Revisionsrapport 7/2018
Genomförd på uppdrag av revisorerna

Upplands Väsby kommun

Granskning av informationssäkerhet

13 december 2018

Building a better working world

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Upplands Väsby kommun har EY genomfört en granskning av informationssäkerhet vad gäller policyer, riktlinjer och hantering av informationssäkerhetsstyrning på övergripande nivå i kommunen. Syftet med granskningen har varit att undersöka om kommunen säkerställer tillräcklig styrning och intern kontroll vad gäller informationssäkerhet. Granskningen har gjorts mot etablerad standard inom informationssäkerhetsstyrning och utgått från rekommendationerna i den internationellt erkända standarden för informationssäkerhetsstyrning - ISO27000-serien).

Övergripande slutsatser

Den samlade bedömningen är att ett antal gap noterats vad gäller styrning av informationssäkerhet, men att arbete med att få styrning på plats påbörjats.

I och med att arbetet med informationssäkerhet i kommunen inte tidigare så tydligt varit inriktat på att struktureras utefter ett ledningssystem för informationssäkerhet blir svaren på ett antal av kontrollpunkterna att det ej finns på plats (eftersom kontrollpunkterna som mätts är fokuserade på styrningsfrågor). Detta behöver i sig inte nödvändigtvis innebära att informationssäkerheten i sig är bristfällig.

Av samtliga 78 granskningspunkter är fördelningen av bedömningarna följande:

Överensstämmer med beskrivning och/eller fungerar tillfredsställande	15 %
Överensstämmer delvis med beskrivning och/eller fungerar delvis tillfredsställande	17 %
Inte varit någon uttalad ambition/Överensstämmer ej med beskrivning och/eller ej fungerar tillfredsställande	63 %
Ej applicerbart	5 %

I nuläget finns det gap inom flera av de granskade områdena. Det pågår dock initiativ för att förbättra styrning och kontroll inom samtliga.

De områden där styrningen av informationssäkerhet uppvisat störst gap ligger inom planering/riskhantering (har inte varit någon uttalad ambition med sammanhållen riskanalysprocess), resurser (huruvida informationssäkerhetsarbetet tilldelats tillräckliga resurser för att bedriva systematiskt informationssäkerhetsarbete och styrning av detsamma) samt processer (för att säkerställa att verksamheten möter krav och driver fram handlingar för att säkerställa att man uppfyller målen för informationssäkerhetsarbetet) och utvärdering av styrningsarbetet (detta handlar om att följa upp så att styrningen av informationssäkerhet är rätt riktad och att rätt saker görs, på ett bra sätt).

Avsaknad av etablerad komplett styrning tillsammans med avsaknad av uppdaterade kommunicerade riktlinjer för hur anställda ska hantera IT- och informationssäkerhet kan

utsätta verksamheten för större risker.

Kommunen har inlett ett Informationssäkerhetsprojekt som innefattar att få på plats ett omfattande arbete av uppdaterat ramverk och policys och riktlinjer med inspiration från ISO 27000-serien. Detta arbete adresserar flertalet av de gap som noterats.

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Fullständiga iakttagelser och rekommendationer återfinns i kapitel 4.

	Iakttagelse och rekommendation	Prioritet
1	Resurser Det har inte varit en uttalad ambition att ha styrning på plats i nivå med ledningssystem för informationssäkerhet. Det rekommenderas att säkerställa en nivå av resurser, med rätt kompetenser, som kan upprätthålla och underhålla ett systematiskt arbete med styrning av informationssäkerhet. Det är grunden för alla andra frågor kopplade till arbetet med informationssäkerhet.	Hög
2	Riskbaserade kontroller och aktiviteter Det har inte varit någon uttalad ambition att ta fram kontroller och aktiviteter utifrån riskanalyser för verksamheten. För att säkerställa att rätt resurser läggs på rätt aktiviteter rekommenderas att riskanalys och hantering integreras i arbetet med informationssäkerhetsstyrning.	Hög
3	Monitorering av styrning Det har inte varit någon uttalad ambition att kontinuerligt övervaka, och utvärdera hur väl styrningen av informationssäkerhet fungerar. Det rekommenderas att ledningssystemet definieras, och att mätkriterier därefter definieras så att kommunen kan säkerställa kvaliteten i sin styrning av informationssäkerhet.	Hög
4	Policyarbete Kommunen har inte uppdaterat sin informationssäkerhetspolicy på två år vilket innebär en risk att den inte är anpassad efter förändrade omständigheter i organisationen och omvärlden. Policyn är i sådant fall bristfällig och det rekommenderas att den ses över löpande, åtminstone en gång per år. Notering: Enligt information är organisationen på gång att implementera vedertagen metod för ledning av informationssäkerhetsarbetet (med inspiration från ISO27000-serien). En sådan implementering skulle hantera flertalet av de frågor som berörs i materialet.	Medel
5	Uppföljning avtal Kommunen förlitar sig på att leverantörerna håller sina delar av avtalen och genomför inte själva några systematiska säkerhetstester för att identifiera sårbarheter. Samtidigt sker det i flera fall inte någon uppföljning av leverantörerna förutom den granskning som sker då avtalen skrivs under. Det rekommenderas att Upplands Väsby implementerar en process för regelbunden granskning och revidering av avtal.	Medel
6	Utbildningsinsatser Det saknas ett strukturerat utbildningsprogram inom organisationen för att säkerställ adekvat kunskapsnivå inom informationssäkerhet inom organisationen. I och med detta riskerar bristande kunskap och medvetenhet exponera och utsätta organisationen för informationssäkerhetsrisker. Det rekommenderas att ett strukturerat och gediget utbildningsinitiativ implementeras.	Medel

Innehåll

1. Bakgrund

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå målen för en kommuns verksamhet krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har starkt skydd och är spårbar.

