Stiftelsen Tjolöholm, Kungsbacka kommun

Granskning av IT- och informationssäkerhet

Building a better working world

Sammanfattning

EY har på uppdrag av stiftelsens valda revisorer genomfört en granskning av Stiftelsen Tjolöholms (nedan kallad Stiftelsen) arbete med IT- och informationssäkerhet. Granskningens syfte har varit att på övergripande nivå granska huruvida Stiftelsen har ett ändamålsenligt arbete med informationssäkerhet med fokus på styrning och organisation.

Vår sammanfattande bedömning utifrån granskningens syfte är att Stiftelsen inte bedriver ett ändamålsenligt arbete med IT- och informationssäkerhet.

Granskningen visar på att Stiftelsen har ambitionen och strävar efter att etablera ett robust IT- och informationssäkerhetsarbete, detta bland annat genom en övergripande kartläggning av de IT system som används i verksamheten idag. Däremot saknar Stiftelsen en strukturerad metod för att identifiera den information som hanteras i verksamheten. Därmed har Stiftelsen ännu inte upprättat lämpliga kontroller och åtgärder för att skydda information från obehörig åtkomst, användning, avslöjande eller ändring. I dagsläget saknas beslut, styrande dokument och därmed även en dokumenterad plan för hur arbetet ska bedrivas på ett ändamålsenligt sätt. Avsaknaden av styrande dokument medför att arbetet saknar kontinuitet och struktur som medför en risk i att informationssäkerhetsarbetet inte bedrivs på ett säkert sätt.

På ett övergripande plan[1] rekommenderas Stiftelsen att:

- Identifiera och kartlägga informationstillgångarna i verksamheten för att tydligt definiera handlingsplaner utefter de mål som Stiftelsen vill uppnå kopplat till IT- och informationssäkerhet.
- Etablera ramverk, i form av förvaltningsmodell, policy, riktlinjer och rutiner för IT- och informationssäkerhetsarbetet.
- Definiera roller och ansvar för att samordna och driva Stiftelsens arbete med informationssäkerhet.
- Utvärdera vilka kompetenser som behövs för att kunna implementera och bedriva ett ändamålsenligt arbete med IT- och informationssäkerhet.
- Utvärdera huruvida tillräckliga resurser finns inom verksamheten idag för att uppfylla behovet.

[1] Här presenteras sammanfattande rekommendationer för Stiftelsen. I kapitel 3 återfinns detaljerade rekommendationer.

Innehåll

1. Inledning

1.1 Bakgrund

Tjolöholms gods ägs sedan 1987 av Stiftelsen Tjolöholm med Kungsbacka kommun som stiftelsens huvudman. Stiftelsens uppdrag består av att förvalta egendomen, driva affärsverksamheten samt utveckla besöksmålet i områdets värdefulla natur- och kulturvärden till ett västsvenskt turistmål. På senare år har Stiftelsen lockat ett större antal besökare och vuxit i snabb takt, vilket inneburit nya utmaningar då högre krav ställs på effektivitet, definierade processer och mer administrativt arbete, däribland IT- och informationssäkerhet.

Offentlig verksamhet hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god IT- och informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att information och system är tillgängliga, riktiga samt har tillräckligt starkt skydd. I takt med att alltmer digitaliseras blir fler enheter uppkopplade och fler processer blir IT-beroende. Därmed ökar kraven på att känslig information, såsom exempelvis kunddata eller dokumentation från verksamheten, får ett ändamålsenligt och välanpassat skydd ifrån stöld eller förstörelse, samtidigt som den görs tillgänglig för rätt personer i rätt tid.

Under 2000-talet har ett antal olika direktiv, lagar och riktlinjer tagits fram för att stötta och tydliggöra, men också sätta krav på organisationer i deras arbete med informationssäkerhet.

Mot bakgrund av ovan har de valda revisorerna beslutat om att en granskning av Stiftelsen Tjolöholms (nedan kallad Stiftelsen) styrning och arbete med IT- och informationssäkerhet bör genomföras.

