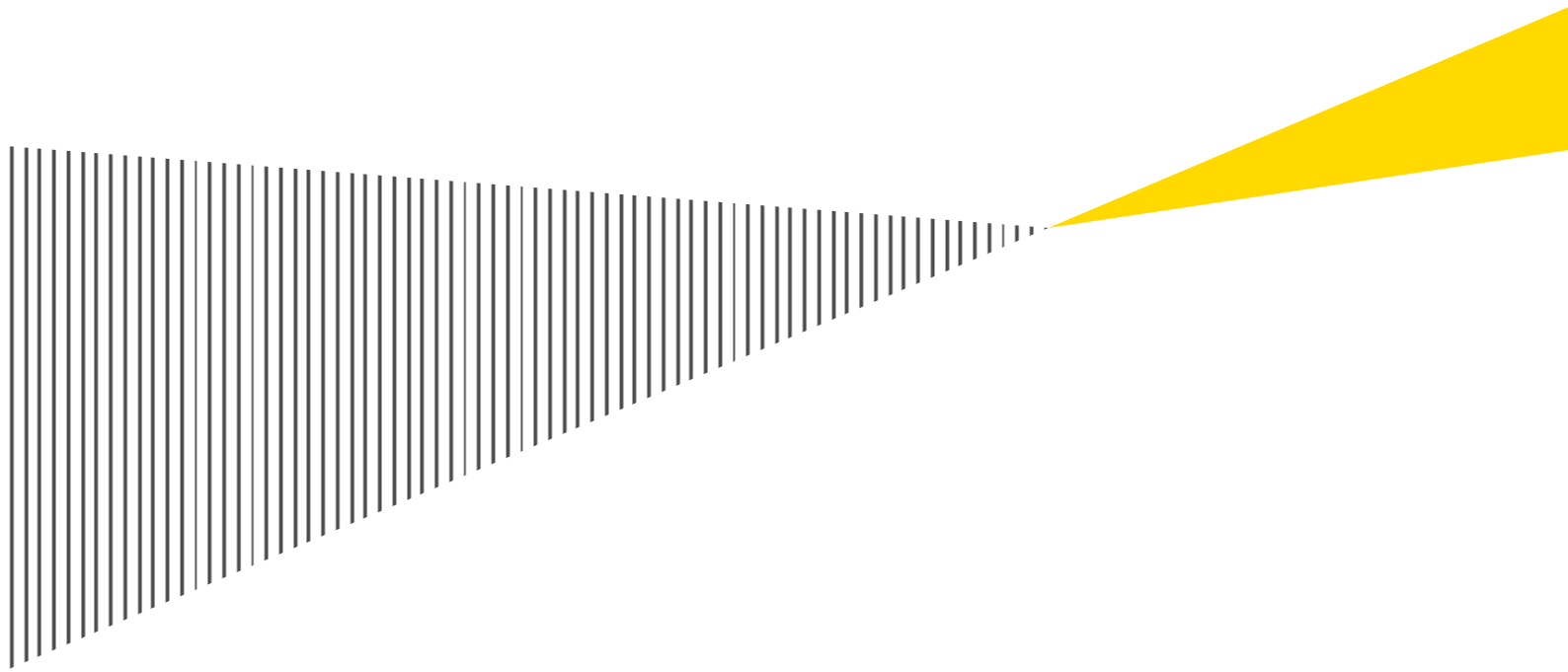
Revisionsrapport 2013
Genomförd på uppdrag av de förtroendevalda revisorerna i Vetlanda kommun



Vetlanda kommun

Granskning avseende IT- och informationssäkerhet enligt BITS

Innehållsförteckning

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Vetlanda kommun har Ernst & Young genomfört en granskning av IT- och informationssäkerhet, vad gäller policys, riktlinjer och hantering av säkerhetsfrågor på övergripande nivå i kommunen. IT-revisionens syfte har varit att granska och bedöma informationssäkerheten på en övergripande nivå i kommunen. Granskningen har gjorts mot Myndigheten för samhällsskydd och beredskaps ramverk för informationssäkerhet, BITS.

Övergripande slutsatser

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Aktuellt område i BITS finns adresserat och kontroll bedöms rimligen implementerad:	**21%**
Kontrollen identifierad och bedöms enbart delvis implementerad:	**40%**
Kontroll har ej identifierats/Har inte kunna identifierats som implementerad:	**37%**
(Varav kontroller administrerade av HIT)	(22%)
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2%**

Då kommunen lagt ut stora delar av driften av IT-verksamheten på Höglandets IT (HIT) är det vissa granskningsområden där vi inte kunnat få svar på av våra frågor. Verksamheten i HIT ingår inte i denna granskning. HIT är en sammanslagning av IT-avdelningar på fem närliggande kommuner och drivs i regi av Höglandets Kommunalförbund. I analysen nedan har de kontroller som administreras av HIT hanterats som NEJ. Därmed skulle vissa granskningsområden kunna få högre resultat beroende på hur kontrollen ser ut hos HIT. Orsaken till att vi hanterat granskningsområdena som NEJ beror på att det inte har framkommit att det finns ett skriftligt avtal mellan Vetlanda kommun och HIT, som reglerar de områden som omfattas av granskningen.

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Fullständiga iakttagelser med riskbedömningar och rekommendationer finns i kapitel 4.

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Informationssäkerhetskrav för administration och förvaltning saknas. Vi har noterat att det finns en IT-säkerhetspolicy från år 2001. Policyn finns inte tillgänglig i elektroniskt format, och bedöms därför inte vara lättillgänglig för alla. **Rekommendation:** Vi rekommenderar Vetlanda kommun att uppdatera sin IT-policy och kommunicera den i organisationen, utifrån ett riskperspektiv. Det är även väsentligt att inkludera tydligt definierade ansvar och roller mellan Vetlanda kommun och HIT.	**Hög**
Iakttagelse: Process för programändringar saknas De delar av förändringsprocesserna är formella inom vissa förvaltningar i kommunen. Det finns däremot ingen generell plan i kommunens IT-säkerhetsanvisningar gällande förändringar i system och driftgodkännande. **Rekommendation:** Vi rekommenderar kommunen att utveckla den existerade processen för programförändringar.	**Hög**
Iakttagelse: Kontinuitetsplaner och krav på tillgänglighet saknas Det finns en plan att ta fram kontinuitetsplaner men det saknas i dagsläget för de flesta verksamheter. Det finns inte heller tydliga analyser kring längsta acceptabla tid som systemen kan vara ur funktion innan verksamheten äventyras. **Rekommendation:** I första hand bör analys göras för att bedöma kravet på tillgänglighet av stödet till verksamheten. Utifrån det så rekommenderar vi Vetlanda kommun att skapa rutiner för kontinuitetsplanering.	**Medel**

