denna del bör tydligt ingå i verksamhetsplan.	ISAM och PM3-införare	Medel	Under 2024, med kontrollpunkter i tertialrapporter.
6.1.1	När organisationen planerar sitt ledningssystem för informationssäkerhet (LIS) bör den avgöra riskeroch möjligheter genom att beakta de frågor som hänvisas till i 4.1 och de krav som hänvisas till i 4.2.	Delvis	För att fullfölja målet med informationssäkerhetsarbetet krävs förmåga att se risker och hitta åtgärder. Det finns verktyg i stadens arbete på naturligt sätt med RSA och VOR, men behöver samordnas bättre med informationssäkerhetsfrågor där analyser av tidigare års händelser också kan tas med. I stadens säkerhetsarbete finns snart färdiga mallar för hantering av riskanalyser, i väntan på dessa har förvaltningen framtagit egna. Förvaltningens mallar är till stor del kompatibel med framtida mall från staden då den följer andra risk-bedömningsfaktorer.	Analyser görs i samband med RSA och VOR-arbetet där ISAM involveras tidigt i arbetet för att uppmärksamma vilka delar som kan behöva ses på närmare. När stadens nya riskanalysmetod har tagits fram bör förvaltningens egna rutin anpassa och komplettera denna. Förvaltningen kan fortfarande behöva egna lokala rutiner som visar på vem som äger risker och hur acceptans eller hantering av risker ska göras.	Avdelningschef för verksamhetsstöd och stadsmiljö	Hög	Inför nästkommande VOR och RSA.

6.1.2	Organisationen fastställer och tillämpar en process för bedömning av informationssäkerhetsrisker.	Ja	Process finns både för RSA/VOR och för riskanalyser för enskilda system eller processer. Rutin antagen och arbetas med praktiskt.		ISAM	Ingen	
6.1.3	Organisationen fastställer och tillämpar en process för behandling av informationssäkerhetsrisker.	Delvis	IA-systemet används. Kompletteringar behövs enligt följande: när risker måste åtgärdas, när risker kan klarmarkeras - tvingande riskmatris. En struktur för bedömning av informationssäkerhetsrisker vid riskanalyser finns dock.	Förtydligande rutin om tidsaspekter för risker och behov av att bedöma risker och hur de ska hanteras	HR i samverkan med ISAM	Hög	Föreslås finnas med i nästkommande verksamhetsplan.
6.2	Organisationen fastställer informationssäkerhetsmål för relevanta funktioner och nivåer och planerar hur dessa mål ska uppnås.	Ja	Ingår i ILS och i ledningens genomgång.			Ingen	
7.1	Organisationen fastställer och tillhandahåller resurser för att upprätta, införa, underhålla och ständigtförbättra ledningssystemet för informationssäkerhet (LIS).	Ja	Förvaltningen har tydligt satsat resurser på informationssäkerhet genom tilldela tid till informationssäkerhetssamordnare. För att behålla god kvalitet krävs att ledningen fortsätter ge rollen den tid och vidareutbildning som krävs.			Ingen	

7.2	Organisationen avgör kompetensen hos de personer som behövs för informationssäkerhetens prestanda, och säkerställer att dessa personer har rätt kompetens.	Nej	Dokumentation saknas.	Ledningen bör tillsammans med ISAM sätta upp lista på utbildningsbehov och för specifika roller. Kompetenskravet bör beaktas vid rekryteringar och för kompetensutveckling och följas upp vid årshjul.	Avdelningschef för verksamhetsstöd och stadsmiljö	Låg	Tas fram och hanteras under 2024 i VP
7.3	Personer som arbetar inom eller åt organisationen görs medvetna om informationssäkerhetspolicyn, sina bidrag till ett väl fungerande ledningssystem för informationssäkerhet (LIS), fördelarna med att informationssäkerhetens prestanda förbättras och konsekvenserna av att kraven i ledningssystemet för informationssäkerhet (LIS) inte uppfylls.	Delvis	Obligatorisk utbildning finns, få genomför	Nytt utbildningspaket har tagits fram i staden. Rutin behöver arbetas fram för hur dessa på effektivt sätt kan genomföras och följas upp.	ISAM tillsammans med HR	Låg	Tas fram och hanteras under 2024 i VP
7.4	Organisationen avgör behovet av intern och extern kommunikation som rör ledningssystemet för informationssäkerhet (LIS).	Ja	Information har satts upp som del av process inom informationssäkerhet. Chefer och vissa medarbetare får särskild information årligen.			Ingen	