1.2 Syfte

Granskningen syftar till att översiktligt bedöma om styrelse och VD säkerställt ett ändamålsenligt arbete med styrning och intern kontroll kopplat IT- och informationssäkerhet. Vidare är syftet också att översiktligt bedöma i vilken omfattning styrelse och VD styr och följer upp arbetet på området.

För att uppnå syftet besvaras följande underliggande frågor:

- Kan styrningen av arbetet med IT- och informationssäkerhet, för de behov verksamheten har, bedömas som ändamålsenligt?
- Görs riskanalyser avseende IT- och informationssäkerhet på ett strukturerat sätt och används dessa för att identifiera åtgärder, baserat på upptäckta risker?
- Finns det en strukturerad metod för att identifiera och skydda de viktigaste informationstillgångar?
- Är arbetet med att följa upp att beslut och styrdokument relaterat till IT- och informationssäkerhet efterlevs ändamålsenligt?

1.3 Genomförande och revisionskriterier

Granskningen har genomförts genom intervjuer med identifierade nyckelpersoner i Stiftelsens IT- och informationssäkerhetsarbete och verksamhet. Granskningen är utförd mot god praxis inom IT- och informationssäkerhetsområdet och bygger på EYs granskningsprogram Cyber och Informationssäkerhet (GCI), med fokus på offentlig verksamhet.

GCI baseras på erkända ramverk såsom ISO/EC27000[2] - serien och Myndigheten för Samhällsskydd och Beredskaps (MSBs) metodstöd för informationssäkerhet.

Under uppdraget har EY granskat tre huvudområden:

- Styrning
- Personal och behörighet
- Drift

Intervjuer har genomförts med:

- VD
- Ekonomichef

Stiftelsen har givits möjlighet att sakgranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekt fakta.

Fullständig källförteckning framgår av bilaga 1.

1.4 Avgränsning

De iakttagelser och rekommendationer som presenteras i denna rapport baseras främst på den information som inhämtats under intervjuer.

Stiftelsen har påbörjat arbetet med att kartlägga sina system men har ännu inte några dokumenterade riktlinjer, rutiner och policys kopplat till IT- och informationssäkerhet och kunde därmed inte täckas i granskningen.

Granskningen syftar till att genomföra en bedömning och tillhandahålla en översiktsbild av hur Stiftelsen har utformat sitt arbete med IT- och informationssäkerhet. Granskningen täcker således inte enskilda IT-system eller applikationer. Även den allmänna dataskyddsförordningen (GDPR) har exkluderats då den faller utanför ramen för granskningen syfte.

1.5 Definitioner

Se bilaga 2 för definitioner av begrepp som används i granskningen.

[2] ISO/IEC 27000 är en uppsättning av internationella standarder som tillhandahåller riktlinjer och bästa praxis för informationssäkerhet.

2. Granskningsresultat

I detta kapitel presenteras de övergripande resultatet från genomförd granskning med utgångspunkt från revisionsfrågorna. Iakttagelserna utgår från informationen som presenterats under intervjuerna och erhållna dokument.

Det bör beaktas att även om IT- och informationssäkerhet är kritiskt för stiftelser, bedriver de inte samhällsviktiga funktioner och har därmed inte samma externa kravbild som kommuner och regioner. Stiftelser har ofta mer begränsade resurser, både vad gäller finansiering och bemanning, vilket kan göra det mer utmanande att ha IT- och informationssäkerhet högst på agendan. Trots detta ska stiftelser i samma mån sträva efter att utveckla och upprätthålla ett arbete för informationssäkerhet då de bedriver en affärsverksamhet, men balansera insatserna baserat på deras behov.

2.1 Styrdokument

Utifrån granskningen har vi noterat att Stiftelsen har arbetat med att på övergripande nivå kartlägga de IT-system som används i verksamheten, med ambitionen att identifiera risker och informationsflöden. Däremot saknas det i dagsläget en övergripande strategi kopplat till IT- och informationssäkerhet som på övergripande nivå ska leda arbetet. Vidare finns det inte några dokumenterade policys, riktlinjer eller instruktioner för arbetet med informationssäkerhet. Processer för tilldelning, borttag och ändring av medarbetares behörigheter finns inte definierade idag och det genomförs inga periodiska genomgångar av användare för att säkerställa att alla användare förblir lämpliga över tid. Vid en anställning tilldelas de behörigheter som behövs för det dagliga arbetet efter direktiv från anställande chef.

