Informations-säkerhet i fastighets-organisationen

OFFENTLIGA FASTIGHETER

Offentliga fastigheter

Samarbetet Offentliga fastigheter består av organisationer som förvaltar många av Sveriges offentliga fastigheter. Tillsammans förvaltar vi skolor, myndighetsbyggnader, militära installationer, sjukhus och fängelser. I vårt nätverk finns en enorm bredd, inte bara av olika slags fastigheter utan också i form av olika slags erfarenheter. För att ta tillvara och utveckla vår breda kompetens har vi gått samman i Offentliga fastigheter.

Vi bedriver gränsöverskridande utvecklingsprojekt som bygger upp och sprider kompetens samt effektiviserar och förbättrar förvaltningen av våra gemensamma fastigheter. Projekten ska vara angelägna och väcka nya tankar. De ska visa på inspirerande exempel och erbjuda praktiska verktyg. Med andra ord projekt som inte bara gynnar oss själva utan också kan hjälpa och vägleda många fler. Bakom Offentliga fastigheter står Kommunfonden (FoU-fonden för kommunernas fastighetsfrågor), Fastighetsrådet (FoU-fonden för regionernas fastighetsfrågor), Fortifikationsverket och Samverkansforum genom Statens fastighetsverk och Specialfastigheter.

Mer information hittar du på **www.offentligafastigheter.se**.

Informations-säkerhet i fastighets-organisationen

Informationssäkerhet i fastighetsorganisationen

ISBN 978-91-8047-066-7
Upplysningar om innehållet Bo Baudin, SKR
Text Lars Lidén, META och Thomas Nilsson, Certezza
Omslagsillustration Fingerprint illustrationer
Grafisk form ETC Kommunikation
Produktion Advant
Webbplats www.offentligafastigheter.se

Förord

Ökad globalisering och digitalisering bidrar till förutsättningar för välstånd och tillväxt samtidigt som det ökar sårbarheter och risker. Den ökade informationsmängden som digitaliseringen medför ställer ett antal nya krav. De senaste åren pekar på ett försämrat säkerhetspolitiskt läge och en förändrad hotbild mot Sverige. Informationsägarskap, konfidentialitet, riktighet och tillgänglighet blir centrala begrepp i informationshanteringen.

I denna skrift beskrivs metoder för att hantera dessa utmaningar genom att arbeta med processorienterad informationskartläggning samt informationsklassning. Skriften belyser också vilken information som vanligtvis förekommer i olika system och ger exempel på klassning av information.

Skriften är tänkt att fungera som stöd vid informationshantering och arbete med processorienterad informationskartläggning samt informationsklassning.

Projektet har initierats och finansierats av Offentliga fastigheter. Lars Lidén, META och Thomas Nilsson, Certezza, har varit utredare och skribenter. En styrgrupp bestående av Andreas Persson, Familjebostäder Stockholm; Anders Gidrup, Locum; Henrik Bjerneld, Härnösands kommun; Mats Lidskog, Västfastigheter Västra Götalandsregionen; Kristoffer Hellsten, Regionfastigheter Skåne; Masse Antonsson, Specialfastigheter; John Öberg, Fortifikationsverket och Anna-Karin Wiberg, Statens fastighetsverk har medverkat i arbetet och lämnat värdefulla synpunkter.

Bo Baudin, Sveriges Kommuner och Regioner, har varit projektledare.

Stockholm i september 2022

Gunilla Glasare
Avdelningschef

Peter Haglund
Sektionschef

Avdelningen för tillväxt och samhällsbyggnad

Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

Behovet av att kunna hantera den ökade informationsmängden som digitaliseringen medför ställer ett antal nya krav. Kraften i att ha tillgång till information var och när den än behövs är tydlig men det kräver strategi och struktur för att göra det möjligt. Informationsägarskap, konfidentialitet, riktighet och tillgänglighet blir centrala begrepp i informationshanteringen.

Det är väsentligt att som fastighetsorganisation återkommande göra riskanalyser och ta fram en strategi för vilken information som är känslig och hur både den och olika system ska skyddas. Man bör också se över hur tillgång till rätt information säkras över tid och hur redundans hanteras för olika system. Med den analysen som grund kan man vidta åtgärder som gör att risken och sårbarheten för attacker och informationsförlust minskar väsentligt.

En metod är att arbeta med processorienterad informationskartläggning och klassning av informationen. Syftet med informationsklassning är att skapa en grundläggande förståelse för hur skyddsvärd en viss informationsmängd är, det vill säga hur viktigt det är att informationen är korrekt, att den inte förvanskas avsiktligt eller oavsiktligt samt att den är tillgänglig när den behövs.

Förenklat innebär det att tre perspektiv belyses enligt följande:

- **Konfidentialitet** – Vad blir skadan om informationen hamnar i orätta händer?
- **Riktighet** – Vad blir skadan om informationen inte är korrekt?
- **Tillgänglighet** – Vad blir skadan om informationen inte är tillgänglig?

Begrepp

I denna skrivning används en rad termer och begrepp relaterad till informationssäkerhet. Vi har valt att beskriva följande termer och begrepp för att skapa en tydlighet för läsaren.

Säkerhetsaspekter

Säkerhetsaspekt	Definition i SIS Handbok 550	Definition i SS-ISO/IEC 27001
Konfidentialitet	Skyddsmål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga	Egenskapen att information inte tillgängliggörs eller avslöjas till obehöriga individer, enheter, eller processer
Riktighet	Skyddsmål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning	Egenskapen att skydda exaktheten och fullständigheten gällande tillgångar
Tillgänglighet	Skyddsmål där informationstillgångar ska kunna utnyttjas i förväntad utsträckning och inom önskad tid	Egenskapen att vara åtkomlig och användbar vid begäran av behörig enhet

TABELL 1 ▪ Begrepp säkerhetsaspekter.

Information & data

Begrepp	Beskrivning
Information & data	Data består i första hand av text och siffror medan information är förädlad data som människor förstår. Utan att särskilja information och data så är information text, bild, mätdata, siffror, rapporter, statistik, tal, ljud och mycket mer.
Informationsmängd	En informationsmängd är en gruppering av information, exempelvis i form av dokument, en databas eller liknande, som innehåller flera informationstyper.
Datamängd	En datamängd är en samling data som behandlas tillsammans för ett bestämt ändamål.
Informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information. I begreppet ingår också nätverk och infrastruktur.
Informationstillgång	Innefattar både den information, och de informationssystem som hanterar informationen, som är av värde för en organisation.
Informationsägare	Den person, eller funktion, som har ansvaret för den information som skapas och hanteras inom den egna organisationen.

TABELL 2 ▪ Begrepp information och data.

1

1. Bakgrund, mål och syfte

Ökad digitalisering och tillgång till data

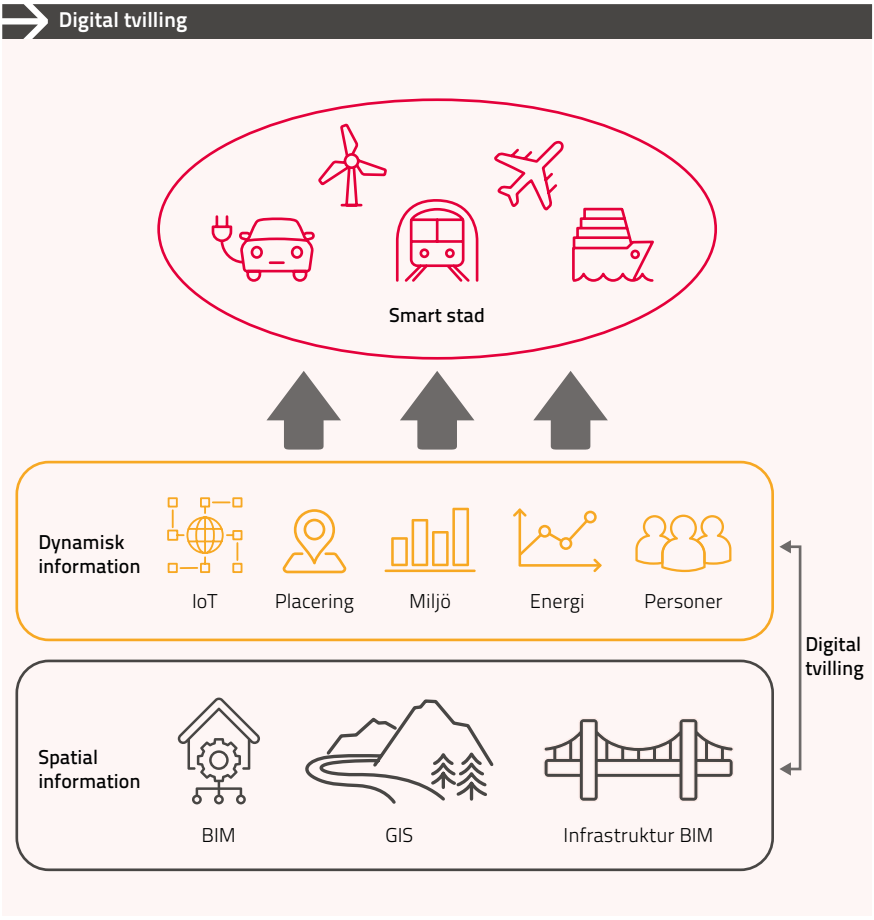
En tydlig trend i samhället är en ökad digitalisering inom alla områden och kopplat till det sker även stora förändringar i affärsmodellerna. Sedan årtionden har mycket investerats i att utveckla it-stöd för att hantera i stort sett oförändrade processer, rutiner och information. Det som sker nu är en digital transformation, dvs radikalt förändrade flöden, förändrad affärslogik och automatisering av funktioner.

Framstegen inom teknik, möjlighet till analys, hantering av stora datamängder (big data), hög mobilitet, användarvänlighet och sociala medier kommer ytterligare skynda på utvecklingen. Det är troligt att ett antal av dagens arbetsuppgifter kommer att vara väsentligt förändrade eller till och med försvunna om tjugo år. Maskiner kan ta över mer repetitiva arbetsuppgifter och människor kan få mer tid över till analys, kunddialog och andra arbetsuppgifter. I den bästa av världar blir kombinationen av människa och maskin ett mycket starkt team som väsentligt kan utveckla samhället. Människor kommunicerar, har empati och kan skapa relationer medan maskiner analyserar data, ställer diagnoser och kommer med lösningar.

Behovet av att kunna hantera den ökade informationsmängden som digitaliseringen medför ställer ett antal nya krav. Kraften i att ha tillgång till information var och när den än behövs är tydlig men det kräver strategi och struktur för att göra det möjligt. Informationsägarskap, konfidentialitet, riktighet och tillgänglighet blir centrala begrepp i informationshanteringen.

Våra byggnader blir allt mer smarta och den byggda miljön spelar också en viktig roll i den smarta staden där allt fler funktioner samverkar. Vi pratar om digitala tvillingar av både byggnader och städer där digital representation av det fysiska och där tvillingen visar både hur det ser ut men också hur byggnaden/staden mår och presterar. I flertalet tillämpningar utgör den digitala tvillingen en digital hybrid av fysisk och virtuell miljö. Exempelvis vid simuleringar inom stadsutvecklingsprojekt. Både fastighetsorganisationer och dess hyresgäster förväntas kunna dra nytta av publikt tillgänglig

information om sådant som kan påverka byggnaden och dess nyttjande. Exempelvis driftstörningar i kollektivtrafiken, skyfall, publika event, ordningsstörningar. Detta ställer krav på bland annat tillgång till data vilket förutsätter att både personer och organisationer är beredda att dela med sig av information. Samtidigt måste vi vara medvetna om säkerhetsaspekten och säkra att inte känslig information sprids och nyttjas felaktigt.



FIGUR 1 ▪ En struktur för en digital tvilling med sin information och tillhörande tjänster enligt japanska Kajima.

Fastighetsorganisationens utmaningar och förväntningar

Kompetensen att förvalta fastigheter kan antingen finnas hos personer som är anställda eller leverantörer inhyrda för att utföra en arbetsuppgift men informationen kring byggnaden behöver oavsett knytas till byggnaden. Fastighetsorganisationen vill inte vara beroende av enskilda individer eller leverantörer utan är angelägen om att säkerställa att all aktuell kunskap/information finns tillgänglig och är åtkomlig för alla dem som behöver den.

Förväntningarna från fastighetsägarens kunder förändras och förstärks successivt med en ökad digitalisering i deras egen verksamhet. Kunderna vill med säkerhet ha samma service och information från sin hyresvärd som man får från andra leverantörer inom till exempel e-handel eller resor. Man vill kunna ställa vilken fråga som helst, närsomhelst, i vilken kanal som helst och bli bemött i ett behagligt gränssnitt med ett informativt svar eller utförd åtgärd.

Fler och fler kunder vill förmodligen också ha en flexibilitet i lokalförsörjningen och kunna hyra en funktion med tillhörande service snarare är en kvadratmeter som man själv måste utrusta och sköta om. För fastighetsägaren kan det t ex innebära att gå från att hyra ut kvadratmeter till att hyra ut en funktion och att vara en aktör som skapar förutsättningar för människor och organisationer att mötas vilket i sin tur kan ge nya affärsmöjligheter, ökad produktivitet eller förbättrad verksamhet.

Det kan dels innebära flexibla hyresformer som arbetsplats eller mötesplats per timme men också olika typer av tilläggstjänster och merförsäljning. Om inte fastighetsägaren kan, eller vill, leverera tilläggstjänsterna finns det ett antal andra aktörer som kommer att vilja erbjuda dessa tjänster. För fastighetsorganisationen kommer det säkert att växla över tid vilken strategi man väljer men det är viktigt att göra ett aktivt val och ta beslut om lämplig strategi.

För att kunna tillhandhålla rätt funktion och tjänst till kunden vill vi ha kunskap om våra kunders rörelsemönster och användning av lokaler och tjänster. Genom det kan vi arbeta proaktivt och prognostisera hur lokal- och servicebehov förändras över tid. Med den kunskapen och verktygen kan fastighetsägare och förvaltare dels anpassa lokalerna efter kundens behov men också tillhandahålla en mer behovsanpassad service. Det förutsätter tillgång till data och att vi också vågar och vill dela med oss av viss information mellan olika organisationer. Olika organisationer och företag kommer att vilja tjäna pengar på information som genereras och att ”data är det nya guldet” blir tydligt.

Både fastighetsorganisationer och dess kunder förväntas kunna dra nytta av publikt tillgänglig information om sådant som kan påverka byggnaden och dess nyttjande. Exempelvis driftstörningar i kollektivtrafiken, skyfall, publika event, ordningsstörningar.

Samtidigt är det ett antal verksamheter som är samhällsviktiga och där behovet av informationssäkerhet ökar vilket leder till att fastighetsägaren behöver ha en dialog med sina hyresgäster/kunder för att kartlägga hur information ska hanteras under byggnadsverkets hela livscykel. Informationsägarskap, konfidentialitet, riktighet och tillgänglighet blir centrala begrepp i informationshanteringen.

För den tänkta målgruppen av denna skrivning är en viktig del att också förhålla sig till SS-EN ISO 19650 som är en serie standarder kring Strukturering av om byggd miljö och som beskriver principer för informationshantering över tillgångens hela livslängd.

Principerna i de standarderna ligger också som grund för de nationella riktlinjerna kring livscykelinformation för byggd miljö som är ett digitalt stöd vid kravställning av digital information.

En bredare och mer komplex hotbild

Digitalisering skapar nya möjligheter för utveckling och tillväxt men innebär också nya sårbarheter i samhället. De senaste åren pekar på ett försämrat säkerhetspolitiskt läge och en förändrad hotbild mot Sverige. Ökad globalisering och digitalisering bidrar till förutsättningar för välstånd och tillväxt samtidigt som det ökar sårbarheter och risker.

I Försvarsberedningens rapport ”Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025”, (Ds 2017:66) framhålls att ökade datavolymer och bearbetningsförmågor i elektroniska kommunikationsnät, it-system och styrsystem ökar riskerna för antagonistisk påverkan genom cyberattacker och andra it-incidenter.

Den tekniska utvecklingen, utbredningen av digitala lösningar och ökade datavolymer skapar stora möjligheter men samtidigt risker och sårbarheter för myndigheter och för samhället i stort. De data som genereras medför i sig både sårbarheter och möjligheter. Många av de system som är kritiska för att upprätthålla samhällets funktionalitet är redan i fredstid sårbara för störningar. Digitalisering, centralisering och tekniska beroenden medför sårbarheter som kan utnyttjas av en antagonist.

Vi kan konstatera att hotet mot Sverige har breddats och blivit mer komplext. Det traditionella underrättelsehotet kvarstår, samtidigt som säkerhetshotande verksamhet intensifieras. Cyberhotet riskerar att få allvarliga konsekvenser för samhällets funktionalitet. Den genomgripande digitaliseringen, att fler enheter kopplas upp mot internet samt fortsatt stora brister i it-säkerheten innebär att riskerna för störningar i samhällsviktiga verksamheter ökar.