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Formella regler saknas för informationsklassning, I vissa förvaltningar finns det styrande dokument som gör klassning av data utifrån BITS områden som Sekretess, Riktighet och Tillgänglighet. Dessa har sedan delats upp i Bas-, Hög och Mycket hög nivå. Inom vissa andra förvaltningar finns inget dokumenterat. **Rekommendation:** Vi rekommenderar Vetlanda kommun att upprätta en informations-klassningspolicy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.	**Medel**
Iakttagelse: Kontroll av data på utrangerad maskinvara Kommunen använder vanligtvis ett företag för destruktion av utrangerad maskinvara, men det är osäkert vilka riktlinjer som HIT följer vid förändringar. **Rekommendation:** Vi rekommenderar Vetlanda kommun att dokumentera och implementera en enhetlig rutin för hur uttjänt maskinvara skall hanteras utifrån risken med data som finns på aktuell dator.	**Medel**
Iakttagelse: Uppföljning av tilldelade behörigheter Det finns ingen formell rutin i kommunen för att följa upp att rätt användare ligger i respektive system och att användaren har rätt behörigheter utifrån ansvarsuppgifter och intern kontroll. **Rekommendation:** Vi rekommenderar Vetlanda kommun att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen.	**Medel**
Iakttagelse: Systemförteckning och ägarskap Vi har noterat att vissa förvaltningar har tydlig systemförteckning där t ex systemägare framgår och riskklassning skett på respektive system. I vissa fall finns detta inte dokumenterat men är ett pågående projekt enligt de intervjuade. **Rekommendation:** Vi rekommenderar Vetlanda kommun att fortsätta och slutföra sitt arbete med att dokumentera systemen och tydliggöra risker och ägarskap.	**Medel**

Iakttagelse och rekommendation	Prioritet
Iakttagelse: Granskning av efterlevnad Inom vissa förvaltningar utförs viss analys av logglistor och andra rutiner för att säkerställa att policys och rutiner efterföljs. Indikationer visar att dessa kontroller inte utförs på samtliga förvaltningar. **Rekommendation:** Vi rekommenderar att kontroller och rutiner verifieras regelbundet för att säkerställa en följsamhet och efterlevnad.	**Medel**

1 Bakgrund

1.1 Syfte

Idag bedrivs den största delen av all verksamhet i en kommun med hjälp av någon form av datoriserat stöd. Stödet har med tiden utvecklats till att bli en förutsättning för att kunna bedriva verksamheten. För att uppnå kommunens verksamhetsmål krävs att informationen i verksamhetsstödet är tillgängligt, riktigt, har korrekt konfidentialitet samt är spårbart.

På uppdrag av kommunrevisorerna i Vetlanda kommun har EY genomfört en granskning av IT- och informationssäkerhet. Granskningen har varit inriktad på policys, riktlinjer och hantering av säkerhetsfrågor på en övergripande nivå i kommunen.

Syftet med granskningen har varit att skapa en utgångspunkt för arbetet med IT- och informationssäkerhet inom Vetlanda kommun. I granskningen har gällande säkerhetsnivåer bedömts mot BITS, Myndigheten för samhällsskydd och beredskaps (tidigare Krisberedskapsmyndigheten) ramverk för informationssäkerhet. BITS står för *Basnivå för informationssäkerhet* och har sitt ursprung i den internationella informationssäkerhetsstandarden ISO/IEC 27000. En jämförelse har även gjorts med resultatet från liknande granskningar i andra kommuner och organisationer.

1.2 Metod

Baserat på erfarenheter från tidigare granskningar inom offentlig verksamhet har EY valt ut ett antal relevanta kontroller som presenteras i BITS, fördelat på elva huvudområden:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

Rapporten redovisar i vilken grad kommunen uppfyller valda rekommendationer ur BITS. Resultatet är en sammanvägd bedömning, som baseras på information som lämnats vid intervjuerna samt genom granskning av erhållen dokumentation.

Den sammanvägda bedömningen av svaren på kontrollerna har bedömts enligt följande alternativ:

Ja	Aktuellt område i BITS finns adresserat och kontroll bedöms vara rimligen implementerad. I förekommande fall ges rekommendationer och kommentarer även till denna bedömning.
Delvis	Kontrollen är identifierad men bedöms enbart delvis vara implementerad.
Nej	Kontroll har ej identifierats/Har inte kunnat identifieras som implementerad.
HIT	Detta område täcks inte av kommunen utan av annan part och hanteras som NEJ i jämförelsen med andra kommuner.
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl.

Analysen baseras på erhållen dokumentation samt på intervjuer med IT-strateg, fastighetschef inom Tekniska kontoret, IT-ansvarig Fastighetsenheten, IT-samordnare på Socialförvaltningen och IT-samordnare Vård- och omsorgsförvaltningen.

Granskningen har genomförts av Per Magnusson, auktoriserad revisor, CISA och IT-revisor och Carin Jesenicnik under maj-juni 2013.

Kvalitetssäkring har skett av auktoriserad och CISA-certifierad revisor inom Ernst & Young samt Helena Patrikson, auktoriserad revisor och certifierad kommunal revisor. Utöver EY:s interna kvalitetssäkring har intervjuade haft möjlighet att lämna saksynpunkter på rapportutkastet. Detta för att säkerställa att revisionsrapporten bygger på korrekta fakta och uttalanden.

1.3 Avgränsningar

Iakttagelser och analyser baseras enbart på information som har inhämtats vid intervjuer och aktuell dokumentation. Inga tester har genomförts, t ex att en kontroll är implementerad. Det kan finnas brister i kommunens hantering av IT som vi inte har identifierat inom ramen för denna granskning. Arbetet har inte omfattat test av generella IT-kontroller eller applikationskontroller.

