VÄSTERVIKS KOMMUN

Kommunens revisorer

2020-06-02

Till:
Kommunstyrelsen

För kännedom till:
Kommunfullmäktige

Uppföljande granskning av IT- och informationssäkerhet

Under 2016 gav kommunrevisionen PwC i uppdrag att genomföra en granskning av IT-verksamheten och arbetet med informationssäkerhet i Västerviks kommun. Syftet med granskningen var att klargöra vilka eventuella områden som kommunen behövde utveckla för att uppnå en optimal IT-leverans i alla delar inklusive IT- och informationssäkerhet. Resultatet av granskningen visade att det fanns ett flertal områden som kommunen i varierande omfattning behövde ta hänsyn till och arbeta vidare med. Granskningsrapporten innehöll ett antal prioriterade rekommendationer uppdelade på ”Optimal IT-leverans” och ”Teknisk IT-säkerhet och ändamålsenlig informationssäkerhet”. Som svar lämnades en handlingsplan avseende delen som berörde ”Optimal IT-leverans”. Handlingsplanen innehöll ett svar utifrån varje rekommendation, ansvarig funktion samt en tidplan. Gällande rekommendationerna kring ändamålsenlig informationssäkerhet avsåg kommunen att ta ett koncernövergripande helhetsgrepp på dessa rekommendationer och frågeställningar.

I slutet av 2017 fick PwC i uppdrag av kommunrevisionen att genomföra en uppföljning av granskningen som genomfördes under 2016. Slutsatsen i denna uppföljande granskning från 2017 var att kommunen visat en tydlig ambition att uppfylla de rekommendationer som gavs i rapporten från 2016. Det konstaterades att nästan samtliga rekommendationer från tidigare granskning tagits i beaktande och ett arbete hade påbörjats. Dock fanns det vissa initiativ som stannat av p.g.a. tids- och resursbrist. I denna uppföljande granskning gavs övergripande rekommendationer kring det förebyggande arbetet och hanteringen av IT-säkerhetsincidenter och bristande teknisk dokumentation. Rapporten innehöll även specifika rekommendationer till respektive kontrollfråga. Kommunrevisionen lyfte fram fem rekommendationer i sitt missiv och svaret från kommunstyrelsens förvaltning (antaget av kommunstyrelsen 9 maj 2018) avsåg dessa rekommendationer. I svaret framhålls att många delar var pågående eller skulle startas upp.

Under våren 2020 har PwC återigen fått i uppdrag av kommunrevisionen att genomföra en uppföljande granskning av de tidigare lämnade rekommendationerna. Granskningen har omfattat följande tre områden:

1. Teknisk säkerhetsanalys av Västerviks IT-infrastruktur.
2. Följa upp tidigare rekommendationer avseende IT- och informationssäkerhet.
3. Genomföra en mognadsanalys av kommunens säkerhetskultur för förståelse av nuläget i form av en enkätundersökning.

För att granska dessa tre områden har det formulerats tre revisionsfrågor och tillhörande kontrollfrågor. Den sammanfattande och övergripande bedömningen av revisionsfrågorna är att de **ej är uppfyllda**. Rapporten innehåller både generella rekommendationer och rekommendationer kopplade till respektive kontrollfråga.

Kommunrevisionen ställer sig bakom granskningens slutsatser och rekommendationer och överlämnar härmed granskningen till kommunstyrelsen och till kommunfullmäktige för kännedom. Tidigare granskning och uppföljning har lyft fram tydliga utvecklingsområden. Den granskning som nu är genomförd konstaterar att flera av dem kvarstår. Mot bakgrund av detta så önskar kommunrevisionen ett svar för varje rekommendation (se bilaga 2) där det tydligt framgår vad kommunen avser att vidta för åtgärd, vilken funktion som är ansvarig för åtgärden och en tidplan för när det ska vara klart. Utifrån kommunens svar önskar kommunrevisionen ha en löpande dialog med ansvariga funktioner för att få en återkoppling kring vilka åtgärder som vidtas.

Kommunrevisionen önskar svar på de rekommendationer som framgår av bilaga 2 till detta missiv senast den 25 september 2020.

För Västerviks kommuns revisorer

Britt-Louise Åberg Källmark
Ordförande

Bilaga 1: Granskningsrapport – Uppföljande granskning av IT- och informationssäkerhet, april 2020

Bilaga 2: Sammanställning av de rekommendationer som kommunrevisionen önskar svar på

Bilaga 2 -Specifikation över de rekommendationer som kommunrevisionen önskar svar

Revisionsfråga 1

Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna aktörer?

Kontrollfråga 1.1	Rekomendationer
Uppfyller Västerviks kommun kraven för vad som anses vara god praxis gällande teknisk IT-säkerhet för sin IT-	IT-säkerhetsarbetet behöver bedrivas fokuserat, strukturerat och det behöver intensifieras. Det är viktigt att IT-säkerhetsarbetet ligger högt på kommunledningens agenda så att IT-säkerheten genomsyrar hela verksamheten och inte bara några enstaka individers arbete Det är viktigt att Västerviks kommun har rutiner och processer implementerade vad gäller IT-säkerhet och informationssäkerhet som verksamheten arbetar efter och kan ta stöd av. Västerviks kommun bör ta fram en IT-strategi som tydligt visar vägen framåt till en trygg och säker IT-miljö. Det är viktigt att IT-säkerhetsarbetet blir strukturerat och följer rutiner för när och hur de olika delarna ska genomföras, t ex nätverks-, server- och klientpatchning, så att inte delar missas, glöms bort eller nedprioriteras. Ett IT-säkerhetsarbete bygger på struktur, kontroll och spårbarhet, därför bör Västerviks kommun ta fram en "Change Management Process". Västerviks kommun bör ta fram en plan för hur och när kommunen ska ha avvecklat servrar med operativsystem som ej längre supportas från tillverkaren. IT-säkerhetsansvarig bör genomföra ett arbete för att avlägsna alla lösenord som finns i klartext, säkerställa att alla fabrikssatta (default) lösenord byts ut till unika lösenord, samt att kända krypteringsnycklar byts ut. Arbetet med att konfigurera brandväggar och segmentera kommunens och kommunbolagens nätverk bör intensifieras så att arbetet når önskat läge. För att IT ska kunna upprätthålla en adekvat nivå avseende kommunens IT-säkerhetsarbete behövs en tydlig kravställning från kommunledning, verksamhet och från kommunens informationssäkerhetsansvarig. Det bör startas en IT-säkerhetsgrupp som arbetar med IT-säkerhet och driver det kommunövergripande IT-säkerhetsfrågorna, där bland annat representanter från verksamhet, informationssäkerhetssamordnare, digitaliseringsstrateg, IT-chef ingår.

Kontrollfråga 1.2	Rekomendationer
Är Västerviks produktionsnät segmenterat på ett sådant sätt att information inte kan flöda obehindrat mellan nätets delar?	Västerviks kommun bör arbeta vidare med sitt segmenterings- och konfigureringsarbete för att säkerställa att inte onödig trafik tillåts mellan de olika segmenten. Västerviks kommun bör ta fram en dokumenterad detaljerad strategi för det fortsatta arbetet med segmenterings- och regelverksarbetet. Strategin bör innefatta både kommunen och kommunbolagen.

Kontrollfråga 1.3	Rekommendationer
Är Västerviks produktionsnät segmenterat på ett sådant sätt att obehöriga inte kan tillskansa sig åtkomst till nätets olika delar?	-

Revisionsfråga 2

Är kommunens konto- och behörighetshantering implementerad enligt etablerad god praxis?

Kontrollfråga 2.1	
Finns en rutin för att kontinuerligt revidera användarkonton?	**Rekommendationer** Västerviks kommun bör ta fram skriftliga rutiner och processer för att få kontroll över kommunens kontohantering. Västerviks kommun bör ha en utpekad funktion som ansvarar för att säkerställa att Västerviks kommuns konton rensas eller revideras. Kommunens informationssäkerhetsansvarig bör vara kravställare på detta arbete och ansvara för att processer, rutiner och riktlinjer efterlevs. Informationssäkerhetsgruppen bör ta fram en kommunövergripande konto- och lösenordsriktlinje som t ex följer "Center for Internet Security" (CIS), som IT-enheten ska införa och verksamheterna följa.

Kontrollfråga 2.2	Rekommendationer
Efterlevs rutinen, t ex genom att icke aktiva konton rensas bort enligt gällande policy, eller enligt god praxis?	

PwC rekommenderar att Västerviks kommun skyndsamt åtgärdar identifierade brister i konto- och lösenordskomplexiteten.
Västerviks kommun bör etablera regelverk och process för kontohantering och lösenordshantering. Detta regelverk bör följa en vedertagen standard och processen bör vara utformad så att arbetet med kontohantering sker strukturerat och återkommande.
Genomgång av alla kommunens konton med särskilda rättigheter bör genomföras skyndsamt för att rensa bort eller ändra konton med password never expire, samt säkerställa att de konton som ska finnas har säkrare lösenord.

Västerviks kommun bör se till att konton som är personliga inte har password never expire utan att detta endast är förbehållet systemkonton men då i kombination med långa komplexa lösenord.
Västerviks kommun bör genomföra en genomgång av kommunens Active Directory och rensa bort inaktiverade konton för att undvika att bryta mot GDPR.

Revisionsfråga 3

Bedriver kommunen ett systematiskt informationssäkerhetsarbete för att säkra konfidentialitet, riktighet och tillgänglighet för sin information?

Kontrollfråga 3.1	Rekommendationer
Finns tydlig organisation, processer, roller och ansvarsfördelning? Är denna ändamålsenlig?	Det bör finnas en informationssäkerhetsansvarig som tydliggör kravställningen mot IT gällande informationssäkerhet och att denna regelbundet följs upp. Säkerställ att arbetsgruppen för informationssäkerhet har tillräckligt med resurser och mandat. Utred och tilldela vem som ytterst är ansvarig för informationssäkerheten i Västerviks kommun Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.

Kontrollfråga 3.2	Rekommendationer
Bedrivs ett aktivt arbete avseende informationssäkerhet med fokus på information och utbildningar för medarbetare och förtroendevalda?	Ta fram en obligatorisk informationssäkerhetsutbildning för samtliga anställda och politiker i Västerviks kommun. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet. Genomför regelbundet informationsinsatser gällande informationssäkerhet på t ex arbetsplatsträffar och ledningsgruppsmöten. Sammanställ all informationssäkerhetsrelaterad dokumentation, säkerställ att den förvaras på ett och samma ställe, samt kommunicera ut var dokumentationen finns tillgänglig.

Kontrollfråga 3.3	Rekommendationer
På vilken nivå bedöms kommunens mognad avseende informationssäkerhet ligga?	Säkerställ att samtliga medarbetare får en genomgång av säkerhetsrelaterad dokumentationen i samband med nyanställning. Specificera aktiviteter som ska genomföras i respektive verksamheter för att främja en god säkerhetskultur. Genomför även systematiska uppföljningar av utbildningsverksamheten.