Informationssäkerhet omfattar hela kommunens verksamhet och all information oavsett om den finns i datorer, i ett telefonsamtal eller på ett papper. Då stora delar av informationen hanteras med hjälp av IT-system så handlar informationssäkerhet även om teknik. Intrång i IT- och informationssystem blir allt mer vanligt och utgör därmed en central risk för en offentlig verksamhet som handhar en mängd känslig information. För att kunna säkerställa en tillräcklig nivå av informationssäkerhet i en kommuns olika förvaltningar och bolag är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt. Brister i kommunens systematiska IT- och informationssäkerhetsarbete kan skada medborgarnas förtroende för kommunen. Det kan också äventyra kommunens efterlevnad av lagkrav och det kan skada kommunens ekonomi genom att säkerhetsincidenter uppstår. I takt med att kommunens verksamheter blir allt mer beroende av IT-stöd ökar även behovet av IT-säkerhet. IT-säkerhet är en del av det övergripande begreppet Informationssäkerhet, vilket omfattar IT-säkerhet och administrativ säkerhet som är relaterad till hantering av information i olika verksamheter.

Standarder kring informationssäkerhet har samlats i standardserien 27000. Den har tagits fram inom ramen för samarbetet i de internationella standardiseringsorganen ISO (International Organization for Standardization) och IEC (International Electrotechnical Commission). Standarderna arbetas fram mot bakgrund av de deltagande internationella experternas samlade erfarenheter av ett systematiskt arbete med informationssäkerhet och är strukturerade i tre nivåer: krav, riktlinjer och stöd. Dessa olika nivåer visar vad (krav) en organisation bör göra när det gäller informationssäkerhet samt hur (riktlinjer och stöd) man kan arbeta. ISO 27000-serien bedöms mot ovan bakgrund vara en lämpad utgångspunkt för granskning av informationssäkerhetsstyrning.

Upplands Väsby kommun har enligt information implementerat ett arbete för att möta kraven för dataskyddsförordningen (General Data Protection Regulation GDPR). EY's GDPR-granskningsmetod har inte ingått i scope/omfattning för den genomförda informationssäkerhets-undersökningen. Med scope avses den omfattning och avgränsning som satts för granskningen.

1.1 Syfte

Syftet med granskningen har varit att undersöka om kommunen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller informationssäkerhet och IT-säkerhet. För att besvara granskningens syfte och bedöma kommunens rutiner har granskningen utgått från följande områden:

- Finns en definierad organisationskontext med identifierade mål och intressenter?
- Finns en tydlig styrning av informationssäkerhet och IT-säkerhet i kommunen genom tydliga och ändamålsenliga policys och styrdokument?

- Finns en process för strukturerad kontroll och uppföljning avseende att policys och styrdokument efterlevs?
- Finns risker gällande kommunens informationssäkerhet dokumenterade och uppdateras denna dokumentation löpande?
- Har kommunen resurser med rätt kompetenser som kan upprätthålla och underhålla ett systematiskt arbete med styrning av informationssäkerhet.
- Får kommunens anställda tillräcklig och ändamålsenlig information och utbildning gällande IT-säkerhet?
- Finns det en tillräcklig intern kontroll och följer ansvariga upp arbetet med informationssäkerhet?
- Finns en utarbetad avvikelsehantering/ incidenthanteringsplan på plats?

1.2 Metod

Revisionsfrågorna har besvarats genom en granskning mot så kallad god praxis inom informationssäkerhetsområdet, genom intervjuer med utpekade personer i kommunen. Granskningen har gjorts mot utvalda delar av ISO 27000-serien.

EY har genomfört en övergripande kartläggning av kommunen och dess informationssäkerhets/IT-styrning genom att fokusera på sju omfattande områden:

1. Organisationskontext – Identifiera syfte, mål, intressenter etc.
2. Styrning – Styrdokument så som dokumenterade policys och Ansvar& roller
3. Planering – Identifiera risker och möjligheter, riskhantering
4. Stöd – Resurser, kompetens, kommunikation
5. Verksamheten/ drift– Operativ planering, processer, kontroller, riskanalys och åtgärder
6. Utvärdering – Ledningssystem, internrevision, Management Review
7. Förbättringsarbete – Avvikelsehantering och uppföljning

Innan granskningen påbörjades hölls ett initierande telefonmöte med Upplands Väsbys kommuns digitaliseringsdirektör Kristina Tormod. Under detta möte beskrevs syftet med granskningen, upplägget samt revisionsfrågorna som skulle besvaras. Granskningen genomfördes sedan först via insamling och granskning av information av befintliga styrande dokument. Därefter genomfördes intervjuer med de personer som ansågs kunna ge en bild över verksamheten, för djupare förståelse för aktuella processer, övergripande rutiner samt verksamma kontroller.

Eftersom majoriteten av de grundläggande kontrollpunkterna besvarats med att de inte är på plats eller att de ej är applicerbara har inte granskningen utökats i omfattning utöver de personer som intervjuats i verksamheten. (Granskarna har inte gett sig ut för att undersöka/motbevisa att kontroller *inte* finns på plats.)

Då Upplands Väsby kommun under denna granskning hade ett pågående arbete med utveckling av riktlinjer för informationssäkerhet har även utkastet till detta dokument inhämtats. Dock har EY inte tagits hänsyn till utkastet vid granskningen. Det eftersom riktlinjerna inte ännu är godkända, varpå de inte spridits inom kommunen och således inte ännu efterlevs.

Under granskningen intervjuades:

- Kristina Tormod- Digitaliseringsdirektör, digitalisering och processutveckling
- Stig Fjeldheim- Systemförvaltare, leder systemförvaltarenheten
- Magnus Gruvstedt, Informationssäkerhetssamordnare

Därefter har denna rapport utformats som underlag för revisorernas bedömning av styrningen av informationssäkerheten i kommunen. Rapporten beskriver vår bedömning av kommunens mognadsgrad per huvudområde samt våra iakttagelser och rekommendationer.