Denna rapport tar endast hänsyn till nuläget i Vetlanda kommun och kontroller som administreras av HIT har inte ingått i denna genomgång. De områden som ingått i denna genomgång är följande:

- Fastighetsenheten inom Tekniska kontoret
- Socialförvaltningen
- Vård- och omsorgsförvaltningen

Höglandets IT, HIT, är ett samgående av IT-avdelningarna för fem kommuner, varav Vetlanda är en av dem. Organisatoriskt finns HIT inom Höglandets kommunalförbund. De olika kommunerna köper tjänster från HIT. Vid granskningstillfället fanns det inte något skriftligt avtal mellan HIT och Vetlanda kommun, varvid vi har klassat alla områden som HIT ansvarar för som NEJ.

2 Iakttagelser

I detta avsnitt presenteras de iakttagelser som framkommit i granskningen. Systemen i tabellen nedan är de verksamhetskritiska system som identifierats av respektive deltagande förvaltning och det är dessa system som ingått i granskningen:

System	Beskrivning	Leverantör
ProCapita	Socialt verksamhetssystem	Tieto
Mobipen	Utförarsystem integrerat med ProCapita	Phoniro-systems
	Kartsystem	
	Ventilation och passersystem	

2.1 Granskningsprotokoll

Granskningsområden		Kommentar	Utvärdering
1 Säkerhetspolicy			
1.1	Har kommunen en informations-/IT-säkerhetspolicy?	Det finns en IT-policy från 2001. Policyn finns inte tillgänglig elektroniskt. Vår bedömning är att policyn behöver uppdateras utifrån dagens förhållanden och risker. Den bör även kommuniceras till verksamheten. Utvärderingen har klassats som Delvis då det funnits uppdaterade policys på förvaltningar där vi granskat.	Delvis
2 Organisation av säkerheten			
2.1	Finns det en informationssäkerhetssamordnare/-funktion för informationssäkerhet	Enligt kommunen är kommunchefen formellt utsedd som säkerhetsansvarig. Vår bedömning är att det är viktigt att den person/funktion som är utsedd att vara säkerhetsansvarig rent praktiskt har möjlighet att hantera säkerhetsarbetet inom kommunen och dess informationssystem.	Delvis
2.2	Har ledningen utsett systemägare för samtliga informationssystem?	Enligt policyn är varje förvaltning utsedd som systemägare till sina respektive system.	Ja
2.3	Har organisationen utsett systemansvariga?	Vissa förvaltningar har på ett tydligt och formellt sätt utsett systemansvariga. Det finns även förvaltningar där systemansvariga mer informellt har fått ansvaret.	Delvis
2.4	Finns det en samordningsfunktion för att länka samman den operativa verksamheten för informationssäkerhet och ledningen?	Enligt de intervjuade finns det informellt en samordningsfunktion. Detta är dock inte tydligt dokumenterat. Enligt de intervjuade personerna så är förvaltningarna inte så stora så det är naturligt att utse en "IT-ansvarig" inom respektive förvaltning eller delområde inom en förvaltning.	Delvis

Granskningsområden		Kommentar	Utvärdering
2.5	Har ansvaret för informationssäkerheten reglerats i avtal för informationsbehandling som lagts ut på en utomstående organisation?	Stor del av IT-driften och dess hantering har lagts ut på Höglandets IT (HIT). Vid vår granskning fanns det inte något skriftligt avtal, varför det är oklart hur ansvars-fördelningen är mellan HIT och respektive kommun.	Nej
3 Hantering av tillgångar			
3.1	Är organisationens information klassad avseende sekretess/riktighet/ tillgänglighet?	De förvaltningar som har system med känslig information har klassat dessa system på ett tydligt sätt. Det finns dock indikationer på att detta inte är genomfört på samtliga förvaltningar. Det finns heller inte någon samlad bild för hela kommunen. Vår uppfattning är att inom de förvaltningar som har högre riskar, av de vi intervjuat, har de även klassificerat sina risker.	Delvis
3.2	Har samtliga informationssystem identifierats och dokumenterats i en aktuell systemförteckning.	Vissa förvaltningar har en dokumenterad systemförteckning. Det finns förvaltningar där detta är ett pågående arbete. Det finns ingen kommunövergripande förteckning över samtliga system.	Delvis
3.3	Finns det en ansvarsfördelning för organisationens samtliga informationstillgångar.	Vissa förvaltningar har detta tydligt dokumenterats i riskanalyser. Det finns förvaltningar där detta ansvar är mer informellt och då inte dokumenterat.	Delvis
3.4	Finns det upprättat dokument för hur informations-behandlingsresurser får användas?	Vissa förvaltningar har detta dokumenterat . De granskade förvaltningar som inte har en tydlig dokumentation har en mindre risk kopplad till sin information och sina system. Det finns ingen kommunövergripande policy rörande detta område.	Delvis
4 Personalresurser och säkerhet			
4.1	Granskas nyanställdas bakgrund vid nyanställning i proportion till kommande arbetsuppgifter?	Nej det görs ingen granskning.	Nej
4.2	Får inhyrd/inlånad personal information om vilka säkerhetskrav och instruktioner som gäller?	Det finns ett centralt dokument framtaget som avser externa konsulter. Det är dock inte tydligt om detta är känt i hela kommunen. Vissa förvaltningar har tagit fram egna dokument som används för externa konsulter/personal.	Delvis
4.3	Har systemägaren definierat vilka krav som ställs på användare som får tillgång till informationssystem och information?	För vissa system är detta klart, men det finns system där det inte är lika tydligt.	Delvis
4.4	Finns det framtagna dokumenterade säkerhetsinstruktioner för användare?	Säkerhetsinstruktioner finns framtagna enligt de intervjuade, men det framkom att det kan finnas behov att uppdatera och omarbeta dem.	Ja
4.5	Genomförs utbildningsinsatser inom informationssäkerhet regelbundet?	Utbildning utförs främst på förfrågan från chefer som identifierat ett behov. Risken ökar vid ändrade lagar och regler, men även vid större personalomsättning. Systematisk och planlagd utbildning utförs inte.	Delvis
4.6	Finns det användarhandledning för ett informationssystem att tillgå?	Ja, berörda leverantörer tar fram detta för aktuella system, enligt förvaltningarna.	Ja