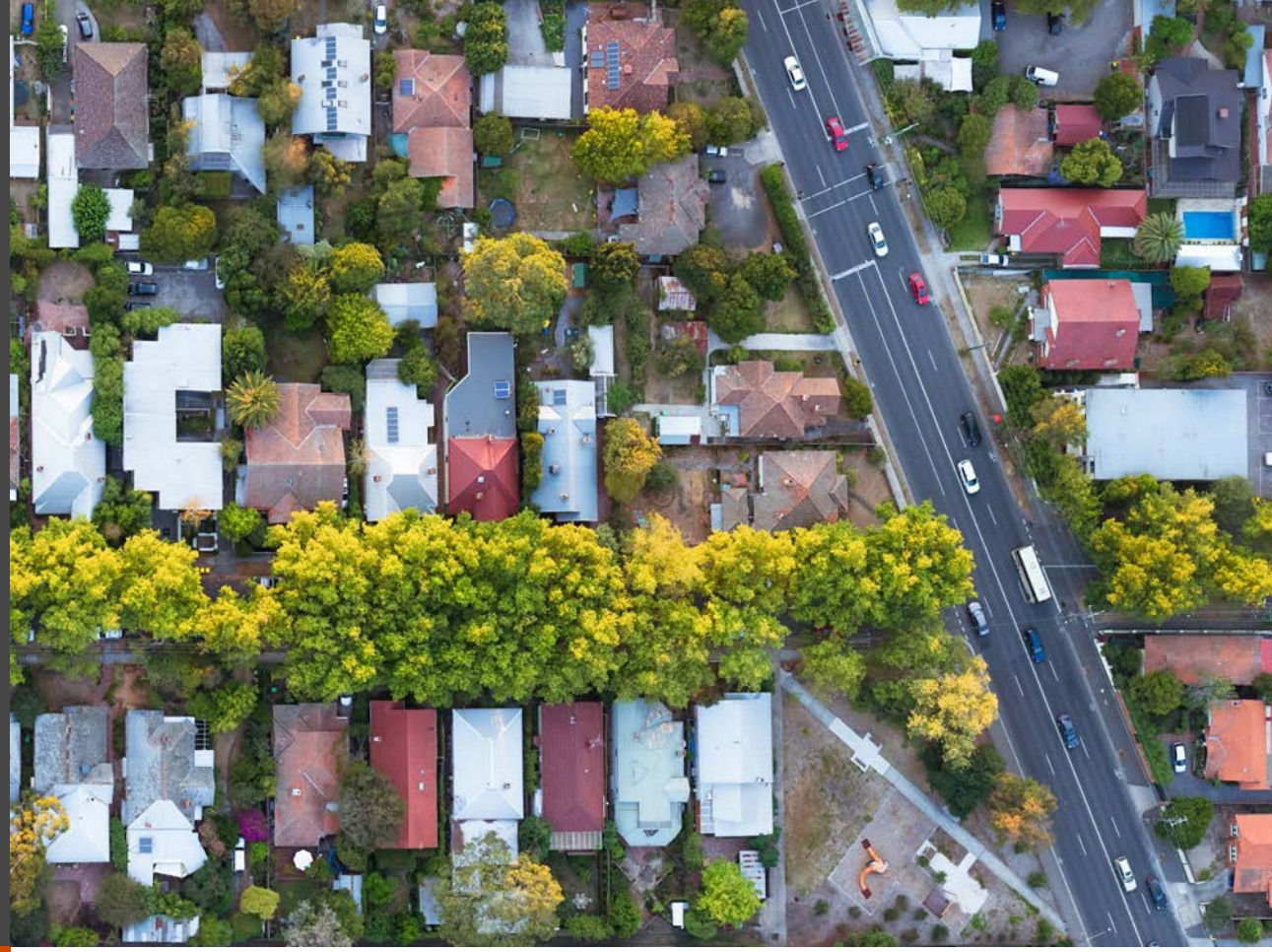
Generella rekommendationer

**Följande rekommendationer är övergripande och inte direkt kopplade till en specifik kontrollfråga.
Däremot anser vi att de är viktiga för den övergripande förståelsen.**

För att uppnå ett effektivt IT-säkerhetsarbete som har kommunledningens stöd och förståelse är det viktigt att kommunledningen är väl insatt i alla aspekter av den stora komplexiteten och snabba förändringstakten inom detta område. Det är viktigt att kommunledningen är tydlig med kommunens ambitioner inom IT- och informationssäkerhetsområdet.
En nyckelfaktor hos många kommuner och organisationer är att IT-chefen tillhör ledningen eller har tät personlig åtkomst till ledningen.
IT-enheten bör göra en kraftansträngning för att få ordning på sin bristande dokumentation.
Västerviks kommun bör arbeta för att IT-säkerhetsansvarig och informationssäkerhetssamordnaren/säkerhetsorganisationen arbetar tätt tillsammans för att på så vis kunna hjälpa och stötta varandra.
Man bör ta fram och definiera en kravställan gällande IT- och informationssäkerhet mellan enheten för räddningstjänst och samhällsskydd och IT-enheten.

Västerviks kommun
Revisionsrapport

Uppföljande granskning av IT- och informationssäkerhet



April 2020

Innehåll

1

Sammanfattning

Sammanfattning

Övergripande revisionsfrågor

Rapporten avser att belysa tre övergripande revisionsfrågor:

1. Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna aktörer?
2. Är kommunens konto- och behörighetshantering implementerad enligt etablerad god praxis?
3. Bedriver kommunen ett systematiskt informationssäkerhetsarbete för att säkra konfidentialitet, riktighet och tillgänglighet för sin information?

Resultat

PwC:s övergripande bedömning avseende de tre revisionsfrågorna ovan är **Ej uppfylld.**

Rekommendationer

Västerviks kommun rekommenderas att:

- Säkerställa att IT- och informationssäkerhet ligger högt på kommunledningens agenda så att IT-säkerheten genomsyrar hela verksamheten.
- Bedriva ett strukturerat och fokuserat IT- och informationssäkerhetsarbete för att uppnå önskad kontroll, skydd och effekt.
- Ta fram och definiera en kravställan gällande IT- och informationssäkerhet mellan enheten för räddningstjänst och samhällsskydd och IT-enheten.
- Starta ett IT-säkerhetsråd som driver de kommunövergripande IT-säkerhetsfrågorna.
- Ta fram en kommunövergripande IT-strategi.
- Ta fram en “Change Management Process” för att förstärka struktur, kontroll och spårbarhet i det dagliga förändringsarbetet.
- Ta fram kommunövergripande konto- och lösenordsriktlinjer samt regelverk, ta vägledning av befintliga standarder, t ex CIS.
- Ta fram rutiner och processer för kontohantering så att detta arbete sker strukturerat.
- Ta fram en dokumenterad strategi och en detaljerad plan för nätverkssegmentering och verifiera strategin och planen med utomstående sakkunnig.
- Skyndsamt genomföra ett fokuserat arbete med att komma till rätta med de brister som finns i kommunens kontohantering och lösenordsnivå.
- Säkerställa att det finns en tydlig dokumentationshierarki i kommunen, att samtlig dokumentation regelbundet revideras och att ansvarig för revidering framgår i dokumenten.
- Ta fram obligatoriska IT- och informationssäkerhetsutbildningar för samtliga anställda i Västerviks kommun. Säkerställa att utbildningar genomförs regelbundet.
- Inrätta uppföljning som en obligatorisk del i Västerviks kommuns IT- och informationssäkerhetsarbete. Detta för att kunna säkerställa att åtgärder genomförs, att dokumentation upprättas i önskad utformning och omfattning samt att utvärderingar och erfarenhetsåterföring genomförs ändamålsenligt.

Revisionell bedömning

Övergripande revisionsfråga 1

Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna aktörer?

Bedömning

PwC:s bedömning av revisionsfråga 1 är **Ej uppfylld.**

- PwC har kunnat påpeka flertalet större brister gällande IT-säkerheten där god praxis ej följs. PwC kan också konstatera att IT-säkerhetsarbetet i Västerviks kommun ej bedrivs på ett strukturerat och tillräckligt fokuserat vis. Det saknas också en tydlig kravställning från kommunledning, verksamhet samt från kommunens informationssäkerhetsansvarige gentemot IT-enheten, vilket är nödvändigt för att denna ska kunna genomföra ett effektivt IT-säkerhetsarbete som speglar kommunens behov och dagens säkerhetshot.
- PwC har kunnat påvisa att segmentering mellan flertalet nätverkssegment finns. Dock är detta ej fullständigt. En dokumenterad strategi för segmenteringsarbetet behövs för att kunna arbeta strukturerat med nätverkssegmentering.
- Att PwC har kunnat tillskansa sig högsta behörighet i domänen “adm.vastervik.se” leder till stora möjligheter att ta sig vidare till flertalet av nätverkssegment.

Revisionell bedömning

Övergripande revisionsfråga 2

Är kommunens konto- och behörighetshantering implementerad enligt etablerad god praxis?

Bedömning

PwC:s bedömning av revisionsfråga 2 är **Ej uppfylld.**

- ➢ Västerviks kommun saknar en rutin för revidering av användarkonton. Det saknas också processer och det bedrivs ej något strukturerat arbete kring detta. Även övervakning och kravställning från informationssäkerhetsansvarig saknas. Avsaknad av kommunövergripande konto- och lösenordsriktlinjer är en stor brist.
- ➢ PwC har kunnat identifiera brister i Västerviks kommuns kontohantering som innebär att man ej följer god praxis. Brister inom detta område har påtalats i tidigare granskningar som PwC har genomfört utan att detta har åtgärdats.

Revisionell bedömning

Övergripande revisionsfråga 3

Bedriver kommunen ett systematiskt informationssäkerhetsarbete för att säkra konfidentialitet, riktighet och tillgänglighet för sin information?

Bedömning

PwC:s bedömning av revisionsfråga 3 är **Ej uppfylld.**

- Det kan konstateras att Västerviks kommun bedriver ett arbete med sitt informationssäkerhetsarbete. Det finns organisation, roller och ansvarsfördelning till viss del. Däremot saknas ett centralt ansvar för området i kommunen och processerna är ännu inte till fullo implementerade. Vidare saknas det i dagsläget kontroll av efterlevnad samt kravställan för informationssäkerhetsfrågor hos verksamheten och IT. Utan formell och definierad kravställning mot såväl verksamheten som IT-enheten blir det svårt att bedriva ett strukturerat och effektivt säkerhetsarbete.
- Bedömningen grundar sig i att det i dagsläget inte genomförts några utbildningsinsatser och att det i en mycket liten utsträckning genomförts informationsinsatser till medarbetare i Västerviks kommun. Att tillägga är dock att det som nämnt planeras att inom kort genomföra en utbildning gällande informationssäkerhet i kommunen.
- Västerviks kommun har ett pågående arbete med att höja kommunens mognad avseende informationssäkerhet. Det saknas medvetenhet om informationssäkerhet hos medarbetare och det genomförs i dagsläget ingen uppföljning eller några åtgärder för att höja medvetenheten. Det finns en diskrepans mellan det som står i policys och riktlinjer samt det som sker i verksamheterna, vilket tyder på att det som beslutas inte till fullo implementeras. Därmed bedöms Västerviks kommuns mognad avseende informationssäkerhet som låg.

2

Bakgrund och revisionsfrågor

Inledning

Bakgrund

PwC har genomfört flera granskningar av IT- och informationssäkerheten i Västerviks kommun på uppdrag av kommunens revisor.

2016 genomfördes en omfattande granskning som bland annat innefattande IT-säkerhet i form av penetrationstester för att identifiera sårbarheten i det interna nätverket genom tekniska analyser. I det arbetet gjordes även en analys av medarbetarnas medvetenhet avseende informationssäkerhetshot i form av mailutskick (så kallat phishingmail).

2017 genomfördes en uppföljning av IT-säkerheten, där de rekommenderade åtgärderna från granskningen 2016 följdes upp.