2. Granskning

2.1 Granskningsprotokoll

Följande avsnitt innehåller de frågor som ingick i granskningen samt varje enskild frågas efterlevnadsbedömning (*Möter*/*Möter ej*/*Möter delvis* eller *N/A*) erhållet från intervjun. Upplands Väsby saknar vissa grundläggande delar för informationssäkerhetssyrning. Under intervjun har det framkommit att organisationen inte haft någon uttalad ambition inom flera områden som presenteras nedan, dessa delkomponenter besvaras med *Möter ej*. För en del av frågorna anser kommunen att bedömningen borde vara *N/A* eftersom att organisationen inte ansett de vara prioriterade. I rapporten kommer det framgå i svaret att "Det har inte varit någon uttalad ambition" men bedömningen kommer vara *Möter ej*.

Överensstämmer med beskrivning och/eller fungerar tillfredsställande	**Möter**
Överensstämmer delvis med beskrivning och/eller fungerar delvis tillfredsställande	**Möter delvis**
Inte varit någon uttalad ambition/Överensstämmer ej med beskrivning och/eller fungerar ej tillfredsställande	**Möter ej**
Ej applicerbart	**N/A**

Standardens frågor är på engelska och är inte översatta till svenska.

På ett antal ställen förekommer förkortningen ISMS, vilket är den engelska förkortningen för information security management system. Detta kallas på svenska "Ledningssystem för informationssäkerhet" (LIS) och är en vanligt förekommande term inom informationssäkerhet och standardserien ISO27000. ISO-standarder finns även på svenska, och kan köpas från ISO-organisationens hemsida.

1. Organisationens kontext			
Delklausul	**Fråga**	**Bedömning**	**Observation / Gap**
4.1 Understanding the Organisation and its context	Has the Organisation identified and documented the internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS?	Möter delvis	Ledningssystem finns, men ej komplett och eller strukturerat enligt ISO 27000. Arbete pågår med att etablera ett Ledningssystem för informationssäkerhet (LIS). Organisationen har gjort en övergripande verksamhetsanalys. Har använt mallarna från informationssäkerhet.se.
	Has the Organisation identified and documented the external issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS?	Möter delvis	Se ovan. Ledningssystem finns, men ej komplett och eller strukturerat enligt ISO 27000.
4.2 Understanding the needs and expectations of interested parties	Has the Organisation identified and documented legal and regulatory requirements or contractual obligations for their ISMS?	Möter delvis	Påbörjat i *Informationssäkerhetsinstruktion Förvaltning*. Arbetsmaterial och första kartläggning finns på plats. Pågående Infosäk-projekt ska uppfylla detta.
	4.2 a) Have interested parties that are relevant to the ISMS been identified and documented?	Möter	Ja, se *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205.* Roller (& Ansvar) s. 3. Även s 1. "Till för Användare, drift och förvaltning"
	4.2 b) Has the Organisation identified and documented the requirements of these interested parties relevant to information security?	Möter	Ja, se *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205.* Roller (& Ansvar) s. 3. Se även sida 4 i *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205.pdf*. Generella krav.
4.3 Determining the scope of the Information Security Management System (ISMS)	Has the scope, including the boundaries and applicability of the ISMS been defined, documented and reviewed on a periodic basis?	Möter delvis	I det nya policyarbetet (Informationssäkerhetsprojektet) ingår definition av information osv. Det finns ett Scope av definitioner men ingen periodisk utvärdering sker.
	4.3 a) Have the external and internal issues referred to in 4.1 been considered in relation to the scope?	Möter delvis	Täcks i det pågående Informationssäkerhetsprojektet (hädan efter benämnt som Infosäk-projektet)

	4.3 b) Have the requirements referred to in 4.2 been considered in relation to the scope?	Möter delvis	Täcks i det pågående Infosäk-projektet
	4.3 c) Have the interfaces and dependencies between activities performed by the Organisation, and those that are performed by other Organisations been considered in relation to the scope?	Möter delvis	Detta täcks i det pågående Infosäk-projektet: Externa parter och hur man arbetar med dessa ingår i det nya arbetet.
4.4 Information security Management system	Has the Organisation established Processes in accordance with the requirements of the Standard to establish, implement, maintain and continually improve an ISMS?	Möter ej	Nej, har inte etablerat något som kan underhållas, förbättras etc. ännu. Det har inte heller varit någon ambition. Finns dock inom GDPR. UV arbetar i nuläget med att sätta processer kopplade till GDPR och systemförvaltning.
2. IT-styrning (ledning)			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**
5.1 Leadership and commitment	5.1 a) Have the information security Policies and the information security Objectives been defined and documented? Are these compatible with the overall strategic direction of the Organisation?	Möter delvis	Se sid 3, Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205. Här täcks målen men ingen förklaring till hur dessa förhåller sig till kommunens övergripande strategi. Säkerhetsdokumenten är inte kopplade till kommunens strategi. Kommande digitala strategi tänkt att täcka detta (ska beslutas 3 dec).
	5.1 b) Has the Organisations Management facilitated the integration of the ISMS requirements into the Organisations Processes?	Möter ej	UV har inte satt något ledningssystem för informationssäkerhet (än). Processer finns och är på agendan. Dock är inte infosäk integrerat i verksamhetsprocesser i nivå med ISO27000.
	5.1 c) Has the Organisations Management provided adequate resources required for the success of the information security management system (ISMS)? (ISMS är den engelska förkortningan av ledningssystem för informationssäkerhet – LIS)	Möter ej	Har inte varit någon uttalad ambition. Tillräckliga resurser har inte avdelats för att hittills få styrning och kontroll av informationssäkerhetsarbetet etablerat fullt ut. Konsult arbetar dock på att ta fram målbild med informationssäkerhetsarbetet.