Granskningsområden		Kommentar	Utvärdering
4.7	Dras åtkomsträtten till information och informations-behandlingsresurser in vid avslutande av anställning eller vid förflyttning?	Vissa förvaltningar har fungerande rutiner för detta. Det finns dock exempel där ansvarig inte får kännedom om vilka personer som slutat/flyttat och då kan konton ligga öppna tills en övergripande genomgång utförs.	Delvis
5 Fysisk och miljörelaterad säkerhet			
5.1	Finns funktioner för att förhindra obehörig fysisk tillträde till organisationens lokaler och information?	Kommunhuset skyddas av kortlås och kod dygnet runt, enligt kommunen. Denna typ av lås finns även inom delar av kommunhuset.	Ja
5.2	Har IT-utrustning som kräver avbrottsfri kraft identifierats?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
5.3	Finns larm kopplat till larmmottagare för: - brand, temperatur, fukt - sker test till larmmottagare	*Enligt uppgift administrerar Höglandets IT detta.* *Höglandets IT administrerar detta enligt uppgift.*	HIT= NEJ
5.4	Finns i direkt anslutning till viktig dator- kommunikationsutrustning kolsyresläckare?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT= NEJ
5.5	Regleras tillträde till utrymmen med känslig information eller informationssystem utifrån informationens skyddsbehov? Tillträdesrättigheter, rutiner för upprättande?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT= NEJ
5.6	Är korskopplingsskåp låsta?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT= NEJ
5.7	Raderas känslig information på ett säkert sätt från utrustning som tas ur bruk eller återanvänds?	Tidigare använde kommunen ett destruktionsföretag och fick då intyg på att all data var korrekt raderad. Efter outsourcingen till HIT finns det en osäkerhet kring hur HIT hanterar denna fråga. Inom kort kommer det att ske ett byte av servrar avseende socialförvaltningens system. Dessa system innehåller känslig data och det är väsentligt att säkerställa att detta hanteras på rätt sätt.	HIT = NEJ
5.8	Finns särskilda säkerhetsåtgärder för utrustning utanför ordinarie arbetsplats?	Ej tillämpligt då ingen utrustning hanteras utanför ordinarie arbetsplats.	E/T
5.9	Finns information och regler som förklarar att informationsbehandlingsresurser inte får föras ut från organisationens lokaler utan medgivande från ansvarig chef?	För system med känslig information finns det regler rörande systemet, men det noteras att det inte är lika tydligt vad gäller t.ex. pappersburen information. Det finns ingen kommungemensam policy.	Delvis
6 Styrning och kommunikation av drift			
6.1	Finns det driftdokumentation för verksamhetskritiska informationssystem?	Driftsdokumentation har tagits fram för de ,enligt förvaltningarna , väsentliga systemen och överlämnats till HIT.	Ja

Granskningsområden		Kommentar	Utvärdering
6.2	Är klockorna i informationssystemen synkroniserade med godkänd exakt tidsangivelse?	HIT administrerar detta. Enligt uppgift har det varit problem med synkronisering tidigare men problemen ska nu vara åtgärdat. Dock har det framkommit att problemet fortfarande finns, eftersom rapportskapande har daterats med ett senare än dagens datum för att rapporten ska kunna tas fram.	HIT = NEJ
6.3	Sker system-/programutveckling samt tester av modifierade system åtskilt från driftmiljön?	För testning av de mest känsliga systemen har kommunen ingen testmiljö utan förändringar införs från konsulterna direkt in i produktionsmiljön. I en av intervjuerna framkom att testning utförs i testmiljö.	Nej
6.4	Finns rutiner för hur utomstående leverantörers tjänster följs upp och granskas?	HIT driftar systemen och kommunen har möten med dem. Det pågår ett arbete med att implementera tydligare SLAer (Service Level Agreement) för att förtydliga förväntningarna från förvaltningar och kommunens organisationer.	Delvis
6.5	Godkänner lämplig personal (systemägaren) driftsättningar av förändrade informationssystem?	I samtliga fall är det systemägare som godkänner driftsättning. I vissa fall finns det dokumenterat och i vissa fall är det mer informellt, därför blir bedömningen Delvis.	Delvis
6.6	Finns det för både servrar och klienter rutiner för skydd mot skadlig programkod?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
6.7	Regleras och dokumenteras rätten att installera nya program, programversioner?	Av information vi fått framgår att användare normalt inte har Admin-rättigheter på sin egen maskin, vilket innebär att de inte kan installera program.	Ja
6.8	Har organisations nätverk delats upp i mindre enheter (segmentering), så att en (virus) attack enbart drabbar en del av nätverket?	Nätverket är segmenterat enligt de intervjuade.	Ja
6.9	Genomförs säkerhetskopiering regelbundet?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT= NEJ
6.10	Genomförs regelbundna tester för att säkerställa att informationssystem kan återstartas från säkerhetskopior?	HIT administrerar dessa tester. En förvaltning har varit involverad i testning ca två gånger om året. Koppling har skett till en speglad server och kontrollerat har skett att systemet kan startas med hjälp av den nya servern. Punkten bedöms som Delvis då vi inte fått enhetlig information om hur det går till för de olika förvaltningarna.	Delvis
6.11	Finns det en aktuell förteckning över samtliga externa anslutningar?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
6.12	Saknas alternativa vägar vid sidan av organisationens brandvägg in till det interna nätverket?	Ja, enligt kommunen ska det inte finnas några alternativa vägar där någon skulle kunna gå förbi det skydd som brandväggen innebär.	Ja
6.13	Är det möjligt att logga säkerhetsrelevanta händelser?	Loggar finns, enligt uppgift, där det framgår vem som gjort vad. I ProCapita (används av Socialförvaltningen) ska det även gå att se vem som tittat på vilken data.	Ja