PwC hade under februari - april 2020 i uppdrag av kommunrevisorerna att genomföra en uppföljande granskning av tidigare rekommendationer. Rapporten avser att belysa nedan listade övergripande områden:

1. Teknisk säkerhetsanalys av Västerviks IT-infrastruktur
2. Följa upp tidigare rekommendationer avseende IT- och informationssäkerhet
3. Genomföra en mognadsanalys av kommunens säkerhetskultur för förståelse av nuläget i form av en enkätundersökning

För att besvara de ovan nämnda områdena har delområden definierats i form av revisionsfrågor och kontrollfrågor, som presenteras på nästa sida.

Revisionsfrågor och kontrollfrågor

Revisionsfråga 1.

Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna aktörer?

1.1 Uppfyller Västerviks kommun kraven för vad som anses vara god praxis gällande teknisk IT-säkerhet för sin IT-infrastruktur?
1.2 Är Västerviks produktionsnät segmenterat på ett sådant sätt att information inte kan flöda obehindrat mellan nätets delar?
1.3 Är Västerviks produktionsnät segmenterat på ett sådant sätt att obehöriga inte kan tillskansa sig åtkomst till nätets olika delar?

Revisionsfråga 2.

Är kommunens konto- och behörighetshantering implementerad enligt etablerad god praxis?

2.1 Finns en rutin för att kontinuerligt revidera användarkonton?
2.2 Efterlevs rutinen, t ex genom att icke aktiva konton rensas bort enligt gällande policy, eller enligt god praxis?

Revisionsfråga 3.

Bedriver kommunen ett systematiskt informationssäkerhetsarbete för att säkra konfidentialitet, riktighet och tillgänglighet för sin information?

3.1 Finns tydlig organisation, processer, roller och ansvarsfördelning? Är denna ändamålsenlig?
3.2 Bedrivs ett aktivt arbete avseende informationssäkerhet med fokus på information och utbildningar för medarbetare och förtroendevalda?
3.3 På vilken nivå bedöms kommunens mognad avseende informationssäkerhet ligga?

3

Metod

Metod

Granskningen har baserats på PwC:s metod ITM (IT Maturity analysis). Metoden bygger på områden som tillsammans representerar IT-verksamheten inom en organisation. Metoden tar även hänsyn till så kallad “good practice” inom IT generellt och jämför erhållet resultat med hur IT hanteras hos andra organisationer. Nedan presenteras vilka områden denna rapport har fokuserat på.

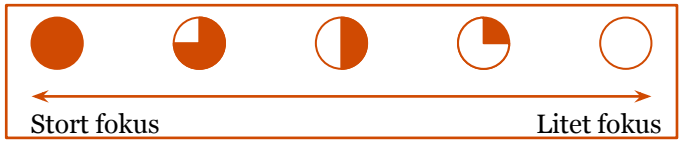
Informationssäkerhet
- Finns det en tydlig målbild och ansvarsfördelning för arbetet med informationssäkerhet? Hur arbetar man med att klassificera och kategorisera data samt känslig data? Kravställning och uppföljning mot verksamhet.

Teknisk säkerhet
- Hur arbetar organisationen med att utveckla och hålla sig á jour med den tekniska säkerheten? Hur säkerställer man säkerheten hos externa system? Hur kontrollerar och managerar man devices? Hur säkerställer man en fullgod säkerhet på servrar/laptops/plattor och mobiler? Är driftorganisationen ordentligt rustad att klara ett systemhaveri?

Drift och utveckling
- Drift: Hur ser den dagliga driften ut? Hur arbetar man aktivt med leverantörsstyrning? Hur ser processer, rutiner, dokumentation samt loggföring ut för driftorganisationen?
- Utveckling: Hur ser utvecklingsarbetet ut? Finns det tydliga, processer, rutiner och dokumentation som reglerar arbetet?

Organisation och personal
- Hur ser rollfördelningen ut inom organisationen? Finns det en tydlig ansvarsfördelning? Är bemanningen i driftorganisationen samt service-desk tillräcklig och har de rätt kompetens? Är organisationen strukturerad och uppbyggd för att inte hamna i beroende till nyckelpersoner?

Utveckling och framtid
- Hur arbetar organisationen med förändringsarbete, utveckling och målsättningar? Finns det planer och strategier för att leda organisationen framåt? Finns tydliga mål och visioner från ledningen uppsatta och dokumenterade?



Metod (forts.)

Vår granskning av kommunens IT- och informationssäkerhet har genomförts genom penetrationstest, BSA (se bilaga 3) och enkätundersökning (se bilaga 2), samt intervjuer med nyckelpersoner inom kommunen (se bilaga 1). Våra bedömningar baseras på utfallet från dessa.

Informationsinsamlingen och grund för granskningen har skett genom analys av rekommendationer från tidigare års granskning samt av erhållna dokument.

Insamling av data

- Teknisk säkerhetsgranskning utfördes med hjälp av ett internt penetrationstest. Det interna penetrationstestet utgick från nätverksutrustning som var inkopplad i Västervik kommuns interna nätverk.
- BSA (Baseline Security Assessment) innebär att PwC med hjälp av ett skript har testat nivån för kontroll- och säkerhetsinställningar samt jämfört resultatet med Center for Internet Securitys (CIS) riktlinjer.
- Enkätutskick till Västerviks kommunanställda, kommunbolag och förtroendevalda.
- Intervjuer.
- Dokumentation genomgång.

Avgränsning

- Observationer, bedömningar och rekommendationer baseras endast på den information som tillgängliggjorts.
- Representanter från Västerviks kommun har intervjuats, där urvalet av intervjudeltagare har gjorts i dialog med beställaren.
- Granskningen avser Västerviks kommuns nät, samt organisation. Bolagen i kommunkoncernen kommer inte att granskas specifikt.
- PwC:s roll är som granskare och rådgivare, vilket innebär att slutliga beslut om genomförande av föreslagna åtgärder tas av Västerviks kommun.

4

Observationer, rekommendationer och bedömning

Revisionsfråga 1

Är kommunens nuvarande IT-säkerhet tillräcklig för att minimera risker för obehörigt intrång av interna aktörer?

Kontrollfråga 1.1

Uppfyller Västerviks kommun kraven för vad som anses god praxis gällande teknisk IT-säkerhet för sin IT-infrastruktur?

Observationer

- IT-chefen är ansvarig för kommunens IT-säkerhetsarbete.
- Det upplevs finnas en osäkerhet i vem som leder kommunens operativa IT-säkerhetsarbete och vad som ingår i detta åtagande.
- Det saknas ett strukturerat operativt IT-säkerhetsarbete, det mesta görs sporadiskt.
- Västervik har inte en patch management-plan att följa, patchning av t ex servrar sker, men inte tillräckligt strukturerat.
- Patchning av nätverksutrustning (brandväggar, switchar, WiFi-access-punkter m.m.) sker endast sporadiskt och även här saknas en dokumenterad plan. Detta kan innebära att det finns utrustning som ej patchas på väldigt lång tid.
- IT-enheten har en del IT-relaterad dokumentation men den är av skiftande karaktär och kvalitet.
- Förändringar i kommunens brandvägg dokumenteras ej utanför brandväggen.
- Kommunen saknar en förändringsprocess (Change Management Process) som möjliggör tydlig spårbarhet i de ändringar och beslut som tagits.
- IT-enheten använder materialet från tidigare granskningar samt MSB:s rekommendationer som vägledning i sitt IT-säkerhetsarbete.
- IT-enheten genomför sårbarhetsskanningar för att hitta sårbarheter i systemen. Men det saknas en nedskriven process för när och hur dessa ska ske så att system inte missas.

Rekommendationer

- Västerviks kommun bör säkerställa att det operativa IT-säkerhetsansvaret är tydligt och klart definierat och tjänsten bör endast fokusera på dessa frågor för att detta ej ska bortprioriteras.
- IT-säkerhetsarbetet behöver bedrivas fokuserat, strukturerat och det behöver intensifieras.
- Det är viktigt att IT-säkerhetsarbetet ligger högt på kommunledningens agenda så att IT-säkerheten genomsyrar hela verksamheten och inte bara några enstaka individers arbete.
- Det är viktigt att Västerviks kommun har rutiner och processer implementerade vad gäller IT-säkerhet och informationssäkerhet som verksamheten arbetar efter och kan ta stöd av.
- Västerviks kommun bör ta fram en IT-strategi som tydligt visar vägen framåt till en trygg och säker IT-miljö.
- Det är viktigt att IT-säkerhetsarbetet blir strukturerat och följer rutiner för när och hur de olika delarna ska genomföras, t ex nätverks-, server- och klientpatchning, så att inte delar missas, glöms bort eller nedprioriteras.
- Ett IT-säkerhetsarbete bygger på struktur, kontroll och spårbarhet, därför bör Västerviks kommun ta fram en “Change Management Process”.
- Som PwC har rekommenderat i tidigare granskningar bör Västerviks kommun genomföra ett strukturerat arbete med att gå igenom all IT-relaterad dokumentation för att se vad som finns och vad som saknas. Kommunen bör ta fram dokumentmallar för rutiner, processer och instruktioner som ska följas vid framtagande av ny dokumentation samt för att säkerställa att nuvarande information håller tillräckligt hög standard.

Kontrollfråga 1.1 (forts.)

Uppfyller Västerviks kommun kraven för vad som anses god praxis gällande teknisk IT-säkerhet för sin IT-infrastruktur?

Observationer

- Det finns inte någon som har det övergripande ansvaret att åtgärda de brister som sårbarhetsskanningen har visat.
- Kommunen har flera servrar med operativsystem som ej längre supporteras, både avseende Microsoft och andra operativsystem.
- Under den tekniska delen av granskningen påträffades flertalet lösenord som var lagrade i klartext.
- Krypterade systemlösenord med svag kryptering påträffades.
- Flera system i det interna nätverket tillhandahåller tjänster som inte kräver autentisering.
- Under granskningen har PwC påträffat utrustning med av leverantören "fabrikssatta" (default) lösenord.
- Det saknas en tydlig kravställning från verksamheten gentemot IT-enheten vad gäller IT-säkerhet.

Rekommendationer

- Västerviks kommun bör ta fram en plan för hur och när kommunen ska ha avvecklat servrar med operativsystem som ej längre supportas från tillverkaren.
- Det bör finnas en sammanställning på vilka olika versioner av klientoperativsystem som kommunens samtliga klienter har, samt en plan för när dessa ska bytas ut/uppdateras.
- IT-säkerhetsansvarig bör genomföra ett arbete för att avlägsna alla lösenord som finns i klartext, säkerställa att alla fabrikssatta (default) lösenord byts ut till unika lösenord, samt att kända krypteringsnycklar byts ut.
- Arbetet med att konfigurera brandväggar och segmentera kommunens och kommunbolagens nätverk bör intensifieras så att arbetet når önskat läge.
- För att IT ska kunna upprätthålla en adekvat nivå avseende kommunens IT-säkerhetsarbete behövs en tydlig kravställning från kommunledning, verksamhet och från kommunens informationssäkerhetsansvarig.
- Det bör startas en IT-säkerhetsgrupp som arbetar med IT-säkerhet och driver det kommunövergripande IT-säkerhetsfrågorna, där bland annat representanter från verksamhet, informationssäkerhetssamordnare, digitaliseringsstrateg, IT-chef ingår.

Bedömning

Ej uppfylld.