	5.1 d) Has the importance of effective information security Management and of conforming to the ISMS requirements been communicated to all relevant stakeholders?	Möter ej	Har inte varit någon uttalad ambition. På gång, Planen är att utbilda och informera alla forum och kontorschefsgruppen.
	5.1 e) Does the Organisations Management validate that the ISMS has achieved its intended outcome(s)?	Möter ej	Har inte varit någon uttalad ambition. Följs inte upp. Det finns inga mål i målstyrningen (Verksamhetens övergripande ledningssystem eller uppföljning så som stickprovstestning i internstyrningen). Tanken är att få in det i ledningssystemet.
	5.1 f) Does the Organisations Management direct and support Personnel to contribute to the effectiveness of the ISMS?	Möter ej	Har inte varit någon uttalad ambition. Nej, har för närvarande inte detta på plats.
	5.1 g) Does the Organisations Management promote continual improvement of the ISMS and related components?	Möter ej	Har inte varit någon uttalad ambition. Finns för närvarande ingen applicerbar struktur.
	5.1 h) Does the Organisations Management support other relevant roles within the Organisation to demonstrate their leadership as it applies to their areas of responsibility in relation to the ISMS?	Möter ej	Har inte varit någon uttalad ambition. Vad gäller GDPR finns utpekade lokala roller. Dock inte kring övrigt Infosäkerhetsarbete.
5.2 Policy Undertaken by top Management	5.2 a) Has an information security Policy been defined and documented that is appropriate to the purpose of the Organisation?	Möter	Det finns en uppsatt policy samt specificerade mål. Se *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205.* Avstämt att det som står är utifrån kommunens funktion/behov.
	5.2 b) Does the information security Policy include Objectives or provide the framework for setting those Objectives?	Möter	Det finns en uppsatt policy samt specificerade mål. Se Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205. Se sid 3, sektion "Mål för informationssäkerhetsarbetet".

	5.2 c) Does the information security Policy include a commitment from the Organisation to satisfy applicable requirements related to information security (this includes, but is not limited to the requirements identified as a part of clause 4)?	Möter	Ja, se *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205* s.4 samt kommande policy.
	5.2 d) Does the information security Policy include a commitment to continual improvement of the ISMS?	Möter	Ja, se *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205* s.4
	5.2 e) Has the information security Policy been made available as documented information?	Möter	Finns på intranätet. Antagna policydokument är publicerade.
	5.2 f) Has the information security Policy been communicated within the Organisation?	Möter	Finns på intranätet. Antagna policydokument är publicerade.
	5.2 g) Has the information security Policy been made available to interested parties, as appropriate (this includes the interested parties identified as a part of clause 4)?	Möter delvis	Policyn kommuniceras inte till intressenter så som t.ex. externa parter vid anlitande av leverantörer. UV kommunicerar relevanta säkerhetskrav under en upphandling. Dock frågetecken kring privata aktörer och vilka krav som ställs i samband med dessa uppdrag.
5.3 Organisational roles, responsibilities and authorities Undertaken by top Management	5.3 a) Has the Organisations Management assigned the responsibility and authority for validating that the ISMS conforms to the requirements of the International Standard?	NA	N/A - Finns ingen ansats att certifiera enligt 27k
	5.3 b) Has the Organisations Management assigned the responsibility and authority to report on the performance of the ISMS?	NA	N/A - Finns ingen ansats att certifiera enligt 27k
3. IT-planering			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**

6.1 Actions to address risks and opportunities	For planning the establishment, management and improvement of the ISMS, has the Organisation considered the issues referred to in 4.1 and the requirements referred to in 4.2 and performed a risk assessment to identify risks and opportunities that achieve the following: a) validate that the ISMS can achieve its intended outcome(s); b) prevent, or reduce, undesired effects; and c) achieve continual improvement.	Möter ej	Har inte varit någon uttalad ambition. Finns inte i dagsläget. Kommunen har inte genomfört någon riskanalys som verifierar att informationssäkerhetsramverket/styrningen fungerar som tänkt, och säkrar kontinuerlig/ständig förbättring.
	Has the Organisation planned the following: a) actions to address the identified risks and opportunities; and b) how to: 1) integrate and implement the actions into its ISMS Processes; and 2) evaluate the effectiveness of these actions.	Möter ej	Har inte varit någon uttalad ambition. Nej, se ovan.

6.1.2 Information security risk assessment	Has the Organisation defined, documented and implemented an information security risk assessment Process that: a) establishes and maintains information security risk criteria that include: 1) the risk acceptance criteria; and 2) criteria for performing information security risk assessments; b) makes certain that repeated information security risk assessments produce consistent, valid and comparable results; c) identifies the information security risks: 1) apply the information security risk assessment Process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS; and 2) identify the risk owners; d) analyses the information security risks: 1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize; 2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and 3) determine the levels of risk; e) evaluates the information security risks: 1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and 2) prioritize the analysed risks for risk treatment.	Möter delvis	Finns ingen sammanhållen process/modell. Men vid behov görs riskanalyser. Delar finns på plats i det pågående Infosäk-projektet. Det finns ett utkast som täcker hur man ska klassa information och system. Här är det även värt att vara medveten om att nivåer för t.ex. riskacceptans är lättare sagt än gjort att få till för offentlig verksamhet.
6.1.3 Information security risk treatment	Has the Organisation retained documented information about the information security risk treatment Process?	Möter ej	Finns en grundläggande riskbedömningsmodell, men har inget med infosäk att göra. Kommunen har en generell riskhanteringsmodell. Det står inte uttryckligen i informationssäkerhetspolicy, men på intranätet går att finna en Risk- och konsekvensanalysmall. I policy står: ”Alla informationssystem ska minst klara en basnivå för informationssäkerhet som myndigheten MSB

			rekommenderar (BITS)". Enligt BITS ska information riskbedömas. Det har aldrig varit ett mål för kommunen att kravställa så specifikt kring informationshantering.
	Has the Organisation defined and applied an information security risk treatment Process to:		
	6.1.3 a) Select appropriate information security risk treatment options, taking account of the risk assessment results?	Möter ej	Nej, ej på plats. Har inte varit någon uttalad ambition.
	6.1.3 b) Determine all controls that are necessary to implement the information security risk treatment option(s) chosen? NOTE Organisations can design controls as required, or identify them from any source.	Möter ej	Ej på plats, se ovan. Har inte varit någon uttalad ambition.
	6.1.3 c) Compare the controls determined in 6.1.3 b) above with those in **Annex A** and verify that no necessary controls have been omitted?	NA	Endast relevant om organisationen vill bli certifierat eller uttryckligen jobbar mot 27k
	6.1.3 d) Produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A?	Möter ej	Ej på plats, se ovan. Har inte varit någon uttalad ambition.
	6.1.3 e) Formulate an information security risk treatment plan?	Möter ej	Ej på plats, se ovan. Har inte varit någon uttalad ambition.