7.5.1	Organisationen ser till att ledningssystemet för informationssäkerhet (LIS) innehåller dokumenterad information som krävs direkt enligt ISO/IEC 27001 och dokumenterad information som organisationen har bestämt är nödvändig för ett väl fungerande ledningssystem för informationssäkerhet (LIS).	Ja	Ständigt förbättringsarbete, men nuvarande riktlinjer och rutiner innebär att det finns ett årshjul och plan för ledningssystemet.			Ingen	
7.5.2	När dokumenterad information skapas och uppdateras ska organisationen säkerställa lämplig identifiering och beskrivning, lämpligt format och medium samt granskning och godkännande.	Ja	Följer de lagar som finns, för rutiner inom ledningssystem finns särskilt årshjul och bestämmelse om vem som fastställer och hur dessa ska se ut.			Ingen	
7.5.3	Organisationen hanterar den dokumenterade informationen under hela dess livscykel och gör den tillgänglig där och när det behövs.	Delvis	Viss störning har skett i framtagandet av nytt intranät.	Lokala anvisningarna för 2024 behöver även beskriva var på intranätet underrutiner för informationssäkerhet finns. Rutinerna behöver uppdateras om hur kommunikation om nya rutiner sker då de inte naturligt är samlade på en plats.	ISAM	Medel	Tas fram med nästa uppdatering av lokala tillämpningsanvisningar.

8.1	Organisationen planerar, inför och styr processer för att uppfylla informationssäkerhetskraven och uppnå sina informationssäkerhetsmål. Organisationen bevarar den dokumenterade information som krävs för att ge tilltro till att processerna genomförs som planerat. Organisationen styr planerade ändringar och granskar konsekvenserna av oavsiktliga ändringar, och ser till att outsourcade processer identifieras, definieras och styrs.	Delvis	Det finns rutiner för incidentrapportering, rutiner för bevarande av information och rutiner för ILS-hantering vad gällller rapporter liksom årshjul och återkommande händelser i lokala tillämpningsanvisningar. I övrigt är detta en fråga för varje objekt	Objektrelaterat och anses uppnådd när samtliga objekt har klassats.	Objektägare - ISAM följer upp	Låg	Uppföljning under 2024
8.2	Organisationen gör bedömningar av informationssäkerhetsrisker och bevarar dokumenterad information om resultaten från dessa.	Delvis	ISAM har inte varit inblandad i RSA-arbetet, dock i VOR. Stockholms stads mallar följs. Viss tillägg behövs även för kontinuerliga informationssäkerhetsrisker i IA - beskriven åtgärd finns i 6.1.3	Förbättrad samordning med RSA-ansvarig och nya säkerhetsstrategen genom informationssäkerhetsarbetet. Informationssäkerhetsrisker måste ingå naturligt i det övergripande riskarbetet.	Säkerhetssamordnare	Medel	December
8.3	Organisationen genomför planen för behandling av informationssäkerhetsrisker och bevarar dokumenterad information om resultaten av behandlingen av informationssäkerhetsrisker.	Delvis	ISAM har inte varit inblandad i RSA-arbetet, dock i VOR. Stockholms stads mallar följs	Förbättrad samordning med RSA-ansvarig och nya säkerhetsstrategen genom informationssäkerhetsarbetet	Säkerhetssamordnare	Medel	December
9.1	Organisationen utvärderar informationssäkerhetsprestandan och effektiviteten hos ledningssystemet för informationssäkerhet (LIS).	Ja	Utvärderas med ledningens genomgång och i VB/tertialrapporter.				

9.2	Organisationen genomför internrevisioner för att få information om i vilken utsträckning ledningssystemet för informationssäkerhet (LIS) överensstämmer med kraven.	Nej	Enligt staden ingår uppgiften i Stadsrevisionens revisorsprogram. ISAMs bedömning: Staden gör dock ingen specifik revision enligt ISO 27001. Förvaltningen behöver själva bedöma om detta är ett relevant krav för organisationen.	Bedöms som inte aktuellt krav för förvaltningen om staden inte har det		Ingen	
9.3	Högsta ledningen går igenom ledningssystemet för informationssäkerhet (LIS) vid planerade intervall	Ja	Finns i årshjul			Ingen	
10.1	Organisationen reagerar på avvikelser, utvärderar dem, gör korrigeringar och vidtar korrigerande åtgärder vid behov.	Delvis	Incidentrapporteringsrutiner finns på plats, synpunkt och klagomålshantering finns på plats. ILS-systemet innehåller åtgärdsfunktioner. Infosäk-gruppen går igenom händelser. Tidsaspekterna har dock visat sig ha brister och många gånger har riskerna inte identifierats.	Utbildning och behov av att vara med i VOR	ISAM och HR	Ingen	2024, i VP
10.2	Organisationen förbättrar ständigt ledningssystemet för informationssäkerhets (LIS) lämplighet, tillräcklighet och verkan.	Ja	Finns i årshjul			Ingen	