Samhällssektor	Exempel på viktiga samhällsfunktioner
Energiförsörjning	Produktion av el, distribution av el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel.
Finansiella tjänster	Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel.
Handel och industri	Bygg- och entreprenadverksamhet, detaljhandel, tillverkningsindustri.
Hälso- och sjukvård samt omsorg	Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor.
Information och kommunikation	Telefoni (mobil och fast), internet, radiokommunikation, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier.
Kommunalteknisk försörjning	Dricksvattenförsörjning, avloppshantering, renhållning, väghållning.
Livsmedel	Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel.
Offentlig förvaltning	Lokal ledning, regional ledning, nationell ledning, begravningsverksamhet, diplomatisk och konsulär verksamhet.
Skydd och säkerhet	Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tull-kontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet.
Socialförsäkringar	Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen.
Transporter	Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik.

FIGUR 2 ▪ MSB - Identifiering av samhällsviktig verksamhet.

Vi ser också exempel på diverse andra hackerattacker som överbelastningsattacker (DDoS), skadlig kod (malware) eller utpressning (ransomware) i syfte att förstöra, låsa funktioner och/eller information.

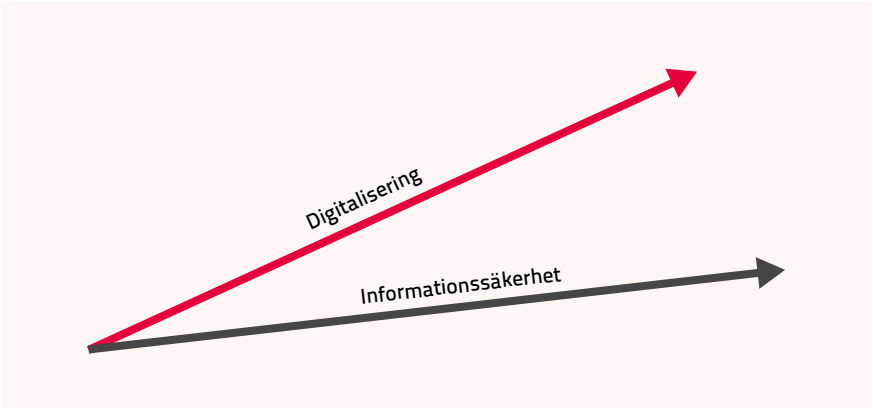
Den ökade informationsmängden och en ökad uppkoppling mot internet medför en ökad sårbarhet och det sker fler och fler attacker även mot fastighetsorganisationer och byggnadsverk. Attackerna kan rikta sig mot system för passage och larm men också mot styrsystem för el, värme, kyla och ventilation. Ofta beror sårbarheten på avsaknad av medvetenhet kring riskerna och att rutiner och strategier saknas.

Mål och syfte

I Säkerhetsskyddslagen (2018:585) och Säkerhetsskyddsförordning (2021:955) tas ett tas ett större grepp kring informationssäkerhet och inte bara ur perspektivet konfidentialitet, utan även riktighet och tillgänglighet. I NIS-direktivet (Informationssäkerhet för samhällsviktiga och digitala tjänster) samt Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster finns det en gråzon där offentliga fastighetsägare är i behov av vägledning och metodik.

Det är väsentligt att som fastighetsorganisation göra en riskbedömning och ta fram en strategi för vilken information som är känslig och hur både den och olika system ska skyddas. Man bör också se över hur tillgång till rätt information säkras över tid och hur redundans hanteras för olika system. Med den analysen som grund kan man vidta åtgärder som gör att risken och sårbarheten för attacker och informationsförlust minskar väsentligt.

Syftet med denna rapport är att stödja offentliga fastighetsägare i arbetet med ett systematiskt informationssäkerhetsarbete. Skrivningen beskriver en praktisk metod för hur fastighetsägare kan arbeta med ökade säkerhets- och informationssäkerhetskrav i fastighetssystem. I arbetet ingår riskinventering, fysisk säkerhet (tillgänglighet och åtkomst till nätverk) samt informationssäkerhet (tillträde till information).



FIGUR 3 ▪ I de undersökningar som görs av bland annat MSB om organisationers mognad avseende informationssäkerhet är det tydligt att mognadsgraden inte står i proportion till den ökade digitaliseringen. Uppfattningen är dessvärre att gapet dessutom ökar över tid.

För mer information läs gärna MSB:s metodstöd kring systematiskt informationssäkerhetsarbete samt Säkerhetspolisens Vägledning i säkerhetsskydd:

MSB – https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/om-systematiskt-informationssakerhetsarbete/

SÄPO – https://www.sakerhetspolisen.se/sakerhetsskydd/vagledningar-sakerhetsskydd

2

2. Metodik

Mot bakgrund av att informationshanteringen blir allt mer komplex och att informationsklassningen utgår från en given informationsmängd är det av yttersta vikt att skapa en förståelse för i vilka sammanhang som information uppstår, hanteras, lagras, bearbetas osv. Inte sällan förekommer samma informationsmängd i olika sammanhang och det kan få stor påverkan på kvalitén på informationsklassning om det inte är känt.

Den processorienterade informationskartläggningen är ett bra redskap för att kartlägga vilken information som uppstår i olika processer. Det kan också vara ett redskap för att förstå ägandeskapet till en viss informationsmängd.

Metodik för informationsklassning

Syftet med informationsklassning är att skapa en grundläggande förståelse för hur skyddsvärd en viss informationsmängd är, det vill säga hur viktigt det är att informationen är korrekt, att den inte förvanskas avsiktligt eller oavsiktligt samt att den är tillgänglig när den behövs.

Förenklat innebär det att belysa tre perspektiv enligt följande:

- **Konfidentialitet** – Vad blir skadan om informationen hamnar i orätta händer?
- **Riktighet** – Vad blir skadan om informationen inte är korrekt?
- **Tillgänglighet** – Vad blir skadan om informationen inte är tillgänglig?

I denna skrivning använder vi en metodik från SKR:s verktyg KLASSA[1] mot bakgrund av att den metodiken till stor del är normerande för många offentliga organisationers informationssäkerhetsarbete. Resonemang och exempel från denna skrivning är dock tillämpbar även för dem som inte använder KLASSA.

1. https://klassa.skr.se.

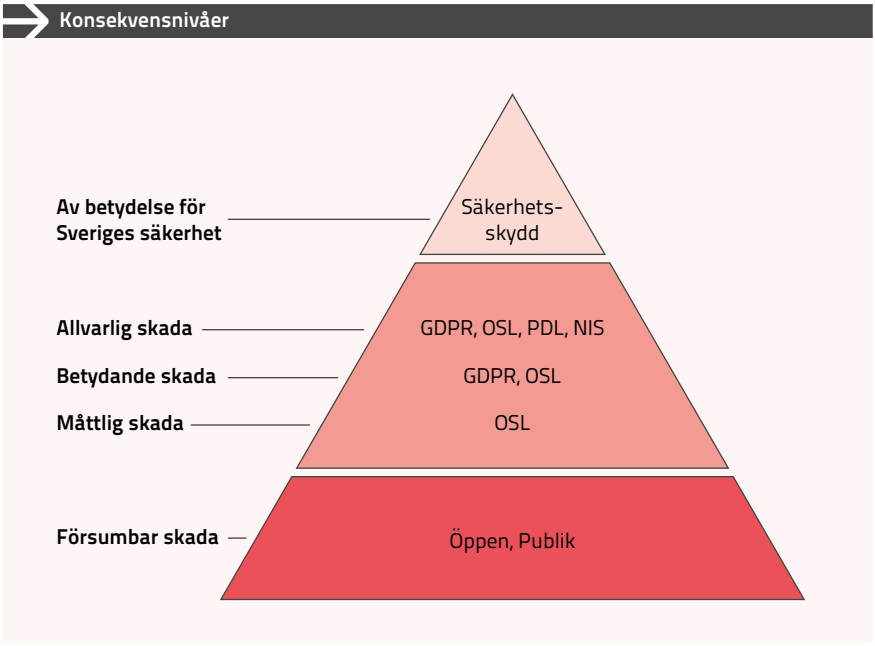
KLASSA utgår från standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 27002 som beskriver en modell och metodik för informationsklassning. Dessa standarder och MSB:s[2] metodstöd har legat till grund för SKR:s verktyg KLASSA. SKR har utformat modellen så att dess medlemmar kan klassa informationstillgångar på ett likartat sätt och i syfte att skapa en gemensam förståelse för krav på skydd och för tillämpningen av lämpliga skydd.

De konsekvensnivåer som används i KLASSA följer den modell[3] för klassificering av information som utarbetats av MSB och Svenska Institutet för Standarder (SIS):

- Synnerligen allvarlig skada (4)
- Allvarlig skada (3)
- Betydande skada (2)
- Måttlig skada (1)
- Försumbar skada (0)

Synnerligen allvarlig skada (4) definierades inte i arbetet av SIS/MSB. I takt med den ökade hotbilden i omvärlden såg SKR och flera av dess medlemmar ett ökande behov av att uppmärksamma dessa informationstillgångar varför den infördes redan år 2013 i KLASSA version 1 som en indikation på att informationstillgången berörs av säkerhetsskyddslagen (2018:585).

2. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/metodstod-for-systematiskt-informationssakerhetsarbete/.
3. https://www.msb.se/RibData/Filer/pdf/25602.pdf.



FIGUR 4 ▪ Denna bild ger viss vägledning hur information som berörs av olika lagrum kan klassificeras. Information som berörs av säkerhetsskyddslagen ska klassificeras i enlighet med de fastställda nivåerna i säkerhetsskyddslagens andra kapitel, 5 §.

Metodik för processorienterad informationskartläggning

Metodiken för att göra en processorienterad informationskartläggning (POIK) har inte lika fasta ramar att förhålla sig till som informationsklassning och har också fler beroenden varför det snarast ska ses som ett tillvägagångssätt.

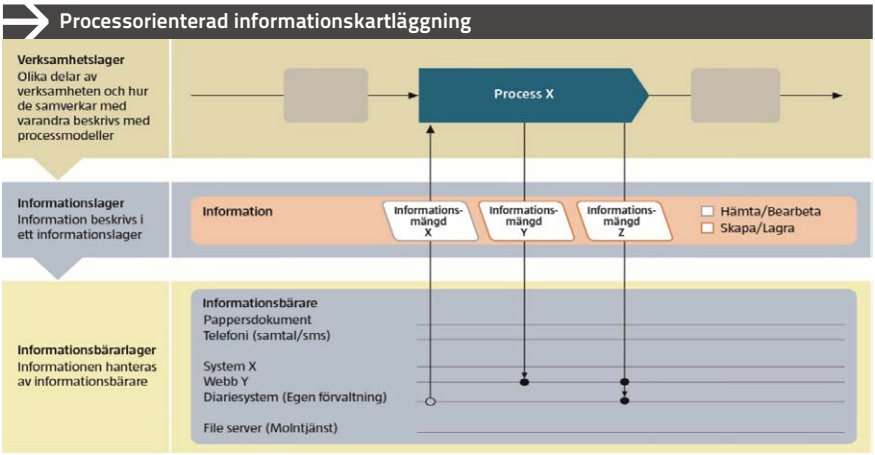
Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet (RA) genomförde ett initiativ 2012 under rubriken Vägledning för processorienterad informationskartläggning[4] som är en bra och ganska enkel vägledning att förhålla sig till. Fördelen med att vägledningen är enkel är att tillämpligheten för vägledningen ökar vilket inte ska underskattas mot bakgrund att vi hanterar ett antal processer och information under en byggnads livscykel.

Ansatsen för den processorienterade informationskartläggningen kan sammanfattas i tre lager:

- Verksamhetslagret, som exempelvis beskrivs genom att följa en verksamhetsprocess
- Informationslagret, som beskriver de informationsmängder som:
  - Skapas
  - Hämtas
  - Bearbetas
  - Lagras
- Informationsbärlager, som beskriver informationsbärare

Sammanfattningsvis kan sägas att en process har relation till en eller flera informationsmängder som i sin tur bärs av ett antal informationsbärare.

4. https://rib.msb.se/filer/pdf/26410.pdf.



FIGUR 5 ▪ MSB – Modell för processorienterad informationskartläggning med identifiering av verksamhetslager, informationslager och informationsbärarlager.[5]

Det synsättet är relativt enkelt att applicera på fastighetsförvaltning där man till exempel kan se en process som styr värme eller kyla i en byggnad med ett antal informationsmängder som grund, exempelvis inom- och utomhustemperatur. Det gör att den processorienterade informationskartläggningen kan användas för att identifiera informationsmängder, informationsägare och de förväntade kraven på de informationsmängderna.

Ur ett informationsklassningsperspektiv går det att kopplat till exemplet ovan göra en bedömning av:

- **Konfidentialitet** – Vad blir skadan om informationen hamnar i orätta händer?
  - Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en byggnad tillgängliggörs blir skadan sannolikt **försumbar (0)**

- **Riktighet** – Vad blir skadan om informationen inte är korrekt?
  - Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en byggnad inte är korrekt blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

5. https://www.msb.se/sv/publikationer/vagledning-for-processorienterad-informationskartlaggning/.

- **Tillgänglighet** – Vad blir skadan om informationen inte är tillgänglig?
  - Om inom- eller utomhustemperatur som används för att styra värme eller kyla i en byggnad inte är tillgänglig blir skadan sannolikt **måttlig (1)** eller **betydande (2)**

Värderingen av skadan beror givetvis på vilken verksamhet som bedrivs i byggnaden, hur lång tid det går från att informationen inte är korrekt eller otillgänglig, likväl som det beror på hur stor avvikelsen är och givetvis vad omgivningstemperaturen är vid det aktuella tillfället.

Om informationen inte hade satts i sitt rätta sammanhang så hade det varit svårt att värdera en informationsmängd som inom- och utomhustemperatur. De aktuella informationsmängderna kan ha fler beroenden som gör att klassificeringen blir annorlunda.

Det säger sig självt att det är viktigt att ha relevant kompetens om den verksamhet som bedrivs och den information som hanteras för att kunna göra en korrekt informationskartläggning vilket också poängteras i MSB/RA:s vägledning.

Verktygsstöd

Det finns stöd att använda för informationskartläggning i form av KLASSA verksamhetsinformation, eller Arkiv-KLASSA och ibland också benämnt Informations-KLASSA[6].

Ett av huvudsyftena med Informations-KLASSA var att utarbeta en hierarkiskt uppbyggd klassificeringsstruktur för verksamheter inom kommuner och regioner. Strukturen är beskriven och systematiserad till ett punktnoterat schema. Schemat kan sedan användas som underlag för en diarieplan men även kunna nyttjas till dokumentmetadata, struktur för e-arkivet etc.

Klassificeringsschemat är uppdelat i tre delar:

- Ledning[7]
- Verksamhetsstöd[8]
- Kärnverksamhet[9]

6. http://samradsgruppen.se/index.php/rad-och-stod.
7. http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-1-LEDN-KLASSA-2.1.xlsx.
8. http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-2-ST%C3%96D-KLASSA-2.1.xlsx.
9. http://www.arkivkonsultab.se/wp-content/uploads/5.Klassa/VT1-VT3/VT-3-K%C3%84RN-KLASSA-2.1.xlsx.

Fastighetsverksamhet betraktas i det här sammanhanget som Verksamhetsstöd och i schemat går det exempelvis att finna notation 2.6.2 som avser processen Drift och underhåll.

Implementering och uppföljning

På motsvarande sätt som att hållbarhet, digitalisering med mera är en naturlig del i fastighetsorganisationens verksamhet måste också säkerhet och informationssäkerhet hanteras integrerat i verksamheten.

Frågorna ska hanteras i verksamhetsplaneringen, beaktas i verksamhetsplaner samt följas upp och uppdateras systematiskt och regelbundet.

3

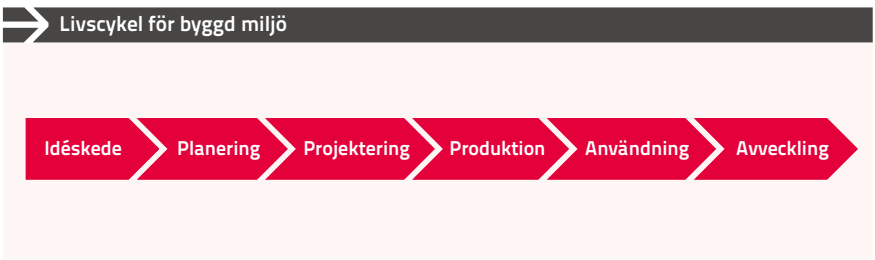
3. Informations-hantering från idé till avveckling

Fastighetsägare och byggherrar hanterar information om anläggningar från tidiga skeden som planprocessen, genom byggnadsverkets hela livscykel fram till avveckling. Det är viktigt att klargöra vad som är viktigt att skydda i respektive skede, men också i varje delprocess.

Vi utgår från den livscykelprocess som använts i Nationella riktlinjer[10] – livscykelinformation för byggd miljö och där innehållet i de olika skedena definierats. Det är först när man bryter ned skedena i delprocesser och även aktiviteter som det blir tydligt vad som görs i respektive skede. Då kan vi också tydligare se vilken information som används/behövs samt hur och var den informationen hanteras.

För respektive skede adderas mer information och informationen hanteras av fler parter och i fler system vilket gör det mer och mer sårbart. En kedja är inte starkare än sin svagaste länk!

Säkerhetsåtgärder och ansvarsförhållanden beträffande informationssäkerheten behöver vara implementerade i samband med att information börjar hanteras, i praktiken redan i samband med idéskedet.