	6.1.3 f) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks?	Möter ej	Ej på plats, se ovan. Har inte varit någon uttalad ambition.
6.2 Information security Objectives and planning to achieve them.	Has the Organisation retained documented information on the information security Objectives?	Möter	Det finns mål för informationssäkerhetsarbetet på s.3 i *Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205,*
	6.2 a) Are these Objectives consistent with the information security Policy?	Möter delvis	Finns mål i policyn, dock inga mål som är mer "dagligt" anpassade
	6.2 b) Are these Objectives measurable (if practicable)?	Möter ej	Har inte varit någon uttalad ambition. Under framtagning.
	6.2 c) Do the Objectives take into account applicable information security requirements, and results from risk assessment and risk treatment?	Möter ej	Har inte varit någon uttalad ambition. Ingen koppling till risk assessments. Finns och kommer finnas koppling till säkerhetskraven.
	6.2 d) Are these Objectives well communicated?	Möter ej	Målen är ej väl kommunicerade i dagsläget, förutom att policyn i sig är publicerad på intranätet. Målen som finns dokumenterade är de som finns i policyn. Policyn är kommunicerad via intranätet. Enligt UV är personerna som arbetar med frågorna troligen väl informerade, men inte gemene man ute i verksamheten.
	6.2 e) Are these Objectives updated as appropriate?	Möter ej	Har inte varit någon uttalad ambition. Pågående Infosäk-arbete uppdaterar mål. Tidigare år har det inte funnits någon ambition att uppdatera styrdokumenten löpande.
	When planning how to achieve its information security Objectives, has the Organisation determined: f) What will be done? g) What resources will be required? h) Who will be responsible? i) When it will be completed? j) How the results will be evaluated?	Möter ej	Har inte varit någon uttalad ambition. Nej, finns inte beslutat.

4. IT-stöd			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**
7.1 Resources	Has the Organisation determined and provided the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS?	Möter ej	Nej, tillräckliga resurser är dock grunden till arbete för god styrning av informationssäkerhet, och i förlängningen informationssäkerheten i sig, en mycket viktig komponent.
7.2 Competence	7.2 a) Has the Organisation determined the necessary competence of Personnel that affect its information security performance?	Möter	Ja, se Informationssäkerhet Användare. Information finns även i kommande riktlinjer om vilka kompetenser som identifierats.
	7.2 b) Has the Organisation validated that these Personnel are competent on the basis of appropriate education, training, or experience?	Möter ej	Utbildning i infosäk och GDPR har skett. Dock ingen uppföljning/validering.
	7.2 c) Has the Organisation, where applicable, taken actions to acquire the necessary competence, and evaluate the effectiveness of these actions taken?	Möter delvis	Projekt pågår för att analysera vilken kompetens som behövs och vilka utbildningsinsatser som erfordras.
	7.2 d) Has the Organisation retained appropriate documented information as evidence of competence?	Möter ej	Har inte varit någon uttalad ambition. Finns ej.
7.3 Awareness	Are persons working for the Organisation aware of: a) The information security Policy b) Their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance c) The implications of not conforming with the ISMS	Möter ej	Har inte varit någon uttalad ambition. Arbete tänkt att ingå i Infosäk-projektet.

7.4 Communication	Has the Organisation determined the need for internal and external communications relevant to the ISMS including: a) On what to communicate? b) When to communicate? c) With whom to communicate? d) Who shall communicate? e) The Processes by which communication shall be effected?	Möter ej	Nej, inte diskuterat.
7.5.1 General	Does the Organisations ISMS include: a) Documented information required by this International Standard? b) Documented information determined by the Organisation as being necessary for the effectiveness of ISMS?	Möter ej	Har inte varit någon uttalad ambition. International Standars. Då organisationen inte siktar på 27k cert så är endast (b) relevant. Dvs om man har analyserat och dokumenterat vilken information som behövs för att säkerställa att ISMS'et fungerar som det ska. Detta finns i dagsläget inte på plats.
7.5.2 Creating and updating	When creating and updating documented information has the Organisation made certain the following are documented: a) Identification and description (e.g. a title, date, author, or reference number) b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic) c) Review and approval for suitability and adequacy	Möter	Ja, denna process är automatiserad

7.5.3 Control of documented information	Has the Organisations documented information required by the ISMS and by this International Standard been controlled to make sure: a) It is available and suitable for use, where and when it is needed b) It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity) c) Distribution, access, retrieval and use d) Storage and preservation, including the preservation of legibility e) Control of changes (e.g. version control) f) Retention and disposition	Möter ej	Täcks vad gäller "vanlig" verksamhetsinformation, dock vad gäller ISMS-dokumentation (den info som ISMS'et kräver) är det inte uppfyllt. Följer inte standard, men policy och riktlinjer hanteras enligt organisationens krav.
5. Verksamheten/ drift			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**
8.1 Operational planning and control	Has the Organisation planned, implemented and controlled the Processes needed to meet information security requirements, and to implement the actions determined in 6.1?	Möter ej	Nej, finns inga processer på plats (6.1 handlar det om att ta fram handlingsplaner/process/aktiviteter för att adressera de internt/internt drivna riskerna man identifierat i tidigare steg).
	Has the Organisation implemented plans to achieve information security objectives determined in 6.2?	Möter ej	Nej, målen är ej satta än. Ett mål ska vara mätbart.
	Has the Organisation kept documented information to the extent necessary to have confidence that the Processes have been carried out as planned?	Möter ej	Nej, se svar ovan.