För lösenordshantering framgår det att varje medarbetares ansvarar för att upprätta rutiner för lösenord. Det finns således ingen central policy eller riktlinjer som definierar vilka lösenordskrav som ska uppfyllas för samtliga system. Stiftelsen använder inte någon autentiseringsmetod som tillåter användare att logga in på flera applikationer eller webbplatser med en enda uppsättning av inloggningsuppgifter, därmed behöver lösenord skapas för respektive system.

2.2 Ansvarsfördelning och organisation

Vid tidpunkten för granskningen var Stiftelsens uppfattning att det fanns ett behov att fortsätta arbetet att implementera och tydliggöra ansvaret och organisationen kopplat till informationssäkerhet. Stiftelsens styrelse ansvarar för att arbetet med IT- och informationssäkerhet sker på ett ändamålsenligt sätt, men i dagsläget finns det inte någon beskrivning eller fastställda riktlinjer om detta. Vidare ser Stiftelsens ett behov av att förbättra de administrativa processerna, hitta effektivare processer och jobba mer enhetligt, vilket inkluderar arbetet med IT- och informationssäkerhet.

Av granskningen framgår att Stiftelsens personalstyrka ökat de senaste åren. Fokus har dock varit på att driva den operativa verksamheten och inte att tillsätta resurser för att driva administrativa tjänster, inkluderat IT- och informationssäkerhet. I takt med detta har det öppnats nya grenar med ansvarsområden, men som informellt fördelats på befintlig personal.

I dagsläget finns det ingen ansvarig för respektive IT-system och därför saknas det någon med ansvar att säkerställa att systemet ska uppfylla de informationssäkerhetskrav som ställs utifrån rådande lagar och riktlinjer. Vidare finns det inte tydligt definierat vem som är ansvarig för att säkerställa att informationsklassning genomförs, att kontinuitetsplaner fastställts och följs. Vid större event finns det däremot internkontrollplaner som inkluderar riskanalyser med olika

scenarion för hur medarbetarna ska agera för att upprätta kontinuitet om någon oplanerad händelse inträffar.

2.3 Personal och utbildning

Utifrån granskningen har vi noterat att Stiftelsens dagliga arbete kopplat till IT- och informationssäkerhet sker utifrån informella roller. Det saknas en tydlig systematik kring de definierade rollerna och det finns inga bestämda ansvarsområden eller kravställningar. Detta till en följd av att verksamheten har vuxit, medan arbetet och medvetenheten om IT- och informationssäkerhet inte har följt utvecklingen. Målbilden för Stiftelsen idag är främst att identifiera den information som används i arbetet, men även öka kunskapsnivån inom området för att utvidga möjligheterna att bedriva ett ändamålsenligt arbete. I dagsläget saknas det ett strukturerat arbete för att över tid säkerställa att medarbetarna har den kompetens som behövs för att bedriva arbetet kopplat till IT- och informationssäkerhet.

Som följd av rådande situation upplever Stiftelsen ett behov av att avsätta mer resurser med tydligt ansvar för att samordna och supportera Stiftelsens informationssäkerhetsarbete.

2.4 Externa leverantörer och hantering av leverantörsavtal

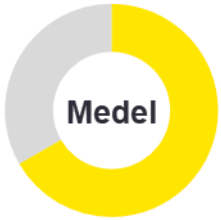
Upphandlingar av informationssystem hanteras internt inom Stiftelsen och i dagsläget saknas det metodstöd eller kravställningar som kan följas vid en eventuell IT-upphandling. För befintliga leverantörer finns inga centrala riktlinjer definierade för uppföljning av informationssäkerhet. Det finns möjlighet att vara del av upphandlingar via Kungsbacka kommun, men då dessa inte går att skräddarsy utifrån Stiftelsens behov är det en metod som inte används i dagsläget. Stiftelsens behov och resursfördelning planeras och ansvaras av verkställande direktören, som i sin tur har en delegationsordning att följa.