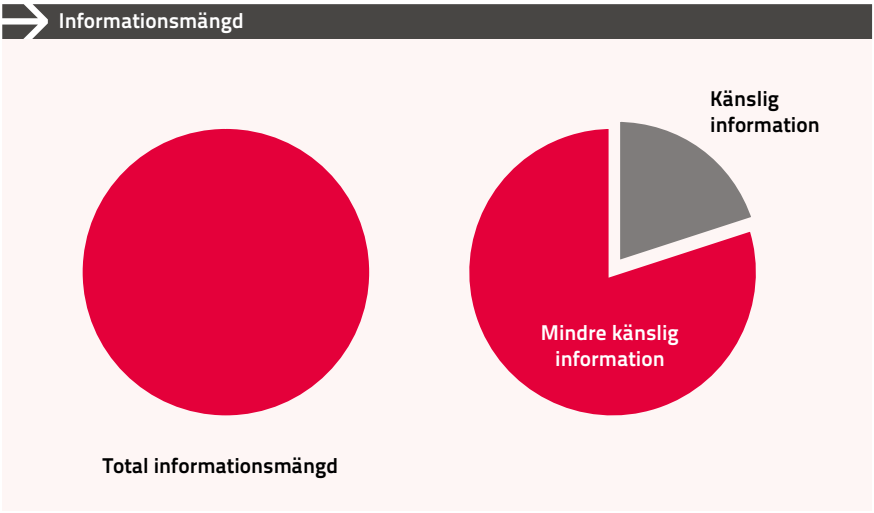


FIGUR 6 ▪ Livscykel för byggd miljö.

10. https://www.nationella-riktlinjer.se/.

Det är lätt att hamna i fällan att all information är känslig och att man därför hamnar på en onödigt hög och fördyrande nivå i sin informationshantering. Med ett systematiskt arbetssätt kan man identifiera vilken information som är känslig, samt utifrån vilka säkerhetsaspekter den är känslig och måste hanteras på ett speciellt sätt. Den informationen kanske kan separeras och hanteras speciellt medan övrig information kan hanteras mer ”normalt”.

Med den analysen som grund kan man välja lämpligt systemstöd för sin verksamhet.



FIGUR 7 ▪ Värdering av känslig information.

Ett mål med denna skrivning är att beskriva hur information kan hanteras i respektive skede och delprocess men också ge exempel på skyddsvärd information. Vi använder metodiken med processorienterad informationskartläggning och definierar vad som görs i respektive skede, vilken information som kommer i spel och vilka informationsbärare som används.

Processerna i följande exempel är endast schematiskt ritade och bör detaljeras för respektive verksamhet. Förhoppningsvis finns redan en processkartläggning i organisationen vilken med fördel används som grund för kartläggningen.

Systemstöd i olika skeden

För varje skede i livscykelprocessen används ett antal olika systemstöd. En del system är interna och hanteras strukturerat under en längre tid medan andra är externa systemtjänster som kanske handlas upp som en tillfällig lösning för att hantera ett visst behov eller ett projekt. Stora informationsmängder hanteras i de olika systemen och det är centralt att ta ett grepp om vilka system som används, vilken information som hanteras samt ställa krav på hur it-miljön är utformad.

Systemfamiljer

System	Idé	Planering	Projektering	Produktion	Användning	Avveckling
Fastighets-förvaltningssystem		x			x	x
Ekonomi- och administrationssystem	x	x	x	x	x	
Projektstyrningssystem		x	x	x		
IT i byggnaden – SCADA/BMS, IoT, passersystem, larm				x	x	
Dokument-hanteringssystem	x	x	x	x	x	x
CAD – Modeller		x	x	x	x	x
GIS – Geodata och kartor	x	x	x	x	x	x
Publicering, presentation	x	x	x	x	x	x
Externa tjänster		x	x	x	x	x
Kravdatabaser		x	x	x	x	
Externa myndighetsdatabaser	x	x	x	x	x	x

TABELL 3 ▪ Beskrivning av systemstöd för respektive skede i livscykeln.

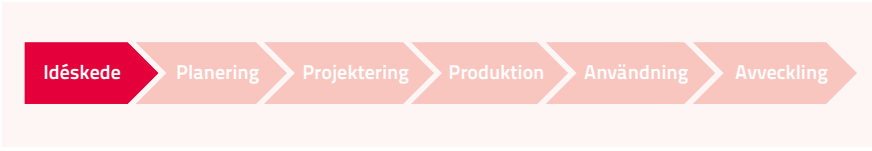
På marknaden finns det ett flertal system som stöd för verksamheten. Vi har i denna skrivning delat in systemen i följande systemfamiljer:

- Fastighetsförvaltningssystem
- Ekonomi- och administrationssystem
- Projektstyrningssystem
- IT i byggnaden - SCADA/BMS (Styr- och Övervakningssystem), IoT, passersystem, larm
- Dokumenthanteringssystem inklusive projektserviceplatser
- CAD- och Ritningshanteringssystem
- GIS – Geodata och kartor
- Publicering, presentation och kommunikation
- Kravdatabaser
- Externa tjänster – miljöbedömning, certifiering, besiktning etc
- Externa myndighetsdatabaser – kommuner, Lantmäteriet, Boverket, Naturvårdsverket etc

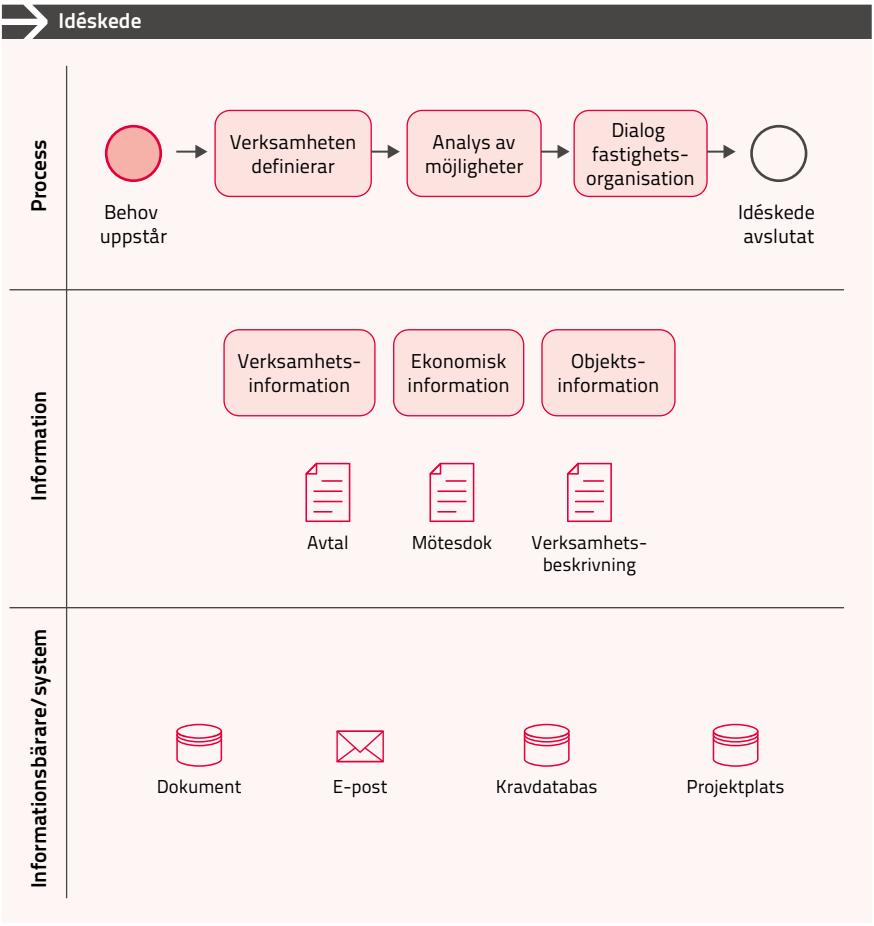
Systemen kan vara mer eller mindre kompletta och innehålla ett flertal integrerade delmoduler eller endast utgöra en sidoordnad del inom affärsområdet. En sidoordnad del kan vara kopplad eller integrerad med en eller flera andra delsystem.

I de följande avsnitten sker en genomgång av olika skedena och den information, system och utmaningar som kan förekomma.

Idéskede



Under idéskedet uppkommer och hanteras verksamhetens behov av funktion och lokaler. Skedet resulterar i verksamhetsbeskrivning, lokalbehov och sambandskrav och den informationen behöver kommuniceras mellan verksamheten och fastighetsägaren.



FIGUR 8 ▪ Exempel på informationskartläggning för idéskedet.

I det här skedet bör en klassning av informationen göras av kärnverksamheten/nyttjaren/hyresgästen och med den analysen som grund kan hantering och kommunikationssätt beslutas.

Vi kan konstatera att beroende på vilken verksamhet som förekommer är ingående informationen olika känslig varför den kan behöva hanteras på olika sätt. Eftersom mejl är att betrakta som ”ett vykort som alla kan läsa” kan det redan i detta skede vara aktuellt att etablera en säker projektserviceplats eller motsvarande för utbyte av information mellan olika organisationer vara aktuell för att undvika mejlkommunikation eller annan osäker kommunikation.

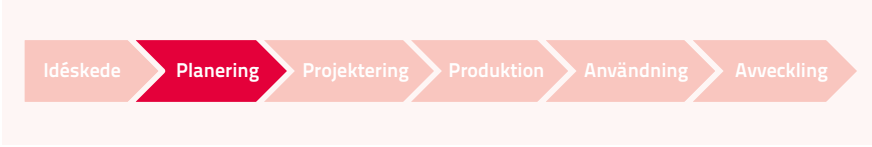
Projektserviceplatserna ger en högre grad av informationssäkerhet avseende både konfidentialitet, riktighet, tillgänglighet och spårbarhet men vilken produkt eller tjänst man använder behöver naturligtvis utvärderas vilket beskrivs vidare under Projekteringsskede nedan.

Information kring verksamhet i tidiga skeden

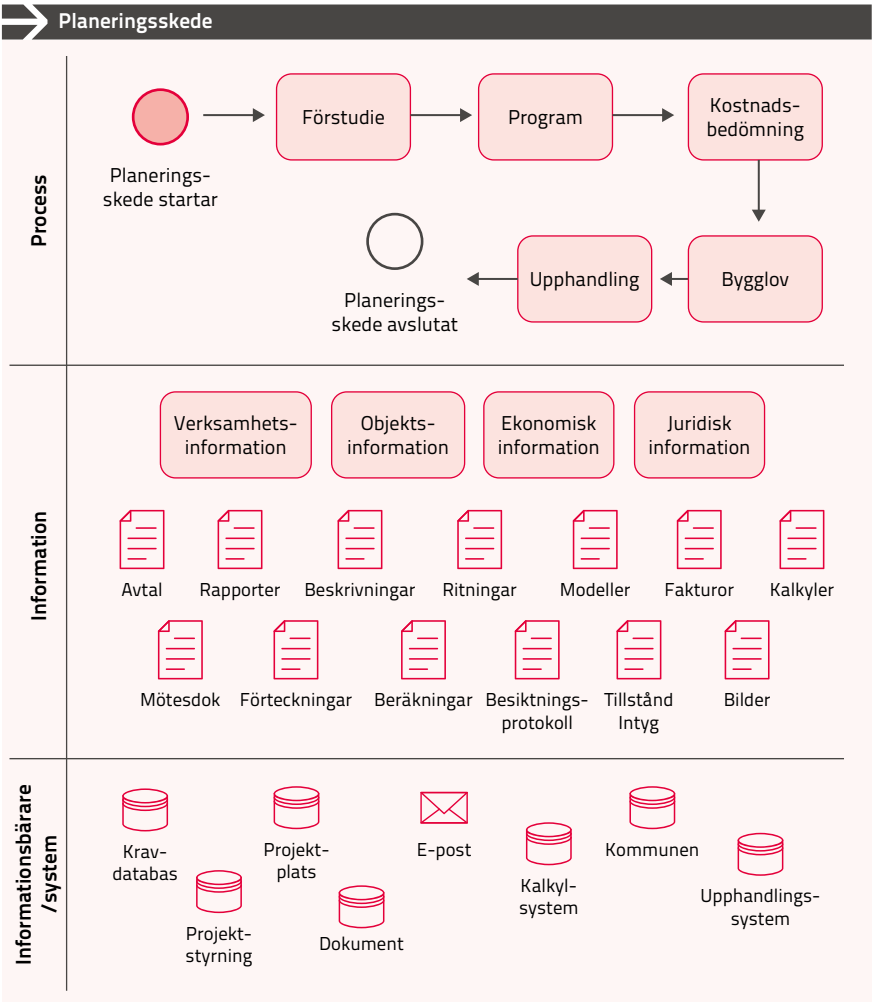
Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Verksamhet	0-4	2	1	
Funktion – behov	0-4	2	1	
Fysiskt samband/ placering	0-4	2	1	
Tidsaspekt	0	1	1	
Budget	0-2	2	1	Beroende på typ av verksamhet
Miljökrav	0	1	1	
Säkerhetskrav	0-4	1	3	
Övriga krav	1	1	1	

TABELL 4 ▪ Exempel på klassning av verksamhetsinformation.

Planeringsskede



Planeringsskedet omfattar fastighetsorganisationens förstudie, utredning, kalkylering och programhandling. Planeringsfasen kan även inkludera stadsplaneprocessen och arbete med bygglovshantering.



FIGUR 9 ▪ Exempel på informationskartläggning för planeringsskedet.

I det här skedet börjar vi bygga upp en större mängd data kring byggnadsverket och information efterfrågas från olika intressenter som olika myndigheter och externa parter. Utmaningen ökar och en eller flera klassningar behöver göras för att identifiera vilken information vi är beredda att släppa ut till bland annat myndigheter för hantering i externa databaser.

Under planeringsskedet förekommer projektstyrningssystem, projektserviceplatser, stöd för kravställning och rumsfunktionsprogrammering samt olika externa tjänster för t ex miljöbedömning. Många av dessa tjänster är molnlösningar som erbjuds av olika aktörer med databaser på olika ställen, en del i Sverige och andra internationellt.

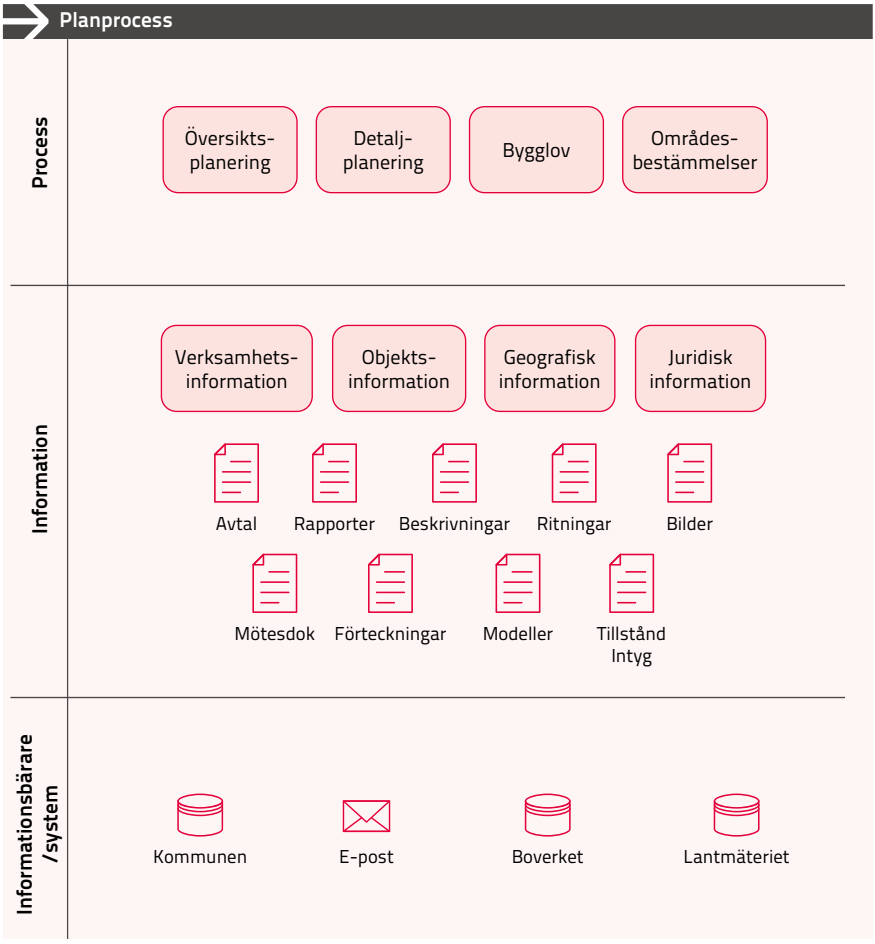
Nedan finns ett exempel på checklista kring övergripande informationssäkerhetsåtgärder som bör gås igenom innan ett projekt startas[11]:

- Informationsklassificera fastighetsinformation
- Upprätta en projektsäkerhetsanalys
- Upprätta säkerhetsinstruktion, utbildningsplan samt kontrollplan för projektsäkerhetsarbetet
- Tydliggör informationsägarförhållanden mot konsulter och entreprenörer
- Identifiera vilka befattningar som eventuellt ska placeras i säkerhetsklass
- Kravställ och/eller upprätta it-system för hantering av aktuella informationssäkerhetsklasser
- Kravställ och upprätta förvaringsutrymmen som möjliggöra hantering av aktuella informationssäkerhetsklasser

Planprocessen enl PBL och myndighetskrav

Kopplingen både till planprocessen enl PBL med kommunens informationsbehov samt Lantmäteriet krav på information är en avgörande fråga. I planprocessen kan det finnas information som är skyddsvärd, det kan röra sig om möjligheter till bergrum, en viss typ av verksamhet eller liknande, varför man måste göra en informationsklassning för att utvärdera hur informationen ska hanteras.