Granskningsområden		Kommentar	Utvärdering
6.14	Finns särskilda skyddsåtgärder för att skydda sekretess och riktighet när data passerar allmänna nät liksom skydd av anslutna system och utrustning?	I de flesta fall finns det ingen känslig information, enligt de intervjuade. I ProCapita ska en användare inte kunna skicka information utanför systemet, vilket då gör att risken inte föreligger.	Ja
6.15	Finns det riktlinjer avseende förvaringstid för datamedia?	Det finns tydliga riktlinjer avseende arkivering för vissa förvaltningar, dock saknas det på andra. Det finns inga centrala riktlinjer framtagna.	Delvis
6.16	Finns det dokumenterade regler avseende vilken information som får skickas utanför organisationen?	Det finns tydliga regler rörande information i systemen lokalt på förvaltningarna som hanterar känslig information men inte lika tydliga regler gällande pappersburen information. Även pappersburen information kan innehålla känslig information. Det finns inga centrala riktlinjer framtagna.	Delvis
6.17	Gäller det för e-postsystem och andra viktiga system att de är isolerade från externa nät? (DMZ) t.ex. genom någon form av brandväggsfunktion.	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
6.18	Finns olika typer av autenticeringsmetoder med olika grad av skydd?	En användare kan enbart koppla upp sig på WebMail hemifrån, enligt kommunen. I övrigt är det enbart Administratörer som har rätt att koppla upp sig på nätet hemifrån på företagets datorer. Enligt information vi fått används engångslösenord vid dessa tillfällen.	Ja
6.19	Sparas revisionsloggar för säkerhetsrelevanta händelser?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
7 Styrning av åtkomst			
7.1	Har organisationen satt upp dokumenterade regler för åtkomst/tillträde för tredjeparts åtkomst till information eller informationssystem?	Det finns ingen kommungemensam policy. Det finns vissa förvaltningar som tagit fram egna regler, som bl.a. avser konsulter.	Delvis
7.2	Tilldelas användare en behörighetsprofil som endast medger åtkomst till informationssystem som krävs för att lösa arbetsuppgifterna?	Behörigheter tilldelas efter behov av ansvar och arbetsuppgifter enligt de intervjuade.	Ja
7.3	Begränsas rätten att installera nya program i nätverket samt den egna arbetsstationen till endast utsedd behörig personal?	Normala användare har inte Admin-rättigheter på sin dator och kan då inte installera programvara själv. Vissa användare ska dock ha fått Admin-rättigheter efter ett godkännande hos chef.	Ja
7.4	Har samtliga administratörer fullständiga systembehörigheter, eller endast i den utsträckning som krävs för arbetsuppgifterna?	Admin-rättigheterna är begränsade till vad den anställde har behov av. Hur rollen som Administratör på HIT hanteras, har vi inga uppgifter kring och därför klassar vi punkten som Delvis.	Delvis
7.5	Har organisationen en dokumenterad rutin för tilldelning, bortag eller förändring av behörighet? Är de kommunicerade till ansvarig för behörigheter?	I vissa fall finns det tydligt framtagna riktlinjer för förändring av åtkomst, och i vissa fall är det mindre tydligt hur det ska gå till. Dokumenterad rutin finns inte hos alla intervjuade förvaltningar och då klassar vi denna punkt som Delvis.	Delvis
7.6	Får nya användare ett initialt lösenord som de måste byta, till ett eget valt lösenord vid första användning?	I nätverket och i systemet ProCapita krävs byte vid första inloggningen. I övriga system finns inte dessa krav, men IT-ansvarig uppmanar användaren att byta lösenord.	Delvis

Granskningsområden		Kommentar	Utvärdering
7.7	Genomförs kontinuerlig (minst en gång per år) kontroll av organisationens behörigheter?	I en intervju framkom att detta görs regelbundet, fyra gånger om året. I övriga fall görs det, men inte så formellt och inte med samma frekvens. Rörande nätverk administrerar HIT detta och vi saknar uppgift hur detta hanteras.	Delvis
7.8	Har systemadministratörer/-tekniker/-användare individuella unika användaridentiteter?	Ja, enligt intervjuade. I något fall finns gruppkonton kopplat till jourprofiler. Det framkommer tydligt vem som arbetar då och har ansvar för inloggningen.	Ja
7.9	Öppnas låsta användarkonton först efter säker identifiering av användaren?	Vanligtvis känner Helpdesk igen personen, rent fysiskt eller t ex röst över telefon, men det saknas en formell rutin för detta. Det finns en önskan om att införa rutiner. I vissa system finns inte funktionen att konton låser sig och då uppstår inte denna fråga. Då det saknas dokumenterad rutin är vår utvärdering NEJ.	NEJ
7.10	Finns en gemensam lösenordspolicy?	Ingår i den kommunala IT-policyn från 2001. Några avdelningar har tagit fram egna riktlinjer, som är mer långtgående än de riktlinjer som finns i IT-policyn	Delvis
7.11	Sker automatisk aktivering av skärmsläckare och automatisk låsning av obevakade arbetsstationer efter visst givet tidsintervall? Upplåsning kan endast ske med lösenord.	Ja, enligt de intervjuade.	Ja
7.12	Är brandväggsfunktionen den enda kanalen för IP-baserad datakommunikation till och från organisationen?	*Enligt uppgift administrerar Höglandets IT detta.* .	HIT = NEJ
7.13	Finns en dokumenterad brandväggspolicy där det beskrivs vilka tjänster brandväggen skall tillhandahålla?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
7.14	Används trådlösa lokala nät? I så fall, finns det åtgärder mot obehörig avlyssning och obehörigt utnyttjande av resurser?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
7.15	Finns det en karta över nuvarande säkerhetsarkitektur (tekniska anvisningar) för interna och externa nät och kommunikationssystem?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
7.16	Har organisationen upprättat dokumenterade riktlinjer avseende lagring?	Detta saknas centralt i kommunen, med undantag från någon förvaltning vi intervjuade, där det fanns egen dokumentation.	Delvis
7.17	Har verksamheten ställt och dokumenterat tekniska säkerhetskrav och krav på praktisk hantering avseende användandet av mobil datorutrustning och distansarbete?	Ej tillämpligt då personal i dagsläget inte arbetar på distans, men där det kan komma att ske i framtiden och därför klassar vi det som NEJ.	NEJ
7.18	Har systemägaren eller motsvarande beslutat om att ett informationssystems information ska få bearbetas på distans med stationär eller mobil utrustning?	Ej tillämpligt, se ovan	NEJ