	Has the Organisation controlled planned changes and reviewed the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary?	Möter ej	Nej, se svar ovan.
	Has the Organisation taken measures to make certain that outsourced Processes are determined and controlled?	Möter ej	Inte "to make certain". Har ingen central styrning av uppföljningen av outsourcade/privata processer.
8.2 Information security risk assessment	Has the Organisation performed an information security risk assessment at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a)?	Möter ej	Har inte varit någon uttalad ambition. Finns inte, tanken är att det ska göras vid upphandlingar och större förändringar.
	Has the Organisation retained documented information of the results of the information security risk assessments?	Möter ej	Har inte varit någon uttalad ambition. Finns inte (till följd av att riskanalyser inte genomförs).
8.3 Information security risk treatment	Has the Organisation implemented the information security risk treatment plan?	Möter ej	Har inte varit någon uttalad ambition. Nej, inget riskarbete.
	Has the Organisation retained documented information of the results of the information security risk treatment?	Möter ej	Har inte varit någon uttalad ambition. Nej, inget riskarbete.

6. Utvärdering			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**
9.1 Monitoring, measurement, analysis and evaluation	Has the Organisation evaluated the information security performance and the effectiveness of the ISMS utilising a Performance Management Process that defines and documents: a) what needs to be monitored and measured, including information security Processes and controls b) The Methods for monitoring, measurement, analysis and evaluation, as applicable, to deliver valid results c) When the monitoring and measuring shall be performed d) Who shall monitor and measure e) When the results from monitoring and measurement shall be analysed and evaluate f) Who shall analyse and evaluate these results	Möter ej	Har inte varit någon uttalad ambition. Har ännu inte definierat ledningssystemet och hur man ska mäta det. Mätaktiviteter ej definierade än.
9.2 Internal audit	9.2 a) 1) Has the Organisation conducted internal audits at planned intervals to provide information on whether the ISMS conforms to its requirements for its ISMS?	Möter ej	Har inte varit någon uttalad ambition. Nej, Interngranskning sker ännu endast för kvalitetsledning, miljöledning men inte infosäk
	9.2 a) 2) Has the Organisation conducted internal audits at planned intervals to provide information on whether the ISMS conforms to the requirements of this International Standard?	NA	Endast relevant om organisationen vill bli certifierat eller uttryckligen jobbar mot 27k
	9.2 b) Has the Organisation conducted internal audits at planned intervals to provide information on whether the ISMS is effectively implemented and maintained?	Möter ej	Har inte varit någon uttalad ambition. Nej, ingen internrevision av informationssäkerhet.
	9.2 c) Has the Organisation planned, established, implemented and maintained an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting? The audit programme(s) shall take into consideration the importance of the Processes concerned and the results of previous audits?	Möter ej	Har inte varit någon uttalad ambition. Nej, ingen internrevision av informationssäkerhet.

	9.2 d) Has the Organisation defined the audit criteria and scope for each audit?	Möter ej	Har inte varit någon uttalad ambition. Nej, ingen internrevision av informationssäkerhet.
	9.2 e) Has the Organisation selected auditors and conduct audits that will bring objectivity and impartiality to the audit Process?	Möter ej	Har inte varit någon uttalad ambition. Finns inte någon process.
	9.2 f) Has the Organisation facilitated a Process to deliver the results of the audits to relevant Management?	Möter ej	Har inte varit någon uttalad ambition. Finns inte någon process.
	9.2 g) Has the Organisation retained documented information as evidence of the audit programme(s) and the audit results?	Möter ej	Har inte varit någon uttalad ambition. Redig internrevision finns i verksamheten men inte inom informationssäkerhet. Dataskyddsombudet kommer rapportera om GDPR.
9.3 Management review	Has the Organisations Management reviewed the Organisations ISMS at planned intervals to validate its continuing suitability, adequacy and effectiveness by taking into consideration: a) the status of actions from previous management reviews; b) changes in external and internal issues that are relevant to the information security management system; c) feedback on the information security performance, including trends in: 1) nonconformities and corrective actions; 2) monitoring and measurement results; 3) audit results; and 4) fulfilment of information security Objectives; d) feedback from interested parties; e) results of risk assessment and status of risk treatment plan; and f) opportunities for continual improvement	Möter ej	Har inte varit någon uttalad ambition. Nej, regelbunden utvärdering/granskning av informationssäkerhetsstyrningen är inte etablerad.

	Do the outputs of the Management Review include decisions related to continual improvement opportunities and any needs for changes to ISMS?	Möter ej	Har inte varit någon uttalad ambition. Nej, se ovan.
	Has the Organisation retained documented information as evidence of the results of Management reviews?	Möter ej	Har inte varit någon uttalad ambition. Nej, se ovan.
7. Förbättringsarbete			
Delklausul	**Fråga**	**Bedömning**	**Observation/Gap**
10.1 Nonconformity and corrective action	When a nonconformity occurs can and does the Organisation perform the following: a) react to the nonconformity, and as applicable: 1) take action to control and correct it; and 2) deal with the consequences; b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: 1) reviewing the nonconformity; 2) determining the causes of the nonconformity; and 3) determining if similar nonconformities exist, or could potentially occur; c) implement any action needed; d) review the effectiveness of any corrective action taken; and e) make changes to the ISMS, if necessary.	Möter	Avvikelser hanteras. Analys av nuläge pågår samt ett aktivt förbättringsarbete.

	Has the Organisation developed and maintain a Non Conformity and Corrective actions (NCCA) tracker that is appropriate to the effects of the nonconformities encountered? Does it capture: f) the nature of the nonconformities and any subsequent actions taken, and g) the results of any corrective action.	Möter delvis	Finns avvikelsehantering, dock ej vad gäller infosäkerhetsavvikelser. Detta ingår dock i pågående infosäk-projekt.
10.2 Continual improvement	Does the Organisation implement Processes to continually improve the suitability, adequacy and effectiveness of the ISMS?	Möter ej	Har inte varit någon uttalad ambition. Nej, inte ännu.