11. Locum, Region Stockholm.



FIGUR 10 ▪ Exempel på informationskartläggning för myndighetskrav samt planprocessen enl PBL.

I Lantmäteriets fastighetsinformationsregister ska finnas/finns information om fastigheter, byggnader men också verksamhet och i samband med utvecklingen av den nationella geodataplattformen finns mer och mer av information tillgänglig digitalt. Exempel på byggnadsinformation som är aktuell i plattformen listas nedan och här måste varje fastighetsägare göra en klassning och bedömning av varje informationsmängd.

Det obligatoriska attributet Ändamål måste värderas eftersom det kan vara skyddsvärt för viss verksamhet. I övrigt kan antal våningar under mark vara skyddsvärt känslig men det är inte identifierat som en obligatorisk uppgift att rapportera.

Information om byggnad/byggnadsdel i den nationella geodataplattformen

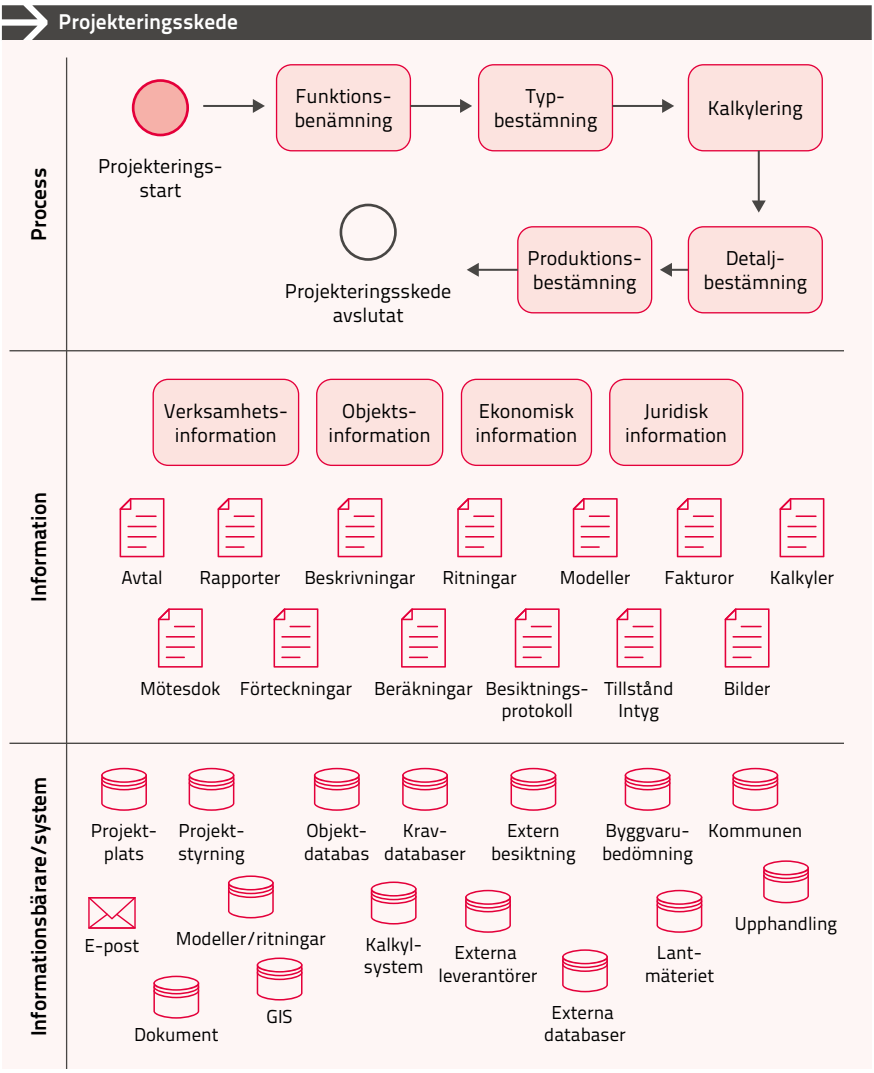
Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
ID – UUID*	0	1-2	1	Koppling till andra databaser ger riktighet
Benämning	0-1	0	0	
Ändamål*	0-3	0	0-3	Beroende på verksamhet
Areor	0	2	1	
Bygglov	0-2	1	1	
Antal våningar	1	0	0	
Antal våningar över mark	0	0	0	
Antal våningar under mark	0-3	1	1	Beroende på verksamhet
Status*	0	1	1	
Höjd	0	1	1	
Vind	0	1	1	
Källare	0-3	1	1	Beroende på verksamhet
Antal lägenheter	0	1	1	
Klassning - CoClass	0-3	0	0-3	Jmfr Ändamål
Byggår	0	1	1	

*Obligatorisk

TABELL 5 ▪ Information om byggnad/byggnadsdel i den nationella geodataplattformen.

Projekteringsskede

I projekteringsskedet har vi ett antal externa medverkande leverantörer. Information hanteras i modeller, i projektserviceplatser och i externa databaser. Informationsmängden och detaljeringsgraden kring byggnadsverken ökar successivt.



FIGUR 11 ▪ Exempel på informationskartläggning för projekteringsskedet.

Projektstyrningssystem ska primärt stödja planering och uppföljning av både enskilda projekt och hela projektportföljer. Systemen innehåller moduler för budget/prognos och kostnadsuppföljning, processtyrning, tids- och aktivitetsplanering, uppföljning av beslutspunkter och grindar, riskanalyser samt kanske även projektserviceplats för ritningar, modeller och dokument. Genom att integrera med ekonomisystemet avseende beställningar och leveransgodkännande kan uppföljning effektiviseras.

Projektserviceplatserna är centrala för utbyte av information och dokument mellan olika aktörer och är i de flesta fall molnlösningar som erbjuds av olika leverantörer. Här finns en källa för ”informationsläckage” och det är väsentligt att analysera vilken information som hanteras i lösningen samt säkra hur leverantören av lösningen hanterar sin it-miljö. Vid högre informationssäkerhetskrav får beaktas om andra lösningar måste finnas, exempelvis placering av projektserviceplatsen i egen it-miljö.

Externa databaser som Byggvarubedömningen, Sunda hus etc innehåller mycket information om ingående komponenter och produkter i byggnadsverket. Här kanske det räcker att man i dessa databaser har registrerat en (1) komponent av en viss typ för bevakning av ingående ämnen men inte var den komponenten är placerad eller hur många för att inte röja hur byggnadsverken i detalj är uppbyggda.

Referensbeteckningar

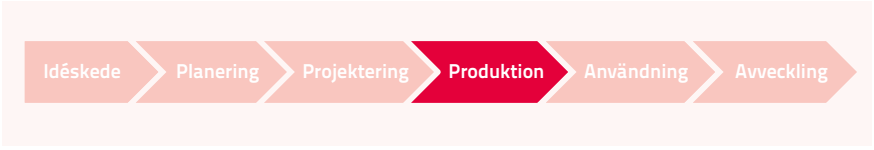
En generell regel för att inte röja information är att undvika att ha med benämning/användning och funktion i referensbeteckningar. Genom att använda neutrala identifierare, ID:n, kan en lägre klassning erhållas. ID:n ska för att vara tillförlitliga vara unika över tid och eftersom användning ofta förändras över tid bör detta hanteras som en egenskap för att ge robusta ID:n som håller under byggnadsverkets hela livscykel.

Upphandling

Upphandling kan beroende på syfte ske när som helst under en byggnads livscykel. Det kan vara upphandling av olika tjänster som projektledning eller projektering, upphandling av byggentreprenad, upphandling av driftentreprenad eller upphandling av demonteringsentreprenad. Oavsett hanteras en mängd information om både byggnadsverk och ingående verksamhet varför bedömning måste ske av vilken information som hanteras på vilket sätt. Det gäller både upphandlingssekretess och övrig sekretess.

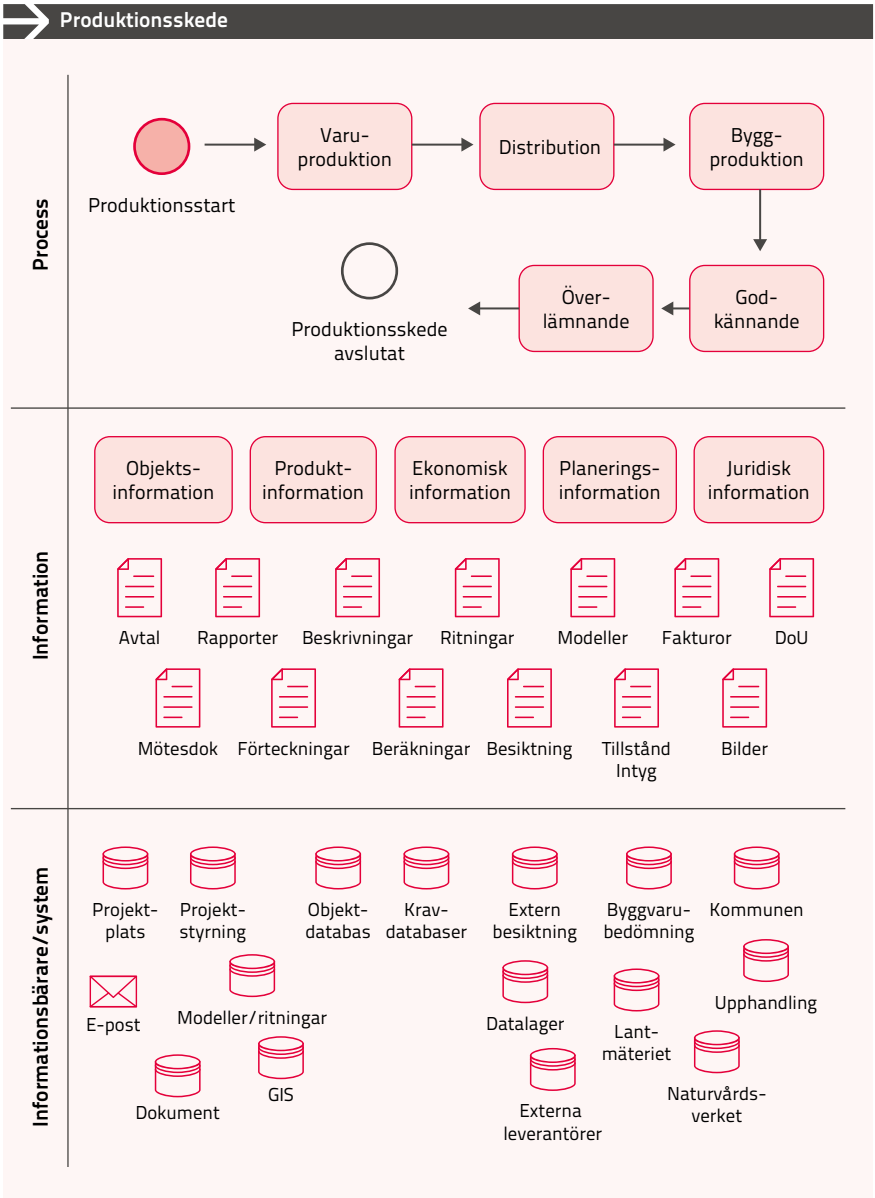
I offentlig verksamhet används ofta olika molnbaserade upphandlingstjänster, vilken information som tillgängliggörs där måste värderas avseende såväl konfidentialitet som riktighet och tillgänglighet.

Produktion



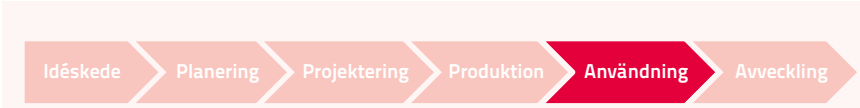
Under produktionsskedet ökar mängden leverantörer och mängden personer som är inblandade i projektet. I skedet hanteras både varuproduktion, distribution, transporter och byggproduktion. Ytterligare aktörer tillkommer i form av entreprenörer, underentreprenörer i olika led samt materialleverantörer. Information måste finnas tillgänglig på de platser och för dem som utför arbete varför personkontroller samt fysiskt skydd/tillträdeskontroll blir centralt för att säkra informationstillgångarna.

Systemstöden är i stort de samma som för projekteringsskedet men utökas eftersom det är fler parter som är inblandade. Informationsmängden och detaljeringsgraden kring byggnadsverken ökar ytterligare och det blir än viktigare med riktighet och tillgänglighet.



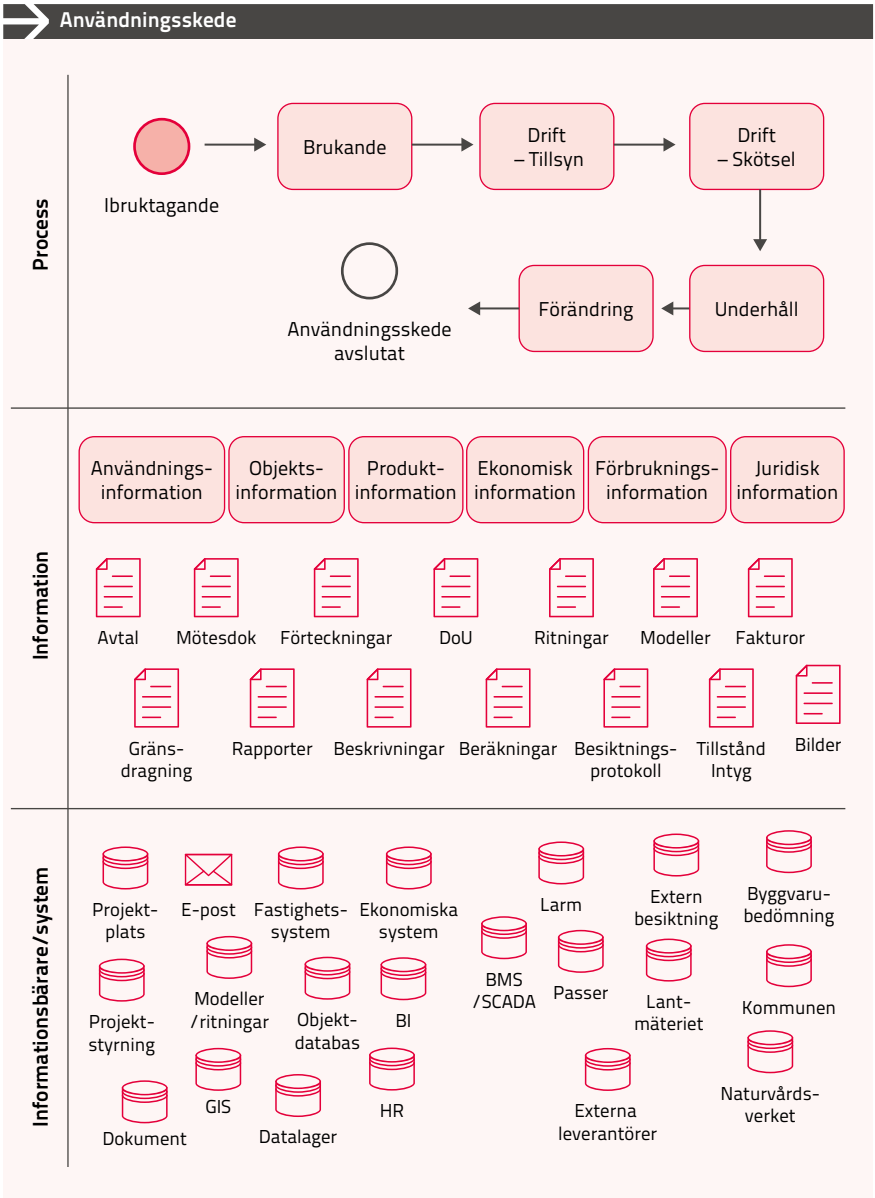
FIGUR 12 ▪ Exempel på informationskartläggning för produktionsskedet.

Användningsskedet



Användningsskedet, det vi ofta kallar förvaltningsskedet. Här har vi komplett information om våra byggnadsverk, hur de ser ut, hur de mår, hur de används och oftast också vilken verksamhet som bedrivs.

Verksamhetens affärsidé och mål styr behovet av information. Informationsbehovet utgör således basen, man vill dels veta vad man byggt in i byggnaderna, dels kunna effektivisera arbetsrutiner och processer i förvaltningsskedet varför mycket information hanteras i systemen. Med målsättningen att möta behovet beskrivet i kapitel 3 krävs ökade integrationer mellan olika informationskällor och databaser.



FIGUR 13 ▪ Exempel på informationskartläggning för användningsskedet.