3. Sammanfattande iakttagelser och detaljerade rekommendationer

Under granskningen har EY identifierat iakttagelser inom granskade områden. För varje iakttagelse har EY lämnat rekommendationer som syftar till att stödja Stiftelsen Tjolöholm i dess framtida arbete med informationssäkerhet.

De av EY identifierade iakttagelserna har klassificerats enligt tre risknivåer avseende hur omfattande dess eventuella inverkan anses vara, vilka beskrivs nedan:

Prioritering låg: Observation som ej direkt påverkar verksamhetens mål, men som kan medföra ineffektiv verksamhet, mindre brister i IT- och informationssäkerhet, efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.



Prioritering medel: Observation som anses kunna ha påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av verksamhetens resurser.

Prioritering hög: Observation av större karaktär som anses kunna ha hög påverkan på verksamhetens mål, rykte, IT- och informationssäkerhet och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer.

3.1 Identifiera informationstillgångar

Iakttagelse

Vid granskningen noterades det att informationstillgångar som dagligen hanteras och bearbetas av Stiftelsen inte är formellt identifierade, vilket behöver ligga till grund i utformningen av arbetet kring IT- och informationssäkerhet.

Att definiera informationstillgångar är kritiskt då det möjliggör för Stiftelsen att identifiera vilken information som är värdefull, för att därmed kunna upprätta lämpligt skydd. Genom att förstå informationens natur kan organisationer upprätta lämpliga säkerhetskontroller och åtgärder för att skydda den från obehörig åtkomst, användning, avslöjande eller ändring. Vidare kan det även vara en metod för att identifiera det information som inte behöver någon sekretess, utan kan vara tillgänglig för medarbetare eller kunder.

Vid granskningen observerades det att Stiftelsen har påbörjat arbetet med att kartlägga de olika IT-system som används och integrationen mellan dessa. Däremot saknar Stiftelsen dokumentation vilken information som hanteras och bearbetas i och utanför respektive IT-system.

Rekommendationer

Stiftelsen rekommenderas att:

- Genomföra en kartläggning för att identifiera de mest kritiska och känsliga informationstillgångarna i Stiftelsen.
- Kategorisera de identifierade informationstillgångarna i klassificeringar utifrån parametrarna tillgänglighet, spårbarhet, riktighet och konfidentialitet.
- Genomföra en risk- och verksamhetsanalys och utvärdera Stiftelsens nuvarande säkerhetsinfrastruktur för att identifiera risker kopplat till Stiftelsens informationstillgångar och eventuella utvecklingsområden kopplat till informations-säkerhetsarbetet och huruvida informationen skyddas ändamålsenligt.

3.2 Styrning av informationssäkerhetsarbetet

Iakttagelse

Långsiktigt hållbart arbete med IT- och informationssäkerhet kräver ett helhetsgrepp och fungerande arbetssätt för att säkerställa att Stiftelsens information ges ändamålsenligt skydd över tid. Stiftelsen saknar i dagsläget ett etablerat ramverk, i form av förvaltnings-modell, policy, riktlinjer och rutiner för sitt IT- och informationssäkerhetsarbete. Därmed saknar arbetet med informationssäkerhet tydlighet avseende styrning, ansvar och mandat.

Vidare saknas det också en handlingsplan som bryter ner den långsiktiga strategin i verksamheten och hur eliminering av informationssäkerhetsrelaterade risker och brister ska ske. För att viljeriktningen ska vara tydlig för verksamheten och dess medarbetare är det avgörande att även bryta ned den långsiktiga strategin till kortsiktiga mål för att kunna realisera och uppnå strategin.

Rekommendationer

Stiftelsen rekommenderas att:

- Tydligt definiera och prioritera kortsiktiga och långsiktiga mål kopplat till IT- och informationssäkerhet, som en del av Stiftelsens övergripande vision och strategi.
- Definiera handlingsplaner med utgångspunkt från Stiftelsens nuvarande position och de uppsatta målen för IT- och informationssäkerhet. Utöver tidsplan bör handlingsplanen innehålla (men inte begränsas till) aktiviteter för att:
  - Utveckla policy för informationssäkerhet
  - Utveckla riktlinjer, exempelvis inom åtkomstkontroll, informationsklassificering, datalagring och incident-hantering.
  - Ta fram metodik för identifiering och hantering av risker kopplat till informationssäkerhet.
- Regelbundet följa upp handlingsplanerna för att säkerställa att målen uppfylls och vid behov eventuellt identifiera nya utvecklingsområden.