3. Analys

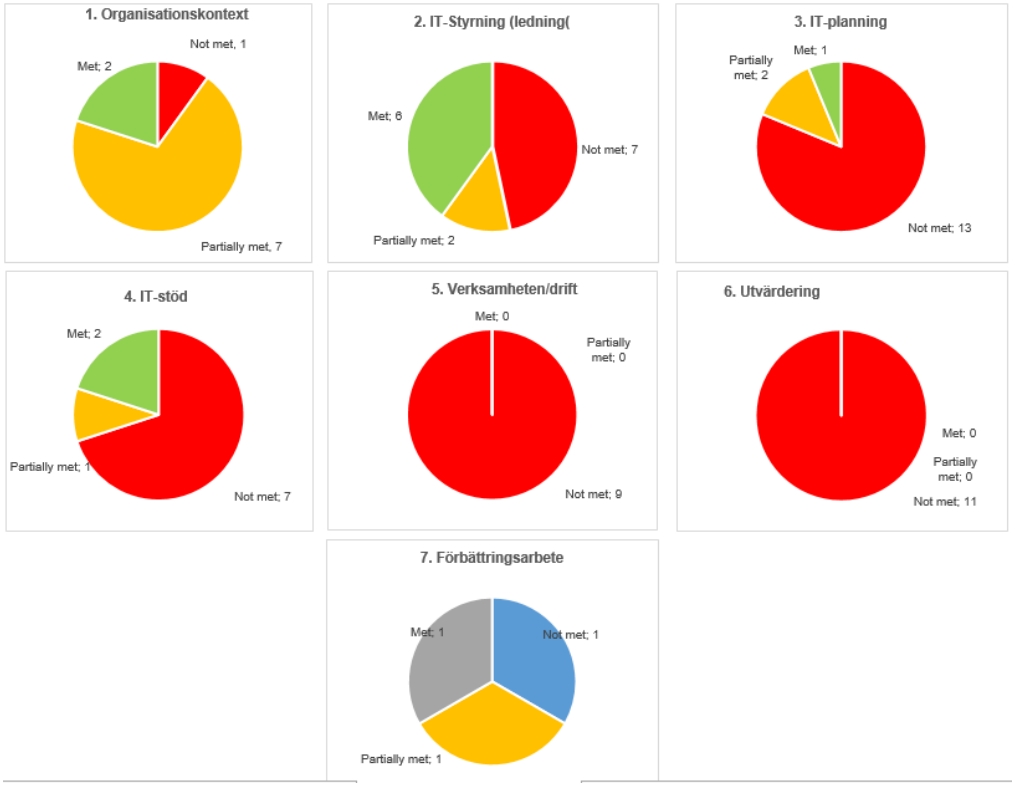
3.1 Analys

Av samtliga 78 granskningspunkter är fördelningen av bedömningarna följande:

Överensstämmer med beskrivning och/eller fungerar tillfredsställande	15 %
Överensstämmer delvis med beskrivning och/eller fungerar delvis tillfredsställande	17 %
Inte inte varit någon uttalad ambition/Överensstämmer ej med beskrivning och/eller fungerar ej tillfredsställande	63 %
Ej applicerbart	5 %

Kommentarer till granskningsprokoll

I nuläget finns det gap inom flera av de granskade områdena (7 stycken). Det pågår initiativ för att förbättra styrning och kontroll inom samtliga. Kommunen behöver resurser, tid och arbetskraft för att nå en effektivt och ändamålsenligt styrning kring informationssäkerhet. Det pågående Informationssäkerhetsprojektet innefattar ett omfattande arbete av ramverk och policys med inspiration från ISO 27000-serien. Upplands Väsby kommun har börjat utarbeta policy och riktlinjer vilka berör många av områdena kring informationssäkerhet (1-7). Att några av cirklarna nedan är röda beror på att man inte identifierat processer eller kontroller (5) för informationssäkerhet. En annan bidragande orsak är att Upplands Väsby kommun saknar riskanalys och ett komplett, utarbetat ledningssystem (6). Dock har detta inte tidigare varit någon ambition.



I dagsläget finns riktlinjer och policyer (2) tillgängliga på intranätet för medarbetare. Styrdokumenten är utdaterade men ett pågående arbete med ny policy och nya styrdokument är igång. Kommunen förmedlar relevanta säkerhetskrav under upphandling med externa leverantörer. Dock framgår vissa frågetecken kring privata aktörer och vilka krav som ställs i samband med dessa uppdrag gällande uppföljning inom informationssäkerhet och IT.

Kommunen har inte genomfört någon riskanalys som verifierar att informationssäkerhets-ramverket/styrningen fungerar som tänkt, och säkrar kontinuerlig/ständig förbättring (3). Det finns ingen sammanhållen process/modell men vid behov görs riskanalyser. Delar finns redan i dagsläget på plats i det pågående Informationssäkerhetsprojektet. Organisationen har tagit fram ett utkast som täcker hur man ska klassa information och system. Här är det även värt att nämna att nivåer för t.ex. riskacceptans är lättare sagt än gjort att få till för offentlig verksamhet.

Informationsdelning inom området Informationssäkerhet har skett. Det finns dock ingen obligatorisk utbildning kring informationssäkerhetshantering och inga implementerade processer (4). Processen kring dokumentationsuppdatering är automatiserad. I nuvarande policy finns kompetens och resurser nämnt. Projekt pågår för att analysera vilken kompetens som behövs och vilka utbildningsinsatser som erfordras.

Kommunen har ännu inte några processer eller en avvikelsehantering för informationssäkerhet på plats (5). Upplands Väsby saknas skriftliga processer och rutiner för incidenthantering samt rutiner för genomförande av riskanalyser och riskbedömningar. Detta har inte varit en ambition hos kommunen. Dock saknas en avvikelsehanteringsplan gällande informationssäkerhet som är övergripande, konkret och praktisk användbar.

Det finns ingen central styrning av uppföljningen av outsourcade/privata processer. Upplands Väsby kommun är delvis en decentraliserad organisation som är beroende av externa leverantörer. I och med Upplands Väsbys användning av leverantörer finns det ett extra behov av styrning och uppföljning även av dessa för att säkerställa att avtal uppfylls. Osäkerhet råder inom uppföljning av IT-leverantörerna, om än inte att någon granskning av avtalet sker.