PwC har kunnat påpeka flertalet större brister gällande IT-säkerheten där god praxis ej följs. PwC kan också konstatera att IT-säkerhetsarbetet i Västerviks kommun ej bedrivs på ett strukturerat och tillräckligt fokuserat vis. Det saknas också en tydlig kravställning från kommunledning, verksamhet samt från kommunens informations-säkerhetsansvarig gentemot IT-enheten, vilket är nödvändigt för att denna ska kunna genomföra ett effektivt IT-säkerhetsarbete som speglar kommunens behov och dagens säkerhetshot.

Kontrollfråga 1.2

Är Västerviks produktionsnät segmenterat på ett sådant sätt att information inte kan flöda obehindrat mellan nätets delar?

Observationer

- PwC har under den tekniska granskningen identifierat ett stort antal nätverk och tester genomfördes mot utvalda nätverkssegment.
- Nätverksskanningen påvisade att det delvis saknas begränsning mellan delar av nätverkssegment.

Rekommendationer

- Västerviks kommun bör arbeta vidare med sitt segmenterings- och konfigureringsarbete för att säkerställa att inte onödig trafik tillåts mellan de olika segmenten.
- Västerviks kommun bör ta fram en dokumenterad detaljerad strategi för det fortsatta arbetet med segmenterings- och regelverksarbetet. Strategin bör innefatta både kommunen och kommunbolagen.

Bedömning

Delvis uppfylld.

PwC har kunnat påvisa att segmentering mellan flertalet nätverkssegment finns. Dock är detta ej fullständigt. En dokumenterad strategi för segmenteringsarbetet behövs för att kunna arbeta strukturerat med nätverkssegmentering.

Kontrollfråga 1.3

Är Västerviks produktionssätt segmenterat på ett sådant sätt att obehöriga inte kan tillskansa sig åtkomst till nätets olika delar?

Observationer

- Under granskningen kunde PwC tillskansa sig högsta behörighet i domänen.
- Med hjälp av ovanstående behörigheter, och i anslutning till att det fortfarande pågår arbete med segmentering, kunde man göra vissa förflyttningar mellan segment.

Rekommendationer

- Västerviks kommun bör arbeta vidare med sitt segmenteringsarbete för att säkerställa att inte onödig trafik tillåts mellan de olika segmenten.
- Västerviks kommun bör införa en “Change Management Process” som “alltid” ska följas när man genomför förändringar, detta för att alla förändringar ska vara spårbara till när, av vem och varför dessa gjordes.
- Tillfälliga ändringar ska alltid vara tidsbestämda.

Bedömning

Delvis uppfylld.

Att PwC har kunnat tillskansa sig högsta behörighet i domänen “adm.vastervik.se” leder till stora möjligheter att ta sig vidare till flertalet av nätverkssegment.

Revisionsfråga 2

Är kommunens konto- och behörighetshantering implementerad enligt etablerad god praxis?

Kontrollfråga 2.1

Finns en rutin för att kontinuerligt revidera användarkonton?

Observationer

- Det saknas processer och rutiner för att löpande och systematiskt revidera kommunens användarkonton.
- Det saknas kravställning från verksamheten vad gäller rensning och revidering av användarkonton.
- Det saknas kravställning från informationssäkerhetsansvarig vad gäller rensning och revideringen av kommunens konton.
- Det finns ingen utpekad funktion som ansvarar för att säkerställa att Västerviks kommuns konton rensas eller revideras. Detta gäller oavsett om dessa styrs via “Active Directory”, eller de konton som verksamheten ansvarar för själva. Det pågår inte heller något strukturerat arbete avseende detta.
- Det saknas en kommunövergripande konto- och lösenordsriktlinje i Västerviks kommun.

Rekommendationer

- Västerviks kommun bör ta fram skriftliga rutiner och processer för att få kontroll över kommunens kontohantering.
- Västerviks kommun bör ha en utpekad funktion som ansvarar för att säkerställa att Västerviks kommuns konton rensas eller revideras.
- Kommunens informationssäkerhetsansvarig bör vara kravställare på detta arbete och ansvara för att processer, rutiner och riktlinjer efterlevs.
- Informationssäkerhetsgruppen bör ta fram en kommunövergripande konto- och lösenordsriktlinje som t ex följer “Center for Internet Security” (CIS), som IT-enheten ska införa och verksamheterna följa.

Bedömning

Ej uppfylld.

Västerviks kommun saknar en rutin för revidering av användarkonton. Det saknas också processer och det bedrivs ej något strukturerat arbete kring detta. Även övervakning och kravställning från informationssäkerhetsansvarig saknas. Avsaknad av en kommunövergripande konto- och lösenordsriktlinjer är en stor brist.

Kontrollfråga 2.2

Efterlevs rutinen, t ex genom att icke aktiva konton rensas bort enligt gällande policy, eller enligt god praxis?

Observationer

- Västervik har tre domäner som skiljer användare åt; skola, gemensam och administrativ.
- Brister i kontohantering har identifierats hos Västerviks kommuns samtliga domäner.
- Brister i lösenordskomplexitet och längd har identifierats. Även en oförsvarbar mängd konton med *password never expire* har identifierats i samtliga domäner.
- Det finns flera personliga konton i IT-enheten som har domän-administratörsrättigheter och samtidigt har *password never expire*.
- Det finns konton med ökade rättigheter som tillhör leverantörer och IT-personal som inte har bytt lösenord på över 10 år.
- Det finns en oförsvarbar mängd konton som har domänadministrativa rättigheter.
- Det finns konton i Västerviks Active Directory som är inaktiverade sedan lång tid men ej är borttagna, en del av dessa konton innehåller uppgifter som faller under GDPR.

Rekommendationer

- PwC rekommenderar att Västerviks kommun skyndsamt åtgärdar identifierade brister i konto- och lösenordskomplexiteten.
- Västerviks kommun bör etablera regelverk och process för kontohantering och lösenordshantering. Detta regelverk bör följa en vedertagen standard och processen bör vara utformad så att arbetet med kontohantering sker strukturerat och återkommande.
- Genomgång av alla kommunens konton med särskilda rättigheter bör genomföras skyndsamt för att rensa bort eller ändra konton med *password never expire,* samt säkerställa att de konton som ska finnas har säkrare lösenord.
- Västerviks kommun bör se till att konton som är personliga inte har *password never expire* utan att detta endast är förbehållet systemkonton men då i kombination med långa komplexa lösenord.
- Västerviks kommun bör genomföra en genomgång av kommunens Active Directory och rensa bort inaktiverade konton för att undvika att bryta mot GDPR.

Bedömning

Ej uppfylld.

PwC har kunnat identifiera brister i Västerviks kommuns kontohantering som innebär att kommunen ej följer god praxis. Brister inom detta område har påtalats i tidigare granskningar som PwC har genomfört, utan att dessa har åtgärdats.

Revisionsfråga 3

Bedriver kommunen ett systematiskt informationssäkerhetsarbete för att säkra konfidentialitet, riktighet och tillgänglighet för sin information?

Kontrollfråga 3.1

Finns tydlig organisation, processer, roller och ansvarsfördelning? Är denna ändamålsenlig?

Observationer

- Enheten för räddningstjänst och samhällsskydd ansvarar för samordning av kommunens informationssäkerhet.
- Ansvaret för informationssäkerhet är fördelat mellan cheferna för respektive bolag och förvaltning men det saknas kravställning och uppföljning.
- Det finns en informationssäkerhetsgrupp som arbetar med informationssäkerhet där bland annat informationssäkerhetssamordnare, digitaliseringsstrateg, IT-ekonom och IT-chef ingår.
- Upplevs varierande nivå av tillgänglighet och engagemang i informationssäkerhetsgruppen.
- Informationssäkerhetsgruppen är organiserad under KLG.
- Det saknas en formell och definierad kravställning mot IT-enheten och verksamheten gällande informationssäkerhet.
- De informationssäkerhetsrelaterade beslut som fattas implementeras i verksamheterna genom informationssäkerhetssamordnare till respektive verksamhetschefer som sedan ansvarar för implementationen. Det sker dock ingen uppföljning.
- I Västerviks kommuns *Handlingsprogram trygghet och säkerhet 2019-2022* framkommer att det är enheten för räddningstjänst och samhällsskydd som ansvarar för de definierade prestationsmålen för kommunens informationssäkerhet.

Rekommendationer

- Det bör finnas en informationssäkerhetsansvarig som tydliggör kravställningen mot IT gällande informationssäkerhet och att denna regelbundet följs upp.
- Utred möjligheten att implementera ett ledningssystem för informationssäkerhet (LIS) i kommunen.
- Säkerställ att arbetsgruppen för informationssäkerhet har tillräckligt med resurser och mandat.
- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- Säkerställ att samtlig dokumentation regelbundet revideras och att ansvarig för revidering framgår i dokumenten.
- Utred och tilldela vem som ytterst är ansvarig för informationssäkerheten i Västerviks kommun.
- Informationssäkerhetsgruppen bör regelbundet rapportera till KLG.
- Informationssäkerhetssamordnaren i kommunen bör få en erfaren och rutinerad mentor eller rådgivare som stöd i det fortsatta arbetet (t ex planering, beslut, vägval och prioriteringar) för att få en större utveckling i kommunens informationssäkerhetsfrågor.

Bedömning

Delvis uppfylld. Det kan konstateras att Västerviks kommun bedriver ett arbete med sitt informationssäkerhetsarbete. Det finns organisation, roller och ansvarsfördelning till viss del. Däremot saknas ett centralt ansvar för området i kommunen och processerna är ännu inte till fullo implementerade. Vidare saknas det i dagsläget kontroll av efterlevnad samt kravställan för informationssäkerhetsfrågor hos verksamheten och IT. Utan formell och definierad kravställning mot såväl verksamheten som IT-enheten blir det svårt att bedriva ett strukturerat och effektivt säkerhetsarbete.

Kontrollfråga 3.2

Bedrivs ett aktivt arbete avseende informationssäkerhet med fokus på information och utbildningar för medarbetare och förtroendevalda?

Observationer

- Det framkommer i *Handlingsprogram trygghet och säkerhet 2019-2022* att det ska genomföras minst en utbildningsinsats under 2020 samt minst tre riktade informationsinsatser.
- Ett intranät för medarbetare i Västerviks kommun lanserades i oktober 2019. Där har informationssäkerhet en egen sida där information om ämnet läggs upp, t ex från MSB.
- I september 2019 skaffade Västerviks kommun en licens i ett verktyg för nanolearnings (Junglemap) som ska användas för informationssäkerhets-utbildningar och har tidigare används för epost-säkerhet.
- Det beslutades i december 2019 att det ska genomföras en grundläggande utbildning i informationssäkerhet för att höja nivån av medvetenhet.
- Informationsinsatser kopplat till informationssäkerhet har genomförts på ett antal ledningsgruppsmöten för att tydliggöra syftet med kommande utbildningar.
- Det är respektive verksamhetschefs ansvar att informera nyanställda om de policys och riktlinjer som finns gällande informationssäkerhet.
- Det sker ingen systematisk uppföljning gällande efterlevnad av rutiner, riktlinjer och policys gällande informationssäkerhet.

Rekommendationer

- Ta fram en obligatorisk informationssäkerhetsutbildning för samtliga anställda, förtroendevalda och folkvalda i Västerviks kommun. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- Genomför regelbundet informationsinsatser gällande informationssäkerhet på t ex arbetsplatsträffar och ledningsgruppsmöten.
- Sammanställ all informationssäkerhetsrelaterad dokumentation, säkerställ att den förvaras på ett och samma ställe, samt kommunicera ut var dokumentationen finns tillgänglig.
- Implementera rutiner för säkerhet vid arbetsstationer, t ex att datorer ska låsas när medarbetare inte har uppsikt över dem.