Granskningsområden		Kommentar	Utvärdering
7.19	Finns det aktuell dokumentation med regler för distansarbete?	Ej tillämpligt, se ovan.	NEJ
8 Anskaffning, utveckling och underhåll av informationssystem			
8.1	Har en systemsäkerhetsanalys upprättats och dokumenterats för varje informationssystem som bedöms som viktigt?	För systemen med sekretess-information finns det analyser framtagna. För övriga saknas detta.	Delvis
8.2	Krypteras persondata som förmedlas över öppna nät?	Ej tillämpligt då inga persondata förmedlas över öppna nät.	E/T
8.3	Finns det angiven personal som ansvarar för systemunderhåll?	I något fall finns det tydligt dokumenterat vem som är ansvarig, i något fall mer informellt. Mer och mer läggs dessa uppgifter över på HIT.	Delvis
8.4	Finns det regler för hur system- och programutveckling ska genomföras?	Inga formella regler finns framtagna.	Nej
8.5	Finns det regler och riktlinjer avseende beslut om programändringar?	I vissa fall finns informella regler och i vissa fall finns det mer tydligt dokumenterat vem som är ansvarig. Det finns inga kommunövergripande regler.	Delvis
8.6	Finns det dokumenterade rutiner för hur utbildning ska genomföras för köpta system? Omfattar rutinen även kompletterande utbildning vid program- och funktionsändringar?	Det finns inget dokumenterat krav gällande utbildning, även om det vanligtvis genomförs utbildningar.	NEJ
8.7	Finns det en uppdaterad och aktuell systemdokumentation för ett informationssystem?	Kommunen håller på att dokumentera detta i ett pågående projekt, men är vid intervjutillfället inte helt färdiga.	NEJ
9 Hantering av informationssäkerhetsincidenter			
9.1	Finns det dokumenterade instruktioner avseende vart användare skall vända sig och hur de skall agera vid funktionsfel, misstanke om intrång eller vid andra störningar?	För systemen med sekretessinformation, som finns i vissa förvaltningar, finns det tydliga instruktioner. I övrigt saknas detta.	Delvis
10 Kontinuitetsplanering i verksamheten			
10.1	Finns det en gemensam kontinuitetsplan dokumenterad för organisationen?	Inga formella planer fanns framtagna vid intervjutillfället.	Nej
10.2	Har systemägaren eller motsvarande beslutat om den längsta acceptabla tid som informationssystemet bedöms kunna vara ur funktion innan verksamheten äventyras?	För systemet ProCapita finns det tydliga riktlinjer, som HIT fått ta del av. Annars finns det inga tydliga krav framtagna. Kommunen håller på att titta över SLAer, som innebär att de tydliggör t ex tillgänglighets krav för HIT.	Delvis
10.3	Finns det en dokumenterad avbrottsplan med återstarts- och reservrutiner för datadriften som vidtas inom ramen för ordinarie driften?	*Enligt uppgift administrerar Höglandets IT detta.* .	HIT = NEJ
10.4	Kan verksamheten bedrivas med manuella eller maskinella reservrutiner under begränsad tid? Är befintliga reservrutiner dokumenterade?	I vissa fall finns dokumenterade reservrutiner, ex. hantering av fastigheter utan stöd av IT-system. Det finns dock områden som saknar reservrutiner.	Delvis

Granskningsområden		Kommentar	Utvärdering
10.5	Har omständigheter som ska betecknas som kris/katastrof (extraordinära händelser) för verksamheten kartlagts?	Nej	Nej
11 Efterlevnad			
11.1	Användas endast programvaror i enlighet med gällande avtal och licensregler?	Ja. Genomgång görs regelbundet och användare har i normalfallet inte rätt att installera programvaror själva. Det finns dock ingen kommungemensam policy som beskriver hur ofta genomgångar ska ske och vem som ansvarar för dem.	Delvis
11.2	Finns det regler för godkännande och distribution av programvaror för att efterleva rådande upphovsrättsliga regler?	Ja. Genomgång görs regelbundet och användare har i normalfallet inte rätt att installera programvaror själva, enligt information vi fått.	Ja
11.3	Har organisationen förtecknat och anmält personuppgifter till personuppgiftsombud?	Ja, för de system som kräver det ska detta ha skett.	Ja
11.4	Genomförs interna och externa penetrationstester kontinuerligt?	*Enligt uppgift administrerar Höglandets IT detta.*	HIT = NEJ
11.5	Granskar ledningspersoner regelbundet att säkerhetsrutiner, -policy och -normer efterlevs.	I en intervju framkom det att det görs uppföljningar regelbundet och dokumentation görs på t ex loggfiler. I övriga fall finns inte denna rutin.	Delvis

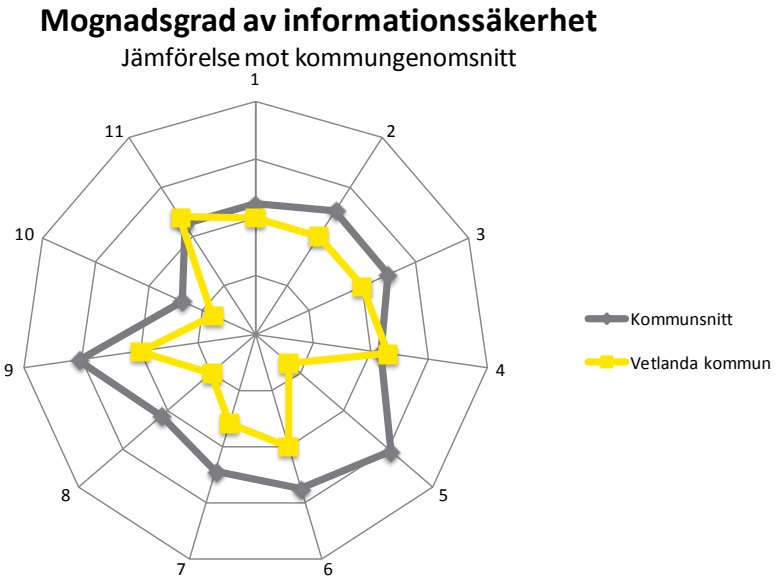
3 Jämförelse mot andra kommuner

EY har gjort 17 gapanalyser mot BITS bland Sveriges kommuner. Tack vare detta kan vi mäta Vetlanda kommuns mognadsgrad rörande informationssäkerhet mot ett genomsnitt av de kommuner vi granskat.

Siffrorna anger respektive område i BITS enligt:

1. Säkerhetspolicy
2. Organisation av säkerheten
3. Hantering av tillgångar
4. Personalresurser och säkerhet
5. Fysisk och miljörelaterad säkerhet
6. Styrning och kommunikation av drift
7. Styrning av åtkomst
8. Anskaffning, utveckling och underhåll av informationssystem
9. Hantering av informationssäkerhetsincidenter
10. Kontinuitetsplanering i verksamheten
11. Efterlevnad

I diagrammet nedan representerar ytterkanten 100 % måluppfyllnad, medan mittpunkten anger 0% måluppfyllnad.



Vetlanda kommun ligger under kommunsnittet totalt sett, men enligt diagrammet ovan så framgår det att några områden ligger högre, t.ex. 11 (Efterlevnad), och några lägre än snittet, t.ex. 9 (Hantering av informationsincidenter). Stor orsak till att snittet ligger under medel beror på osäkerheten runt HITs hantering av IT-stödet i kommunen. De områden som HIT enligt uppgift utför, och där inget skriftligt avtal föreligger som tydliggör ansvarsfördelning och uppdrag, har vi klassat som NEJ. Detta gör att jämförelsen mot andra kommuner då inte är helt jämförbar.