Upplands Väsby har ännu inte utarbetat och definierat ett ledningssystem med uppföljning, analys eller mätaktiviteter (6). Internrevision finns i verksamheten, dock sker interngranskning endast för kvalitetsledning, miljöledning men inte informationssäkerhet. Det sker för nuvarande ingen regelbunden utvärdering/granskning av informationssäkerhetssyrningen. Detta har inte varit en ambition hos kommunen.

Avvikelser hanteras (7) och utvärderas av kommunen. Analys av nuläge pågår samt ett förbättringsarbete. Det finns i dagsläget ingen utarbetat avvikelsehantering, men detta ingår i det pågående Infosäk-projektet.

4. Rekommendationer

Nedan följer våra rekommendationer samt förslag på prioritering utifrån bedömd risk och väsentlighet. Rekommendationerna är prioriterade enligt följande:

Hög	Observation av kritisk karaktär som kan riskera kommunens möjlighet att effektivt driva verksamhet eller leda till materiella förluster för kommunen. Observation som graderas som "hög" bör omedelbart åtgärdas.
Medel	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, finansiell information, materiella tillgångar och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av kommunens resurser. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre fel i information, mindre brister i efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

ID	Iakttagelse och rekommendationer	Prioritet
1.	**Kommunen har inte tillräckliga resurser** Att kommunen har tillräckliga resurser är grunden för alla andra frågor kopplade till arbetet med informationssäkerhet. **Risk** Bristande resurser påverkar i sin tur alla andra delar i informationssäkerhetsarbetet. **Rekommendation** Det rekommenderas att säkerställa en nivå av resurser, med rätt kompetenser, som kan upprätthålla och underhålla ett systematiskt arbete med styrning av informationssäkerhet. Det har inte varit en uttalad ambition att ha styrning på plats i nivå med ledningssystem för informationssäkerhet. Det rekommenderas att säkerställa en nivå av resurser, med rätt kompetenser, som kan upprätthålla och underhålla ett systematiskt arbete med styrning av informationssäkerhet. Det är grunden för alla andra frågor kopplade till arbetet med informationssäkerhet.	**Hög**
2.	**Riskbaserade kontroller och aktiviteter** Kommunen saknas riskbaserade kontroller och aktiviteter för informationssäkerhet. **Risk** Utan riskbaserade kontroller och aktiviteter i verksamheten är det svårt att fördela rätt resurser på rätt aktivitet. **Rekommendation** Kommunen rekommenderas att riskanalys och hantering integreras i arbetet med informationssäkerhetsstyrning. Det har inte varit någon uttalad ambition att ta fram kontroller och aktiviteter utifrån riskanalyser för verksamheten. För att säkerställa att rätt resurser läggs på rätt aktiviteter rekommenderas att riskanalys och hantering integreras i arbetet med informationssäkerhetsstyrning.	**Hög**

ID	Iakttagelse och rekommendationer	Prioritet
3.	**Brister i monitorering av styrning av informationssäkerhetsarbetet i sig** **Risk** Utan ett ledningssystem med definierade mätkriterier är det svårt för kommunen att säkerställa kvaliteten i sin styrning av informationssäkerhet. **Rekommendation** Det rekommenderas att ledningssystemet definieras och man därefter tar fram mätkriterier. Det har inte varit någon uttalad ambition att kontinuerligt övervaka, och utvärdera hur väl styrningen av informationssäkerhet fungerar. Det rekommenderas att ledningssystemet definieras, och att mätkriterier därefter definieras så att kommunen kan säkerställa kvaliteten i sin styrning av informationssäkerhet.	**Hög**
4.	**Kommunen har inte uppdaterat sin informationssäkerhetspolicy** Policyn förförfattades för ca 2 år sedan och har inte uppdaterats sedan dess. **Risk** I och med en snabb IT-utveckling finns risk att policyn och åtgärder inte täcker viktiga områden eller är anpassad till organisations och omvärldens förändrade omständigheter. **Rekommendation** Uppdatera policyn kontinuerligt så att den reflekterarar organisations nuvarande behov och omvärldens möjligheter och krav. Därtill rekommenderas det att Implementera ett ledningssystem som säkerställer att verksamheten aktivt jobbar med styrning och kontroll av verksamhetens informationssäkerhetsarbete.	**Medel**
5.	**Kommunen förlitar sig på leverantörerna gällande säkerheten av systemen utan att uppföljning sker** Kommunen genomför ex. inte några penetrationstester utan förlitar sig på att leverantörerna och att verksamheterna själva uppfyller säkerhetskraven. Identifiering av tekniska sårbarheter som kan vara blottade för en eventuell angripare säkerställs således enbart genom avtal med leverantörerna, vilka i de flesta fall inte följs upp. **Risk** Om kontrakt och avtal och teknisk säkerhet inte följs upp och om kommunen inte själva utför tester medför det risker för otillräcklig informationssäkerhet. **Rekommendation** Införa regelbundna leverantörsgranskningar (tekniskt och avtalsmässigt). Att granska och se över avtal med leverantörer är även ett essentiellt steg för att vara förenlig med GDPR.	**Medel**
6.	**Kommunen följer inte upp utbildningsinsatser inom informationssäkerhet** Det saknas ett strukturerat utbildningsprogram inom organisationen för att säkerställ adekvat kunskapsnivå inom informationssäkerhet. **Risk** Utan utbildning kan brister uppstå avseende medvetenhet kring informationssäkerhetsfrågor, vilket kan utsätta organisationen för flertalet risker. **Rekommendation** Det rekommenderas att kommunen startar ett utbildningsinitiativ för att öka och regelbundet säkerställa medvetenheten samt kunskapsnivåerna för att på så sätt minska risken för informationssäkerhetsbrister	**Medel**

5. Källförteckning

5.1 Kommungemensamma dokument

- Informationssäkerhetspolicy - beslutad av kommunfullmäktige 21 november 2016 § 205
- IT-policy- beslutad av kommunfullmäktige 21 november 2016 § 205
- Informationssäkerhetsinstruktion Användare (Giltig till 2017-12-31)
- Informationssäkerhetsinstruktion Förvaltning (Giltig till 2017-12-31)