Fastighetsförvaltningssystem

Fastighetsförvaltningssystemen omfattar stöd för objektsdata, hyresadministration/avtalshantering, avisering, uthyrning/marknadsplats, kundportal, entreprenörsportal, besiktningar, planerat underhåll, tillsyn och skötsel, serviceorder/felanmälan, energi och media, tillvalshantering och beställningar för att nämna de vanligaste övergripande funktionerna. Man vill att systemen stödjer ett mobilt arbetssätt för tekniker, förvaltare och entreprenörer och innehåller portaler för kunder/hyresgäster/lokalnyttjare och entreprenörer för att lägga grunden för en effektiv verksamhet.

Ofta sitter hela processen, från kommunikation med kunden via intern hantering och ut till externa utförare, ihop i samma system med en gemensam databas. På den svenska marknaden finns ett antal leverantörer som levererar fastighetssystem för ekonomisk och teknisk förvaltning i helhetslösningar.

Utöver de mer heltäckande systemen finns det leverantörer av system som fokuserar på delar av fastighetsbolagens efterfrågade funktionalitet. Fördelen med den lösningen är att det kan ge den bästa funktionaliteten för varje enskilt delområde men nackdelen är fler gränssnitt för användaren och ett utökat integrationsarbete mellan systemen.

Olika systemleverantörer har olika strategier kring teknisk lösning, en del satsar på SaaS-lösning (Software as a Service) med installation i någon molnlösning och andra tillhandahåller sina system med on-premise installation. Här är det viktigt att utvärdera om leverantörens strategi passar den egna strategin för att hitta en över tid hållbar lösning.

Ekonomi- och administrationssystem

Systemfamiljen omfattar ekonomisystem, HR-system och analysverktyg/BI.

Då datamängderna successivt ökar behövs system för att förädla, analysera och presentera informationen för att underlätta att rätt beslut fattas baserat på underlaget. I BI-systemen (Business Intelligence) samlas och lagras mycket data vilket kan utgöra en risk av konfidentialitetsskäl men eftersom beslut kommer att fattas baserat på underlaget är också riktighet och tillgänglighet centrala frågor.

Dokumenthanteringssystem

Dokumenthanteringssystem kan både utgöras av projektserviceplatser för effektivare projektstyrning och samarbete mellan aktörer samt kvalitetssäkring av tekniska dokument och ritningar i projekt samt dokumenthantering för kvalitetssäkring av styrande dokument i verksamhetens olika ledningssystem.

Under förvaltningsskedet behövs systemstöd för att hantera ritningar, modeller och andra dokument kopplade till förvaltningen. Genom integration med fastighetsförvaltningssystemet kan den obrutna leveranskedjan uppnås så att information kopplad till lokaler och installationer är tillgänglig och hanteras fortlöpande i drift och förvaltning.

Även här förekommer olika alternativ av it-lösningar, många finns i molnet och andra kan hanteras on-premise. En analys av vilka informationssäkerhetskrav som finns behöver ske innan val av lösning.

IT i byggnaden – SCADA/BMS (Styr- och Övervakningssystem), passersystem, IoT och AI

Här finns den kanske största potentialen med digitalisering men också de största hoten och riskerna. Det finns ett antal exempel på attacker där styrsystem för olika anläggningar har tagits över av externa hackare och även om inte ”vanliga byggnadsverk” har påverkats i så stor omfattning finns det all anledning att vara uppmärksam.

Frågor att belysa:

- ➔ Vad kan vara uppkopplat på distans?
- ➔ Vad ska inte vara uppkopplat?
- ➔ Back-up lösning för redundans
- ➔ Frånkoppling med lokal styrning

För mer information hänvisas till Offentliga fastigheters rapport – Digital Fastighetsautomation samt Kommunfondens rapport – Informationssäkerhet inom fastighetsområdet och IoT.

En förutsättning för den smarta byggnaden är att vi har en digital tvilling där vi både vet hur byggnadsverket ser ut och hur det presterar. Den smarta byggnaden kommer att klara av att hantera en del själv utan större inblandning av mänsklig hand. Den tekniska förvaltningen kommer att få hjälp av maskiner och artificiell intelligens, AI, där människa inte behöver vara mellanhand utan maskiner pratar med maskiner och ställer in byggnaden utifrån trender och signaler. Sensorer kan också ropa på hjälp och skapa underlag till arbetsorder, när ett visst värde har passerats under en viss tid kommer information om objektet, typ av fel, plats och tid.

Maskiner kan även mer effektivt analysera användande av lokaler och med hjälp av prognoser kring både klimat och användning effektivt styra kyla och värme med väsentligt minskad energiförbrukning. Det finns exempel där energiförbrukningen minskade med fyrtio procent när man lät maskinerna helt ta hand om styrning av fläktar och kylning i en serverhall.

Digitaliseringen gör det enklare att både generera och samla in stora datamängder med hjälp av sensorer och ”smarta” system. Det möjliggör i sin tur samkörning av varierande information i stora mängder, vilka kan användas till bland annat automatisering och prognoser.

Utvecklingen av Internet of Things, IoT, och sensorer gör att mycket mer information om byggnadsverkens användning och skick uppkommer. Allt fler komponenter som installeras innehåller en ”sändare”. Som fastighetsägare måste man vara medveten om detta och ta medvetna beslut om man är ok med att ”släppa ut” informationen till leverantören[12].

För att nå full potential vill man ha analyshjälp och automatisering i form av machine learning och AI. En utmaning är att dessa analysverktyg bygger på stora mängder data från olika byggnadsverk och att det per definition förutsätter molnbaserade lösningar och ”öppna data”.

Det är en utmaning att hitta lösningar för att nå tillförlitliga analysmöjligheter. Har man ett stort eget bestånd kanske ett analysverktyg kan installeras i egen miljö och ändå ha tillräcklig mängd data för att ge tillförlitliga analyser. Om beståndet är mindre kommer det att kräva tillgång även till andra byggnadsverks data och då måste viss information tillgängliggöras för dessa system.

12. https://skr.se/offentligafastigheter/publikationer/publikationer/informationssakerhetinomfastighetsomradetiot.

Externa databaser

Myndighetskrav är ett speciellt område att beakta, det berör dels lagstadgade besiktningar som OVK, tryckkärl, elrevision, lekplatser, sotning, skyddsrum, radon, hissar, portar, traverser, brandlarm vilka oftast hanteras via externa besiktningsorgan. Här hanteras en hel del information om anläggning hos besiktningsorganet vilket dels kan vara en risk ur konfientialitetssynpunkt, dels kan skapa problem kopplat till tillgänglighet den dagen man ska byta besiktningsorgan. Det gäller med andra ord även här att göra en informationsklassning och att säkra informationstillgångarna.

En annan del av myndighetskraven gäller rapportering i olika former, t ex förbrukning av media, energideklarationer och klimatdeklarationer. Även här finns risker eftersom rapportering av exempelvis förbrukning kan avslöja kapacitet och förmåga vilket exemplet kring reservkraftsaggregat och rapportering av förbrukad media i bilaga 1 visar.

Informationsklassning

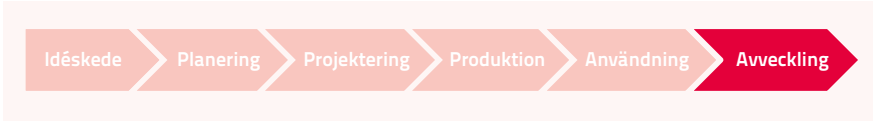
I bilaga 1 finns exempel på informationsklassningar för byggnadsverk, utrymmen, tekniska system och komponenter samt ett antal aktiviteter kopplat till användningsskedet som tillsyn, skötsel, underhåll, lagstadgade besiktningar och miljörapportering.

Vi har valt ett reservkraftsaggregat som exempel på en komponent på grund av att den är verksamhetskritisk. Andra komponenter är mindre kritiska och kan klassas på en annan nivå varför klassning bör göras för ett antal olika komponenttyper.

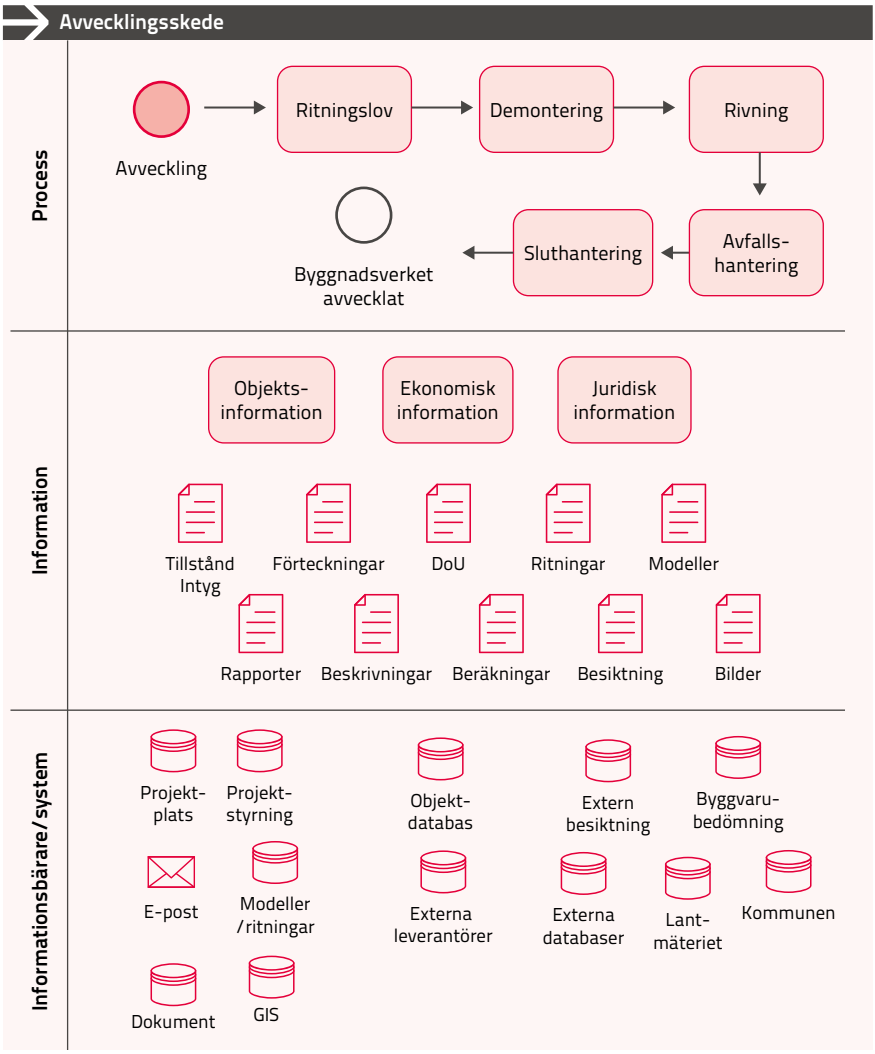
Vid klassning av reservkraftsaggregatet kan konstateras att t ex förbrukning av media kan röja kapacitet och i och med det förmåga vilket kan vara känsligt för vissa verksamheter. Det gör att vissa myndighetsrapporteringar kan vara svåra att göra.

Beakta att aggregerade informationsmängder ofta kan medföra en högre klassning.

Avveckling



Under avvecklingsskedet av ett byggnadsverk är det kanske i första hand krav på riktighet och tillgänglighet som är avgörande för en bra hantering och möjligheter för demontering, återbruk och återvinning.



FIGUR 14 ▪ Exempel på informationskartläggning för avvecklingsskedet.

4

4. It-miljön

Utkontraktering av it-drift och andra it-relaterade tjänster skapar både möjligheter och risker i samhället. Nya leveransformer kan vara ett sätt att öka kvaliteten och sänka kostnaderna i en verksamhet, men de kan också leda till en ökad koncentration av it-drift som innebär att flera aktörer kan komma att drabbas samtidigt av en incident och att konsekvenserna för samhället kan bli allvarliga.

Information samlas i olika databaser och hanteras i ett antal olika system under byggnadsverkets livscykel och det är väsentligt att ta kontroll över samtliga dessa databaser och system. Lösningar där man köper infrastruktur och system som tjänster och där data lagras i molnet är mer och mer vanliga ställer än högre krav på en strategi kring säkerhets- och informationssäkerhetsfrågor.

On-premise, innebär att IT system körs på bestämd hårdvara på en bestämd plats till skillnad från i molnet. Det är vanligtvis i ägarens lokaler men det kan också vara på annan plats men på en bestämd hårdvara som ägaren helt eller delvis förfogar över.

När affärssystemet ligger på egen eller hyrd server har det egna företaget full kontroll av sitt data och tar även ansvar för risker och säkerhet. Löpande underhåll, att köra uppdateringar, patchar och säkerhetskopior för att säkerställa stabilitet och åtgärda fel är företagets ansvar och det kräver både resurser och tekniskt kunnande.

Företaget har kostnader för att köra mjukvara och hårdvara och ofta en underhållsavgift till systemleverantören. En anledning till att välja detta alternativ kan vara att möjligheten att skräddarsy mjukvaran är enklare. Det är dock alltid en standardmjukvara som är grunden. Anpassningar av denna medför kostnader och kommande uppdateringar som senare är nödvändiga blir då svårare och dyrare.

Med den här modellen har företaget all sin data i sitt eget datacenter. Det kan göra det enklare att följa lagstadgade dataskyddsregler eftersom molnservrar finns i länder med olika dataskyddsregler.

Molnbaserade lösningar

Lösningar där man köper infrastruktur och system som tjänster och där data lagras i molnet kan ge en flexibel lösning men i samband med det måste informationssäkerheten beaktas. Det finns också olika varianter och nivåer av molnbaserade lösningar att ta hänsyn till.

Den kortaste beskrivningen av molnbaserade affärssystem är kanske att det är affärssystem som tillhandahålls över internet. Att det finns fördelar i form av reducerade kostnader för exempelvis hårdvara och minskat behov av egen it-kompetens och drift.

Men är alltid ett affärssystem som hålls tillgängligt över internet ett molnbaserat affärssystem?

Bakom den webbläsare som används för att jobba i ett system kan ligga ett ganska traditionellt affärssystem som är installerat på en egen eller hyrd server och driftas av det egna företaget eller av en IT driftleverantör.

Olika typer av molntjänster privat moln, publikt moln och hybrid moln

I ett privat moln har det egna företaget fortfarande ansvar för datasäkerhet och alla tjänster.

Ett privat moln är molntjänster som erbjuds via internet eller privat internt nätverk och som enbart är tillgängligt för utvalda användare, inte för allmänheten. Det är anpassat efter en specifik verksamhets affärsbehov. Infrastrukturen och nätverket är privat och uteslutande till för den organisationen som utnyttjar tjänsten. Kostnaderna för personal och underhåll blir det samma som med traditionellt datacenter. Används ofta när säkerhet och tillgänglighet är viktigt.

Man kan ha ett privat moln hos extern leverantör exempelvis i ett fjärrserverkluster. Då kan man få flera av fördelarna med ett publikt moln men med mer datasäkerhet.

Ett publikt, delat eller offentligt moln är lite förenklat en samling servrar som står i stora datacenter, tillgängligt för alla som vill använda och/eller betala för det.

Det är molntjänstleverantören som ansvarar för skötsel och underhåll av systemen. Denna plattform är skalbar och kunden betalar för faktiskt förbrukning. Exempel på publika molntjänster är Microsoft Azure och Amazone Web Services. Resurser i ett publikt moln delas mellan kunder på samma hårdvara och nätverk. En attack mot en organisation på det publika molnet kan påverka andra som använder samma del av molnet. En nackdel med det publika molnet är att kunden inte alltid kan välja var deras data

ska lagras. Det kan vara ett problem om exempelvis kunden har bokföringskrav eller andra informationssäkerhetskrav som säger att deras data måste lagras i samma land som de är verksamma.

I augusti 2021 uppmärksammades att datahantering i videoverktyget Teams från Microsoft som ingår i Office 365 för företag kan strida mot EU:s Dataskyddsförordning GDPR och Sveriges offentlighets – och sekretesslagstiftning. Detta eftersom personuppgifter om användarna ligger lagrade på servrar i USA och vissa amerikanska myndigheter kan begära ut denna information. Vissa myndigheter har valt att använda alternativa verktyg som följer svensk lagstiftning.

Under november 2021 öppnade Microsoft ett datacenter i Sverige för kunder som köper tjänsterna Microsoft Azure och Office 365. Detta innebär att kunder i Sverige nu kan välja att behålla sin data i Sverige men det är oavsett fortfarande en molntjänst ägt av ett amerikanskt företag. Det är oklart om data i det här fallet är skyddad av svensk lagstiftning eller ej.

Ett hybridmoln eller hybrid molntjänst är en kombination av privat moln, sitt eget datacenter och/eller ett publikt moln. Anledning till att man kombinerar dessa kan vara för att optimera säkerhet och kostnader. Exempelvis kan affärskritisk information hanteras on-prem i egna servrar, annan mindre kritisk information i det privata molnet medan företagets webbplats kan ligga i det publika molnet.

Säkerheten är en angelägen fråga för alla som väljer att köra helt webbaserade system. Leverantörer som erbjuder helt webbaserade system är ansvariga för att skydda informationen.