4 Slutsatser och rekommendationer

4.1 Generella slutsatser

Vetlanda kommun har förutsättningar för ett effektivt arbete med informationssäkerhet. Då allt fler rutiner och kontroller blir outsourcade till HIT är det viktigt att samarbetet inkluderar tydligt definierade ansvar och roller samt hur kommunen vill att dess data och system ska hanteras. I dag finns oklarheter, vilket starkt påverkar bedömningen mot BITS. Vissa områden finns på plats, men vi noterar samtidigt att det är hos enskilda förvaltningar, som särskilt arbetar med IT-frågor, man uppnår en högre säkerhetsnivå och bättre struktur.

Av samtliga granskningspunkter är fördelningen av bedömningarna följande:

Ja	Aktuellt område i BITS finns adresserat och kontroll bedöms rimligen implementerad:	**21 %**
Delvis	Kontrollen identifierad och bedöms enbart delvis implementerad:	**40 %**
Nej	Kontroll har ej identifierats/Har inte kunna identifierats som implementerad:	**37 %**
	Varav kontroller administrerade av HIT	(22 %)
E/T	Ej tillämplig, kontrollen behövs ej av särskilda skäl:	**2 %**

4.2 Rekommendationer

Nedan följer våra rekommendationer samt ett förslag på prioritering av dessa. Vi har valt att presentera de iakttagelser som vi anser är mest väsentliga. Rekommendationerna är prioriterade enligt följande:

Hög	Nyckelkontroll är inte på plats/är inte effektiv. Bristen bör åtgärdas snarast för att säkerställa god intern kontroll på kort sikt.
Medel	Nyckelkontroll delvis på plats/delvis effektiv. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Nyckelkontroll på plats men effektivitet kan förbättras. Bristen bör åtgärdas på lång sikt.

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Informationssäkerhetskrav för administration och förvaltning saknas. Vi har noterat att det finns en IT-säkerhetspolicy från år 2001. Policyn finns inte tillgänglig i elektroniskt format och bedöms därför inte vara lättillgängligt för alla. Det finns heller inte tydliga instruktioner om vem som är ansvarig för säkerhetsfrågor. Vid granskning rörande outsourcingen av driften av IT-stödet till HIT framkom också stor osäkerhet kring vem som är ansvarig för vad och vilka instruktioner som HIT har tillgång till. **Risk:** Att inte ha tydligt definierade och kommunicerade informations-säkerhetsregler kring administration och förvaltning av system kan öka riskerna för incidenter som stöld, förlust av information, bedrägeri, driftavbrott och lagbrott. Då stor del av driften även är outsourcad ökar det ytterligare komplexiteten i ansvarsfrågan. Om otydlighet finns rörande kommunikationen finns det även en risk att kommunen har svårare att hävda sin rätt vid en eventuell juridisk tvist. **Rekommendation:** Vi rekommenderar Vetlanda kommun att uppdatera sin IT-policy och kommunicera den i organisationen, utifrån ett riskperspektiv. Det är även väsentligt att inkludera tydligt definierade ansvar och roller mellan Vetlanda kommun och HIT samt införa rutiner och kontroller som på ett tillfredsställande sätt täcker identifierade risker. Detta inkluderar en tillräckligt fördelad organisation med t ex systemansvariga, informationssäkerhetsansvarig m.m.	**Hög**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Process för programändringar saknas De delar av förändringsprocesserna är formella inom vissa förvaltningar i kommunen. Det finns däremot ingen generell plan i kommunens IT-säkerhetsanvisningar gällande förändringar i system och driftgodkännande. Det finns då inte en formell process för programförändringar, med tillhörande stödjande dokumentmallar för ändringsbegäran, testprotokoll och driftgodkännande. För vissa väsentliga system finns det heller inte någon testmiljö, att testa förändringar innan de förs in i produktionsmiljön. Då de kommuner som är med i samarbetet HIT byter ut sina system för att få en enhetlighet i HIT-miljön, så sker det kontinuerligt installationer och uppgraderingar i kommunen. Det finns däremot begränsad egen utveckling och det de flesta förändringar avser standardprogram. **Risk:** Att inte ha en dokumenterad och förankrad rutin för programförändringar ökar sannolikheten att förändringar ej testas fullständigt, vilket i sin tur ökar risken för att förändringar påverkar data och/eller funktionalitet i systemet på ett felaktigt sätt. **Rekommendation:** Vi rekommenderar kommunen att utveckla den existerade processen för programförändringar. Följande kontroller och aktiviteter bör finnas med: • Om skillnad skall göras mellan processen för stora och små förändringar bör det tydligt definieras vad en stor och en liten förändring innebär. • Det skall framgå vem som får beställa förändringar. • Alla beställningar av förändringar skall vara dokumenterade. • Riskanalys ska föregå projektet. • Informationssäkerhetsaspekten ska vara med som del i projektstyrning, för att säkerställa att t ex arkiveringsregler följs och att information hanteras korrekt i testmiljö och i framtida behörighetsregler. • Dokumentationen av beställningen bör innehålla numrerade krav. • Beställning skall godkännas av systemägare (eller liknande). • Utveckling av förändring skall göras i separat testmiljö. • Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning. • Testresultat skall godkännas av systemägare (eller liknande). • Migrering av förändring till produktionsmiljö skall ej göras av samma person som utvecklat förändringen. • Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras.	**Hög**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Kontinuitetsplaner och krav på tillgänglighet saknas Det finns en plan att ta fram kontinuitetsplaner men de saknas i dagsläget för de flesta verksamheter. Det finns inte heller tydliga analyser kring längsta acceptabla tid som systemen kan vara ur funktion innan verksamheten äventyras. Vi har noterat i våra samtal att de intervjuade bedömer att verksamheten utan IT-stöd ändå kan fortsätta under viss period, t ex med framtagna kompenserande rutiner. **Risk:** Avsaknad av formell kontinuitetsplanering ökar risken för att avbrott inte hanteras på ett för verksamheten optimalt sätt. Vidare är sannolikheten att verksamheten skall drabbas hårdare vid händelse av en incident, om kontinuitetsplaner saknas. Om inte analys har görs av verksamheten för att bedöma hur länge den klarar sig utan stöd av IT-systemen, blir det svårt att ge direktiv till leverantör och även att kunna köpa in rätt nivå på service. **Rekommendation:** I första hand bör analys ske för att bedöma kravet på tillgänglighet av stödet till verksamheten. Utifrån det så rekommenderar vi Vetlanda kommun att skapa rutiner för kontinuitetsplanering. Rutinerna bör utgå från en processbaserad riskanalys och adressera: • Vad som betecknas som kris/katastrof. • Reservrutiner vid avbrott för tänkta scenarios. • Rutiner för återställning av system. • Rutiner för återskapande av förlorad information. • Rutiner för inmatning av data från reservrutiner. • Periodisk testning av rutiner.	**Medel**
	Iakttagelse: Brister i dokumentation av behörighetsrutiner För vissa av systemen finns en något mer formell rutin rörande förändring av behörigheter, medan det för andra system är helt informellt. Vi har även fått information om att upplåsning av konton sker över telefon, för de känsliga systemen, utan att riktigt säkerställa att det är rätt användare som kontaktat Helpdesk. **Risk:** Att inte ha en formell rutin för behörighetsadministration kan öka risken att icke-auktoriserade personer får åtkomst till system och information**.** **Rekommendation:** Vi rekommenderar Vetlanda kommun att dokumentera och implementera en enhetlig process för att skapa nya/ta bort/förändra rättigheter i systemen. Detta gäller även konsulter och andra externa användare. Följande kontroller och aktiviteter bör finnas med: • Det skall framgå vem som får beställa nya/ta bort/ändra rättigheter och ska då även ha kunskap kring detta område. Det är viktigt att man vet vad Admin-rättigheter innebär innan de delas ut. • Internkontrollperspektivet ska analyseras vid upprättande av roller och tilldelande av behörigheter.	**Medel**