3.3 Resursplanering/resursfrågor

Vid tidpunkten för granskning har Stiftelsen ingen dedikerad funktion för IT- och informationssäkerhet, utan ansvaret för fördelas informellt på befintliga medarbetare. Vidare finns det i dagsläget ingen definierad förväntad allokering av tid mellan rollerna i det löpande informationssäkerhetsarbetet.

Iakttagelse

För att kunna genomföra ett ändamålsenligt arbete med informationssäkerhet är resursplaneringen en viktig aspekt. Resursplanering innebär att identifiera de resurser och kompetenser som krävs för att kunna implementera och bedriva ett effektivt IT- och informationssäkerhetsprogram. Detta kan variera stort mellan organisationer och därför är det viktigt att identifiera det behov som finns och utefter detta analysera rollen/de roller som krävs specifikt för Stiftelsen.

I dagsläget saknas en plan för hur Stiftelsen säkerställer kompetens och resurser över tid för att möta behovet och täcka nödvändiga roller och aktiviteter inom informationssäkerhetsarbetet.

Rekommendationer

Stiftelsen rekommenderas att:

- Definiera den roll/de roller som ska ansvara för att samordna och driva Stiftelsens arbete med informationssäkerhet och analysera om rollen ska fördelas på befintliga resurser eller om det finns behov av att anställa en ny person med dedikerat ansvar för frågan.
- Utvärdera vilket behov som finns för att kunna implementera och bedriva ett ändamålsenligt arbete med IT- och informationssäkerhet, och huruvida rätt kompetens finns inom verksamheten idag för att uppfylla behovet.
- Etablera processer och instruktioner för tydlig uppföljning av verksamheternas informationssäkerhetsarbete.

4. Samlad bedömning

4.1 Bedömning utifrån revisionsfrågorna

Revisionsfrågor	Bedömning
Kan styrningen av arbetet med IT och informationssäkerhet, för de behov verksamheten har, bedömas som ändamålsenligt?	**Nej.** Utifrån verksamhetens behov anses Stiftelsen inte bedriva ändamålsenligt arbete med IT- och informationssäkerhet. Av granskningen framgår att Stiftelsen har ambitioner att organisera sig och skapa ett välfungerande IT- och informationssäkerhetsarbete. Däremot har kunskap och kompetens inom området inte följt utvecklingen av verksamheten, vilket försvårat styrningen. Stiftelsen saknar exempelvis dokumenterade mål, policys, rutiner relaterat till ansvarsfördelning eller periodiska genomgångar av behörigheter och resurser.
Görs riskanalyser avseende IT – och informationssäkerhet på ett strukturerat sätt och används dessa för att identifiera åtgärder, baserat på upptäckta risker?	**Nej.** Stiftelsen bedöms inte genomföra strukturerade riskanalyser för IT- och informationssäkerhet. Under granskningen noterades det att det inte bedrivs något systematiskt arbete med att identifiera och adressera risker relaterade till IT- och informationssäkerhet. Stiftelsen saknar tydligt ansvar inom IT- och informationssäkerhetsarbetet vilket resulterar i avsaknad av övergripande riskanalys, informationsklassning och kontinuitetsplan.
Finns det en strukturerad metod för att identifiera och skydda de viktigaste informationstillgångar?	**Nej.** Det finns ingen strukturerad metod för att identifiera och skydda de viktigaste informationstillgångar i Stiftelsen Tjolöholm. Stiftelsen har på ett övergripande plan kartlagt sina IT-system men har ännu inte identifierat sina informationstillgångar. Avsaknaden av en strukturerad metod för att identifiera information medför att Stiftelsen ännu inte upprättat lämpliga kontroller och åtgärder för att skydda information från obehörig åtkomst, användning, avslöjande eller ändring.
Är arbetet med att följa upp att beslut och styrdokument relaterat till IT- och informationssäkerhet efterlevs ändamålsenligt?	**Nej.** I dagsläget saknas beslut och styrdokument relaterad till IT- och informationssäkerhet och därmed bedöms arbetet med uppföljning inte vara ändamålsenligt. Avsaknaden av styrdokument medför att det saknas ett kontinuerligt och strukturerat arbete, som medför en risk i att informationssäkerhetsarbetet inte bedrivs på ett säkert sätt.