Bedömning

Ej uppfylld. Bedömningen grundar sig i att det i *dagsläget* inte genomförts några utbildningsinsatser och att det i en mycket liten utsträckning genomförts informationsinsatser till medarbetare i Västerviks kommun. Att tillägga är dock att en utbildning gällande informationssäkerhet planeras att genomföras inom kort.

Kontrollfråga 3.3

På vilken nivå bedöms kommunens mognad avseende informationssäkerhet ligga?

Observationer

- Det kan konstateras att det finns rutiner, riktlinjer och policys kopplade till informationssäkerhet, men att dessa inte till fullo är implementerade i verksamheterna.
- Det finns en osäkerhet kring var informationssäkerhetsrelaterad dokumentation återfinns.
- Nästan hälften av medarbetarna i Västerviks kommun vet inte vad som utgör en informationssäkerhetsincident.
- Majoriteten av medarbetare vet inte hur en informationssäkerhetsincident ska rapporteras. Vidare vet inte heller majoriteten av medarbetarna huruvida det finns en dokumenterad rutin för hantering av informations-säkerhetrelaterade incidenter eller ej.
- Lärdomar efter inträffade informationssäkerhetsincidenter kommuniceras inte alltid ut till medarbetare.
- Informationssäkerhetsinstruktionen ingår inte i rutiner för arbetsplatser.
- Medarbetare i Västerviks kommun har inte genomgått någon informations-säkerhetsrelaterad utbildning.
- Enligt 58% av de svarande på enkäten uppnår Västerviks kommun en medelnivå av säkerhetskultur.

Rekommendationer

- Säkerställ att samtliga medarbetare får en genomgång av säkerhetsrelaterad dokumentationen i samband med nyanställning.
- Specificera aktiviteter som ska genomföras i respektive verksamheter för att främja en god säkerhetskultur. Genomför även systematiska uppföljningar av utbildningsverksamheten.
- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.

Bedömning

Ej uppfylld. Västerviks kommun har ett pågående arbete med att höja kommunens mognad avseende informationssäkerhet. Det saknas medvetenhet om informationssäkerhet hos medarbetare och det genomförs i dagsläget ingen uppföljning eller några åtgärder för att höja medvetenheten. Det finns en diskrepans mellan det som står i policys och riktlinjer samt det som sker i verksamheterna, vilket tyder på att det som beslutas inte till fullo implementeras. Därmed bedöms Västerviks kommuns mognad avseende informationssäkerhet som låg.

5

Generella observationer och rekommendationer

Generella observationer

Följande observationer är övergripande och inte direkt kopplade till en specifik kontrollfråga. Däremot anser vi att de är viktiga för den övergripande förståelsen.

- Västerviks kommun saknar en fastställd IT-strategi.
- Den genomgångna dokumentationen håller en varierande kvalitet och det saknas en standard för vad som ska ingå i ett dokument, som t ex ägare, datum, versionsnummer, versionshistorik, om det är ett godkänt dokument eller ej. Det saknas en process för hur och när ett dokument ska revideras. Arbete med detta pågår och det är viktigt att detta arbete slutförs.
- Som PwC har observerat under tidigare granskningar är IT-chefens roll organiserad relativt långt ner i organisationen och långt ifrån kommunledningen.

Generella rekommendationer

Följande rekommendationer är övergripande och inte direkt kopplade till en specifik kontrollfråga. Däremot anser vi att de är viktiga för den övergripande förståelsen.

- För att uppnå ett effektivt IT-säkerhetsarbete som har kommunledningens stöd och förståelse är det viktigt att kommunledningen är väl insatt i alla aspekter av den stora komplexiteten och snabba förändringstakten inom detta område. Det är viktigt att kommunledningen är tydlig med kommunens ambitioner inom IT- och informationssäkerhetsområdet. En nyckelfaktor hos många kommuner och organisationer är att IT-chefen tillhör ledningen eller har tät personlig åtkomst till ledningen. Det är inte att rekommendera att information mellan ledning och IT-chef behöver passera flera nivåer, då har nämligen information en förmåga att förändras. Det är också av vikt att personer på ledningsnivå på ett enkelt sätt har tillgång till den sakkunskap som IT-chefen besitter, eller har tillgång till, för att kunna fatta beslut som har påverkan på IT, både ur ett kostnads- och ur ett säkerhetsperspektiv.
- Västerviks kommun har arbetat fram en digitaliseringsstrategi, detta arbete bör följas upp med framtagandet av en IT-strategi. Utan en IT-strategi blir det svårt för IT och verksamheten att bedriva ett effektivt IT-arbete som följer den strategi som kommunen har beslutat.
- Kommunen bör ta fram en mall för olika typer av IT-dokumentation så att dokumenten håller en ensad standard vad gäller innehåll. Man bör också ta fram regelverk för hur ofta ett dokument ska revideras så att man håller nödvändig dokumentation uppdaterad och relevant.
- IT-enheten bör göra en kraftansträngning för att få ordning på sin bristande dokumentation.
- Västerviks kommun bör genomföra ett genomgång av alla kommunens konton för att rensa bort sådant som ej bör finns kvar både ur säkerhets- och GDPR-synpunkt.
- Västerviks kommun bör arbeta för att IT-säkerhetsansvarig och informationssäkerhetssamordnaren/säkerhetsorganisationen arbetar tätt tillsammans för att på så vis kunna hjälpa och stötta varandra.
- Man bör ta fram och definiera en kravställan gällande IT- och informationssäkerhet mellan enheten för räddningstjänst och samhällsskydd och IT-enheten.
- Det är viktigt att det arbete med dokumenthanteringssystemet och standardmallar som pågår slutförs.

6

Bilagor

Bilaga 1 - Intervjulista

Namn	Roll	Verksamhet
Roger Hassel	Avgående IT-chef	Kommunservice / IT
Christer Lundh	Administrativ chef/Tf IT-chef (personal)	Kommunstyrelsens förvaltning
Per Larsson	Tf IT-chef (drift)	Kommunservice / IT
Per Inge Stenberg	IT-kommunikation	Kommunservice / IT
Gisela Lejonqvist	Digital Strateg/ Informationssäkerhetsansvarig	Västervik Miljö och Energi
Andrea Brändström	Säkerhetsskyddschef	Räddningstjänst och samhällsskydd
Anna Grandalen	Informationssäkerhetssamordnare	Räddningstjänst och samhällsskydd

Bilaga 2 - Enkät

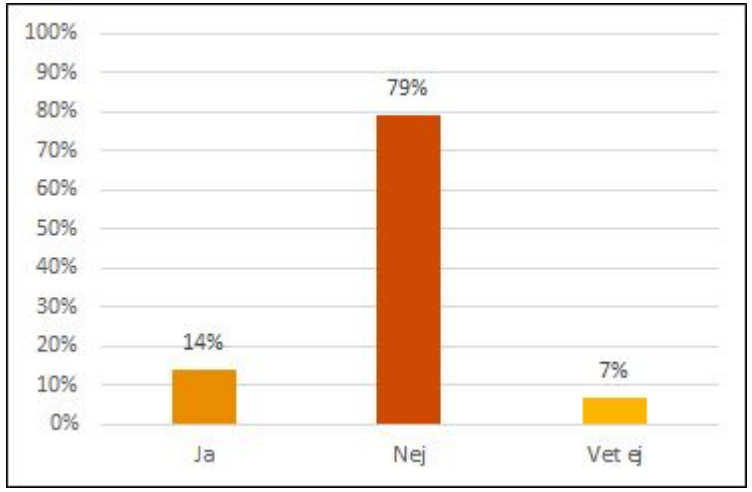
I denna bilaga presenteras en sammanställning av resultaten från den enkät som skickats ut i syfte att mäta anställda/förtroendevalda i Västerviks kommuns säkerhetsmedvetande inom ramen för granskning av kommunens IT- och informationssäkerhet (kontrollfråga 3.2 och 3.3).

Enkäten skickades ut till 4 210 personer, varav 1 748 personer slutförde enkäten. Det gav en svarsfrekvens på ungefär 42 procent. Svaren har en relativt god spridning mellan verksamhetsområdena. Högst svarsfrekvens finns inom Västerviks Resort AB och Miljö- och byggnadskontoret med 70 respektive 69 procent. Barn- och utbildningsförvaltningen och Socialförvaltningen har dock en förhållandevis låg svarsfrekvens på 39 respektive 32 procent.

Bilaga 2 - Enkät - Säkerhetsmedvetenhet

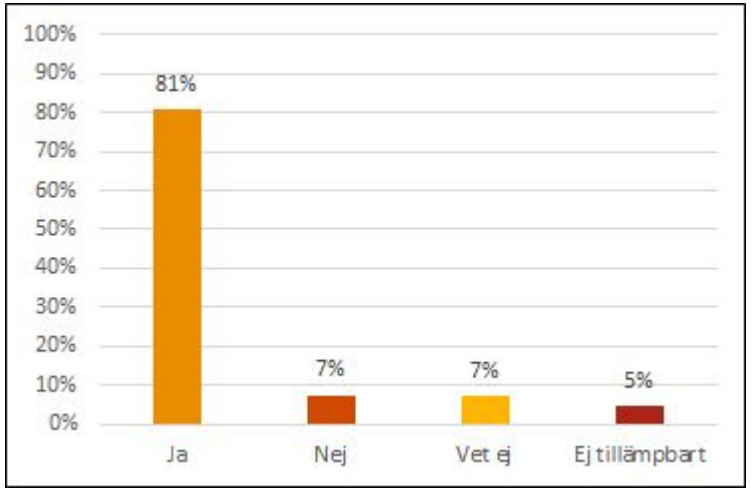
Har du någon gång hört en kollega diskutera känsliga uppgifter med obehöriga på allmän plats?

	Antal svar	Procent
Ja	244	14%
Nej	1384	79%
Vet ej	120	7%
Ej tillämpb	-	-
Totalt	1748	100%



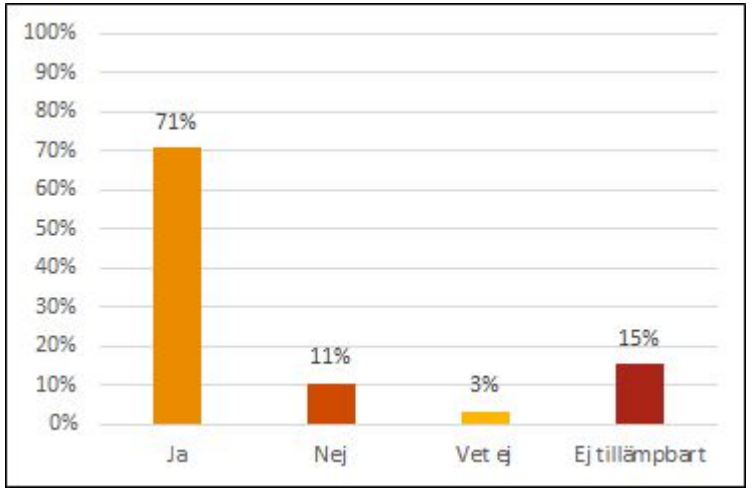
Vet du hur du ska hantera känsliga pappersdokument och utskrifter på din arbetsplats (t.ex. om dokumenten ska hållas under uppsikt, vara inlåsta eller om användarbox ska användas vid utskrifter)?

	Antal svar	Procent
Ja	1410	81%
Nej	129	7%
Vet ej	126	7%
Ej tillämpb	83	5%
Totalt	1748	100%



Tänker du aktivt på att inte släppa in någon efter dig när du går igenom skalskyddet t.ex.ytterdörrar och grindar?