Större molntjänstleverantörer har specialistkompetens kring it-säkerhet. Informationssäkerheten är därför ofta hög och leverantörerna erbjuder avancerade rutiner för säkerhetskopiering och processer för återställning av data. Men enskilda användaren har också ett ansvar vilket kan innebära att ha flerfaktorsautentisering, använda starka lösenord, inte dela information via offentliga nätverk och hålla sin it-miljö uppdaterad. System som inte uppdateras regelbundet är mer sårbara. När man använder sig av molntjänster uppdateras i de flesta fall både hård- och mjukvara regelbundet.

Driftsäkerheten är ofta hög för molnbaserade lösningar. Alla delar av systemet har backup, exempelvis har en server flera kopior i molnet. Om något havererar ersätts det omgående och driften kan fortsätta utan avbrott.

Olika distributionsmodeller för molntjänster

Den första modellen är *IaaS* – Infrastructure as a service – Infrastruktur som en tjänst. Företaget köper då infrastrukturresurser. Det är ofta en virtualiserad miljö som innefattar servrar, nätverk, lagring och säkerhet.

Den andra modellen är *PaaS* – Plattform as a service – Plattform som en tjänst. Det är en tjänst som ligger mellan IaaS – hårdvara och SaaS – mjukvara. Den innefattar operativsystem, databaser och programvara som ger utvecklare möjlighet att utveckla, bygga, testa och driftsätta applikationer.

Den tredje modellen är *SaaS* – Software as a service – Mjukvara som en tjänst. Då levereras applikationer till användare eller klienter över internet. Mjukvaran körs på leverantörens servrar som oftast ligger i det publika molnet.

Användaren når applikationen via en webbläsare och internet oavsett var man befinner sig. Drift, underhåll och uppdateringar sköts av leverantören. Några exempel på SaaS tjänster som många känner till och använder är Gmail som ligger i Googles moln, Office 365 som ligger i Microsofts moln, Netflix, Spotify och Facebook. Men även system för exempelvis CRM, Tidrapportering, Ekonomi, Personal och Fastighetssystem finns nu ofta att köpa som SaaS tjänst. Istället för att göra en större investering och köpa en mjukvara så prenumererar man på samma mjukvara och betalar en relativt låg månadskostnad.

Konfidentialitet, riktighet och tillgänglighet ingår i begreppet informationssäkerhet. Detta handlar om att endast behöriga personer får tillgång till information, att information inte ska kunna förändras eller förstöras av misstag eller av obehörig samt att informationstillgångar är tillgängliga för behöriga personer inom förväntad utsträckning och inom önskad tid.

För att som kund våga ta steget och använda sig av en molntjänst är det därför av stor vikt att veta vilka krav som behöver uppfyllas för att molntjänsten skall anses som säker utifrån ett informationssäkerhetsperspektiv.

Krav på konfidentialitet ska garantera att data som finns i molntjänsten inte kan nås av obehörig. Det handlar då om tjänster för nätverkssäkerhet, autentisering och kryptering.

Vad gäller riktighet/integritet så handlar det om att data inte har förändrats varken avsiktligt via en säkerhetsattack eller oavsiktligt av en användare. För att minska risken för dessa händelser används brandväggstjänster, kommunikationssäkerhet och intrångsskydd.

Begreppet tillgänglighet refererar till faktorer som skapar tillförlitlighet och stabilitet i nätverk och system. I begreppet ingår att behöriga användare ska komma åt system och nätverk när så önskas. Tillgänglighet är en av de viktigaste informationssäkerhetskraven för molntjänster och kan vara avgörande beslutsfaktor vid val av leveransmodell och typ av molntjänst.

För att försäkra sig om tillgänglighet används bland annat backuper, dubbletter av disksystem, säkerhetsprocesser och nätverkssäkerhetsmekanismer.

Systemstruktur

Det är nu tydligt att det förmodligen inte finns någon organisation som klarar sig med endast ett system. Det finns alltid behov som går utanför det stora eller mindre affärssystemet.

Många organisationer förändras genom förvärv och omorganisationer och det leder till att nya externa applikationer kommer in i organisationen. I samband med att molnet har introducerats har många molnbaserade applikationer blivit tillgängliga på marknaden vilket innebär en snabbare uppstart och möjlighet att använda en applikation utan en stor investering.

Fördelen med mer heltäckande system kan vara att man får ökad funktionalitet, att informationen hänger ihop bättre, att det är flexibelt och skalbart, att man har färre system som ska driftas och integreras med varandra samt och att man har färre systemleverantörer att hålla reda på.

Nackdelar kan vara att vissa funktioner inte är så bra vilket innebär kompromisser och ett sämre stöd till verksamheten eller många anpassningar som är svåra och dyrbara att underhålla. Nackdelen är också att ”alla ägg samlas i samma korg” och att det i och med det finns en sårbarhet i lösningen.

Vill man ha de bästa systemen för varje funktion i verksamheten kan en “Best-of-breed” strategi vara bra då man använder olika nischade system. Varje system utgör en delmängd av ett komplett verksamhetssystem och gör då färre saker men kan göra det bättre. Utmaningen kan vara att få dem att fungera tillsammans men det kan underlättas med en integrationsplattform. Med modern webbteknik kan det gå enklare, och ibland billigare, att skapa integrationer som utbyter information mellan system. Om man har designat för att ha en integrerad ”best of breed”-modell så har man byggt in flexibilitet i sin arkitektur, vilket i sig kan göra att man blir mindre sårbar för t.ex. intrångsattacker.

En relationsdatabas består av flera tabeller med delvis överlappande information. Detta har länge varit den vanligaste typen av databas i professionella sammanhang. Istället för att ha all information i en enda stor tabell delas informationen upp i flera tabeller. Man har ex en tabell för Kundinformation, en tabell med information om Order och en tabell med Orderrader. Den överlappande informationen kan då vara Kundnummer och Ordernummer. En kund kan ha flera order och en order kan ha flera orderrader. Fördelen är att tabeller kan samköras på olika sätt, data lagras bara på ett ställe och behöver därför bara ändras på ett ställe. Det är också lätt att lägga till ny information genom att lägga till en ny tabell.

Man söker ofta i relationsdatabaser med hjälp av frågespråket SQL. Därför kallas ofta relationsdataser för SQL databaser. Den här typen av databas lämpar sig bäst för information som går att lagra i tabeller, lämpar sig inte för bilder, musik eller websidor.

Nätverkssegmentering

Det är varken praktiskt eller ekonomiskt försvarbart att skydda all information på samma sätt och ett sätt att öka både säkerhet och prestanda i sin datamiljö är att dela upp sitt nätverk i olika delnätverk eller segment som har minsta möjliga kontakt med andra delar av nätverket. Nätverkssegmentering begränsar skadan vid en cyberattack. Utan segmentering finns det risk att känslig information kan läckas eller manipuleras samt att malware och ransomware sprider sig okontrollerat och snabbt.

Segmentering kan nås genom en kombination av fysisk och logisk separation. Fysisk separation innebär att säkerhetszoner definieras och fördelas på olika fysiska hårdvaror. Logisk separation innebär att olika zoner eller nätverkstrafik tillåts samexistera på samma hårdvara eller i samma nätverkskabel vilket gör den mindre tydlig och därmed medför lägre förtroende för separationsmekanismens styrka än vid fysisk separation.

Den mest skyddsvärda informationen kräver fysisk separation vilket innebär att man skapar en isolerad ö utan koppling till omvärlden. Detta minimerar risken för angrepp eftersom ingen uppkoppling finns mot den isolerade ön men det medför utmaningar kopplat till tillgänglighet och på sikt även riktighet vilket gör att man måste tillse att ett kontrollerat informationsutbyte kan ske utan att göra avkall på isoleringen. Här finns det certifierade lösningar som gör att man kan uppnå både funktion och säkerhet.

Logisk separation kan användas för det mesta utom just för den mest skyddsvärda informationen. Verksamhetens olika delar kan ha olika segment – förvaltning, projekt, ekonomi etc. – med olika behörighet. Som medarbetare har man bara tillgång till det som rör ens eget jobb. Man når t ex relevanta dokument men inte hela mappstrukturen.

Alla segmenten fungerar som ett gemensamt nätverk men tekniskt sett är det separata lokala nätverk. Attacker riktar sig inte alltid direkt mot målet, till exempel styr- och övervakningssystemet. Ofta sker de mot svaga punkter långt ute i arkitekturen, via mejl eller kundtjänst, för att sen ta sig vidare till målet. Genom logisk separation byggs inre murar vilket minskar risken för att attacker och skadliga program når hela it-miljön, se bilaga 3.

Lokalt eller på distans

En organisation kan ha sin IT infrastruktur lokalt eller på distans. Många organisationer har stävat efter att ha så lite IT infrastruktur som möjligt lokalt men vad medför det.

Varje anställd får en dator, oftast en bärbar en telefon och kanske några tillbehör. Men allt annat som programvara, servrar, affärsapplikationer mm ligger i molnet eller i extern serverhall. Några av de stora fördelarna med detta är att man som företag inte behöver oroa sig för om en server behöver uppgraderas eller en hårddisk bytas ut. Leverantören som är värd för företagets servrar eller programvara är ansvariga för att hantera drift, underhåll och säkerhet.

Om företagets servrar står i en extern serverhall kan de fortfarande ligga inom företagets lokala nätverk och programvaran kan då hanteras som en on-premise installation. När de anställda arbetar hemifrån används alltid en VPN uppkoppling för åtkomst till applikationer men när de anställda är på kontoret används en trådlös Wifi eller nätverkssladd. Den externa leverantören är ansvarig för drift och säkerhet på servrar och nätverk men den egna personalen ansvarar för underhåll och utveckling av applikationerna. I de fall företaget har valt att köra hela eller delar av sin IT infrastruktur som SaaS-tjänster via internet är det leverantören av SaaS tjänsten som ansvarar för drift, underhåll och säkerhet. Som kund betalar man endast för användning av tjänsten.

Redundans – alternativa driftställen

Vid höga krav på säkerhet och tillgänglighet kan det för många organisationer vara viktigt att ha en speglad datamiljö, ett alternativt driftställe även kallad en tvillinghall för att öka säkerheten och för att kunna garantera en hög servicenivå. En tvillinghall innebär att man har en komplett kopia av sitt it-nätverk och datamiljö på annan plats. Information som lagras i systemet i den ordinarie datamiljön finns också i tvillinghallen. Om något skulle hända som gör att datamiljön i ordinarie datamiljö är oåtkomlig kan personalen logga in i tvillingmiljön där man har redundant data. Behovet av en speglad miljö beror på hur höga krav man har på tillgänglighet. I många fall kan backuper och återläsning av data vara tillräcklig lösning.

De flesta verksamheter är idag beroende av internetuppkoppling och får stora problem om den inte fungerar. En lösning kan vara att ha redundant internet förbindelse. Redundans i detta fall innebär att företaget har tillgång till dubbla internetanslutningar med olika fysiska framföringsvägar, den ena är aktiv och den andra är passiv. Om den primära anslutningen drabbas av problem flyttas trafiken till den sekundära. Redundansen blir som en försäkring för att verksamheten ska kunna fortsätta även vid avbrott i internetuppkoppling.

Följande punkter vara en grund att förhålla sig till:

- Installera säkerhetsuppdateringar så fort det går
- Förvalta behörigheter och använd starka autentiseringsfunktioner
- Begränsa och skydda användningen av systemadministrativa behörigheter
- Inaktivera oanvända tjänster och protokoll (härda systemen)
- Gör säkerhetskopior och testa om informationen går att läsa tillbaka
- Tillåt endast godkänd utrustning i nätverket
- Säkerställ att endast godkänd mjukvara får köras (vitlistning)
- Segmentera nätverken och filtrera trafiken mellan segmenten
- Uppgradera mjuk- och hårdvara
- Säkerställ en förmåga att upptäcka säkerhetshändelser

5. Organisation, personalsäkerhet och fysisk säkerhet

Organisation, utbildning och beteenden

Den svagaste länken är ofta vi som enskilda personer så vikten av ökade medvetenhet kan inte nog poängteras. Att utbilda både personal och leverantörer i säkerhetsfrågor är en bra investering.

Utbildning tydliggör att säkerhet är allas ansvar och omfattar bland annat regler för korrekt hantering av information, säker hantering av it-resurser, säker hantering av utomstående besökare, allmänt säkerhetsmedvetande och säkert beteende.

Exempel på frågor att lyfta fram:

- Information eller utrustning lämnas aldrig utan uppsikt, till exempel på tåg, i bilar, på hotellrum eller på restauranger.
- Känslig information diskuteras aldrig på offentliga platser, till exempel i telefonsamtal.
- Information ska skickas med eftertanke. Ett e-postmeddelande är inte säkert.
- Åtkomsten till olika it-system begränsas genom behörigheter och roller.
- Lösenord och koder hålls alltid privata.
- Nycklar, kort och personliga tillhörigheter förvaras på en säker plats.
- Principen ”rent skrivbord och tom bildskärm” tillämpas.

Distansarbete – publika nät, hemnätverk med sämre skydd, mobilitet

Informationssäkerhet är något som blivit extra aktuellt när många arbetar hemifrån. Distansarbete ställer krav på säkerhet, det är viktigt att tänka på att all information måste hanteras på ett säkert sätt även när man inte sitter på kontoret utan är uppkopplad via ett hemmanätverk. För att minska risker vid distansarbete behöver alla medarbetare ta reda på vilka rutiner som gäller för sin specifika organisation. Detta för att information inte ska bli tillgänglig för obehöriga, förstöras eller bli felaktig. Ett hemmanätverk kan av olika anledningar ibland vara osäkert. Därför kan det vara ett krav att man ska använda en VPN lösning och/eller tvåfaktorsautentisering. Tvåfaktorsautentisering innebär att ett lösenord inte räcker för att visa vem du är, ytterligare en bekräftelse behövs för att kunna logga in och det kan då vara med hjälp av ett sms eller en app. Det är alltid viktigt att alla användarkonton har säkra lösenord. Det kan ibland finnas krav på att man kopplar upp sig via mobilen och enbart använder mobildata i stället för det egna Wifi man har hemma.

Viktigt att arbetsutrustning så som dator, telefon eller surfplatta inte används för privat bruk. Denna utrustning är personlig och ska inte användas av någon annan. Därför bör man logga ut och stänga av sin dator när den lämnas.

Att koppla upp sig på att öppet/gratis Wifi som man kan hitta på flygplatser, caféer, hotell eller liknande kan vara en säkerhetsrisk. Det kan då vara viktigt att använda en VPN (Virtual private network). En VPN anslutning är en teknik som används för att skapa en krypterad säker förbindelse. Ett alternativ kan också vara att surfa från mobilen, alternativt koppla mobilens internet till sin dator i stället för att använda ett öppet/gratis Wifi. En bra regel är att aldrig logga in på sin internetbank eller andra känsliga konton eller appar när man är uppkopplad på ett öppet Wifi.

Externa leverantörer

Det finns en risk att leverantörer har sämre skydd och säkerhetstänk än beställarorganisationen varför informationsläckage/angrepp på leverantörer har blivit allt vanligare. Så kallade leveranskedjeangrepp är en företeelse där attacker i form av skadlig programvara eller liknande installeras via betrodda leverantörskanaler.

Det är därför viktigt att kontrollera sina leverantörer och säkerställa att de har samma kunskap och rutiner som den beställande organisationen. Samtliga samarbetspartners och leverantörer som har tillgång till konfidentiell information bör omfattas av sekretessavtal som tydliggör regler och ansvar för hantering av information. Tillse även att leverantörer är utbildade i säkerhetsskydd.

Fysisk säkerhet

Hot mot it-lösningar kan även ske genom fysiska angrepp eller incidenter varför lokalfrågorna också är viktiga.

Tillse att lokaler är tillträdesskyddade och att det finns detektering för olika händelser genom sensorer och larm som brandlarm och inbrottslarm. Rutiner behöver också finnas för hantering av besökare. Beakta också sektionering av lokaler så att t ex besökare inte kan röra sig i delar där känslig information hanteras.

För mer information hänvisas till Säkerhetspolisens vägledning kring fysiskt skydd: https://www.sakerhetspolisen.se/sakerhetsskydd/vagledningar-sakerhetsskydd.html

6

6. Redogörelse över praktiska användarfall

Processorienterad informationskartläggning inom Region Gävleborg

Region Gävleborg har genomfört en processorienterad informationskartläggning över hela regionen som en del i ett större pågående arbete med att utveckla informationsförvaltning inom regionen.