	Iakttagelse och rekommendation	Prioritet
	• Service desk, eller mottagare av beställning, bör kontrollera att beställaren har befogenheter att göra beställning, t ex via mail eller förbestämt säkerhetsord. • Information om att konto har skapats bör skickas med kopia till beställaren. • Användaren bör byta lösenord vid första inloggning. • Det bör vara klarlagt vem som ansvarar för att en person som inte slutar längre har rättigheter till systemen (linjechef eller personalavdelning).	
	Iakttagelse: Formella regler saknas för informationsklassning, I vissa förvaltningar finns det styrande dokument som gör klassning av data utifrån BITS områden som Sekretess, Riktighet och Tillgänglighet. Dessa har sedan delats upp i Bas-, Hög och Mycket hög nivå. Inom vissa andra förvaltningar finns inget dokumenterat. Vi har inte hittat någon sammanhållen informationsklassningspolicy som definierar de olika klasserna samt beskriver hur information får hanteras per klass och som hela kommunen kan använda som standard. Detta gäller även regler för hur lagring ska ske av respektive klass eller informationsslag. **Risk:** Att inte ha klara regler kring informationsklassning kan öka risken att konfidentiell och/eller känslig information kommer i orätta händer. **Rekommendation:** Vi rekommenderar Vetlanda kommun att upprätta en informations-klassningspolicy som definierar informationsklasser samt anger hur informationen per respektive klass skall hanteras.	**Medel**
	Iakttagelse: Kontroll av data på utrangerad maskinvara Kommunen använder vanligtvis ett företag för destruktion av utrangerad maskinvara, men det är osäkert vilka riktlinjer som HIT följer vid förändringar. **Risk:** Om känslig information kommer i orätta händer, t ex om man skulle välja att sälja utrangerad hårdvara utan att destruera minnen, finns risken att det skulle skada både personen det rör men även Vetlanda kommun. **Rekommendation:** Vi rekommenderar Vetlanda kommun att dokumentera och implementera en enhetlig rutin för hur uttjänt maskinvara skall hanteras utifrån risken med data som finns på aktuell dator.	**Medel**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Uppföljning av tilldelade behörigheter Det finns ingen formell rutin i kommunen för att följa upp att rätt användare ligger i respektive system och att användare har rätt behörigheter utifrån ansvarsuppgifter och intern kontroll. **Risk:** Att inte genomföra genomgång av behörigheter i systemen ökar risken för att personer som slutat eller bytt tjänst fortfarande har tillgång till system och information de inte ska ha tillgång till. **Rekommendation:** Vi rekommenderar Vetlanda kommun att dokumentera och implementera en enhetlig rutin för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med: • IT (eller service desk) bör förse linjechefer med listor över behörigheter två gånger per år. • Linjechefer bör gå igenom listorna, markera felaktigheter, signera samt sända tillbaka listorna till IT (eller service desk). • IT (eller service desk) tar bort eller förändrar rättigheter enligt underlag.	**Medel**
	Iakttagelse: Systemförteckning och ägarskap Vi har noterat att vissa förvaltningar har tydlig systemförteckning där t ex systemägare och riskklassning skett på respektive system. I vissa fall finns detta inte dokumenterat, men är ett pågående projekt enligt de intervjuade. **Risk:** Om inte klassning skett av systemen beroende på risk, finns risken att systemet inte behandlas med de resurser som krävs för att verksamheten ska ha ett systemstöd på tillräcklig nivå. Att inte ha utpekade systemägare och systemansvariga för system kan också öka risken att systemägarens och systemansvariges ansvar inte utövas. **Rekommendation:** Vi rekommenderar Vetlanda kommun att fortsätta och avsluta sitt arbete med att dokumentera systemen och tydliggöra risker och ägarskap.	**Medel**

	Iakttagelse och rekommendation	Prioritet
	Iakttagelse: Granskning av efterlevnad Inom vissa förvaltningar utförs viss analys av logglistor och andra rutiner för att säkerställa att policys och rutiner efterföljs. Indikationer visar att dessa kontroller inte utförs på samtliga förvaltningar. **Risk:** Om det tas fram ändamålsenliga kontroller som säkerställer att identifierade risker hamnar på en rimlig nivå men kontrollerna inte utförs kan istället riskerna hamna på en orimligt hög nivå. **Rekommendation:** Vi rekommenderar att kontroller och rutiner verifieras regelbundet för att säkerställa en följsamhet och efterlevnad. Detta för att säkerställa att riskerna inom kommunerna ligger på en rimlig nivå efter att kontroller utförts.	**Medel**