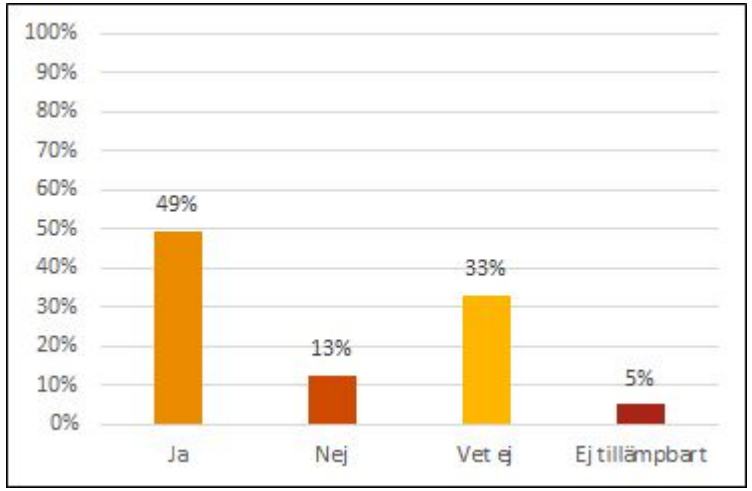
	Antal svar	Procent
Ja	1237	71%
Nej	185	11%
Vet ej	157	3%
Ej tillämpb	269	15%
Totalt	1748	100%



Bilaga 2 - Enkät - Säkerhetsmedvetenhet (forts.)

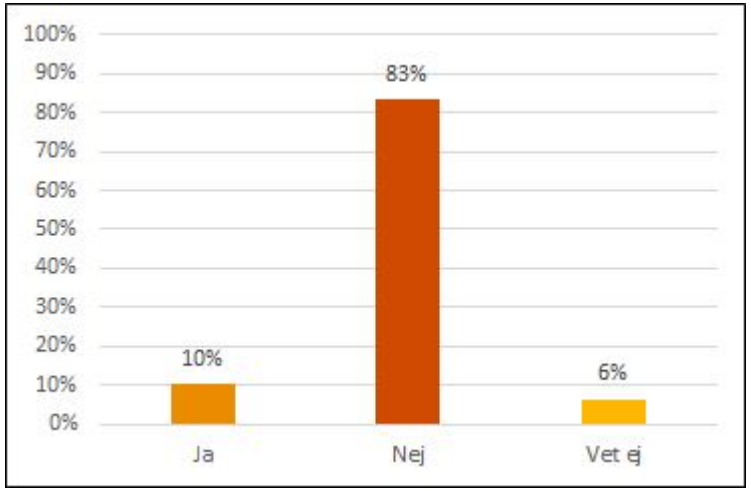
Finns det en rutin för hantering av obehöriga på er arbetsplats?

	Antal svar	Procent
Ja	863	49%
Nej	219	13%
Vet ej	578	33%
Ej tillämpb	88	5%
Totalt	1748	100%



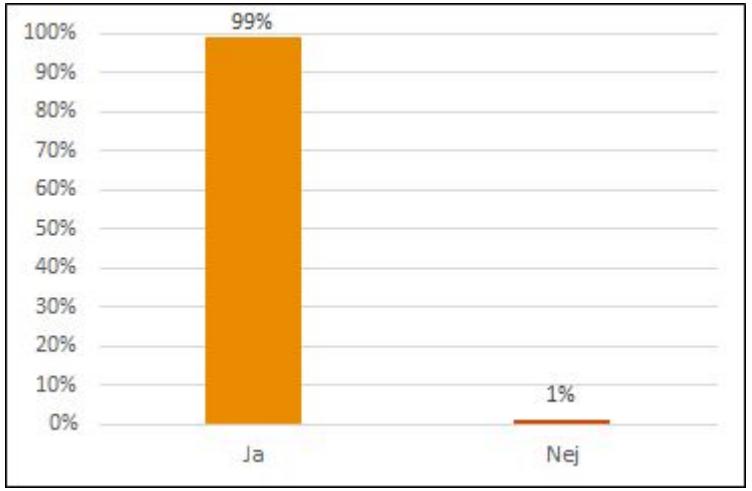
Har du eller har du sett någon publicera information kopplat till ditt arbete som skulle kunna vara känslig på några sociala medier?

	Antal svar	Procent
Ja	181	10%
Nej	1455	83%
Vet ej	112	6%
Ej tillämpb	-	-
Totalt	1748	100%



Har du möjlighet att använda dator eller annan mobil utrustning i ditt arbete?

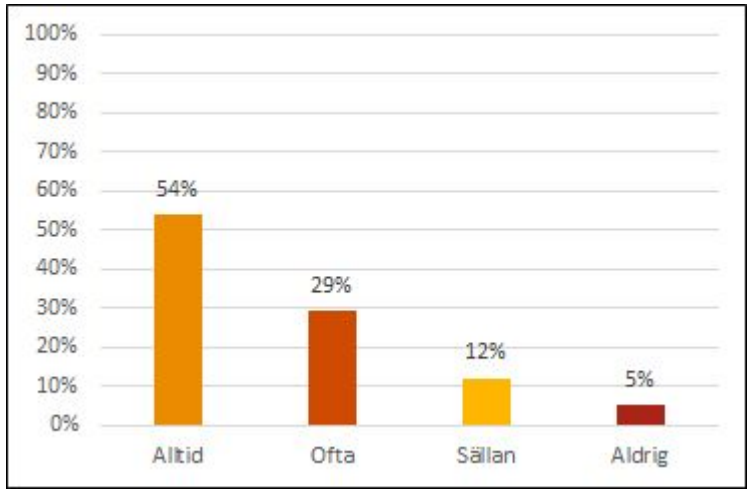
	Antal svar	Procent
Ja	1732	99%
Nej	16	1%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1748	100%



Bilaga 2 - Enkät - Säkerhetsmedvetenhet (forts).

Brukar du låsa din dator (eller annan mobil utrustning) när du lämnar den obevakad?

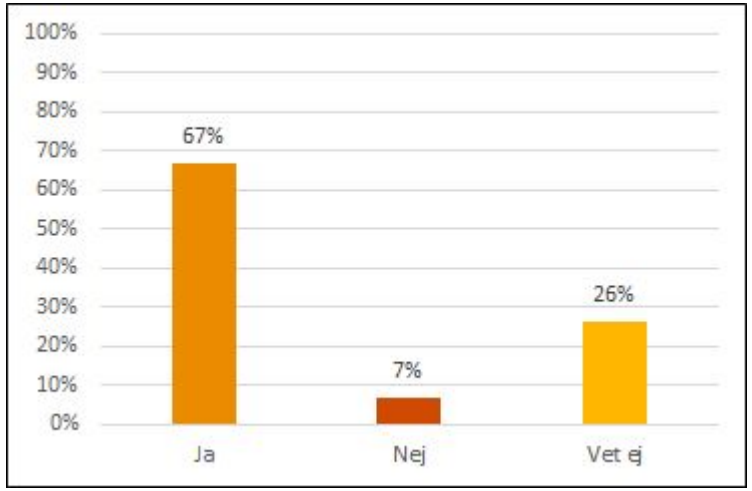
	Antal svar	Procent
Ja	932	54%
Nej	505	29%
Vet ej	207	12%
Ej tillämpb	88	5%
Totalt	1748	100%



Bilaga 2 - Enkät - Styrning, ledning och dokumentation

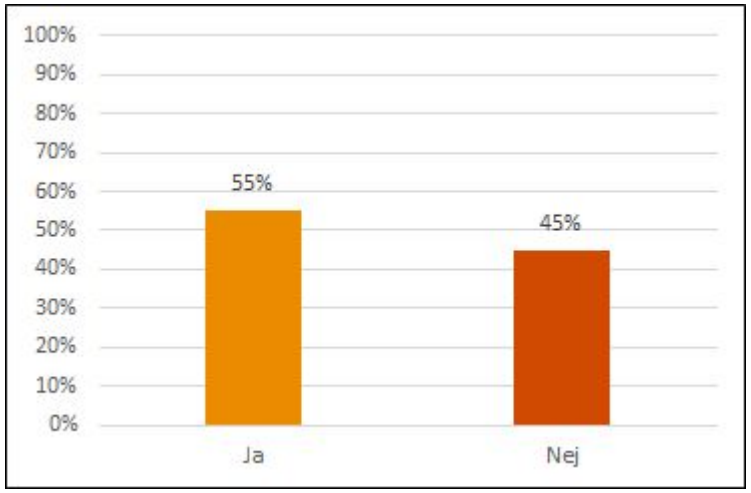
Vet du om det finns några policys, riktlinjer eller andra styrande dokument gällande informationssäkerhet på din arbetsplats?

	Antal svar	Procent
Ja	1167	67%
Nej	119	7%
Vet ej	462	26%
Ej tillämpb	-	-
Totalt	1748	100%



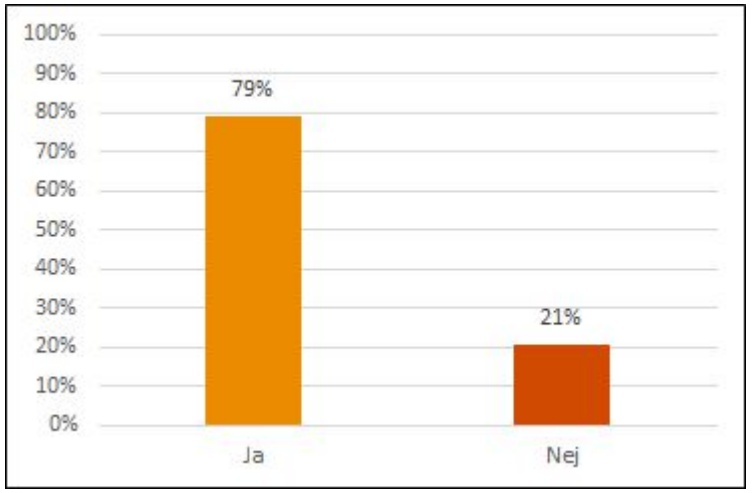
Vet du var du hittar informationssäkerhetsrelaterad dokumentation?

	Antal svar	Procent
Ja	964	55%
Nej	784	45%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1748	100%



Vet du vem du ska vända dig till för frågor som har med informationssäkerhet att göra?

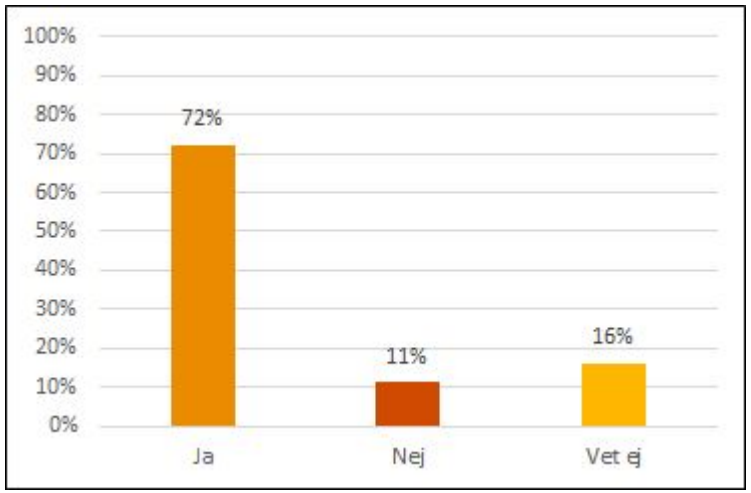
	Antal svar	Procent
Ja	1385	79%
Nej	363	21%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1748	100%



Bilaga 2 - Enkät - Styrning, ledning och dokumentation (forts.)