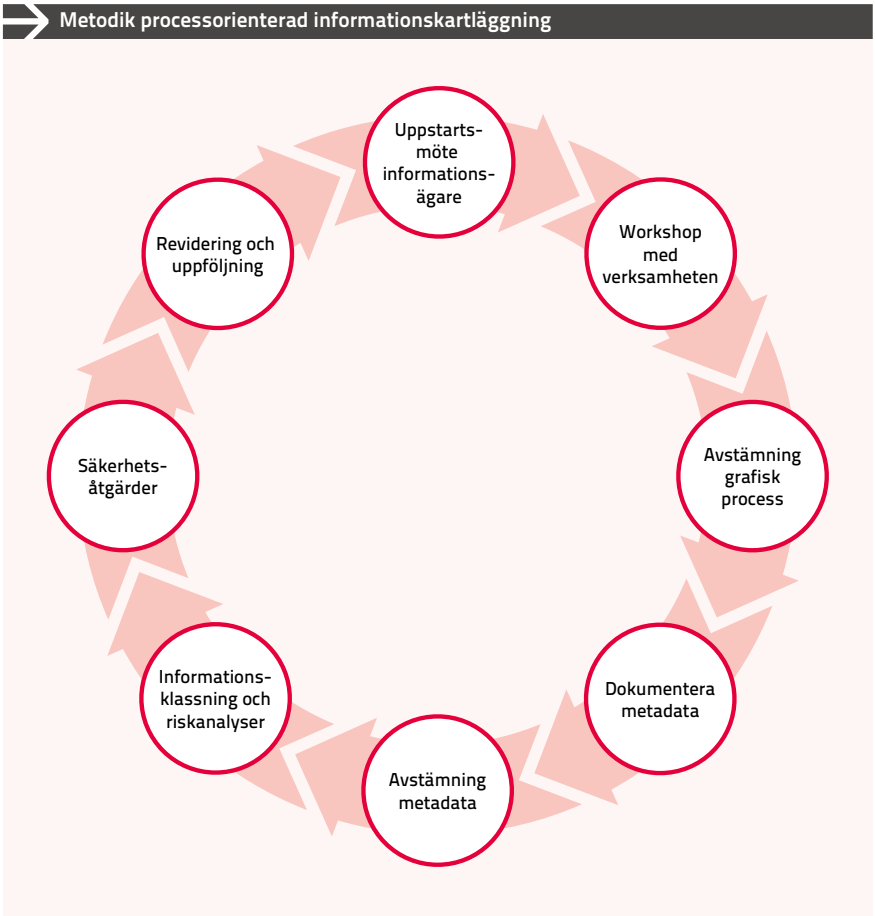
Regionen har tagit avstamp i MSB/RA:s vägledning och Informations-KLASSA:s klassificeringsstruktur med vissa anpassningar. Metodiken har sedan vidareutvecklats för att inkludera perspektiven:

- registratur
- informationssäkerhet
- dataskydd
- regionarkiv

Funktionerna har ett gemensamt mål, det vill säga att ha en god överblick över den information som finns och att informationens konfidentialitet, riktighet och tillgänglighet garanteras och skyddas. Det är en utmaning att tillgodose den egna verksamheten och omvärldens behov av informationsförsörjning, och samtidigt vidmakthålla den enskildes rättigheter och integritet. Detta kan i vissa fall vara motstridiga intressen.

Arbetet är genomfört med ett huvudsakligt fokus på en regions administrativa processer och har inte gått på djupet när det gäller information för byggnader.

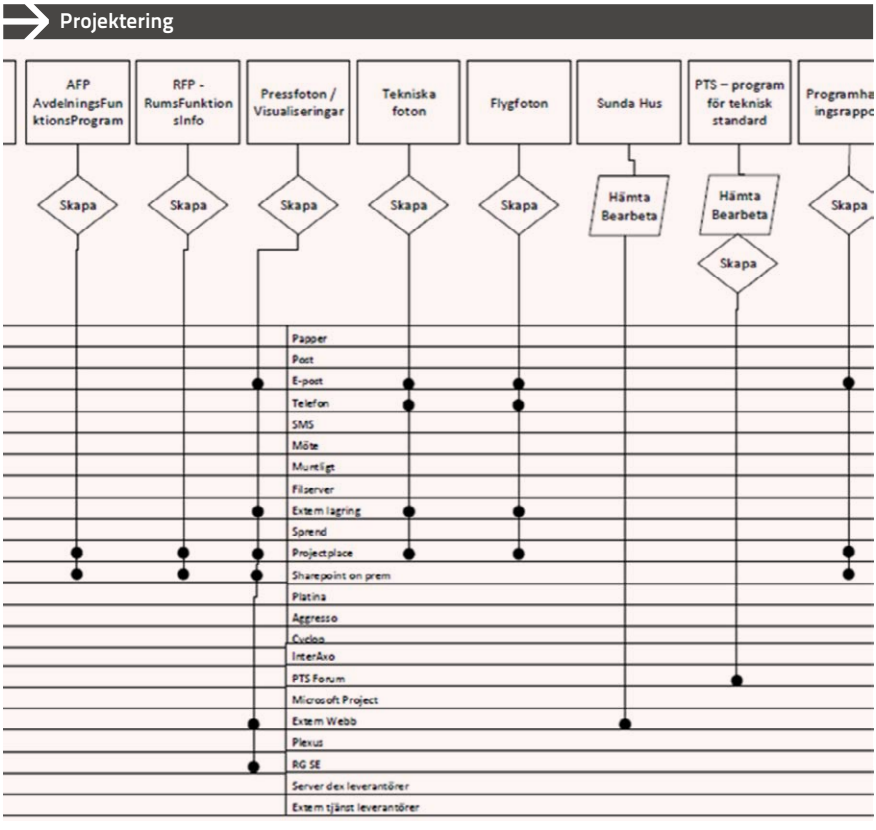
Det är dock viktigt att poängtera att varje verksamhet har ett behov av att göra motsvarande kartläggning vilket inte nog kan understrykas. Inte minst mot bakgrund av att merparten av den offentliga organisationens verksamhetsinformation utgör allmänna handlingar vilket förutsätter en god informations-förvaltning, och en god informationsförsörjning förutsätter att både information och informationsbärare som hanteras i organisationen är identifierade.



FIGUR 15 ▪ Metodik för processorienterad informationskartläggning inom Region Gävleborg.

En erfarenhet från regionen, som känns igen från flera sammanhang, är att det är utmanande att tänka information och informationsbärare. Den process som regionen arbetade fram införlivade de fyra perspektiven som beskrevs inledningsvis som alla har gemensamt att utgå utifrån informationen. Det gjorde samtidigt att det blev en rad synergier när samma informationsmängd analyseras utifrån olika perspektiv vid ett tillfälle istället för fyra. Erfarenheten säger dock att bara för att en informationsmängd analyseras utifrån ett dataskyddsperspektiv betyder det inte med självklarhet att den också analyseras utifrån ett informationssäkerhetsperspektiv, arkivperspektiv eller kontinuitetsperspektiv.

Tidigt tas det fram en ”ritning” av processen som ger den en notation, beskriver lagrum, aktiviteter, informationsmängder och informationsbärare.



FIGUR 16 ▪ Exempel på processorienterad informationskartläggning för projekteringsskedet.

Ritningen blir ett bra diskussionsunderlag för det fortsatta analysarbetet då det skapar en tydlighet och att alla deltagare får samma bild att referera till.

Kopplat till detta görs också en dokumentation av processen som beskriver informationsägare, typ av handling, gallring, arkivering, sekretess (referens till OSL), förekomst av personuppgifter osv. Tillvägagångssättet innebär också att regionen ser i vilka sammanhang en och samma informationsmängd förekommer vilket underlättar informationsklassning. Det blir också tydligt vad breda informationsbärare, exempelvis e-post, får för aggregerad informationsklassning. Just exemplet e-post, där det sannolikt finns en begränsning för vilka skyddsåtgärder som kan påföras, leder till att den inte kan bära information med exempelvis konfidentialitet högre än **måttlig (1)**.

Metodiken rätt tillämpad gör att informationsbärare som inte lämpar sig för en viss informationsmängd kan identifieras och hanteras. Sammantaget innebär metodiken inte bara att det vardagliga informationssäkerhetsarbetet förbättras då metodiken syftar till att naturligt väva in arbetet i verksamheten, det ger också indirekta effekter där olämpliga tillvägagångssätt kan identifieras och hanteras som i exemplet ovan.

Bilaga 1 – Exempel på informations-klassning

Nedan finns några exempel på informationsklassning som kan ge input till hur man bör resonera som fastighetsägare. Informationsklassningen utgår från de tre områdena:

- **Konfidentialitet** – Vad blir skadan om informationen hamnar i orätta händer?
- **Riktighet** – Vad blir skadan om informationen inte är korrekt?
- **Tillgänglighet** – Vad blir skadan om informationen inte är tillgänglig?

Vid bedömning har konsekvensnivåerna använts.

- Synnerligen allvarlig skada (4)
- Allvarlig skada (3)
- Betydande skada (2)
- Måttlig skada (1)
- Försumbar skada (0)

Vi kan konstatera att klassningen för de flesta attribut varierar beror på vilken typ av byggnad det är och hur den används, dvs vilken typ av verksamhet som bedrivs i byggnaden. Om det till exempel är ett bostadshus är klassningen generellt i det lägre spannet då informationen inte är att betrakta som känslig medan en ledningscentral naturligtvis får en betydligt högre klassning. Samlade informationsmängder kan förändra klassningen varför man även måste göra en bedömning av hela informationsmängden.

Exempel på informationsklassning finns även i Bilaga 2 – Lagar, regelverk och standarder.

Byggnadsverk				
Information	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**	**Kommentar**
ID – UUID	0	1–2	1	Koppling till andra databaser ger klassning
Benämning	0–1	0	0	
Ägare	0	0	0	
Fastighetstillhörighet	0	1	1	
Areor	0	1	1	Underlag för beslut
Adresser	0–3	1	1	Beroende på verksamhet
Koordinater	0–3	1	1	Beroende på verksamhet
Klassning - CoClass	0–3	1	1	Beroende på verksamhet
Status	0	1	1	
Byggår	0	1	1	
Ansvar	0	1	1	

TABELL 6 ▪ Exempel på informationsklassning av byggnadsverk.

Klassning av byggnadsverk beror naturligtvis på vilken typ av verksamhet som bedrivs i byggnaden. Vi har här valt att titta på några informationsegenskaper och kan konstatera att klassningen för de flesta attribut beror på vilken typ av byggnad det är och hur den används. Att beakta är att den samlade informationsmängden om byggnadsverket kan förändra klassningen.

Vägledning avseende klassningsnivå – Konfidentialitet

Klassning avseende konfidentialitet beror på vilken verksamhet som bedrivs. En generell regel kan vara att undvika att ange benämning/användning och bara använda ett neutralt ID som har klassning **försumbar (0)**. Benämning/användning och annan information bör separeras från ID för att underlätta en praktisk hantering.

Vägledning avseende klassningsnivå – Riktighet

Även klassning avseende riktighet varierar och beror även här på vilken verksamhet som bedrivs men generellt kan konstateras att det är viktigt att korrekt information men att skadan ändå bedöms som måttlig även om den skulle kunna vara betydande i vissa fall.

Vägledning avseende klassningsnivå – Tillgänglighet

Tillgänglighet till information är delvis kopplat till riktighet men klassas något lägre då det ofta går att få tag på informationen även om det ibland kan kräva mer tid.

Information kring utrymmen

Klassning av utrymmen, eller rum, beror naturligtvis på vilken typ av utrymme som avses och vilken verksamhet som bedrivs i utrymmet eller i byggnaden. Vi har valt att titta på några informationsegenskaper och kan konstatera att klassningen för de flesta attribut beror på vilken typ av utrymme det är.

Utrymmen

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
ID	0	1–2	1	
Benämning	0–3	1–2	1	Beror på rum
Area	0	2	1	
Dimensionerande värden	0–2	0–3	0–3	Beror på rum
Skydd	2–3	2–3	1–3	Beror på rum
Säkerhetsklass	3–4	2–3	1–2	
Hygienklass	1	3	0–2	Verksamhet
Material – ytskikt	0–1	1	0–1	
Försörjning	3–4	3–4	3–4	

TABELL 7 ▪ Exempel på informationsklassning av utrymmen.

Vägledning avseende klassningsnivå – Konfidentialitet

Klassning avseende konfidentialitet beror på vilket utrymme som avses och här måste också tas hänsyn till hela byggnaden. En generell regel kan vara att undvika att ange benämning/användning och bara använda ett neutralt ID som har klassning **försumbar (0)**. Benämning/användning och annan känslig information kan separeras från ID för att underlätta en praktisk hantering.

Vägledning avseende klassningsnivå – Riktighet

Även klassning avseende riktighet varierar och beror även här på vilken verksamhet som bedrivs men generellt kan konstateras att skadan kan bli relativt stor om vi inte ha korrekt information.

Vägledning avseende klassningsnivå – Tillgänglighet

Tillgänglighet till information är delvis kopplat till riktighet men klassas något lägre då det ofta går att få tag på informationen även om det ibland kan kräva mer tid.

Information om tekniska system

Olika tekniska system klassas på olika sätt och även här är det naturligtvis beroende på vilken verksamhet som bedrivs i byggnadsverket varför klassningen kommer att se olika ut för varje byggnadsverk.

Tekniska system

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Mark och grund	1	1	1	
Väggar	1–3	1	1	
Bjälklag	1–3	1	1	
Yttertak	1–3	1	1	
Gas och luft	2	2	2	
Vatten och vätska	2	2	2	
Avlopp och avfall	1	1	1	
Kyla och värme	2	2	2	
Luftbehandling	2	2	2	
Elkraft	2–3	2–3	2	
Belysning och dagsljus	1	1	1	
Automation	2–3	2–3	2	
Information och kommunikation	2–3	2	2	
Transport	1	1	1	
Säkerhet och skydd (larm)	3	3	3	
Utrustning	0	0	0	

TABELL 8 ▪ Exempel på informationsklassning av olika tekniska system.

Attribut tekniska system

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
ID	0	1-2	1	
Benämning	0	0	0	
Placering	1-3	2	2	
Betjäning	1-3	2	2	
Installationsdatum	0	0	0	

TABELL 9 ▪ Exempel på informationsklassning av attribut för tekniska system.

Vägledning avseende klassningsnivå – Konfidentialitet

Klassning avseende konfidentialitet beror på vilket system som avses och här måste också tas hänsyn till hela byggnaden och den verksamhet som bedrivs.

Vägledning avseende klassningsnivå – Riktighet

Även klassning avseende riktighet varierar och beror även här på vilket system som omfattas. De system som omfattar installationer och hanterar media och de som ska styras klassas högre än de som omfattar bygg. Skadan vid t ex läckage kan bli relativt stor om vi inte ha korrekt information.

Vägledning avseende klassningsnivå – Tillgänglighet

Tillgänglighet till information är delvis kopplat till riktighet men klassas något lägre då det ofta går att få tag på informationen även om det ibland kan kräva mer tid.

Komponenter

Klassning av komponenter beror också på vilken typ av komponent det är, till vilket tekniskt system den är kopplad och naturligtvis även vilken verksamhet som bedrivs i byggnaden. Vi har här valt att titta på några informationsegenskaper och kan konstatera att klassningen för de flesta komponenter varierar beroende på byggnadsverk. Även här kommer den samlade informationsmängden kring tekniska system och byggnadsverk att förändra klassningen.

Komponenter				
Information	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**	**Kommentar**
ID	0	1–2	1	
Benämning	0	0	0	
Klass – CoClass, AFF etc	0	2	2	
Placering	1–3	2	2	
Betjäning	1–3	2	2	
Kapacitetsuppg	1–3	2	2	
Installationsdatum	0	0	0	
Garantitid	0	1	1	
Förv. livslängd	0	0	0	
DoU-information	1	1	2	
Tillverkare	0	1	1	

TABELL 10 ▪ Exempel på informationsklassning av komponenter.

Vägledning avseende klassningsnivå - Konfidentialitet

Klassning avseende konfidentialitet beror på vilken verksamhet som bedrivs. En generell regel kan vara att undvika att ange benämning/användning och bara använda ett neutralt ID som har klassning **försumbar (0)**. Tillhörighet och annan information bör separeras från ID för att underlätta en praktisk hantering. Uppgifter om placering, betjäning samt kapacitetsuppgifter är det som klassas högre och hamnar i spannet **måttlig (1)** till **allvarlig (3)** beroende på typ komponent och verksamhet.

Vägledning avseende klassningsnivå - Riktighet

Även klassning avseende riktighet varierar och beror även här på vilken komponent som avses. De komponenter som tillhör tekniska installationssystem och hanterar media eller ska styra flöden klassas högre än de som omfattar bygg. Skadan vid t ex läckage kan bli relativt stor om vi inte ha korrekt information.

Vägledning avseende klassningsnivå - Tillgänglighet

Tillgänglighet till information är delvis kopplat till riktighet och klassas motsvarande. De komponenter som tillhör tekniska installationssystem och hanterar media eller ska styra flöden klassas högre än de som omfattar bygg. Skadan vid t ex läckage kan bli relativt stor om vi inte har tillgång till korrekt information.

Tillsyn av reservkraftsaggregat

Reservkraftsaggregat är centrala för många verksamheter och ska hanteras i processerna Tillsyn (i form av provkörning), Skötsel, Underhåll. Myndighetsbesiktningar.

Provkörning behöver ske regelbundet och utföras av behörig personal.

Tillsyn reservkraftsaggregat

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Planerad åtgärd	1	2	2	För berörda
Objekt	3–4	2	2	
Anmärkning – ger felanmälan	3	3	3	Kan avslöja kapacitet
Tidpunkt	1–2	2	2	
Rutiner/beredskap	3	3	3	
Utförare	0–1	1	1	Extern part kontrollerad

TABELL 11 ▪ Exempel på informationsklassning av tillsyn för ett reservkraftsaggregat.

Vägledning avseende klassningsnivå – Konfidentialitet

Information om provkörning av ett aggregat klassas olika beroende på vilken information det är. Klassning av tidpunkten för utförandet kan vara **måttlig (1)** eller **betydande (2)**. Utförare klassas som **försumbar (0)** eller **måttlig (1)** under förutsättning att extern part är kontrollerad.