4.2 Slutsats

Granskningens syfte har varit att bedöma om Stiftelsen bedriver ett ändamålsenligt IT- och informationssäkerhetsarbete. Vår sammanfattande bedömning utifrån granskningens syfte är att Stiftelsen inte driver ändamålsenligt arbete med IT- och informationssäkerhet.

Stiftelsen har under de senaste åren vuxit och i takt med detta har fokus varit på att driva den operativa verksamheten snarare än tillsätta resurser för att driva administrativa tjänster, inkluderat IT- och informationssäkerhet. Trots att Stiftelsen har ambition att organisera sig för att bedriva ett välfungerande säkerhetsarbete föreligger det bristande framsteg inom området. Tillsammans med avsaknaden av styrdokument och handlingsplaner kan detta innebära en betydande risk för Stiftelsens IT- och informationssäkerhet.

På ett övergripande plan rekommenderas Stiftelsen att:

- Identifiera och kartlägga informationstillgångarna i verksamheten för att tydligt definiera handlingsplaner utefter de mål som Stiftelsen vill uppnå kopplat till IT- och informationssäkerhet.
- Etablera ramverk, i form av förvaltningsmodell, policy, riktlinjer och rutiner för IT- och informationssäkerhetsarbetet.
- Definiera roller och ansvar för att samordna och driva Stiftelsens arbete med informationssäkerhet.
- Utvärdera vilka kompetenser som behövs för att kunna implementera och bedriva ett ändamålsenligt arbete med IT- och informationssäkerhet.
- Utvärdera huruvida tillräckliga resurser finns inom verksamheten idag för att uppfylla behovet.

Elin Silver
Max Wann Adebarh
Mohamed Nazari
Karin Knutsson
Mikaela Gretzer

Ernst & Young AB

Bilaga 1: Källförteckning

Intervjuade roller:

- VD, 2023-04-05, 2020-04-21
- Ekonomichef, 2023-04-25

Dokumentförteckning:

- Systemkarta för Stiftelsen Tjolöholm
- Inkomster och utgifter för Stiftelsen Tjolöholm

Bilaga 2: Definitioner

Systemförvaltare: Ansvarar för att operativt sköta ett systems förvaltning inom givna ekonomiska ramar.

Systemägare: Verksamhetens chef eller särskilt utsedd person med ansvar för administration och drift av ett eller flera informationssystem inom ramen för antagna mål, vilken agerar ledningsfunktion över systemets förvaltning.

Driftansvarig: Ansvar innefattar att ta fram och underhålla driftdokumentation till ett informationssystem samt assistera vid eventuella incidenter eller problem.

Systemleverantör: Leverantör av IT-system som agerar supporterande vid incidenter med systemet och i vissa fall tillhandahåller drift av systemet. Leverantören tillhandahåller uppdateringar av systemversioner samt löpande rättningar av identifierade systemfel.

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet och tillgänglighet.

Riskanalys: Redovisning av de samlade kraven på ett informationssystem avseende tillgänglighet, riktighet och sekretess. Systemsäkerhetsanalysen ska redogöra för vidtagna samt ytterligare nödvändiga säkerhetsåtgärder vilka är nödvändiga för att kraven på informationssystemet ska uppfyllas.

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer.

SLA (Service Level Agreement): Servicenivåavtal mellan beställare och tjänsteleverantör där överenskomna krav som ställs på tjänsten definierats.

Applikation: Datorprogram med olika typer av funktionalitet beroende på applikationens syfte. Applikationen finns lagrad på en dator eller en server.

Databas: En databas är en katalogtjänst med indexerad information om resurser (såsom tex. användare).

Server: En server är ett datorprogram som bidrar med funktionalitet till ett annat program via en nätverksuppkoppling.

Nätverk: Ett nätverk administrerar koppling mellan olika resurser såsom olika program.