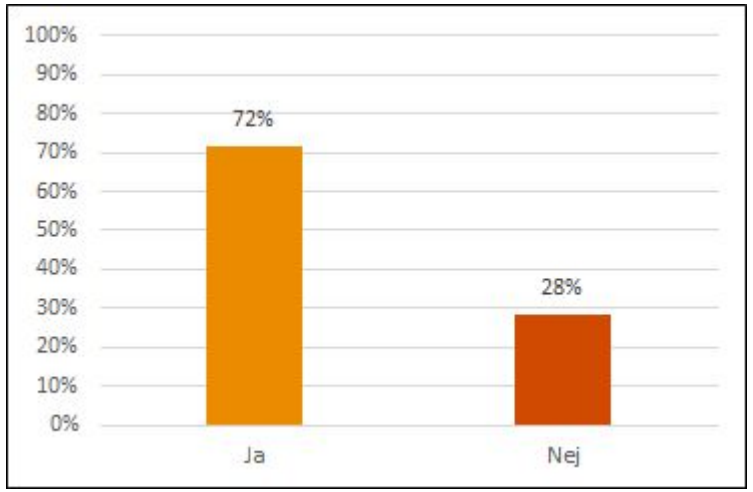
Hanterar du information på olika sätt beroende på hur informationen är klassificerad?

	Antal svar	Procent
Ja	1253	72%
Nej	199	11%
Vet ej	286	16%
Ej tillämpb	-	-
Totalt	1748	100%



Har du fått en genomgång av policys, riktlinjer eller andra styrande dokument gällande informationssäkerhet på din arbetsplats?

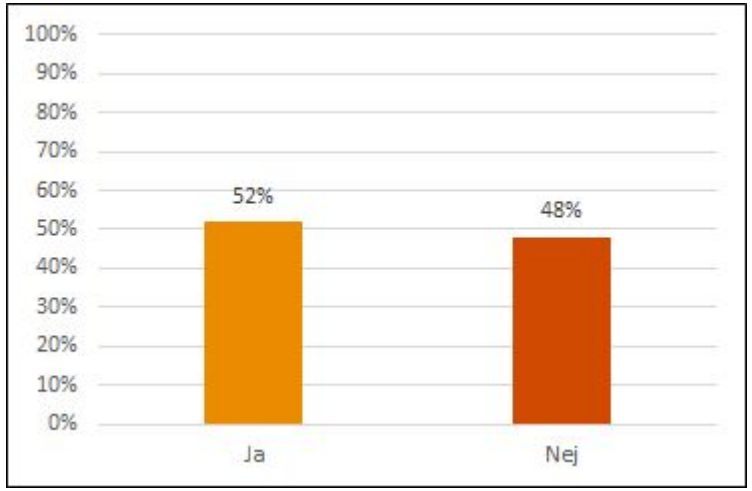
	Antal svar	Procent
Ja	835	72%
Nej	332	28%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1167	100%



Bilaga 2 - Enkät - Incidenthantering och rapporter

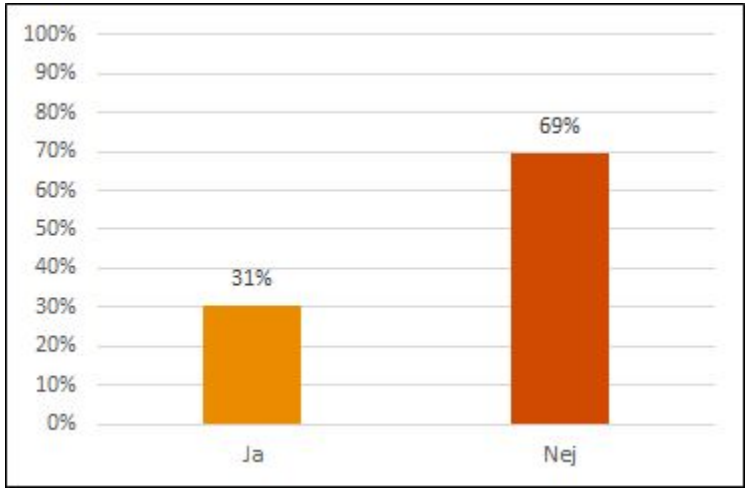
Vet du vad som är en informationssäkerhetsincident?

	Antal svar	Procent
Ja	907	52%
Nej	841	48%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1748	100%



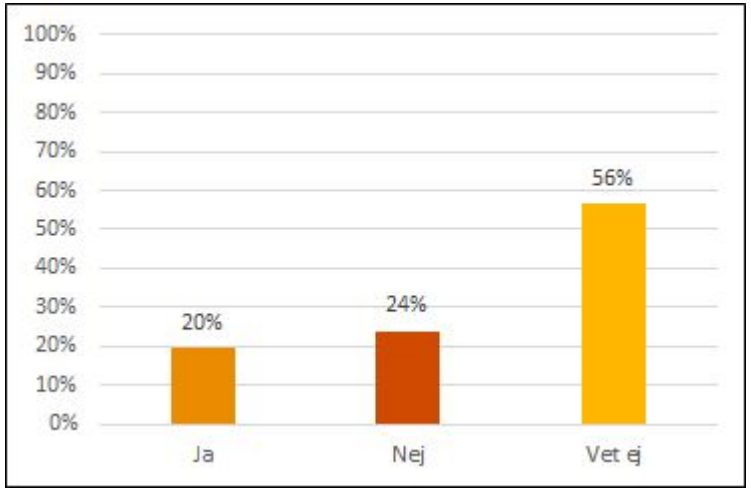
Vet du hur en informationssäkerhetsincident ska rapporteras?

	Antal svar	Procent
Ja	534	31%
Nej	1214	69%
Vet ej	-	-
Ej tillämpb	-	-
Totalt	1748	100%



Vet du om det finns en dokumenterad rutin för hantering av informationssäkerhetsrelaterade incidenter?

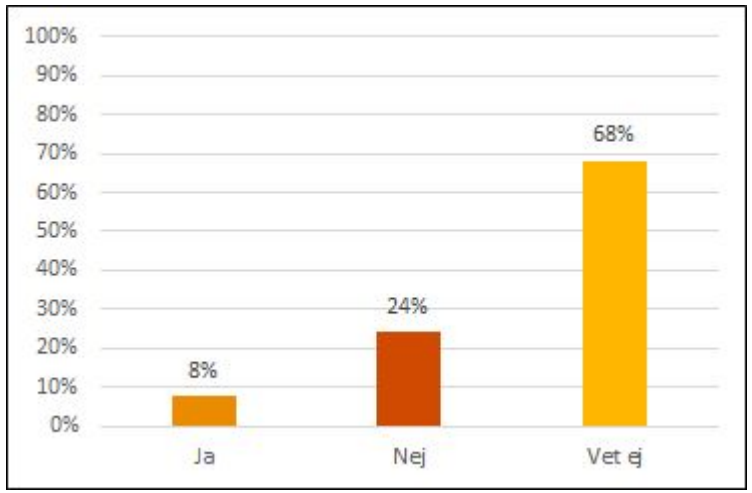
	Antal svar	Procent
Ja	343	20%
Nej	419	24%
Vet ej	986	56%
Ej tillämpb	-	-
Totalt	1748	100%



Bilaga 2 - Enkät - Incidenthantering och rapporter (forts.)

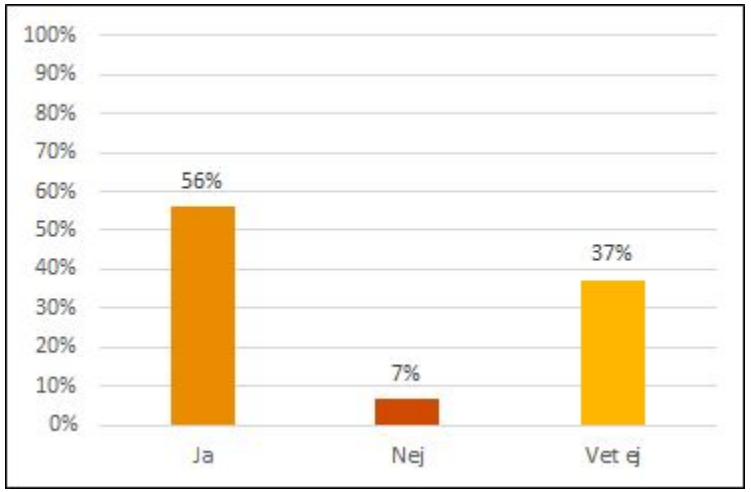
Har det inträffat en informationssäkerhetsincident på din arbetsplats?

	Antal svar	Procent
Ja	134	8%
Nej	424	24%
Vet ej	1190	68%
Ej tillämpb	-	-
Totalt	1748	100%



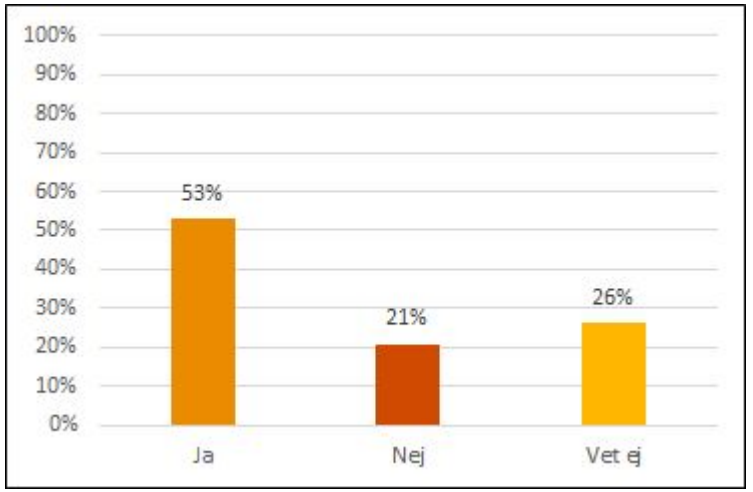
Genomfördes en utvärdering av den inträffade incidenten?

	Antal svar	Procent
Ja	75	56%
Nej	9	7%
Vet ej	50	37%
Ej tillämpb	-	-
Totalt	134	100%



Kommunicerades lärdomar från den inträffade incidenten (t.ex. på intranätet eller via e-post)?

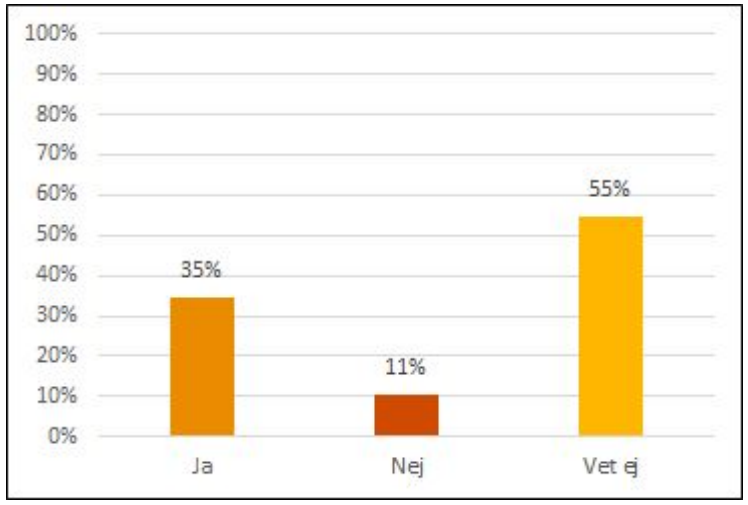
	Antal svar	Procent
Ja	71	53%
Nej	28	21%
Vet ej	35	26%
Ej tillämpb	-	-
Totalt	134	100%



Bilaga 2 - Enkät - Utbildning och övning

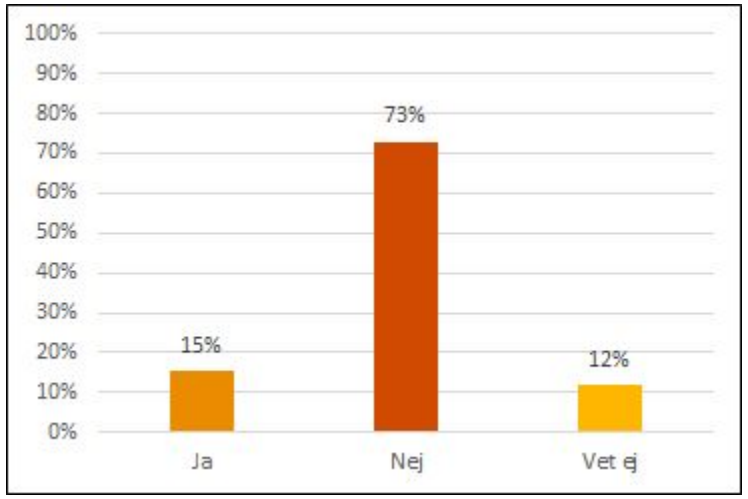
Ingår informationssäkerhetskrav i de rutiner som tagits fram för din arbetsplats?

	Antal svar	Procent
Ja	604	35%
Nej	185	11%
Vet ej	959	55%
Ej tillämpb	-	-
Totalt	1748	100%



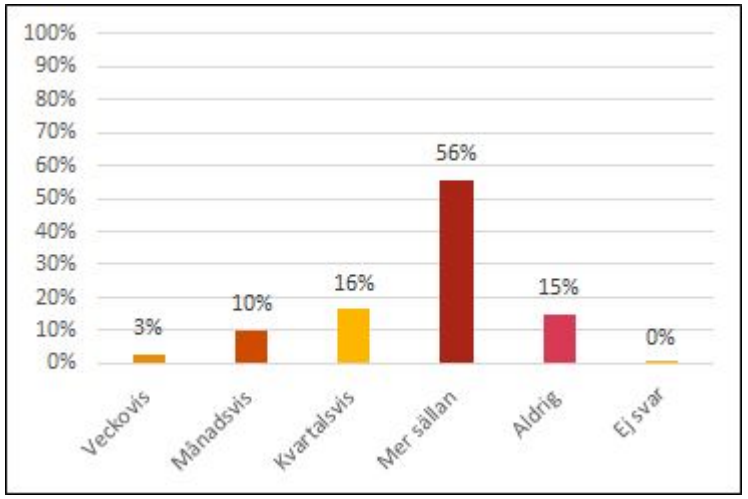
Har du gått någon informationssäkerhetsrelaterad utbildning under de senaste två åren?

	Antal svar	Procent
Ja	269	15%
Nej	1273	73%
Vet ej	206	12%
Ej tillämpb	-	-
Totalt	1748	100%



Hur ofta tar ni upp ämnet informationssäkerhet på t.ex. arbetsplatsträffar eller andra forum?

	Antal svar	Procent
Veckovis	46	3%
Månadsvis	179	10%
Kvartalsvis	287	16%
Mer sällan	971	56%
Aldrig	264	15%
Ej svar	1	0%
Totalt	1748	100%



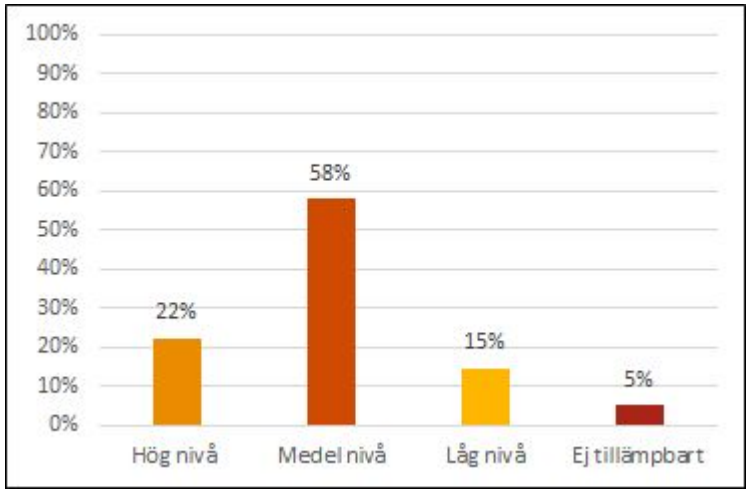
Bilaga 2 - Enkät - Avslutning

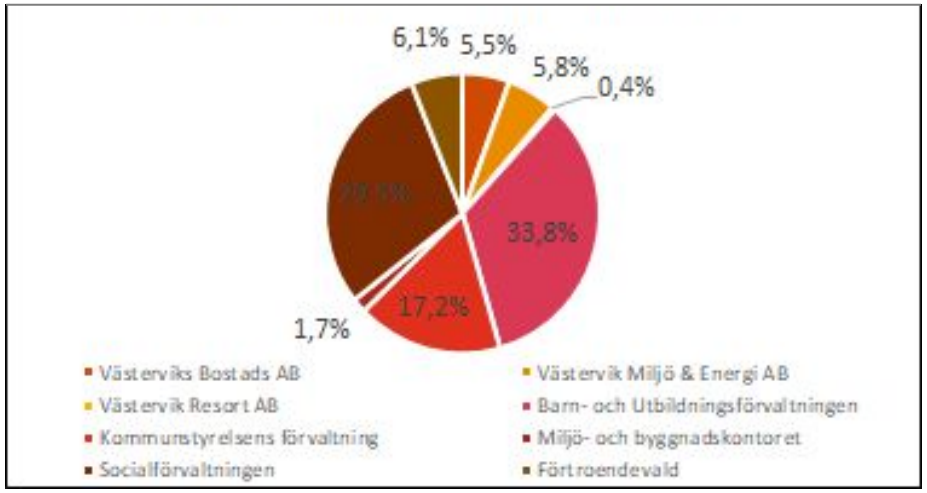
Vilken nivå av säkerhetskultur skulle du säga att din arbetsplats upprätthåller?

	Antal svar	Procent
Hög nivå	391	22%
Medel nivå	1011	58%
Låg nivå	257	15%
Ej tillämpb	89	5%
Totalt	1748	100%

Är du anställd i en kommunal förvaltning på ett kommunalt bolag eller är förtroendevald i Västerviks kommun?

	Antal svar	*Procent av totalt antal svar*
Västerviks Bostads AB	97	5,5%
Västervik Miljö & Energi AB	102	5,8%
Västervik Resort AB	7	0,4%
Barn- och Utbildningsförvaltningen	591	33,8%
Kommunstyrelsens förvaltning	300	17,2%
Miljö- och byggnadskontoret	29	1,7%
Socialförvaltningen	516	29,5%
Förtroendevald	106	6,1%





Kontaktuppgifter

Anders Gustafson

070 929 42 62

anders.gustafson@pwc.com

Niklas Ljung

070 196 03 69

niklas.ljung@pwc.com

Fredrika Jönander

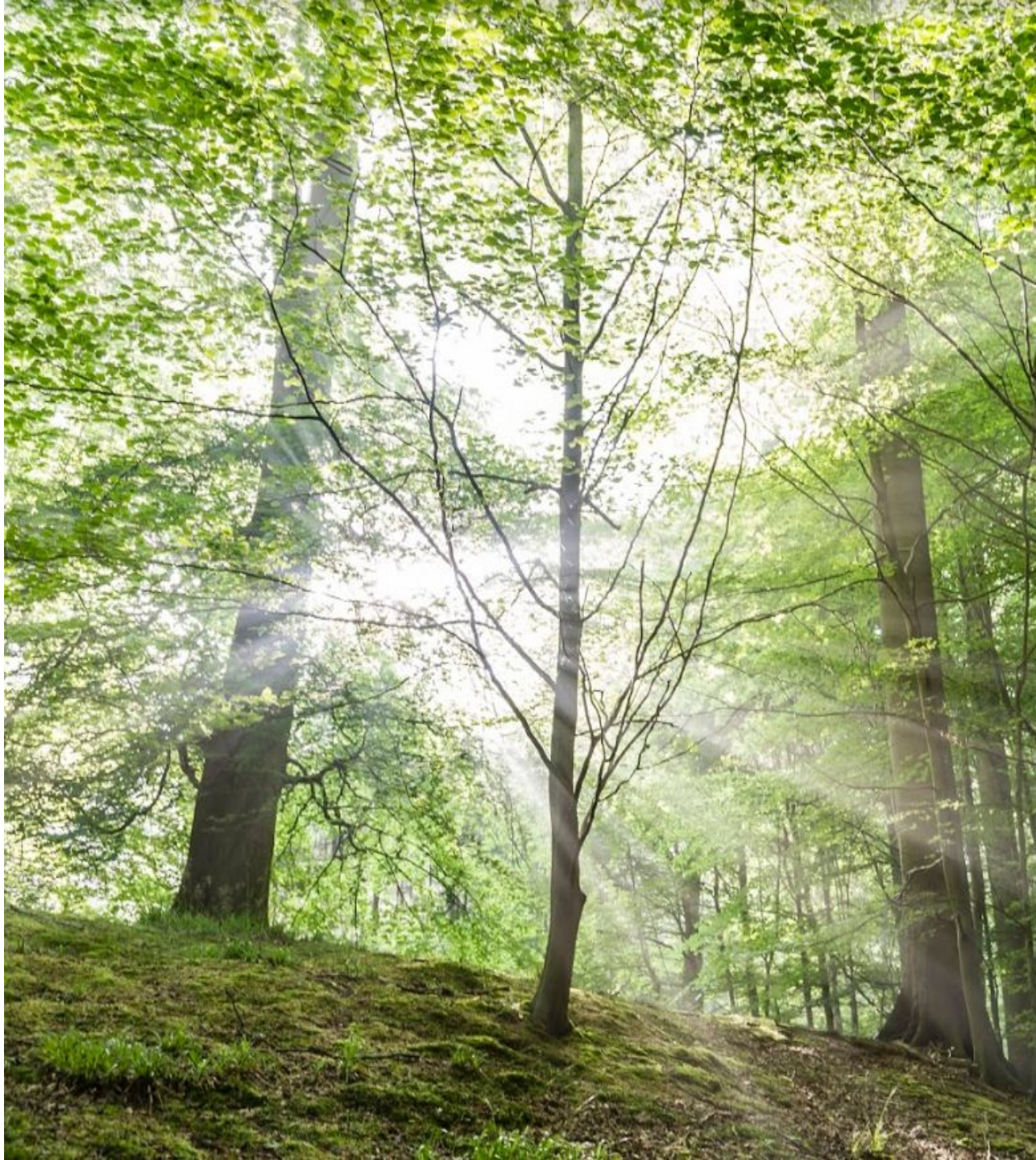
072 880 94 53

fredrika.joenander@pwc.com

Sabina Roos

072 880 96 31

sabina.roos@pwc.com



Tack!

pwc.se