Information om aggregatet klassas som **allvarlig (3)** eller **synnerligen allvarlig (4**) eftersom det ger uppgifter om kapacitet. Även anmärkningar och rutiner/beredskap klassas högt **allvarlig (3)** eftersom det ger information om hantering av eventuella brister och hur de hanteras.

Vägledning avseende klassningsnivå – Riktighet

Information om riktigheten i den planerade åtgärden klassas som **betydande (2)** då det till stor del kan påverka verksamheten. Klassning av tidpunkten för utförandet är på motsvarande sätt **betydande (2)**. Utförare klassas som **måttlig (1)** under förutsättning att extern part är kontrollerad.

Information om aggregatet klassas som **betydande (2)** eftersom det är viktigt med uppgifter om kapacitet. Anmärkningar och rutiner/beredskap klassas högt **allvarlig (3)** eftersom det ger information om hantering av eventuella brister och hur de hanteras.

Vägledning avseende klassningsnivå – Tillgänglighet

Information om tillgänglighet till informationen klassas även den som **betydande (2)** då det till stor del kan påverka verksamheten. Klassning av tidpunkten för utförandet är på motsvarande sätt **betydande (2)**. Tillgänglighet till information utförare klassas som **måttlig (1)**.

Tillgänglighet till information om aggregatet klassas som **betydande (2)** eftersom det är viktigt med uppgifter om bland annat kapacitet. Tillgänglighet till anmärkningar och rutiner/beredskap klassas högt **allvarlig (3)** eftersom eventuella brister måste åtgärdas samt att rutiner måste finnas tillgängliga.

Miljörapportering av reservkraftsaggregat

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Miljöbelastning	3–4	1	0	
Förbrukning	3–4	1	0	Mängder avslöjar förmåga
Objekt	3–4	2	2	

TABELL 12 ▪ Exempel på informationsklassning av miljörapportering för ett reservkraftsaggregat.

Vägledning avseende klassningsnivå – Konfidentialitet

Information om aggregatet samt rapportering av mängder klassas som **allvarlig (3)** eller **synnerligen allvarlig (4)** eftersom mängder ger uppgifter om kapacitet.

Vägledning avseende klassningsnivå – Riktighet

Information om aggregatet klassas som **betydande (2)** eftersom det är viktigt med uppgifter om kapacitet.

Vägledning avseende klassningsnivå – Tillgänglighet

Information om tillgänglighet till informationen klassas även den som **betydande (2)** då det till stor del kan påverka verksamheten. Klassning av tidpunkten för utförandet är på motsvarande sätt **betydande (2)**.

Felanmälan reservkraftsaggregat				
Information	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**	**Kommentar**
Anmälare	0	0	0	
Ärende	3	3	3	
Utförare	0–1	1	1	Extern part kontrollerad
Tidpunkt	1	1	1	
Objekt	3–4	2	2	

TABELL 13 ▪ Exempel på informationsklassning av felanmälan för ett reservkraftsaggregat.

Vägledning avseende klassningsnivå – Konfidentialitet

Information om aggregatet klassas som **allvarlig (3)** eller **synnerligen allvarlig (4)** eftersom t ex mängder ger uppgifter om kapacitet. Även ärendet klassas högt, **allvarlig (3)**, eftersom det kan avslöja en brist.

Vägledning avseende klassningsnivå – Riktighet

För att kunna åtgärda ett fel korrekt är det viktigt med en korrekt beskrivning av felet varför det klassas som **allvarlig (3)**.

Vägledning avseende klassningsnivå – Tillgänglighet

På motsvarande sätt är det viktigt att ha tillgång till felorsak för korrekt bedömning och åtgärdande av felet varför tillgänglighet till informationen klassas som **betydande (2)**.

Planerat underhåll av reservkraftsaggregat

Information	Konfidentialitet	Riktighet	Tillgänglighet	Kommentar
Planerad åtgärd	1	2	2	
Objekt	3–4	2	2	
Kostnad	3	1	1	Kan avslöja kapacitet
Tidpunkt	1	1	1	
Mängd	2	1	1	Kan avslöja förmåga
Utförare	0–1	1	1	Extern part kontrollerad

TABELL 14 ▪ Exempel på informationsklassning av planerat underhåll för ett reservkraftsaggregat.

Vägledning avseende klassningsnivå – Konfidentialitet

Information om objektet aggregatet klassas som **allvarlig (3)** eller **synnerligen allvarlig (4)** eftersom mängder ger uppgifter om kapacitet. Även kostnad klassas högt, **allvarlig (3)**, eftersom kostnaden kan avslöja storlek på aggregat.

Vägledning avseende klassningsnivå – Riktighet

Information om objektet aggregatet klassas som **betydande (2)** eftersom det är viktigt med korrekta uppgifter vid det planerade underhållet.

Vägledning avseende klassningsnivå – Tillgänglighet

Information om tillgänglighet till informationen klassas även den som **betydande (2)** då det till stor del kan påverka utförandet.

Bilaga 2 – Lagar, regelverk och standarder

Det finns en rad regulatoriska krav på informationssäkerhet som påverkar hur informationen klassificeras.

SS-ISO/IEC 27001/2 är bärande för informationssäkerhetsarbetet likaså definitionerna i SIS-TR 50 Terminologi för informationssäkerhet men det finns också andra intressanta standarder som SS-EN ISO 19650-5:2020, ”Principer och krav för ett säkerhetsmedvetet tillvägagångssätt” att beakta.

Ett initiativ att beakta och dela information med är Regeringsuppdraget ”Uppdrag om enhetliga digitala processtöd och gemensamma rutiner för medverkan i samhällsplaneringen”.

Informationssäkerhetsfrågor hanteras även i andra initiativ som:

- Nationella Riktlinjer – livscykelinformation för byggd miljö,
- SKR’s verktyg för klassning, KLASSAv4, samt
- MSB och Riksarkivets Vägledning för processorienterad informationskartläggning

Följande är exempel på regulatoriska krav som kan påverka informationssäkerheten:

- Säkerhetsskyddslagen (2018:585)
- Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174)
- EU:s dataskyddsförordning[13]
- Lagen med kompletterande bestämmelser till EU:s dataskydds-förordning (2018:218)
- Kamerabevakningslagen (2018:1200)
- Patientdatalagen (2008:355) (PDL)
- Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)
- Offentlighets- och sekretesslagen (2009:400)
- Upphovsrättslagen (1960:729)

Säkerhetsskyddslagen (2018:585)

Informationstillgångar som är av betydelse för Sveriges säkerhet är en indikator att informationstillgången omfattas av Säkerhetsskyddslagen (2018:585). Denna vägledning, och även KLASSA, avgränsas från informationstillgångar eller verksamheter som regleras av säkerhetsskyddslagstiftningen. KLASSA innehåller därför inte några förslag till skyddsåtgärder för dessa uppgifter eller verksamheter. Dessa informationstillgångar och verksamheter klassificeras enligt det regelverk som gäller för dem, exempelvis genom Militära underrättelse- och säkerhetstjänstens (MUST) krav på säkerhetsfunktioner (KSF) och den metodik som denna är förenad med. Säkerhetspolisens vägledning i säkerhetsskydd med fokus på informationssäkerhet ger också rekommendationer inom området.

En säkerhetsskyddanalys är det instrument som används för att identifiera om och i vilken utsträckning verksamheten är av betydelse för Sveriges säkerhet eller hanterar information som omfattas av Säkerhetsskyddslagen. Säkerhetsskyddsanalysen ska utreda behovet av säkerhetsskydd.

13. Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Med utgångspunkt i analysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetskyddsklassificerade uppgifter och övriga omständigheter. Säkerhetsskyddsåtgärderna delas in i tre delar, informationssäkerhet, fysisk säkerhet och personalsäkerhet.

Se vidare https://www.sakerhetspolisen.se/sakerhetsskydd.html

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen och kommande uppdateringen av NIS-direktivet)

NIS-lagen gäller för verksamheter inom någon av sektorerna

- energi,
- transport,
- bankverksamhet,
- finansmarknadsinfrastruktur,
- hälso- och sjukvård,
- leverans och distribution av dricksvatten, eller
- digital infrastruktur.

Lagen gäller för leverantörer som är etablerade i Sverige och där tillhandahållandet av tjänsten är beroende av nätverk och informationssystem (NIS) och att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

MSB har preciserat kriterierna för när en verksamhet omfattas av regelverket i Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7)[14].

NIS-lagen implementerar EU:s direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet). I slutet av 2020 presenterade EU-kommissionen ett förslag på ett nytt NIS-direktiv, kallat NIS 2. Syftet med det reviderade förslaget

14. https://www.msb.se/siteassets/dokument/regler/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf.

är att anpassa direktivet till nya och framtida behov. Förslaget har inte fastställts, utan har lämnats för beredning till rådet och EU-parlamentet. Om förslaget fastställs i dess nuvarande lydelse kommer NIS-lagen att behöva anpassas till förändringarna. NIS-regleringens tillämpningsområde kommer därmed att utökas till att även träffa bl.a.

- molntjänstleverantörer,
- statliga myndigheter, vissa regioner och enstaka kommuner,
- distributörer av fjärrvärme,
- företag inom avlopps- och avfallshantering och
- produktions- och tillverkningsindustri inom livsmedel, läkemedel, biogas, fordon, kemikalier, datorer, maskiner och verktyg.

Fastighetsägare utgör inte sådan aktör som direkt omfattas av NIS-regelverket. Att äga och förvalta en anläggning eller byggnad medför inga krav ur ett informationssäkerhetsperspektiv.

Fastighetsägaren kan emellertid bli indirekt påverkade av NIS-regelverket. Det är möjligt att hyresgäster som träffas av regulatoriska krav på sin informationssäkerhet (genom bl.a. NIS eller säkerhetsskyddslagen (2018:585)) kan komma att ställa krav på att anläggningen eller byggnaden de hyr dimensioneras i enlighet med regleringen. Sådana krav på säkerhetsåtgärder bör ställas av hyresgästerna i upphandlingsskedet, men kan även tillkomma vid avtalsförnyelse. Säkerhetsåtgärderna bör syfta till att reducera verkningar av sådana konsekvenser som hyresgästerna identifierat i de riskanalyser som NIS-lagen kräver (12 §).

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggandebranscher (exempelvis avlopps- och avfallshantering, eldistribution, fjärrvärme) träffas av det föreslagna regelverket NIS 2 och att de i sin tur ställer nya krav på säkerhet i samarbetet. Det kan leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

Ett potentiellt hål i NIS 2 avser it-system för fastighetsautomation. Fastighetsägare kan installera it-system för fastighetsautomation för att reglera värme- och kyla på distans. Systemen för fastighetsautomation kan utsättas för attacker med allvarliga konsekvenser för hyresgästerna med potentiell inverkan på samhället i stort. Direktivförslaget NIS 2 omfattar aktörer som distribuerar fjärrvärme eller fjärrkyla via ett nät till flera byggnader eller anläggningar, men inte kunderna (i förevarande fall fastighetsägarna) som ansvarar för reglaget av fjärrvärmen och -kylan.

Störningar som får en betydande inverkan på kontinuiteten i dessa tjänster ska rapporteras till MSB. I MSB:s föreskrift om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9)[15] har myndigheten i detalj definierat vad som innebär betydande störning för dessa verksamheter.

I de allra flesta fall kommer informationstillgångar som omfattas av NIS-lagen att klassa på nivån **betydande (2)** eller **allvarlig (3)** för samtliga säkerhetsaspekter, dels eftersom tjänsterna är samhällsviktiga, dels eftersom konsekvensnivåerna är så tydligt definierade i föreskrifterna.

EU:s Dataskyddsförordning (GDPR)

Dataskyddsförordningen syftar till att skydda levande, fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Enligt dataskyddsförordningen ska den som är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person. Med identifierbar menas att även indirekta uppgifter omfattas av dataskyddsförordningens tillämpningsområde. Personuppgifter kan behöva olika skyddsåtgärder beroende på vilken typ av uppgift det rör sig om eller i vilket sammanhang den förekommer. Vanligt förekommande personuppgifter kan till exempel behöva ett högt skydd om det handlar om skyddade personuppgifter eller om det handlar om mycket omfattande personuppgifter. Utöver detta har Integritetsskyddsmyndigheten identifierat vissa kategorier av personuppgifter som kräver extra skydd.

Extra skyddsvärda personuppgifter – personnummer

Personnummer är enligt Integritetsskyddsmyndigheten (IMY) en extra skyddsvärd uppgift som bör behandlas i så liten utsträckning som möjligt.

Särskilt skyddsvärda personuppgifter – integritetskänsliga personuppgifter

Integritetsskyddsmyndigheten har identifierat vissa typer av uppgifter som myndigheten anser är särskilt skyddsvärda. Exempel på sådana uppgifter är löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter från utvecklingssamtal, resultat från personlighetstester, information som rör någons privata sfär och uppgifter om sociala förhållanden, uppgifter om ekonomisk hjälp eller insatser inom socialtjänsten. Dessa uppgifter hanteras normalt enligt en högre säkerhetsnivå än mindre känsliga uppgifter.

15. https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs2018_9.pdf.

Känsliga personuppgifter

Dataskyddsförordningen identifierar särskilt vissa kategorier av personuppgifter som känsliga och som av den anledningen kräver en högre säkerhetsnivå. Dessa uppgifter är:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- hälsa eller sexualliv
- genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person

Några punkter att beakta i arbetet med att klassificera informationen är bland annat om något av följande behandlas:

- uppgifter om personer med skyddade personuppgifter
- uppgifter om enskildas sociala eller ekonomiska förhållanden
- personuppgifter om ett stort antal personer
- personnummer eller samordningsnummer
- en stor mängd personuppgifter om varje person

Enligt dataskyddsförordningen är en personuppgiftsincident ”en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”. Det innebär att personuppgifter måste hanteras på ett korrekt sätt gällande alla säkerhetsaspekter. Inte bara konfidentialitet, även aspekten tillgänglighet måste vägas in, liksom riktighet.

Med sannolikhet hamnar vanliga personuppgifter i klassificeringen **betydande (2)** för samtliga säkerhetsaspekter. I sammanhang där särskilda kategorier (känsliga personuppgifter och integritetskänsliga personuppgifter) behandlas är klassificeringen **allvarlig (3)** för säkerhetsaspekten konfidentialitet och i vissa fall även riktighet.

Personuppgifter inom hälso- och sjukvården

Patientdatalagen (2008:355) (PDL) tillämpas på vårdgivares behandling av personuppgifter inom hälso- och sjukvården. I Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40) finns krav om att överföring av personuppgifter i öppna nät ska göras på ett sådant sätt att ingen obehörig kan ta del av uppgifterna och att åtkomst till uppgifterna ska föregås av stark autentisering. Vårdgivaren ska säkerställa att uppgifter i en patientjournal inte kan ändras eller utplånas annat än med stöd av PDL.

Patientdata utgör generellt sett känsliga personuppgifter och normalt klassificeras dessa i konsekvensnivån **allvarlig (3)** för säkerhetsaspekten konfidentialitet. I sammanhang med mycket höga krav på riktighet, exempelvis ordinationer, är klassificeringen **allvarlig (3)** för säkerhetsaspekten riktighet.

Sekretessreglerade uppgifter

En handling är en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.

- En handling innehåller därmed vissa uppgifter.
- En handling är allmän, om den förvaras hos en myndighet och är inkommen till eller upprättad hos en myndighet.
- En allmän handling är antingen offentlig eller omfattas helt eller delvis av sekretess.

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Sekretessbelagda uppgifter kan vara uppgifter i allmänna handlingar men kan också vara uppgifter som inte ingår i en allmän handling, till exempel uppgifter som finns i en handling som ännu inte upprättats hos en myndighet.

Det finns tre typer av sekretess; absolut, stark och svag:

- **Absolut sekretess** betyder att inga uppgifter under några förutsättningar får lämnas ut till andra än de anställda som behöver uppgifterna för att kunna utföra sitt arbete. Detta gäller t.ex. för uppgifter i ännu inte avslutade upphandlingsärenden och uppgifter inom kommunal familjerådgivning som enskild lämnar i förtroende eller som inhämtats i förtroende.

- **Stark sekretess** betyder att sekretess är huvudregeln och uppgiften får endast lämnas ut om det står klart att så kan ske utan att visst men eller viss skada uppkommer.
- **Svag sekretess** betyder att offentlighet är huvudregeln och uppgiften omfattas av sekretess om det kan antas att visst men eller viss skada kan uppstå.

Sekretessreglerade uppgifter påverkar endast skyddsnivån konfidentialitet. Skyddsmålen för riktighet och tillgänglighet regleras inte i offentlighets- och sekretesslagen (2009:400).

Konfidentialitet medför inte automatiskt sekretess, även om det kan finnas en koppling. Sålunda ska de två begreppen (konfidentialitet och sekretess) hållas åtskilda. Det kan därför innebära att allmänna handlingar som är offentliga och som skulle lämnas ut till en enskild vid begäran om utlämnande av allmän handling trots detta inte bör ges den lägsta konsekvensnivån (”ingen eller försumbar”) när det gäller konfidentialitet.

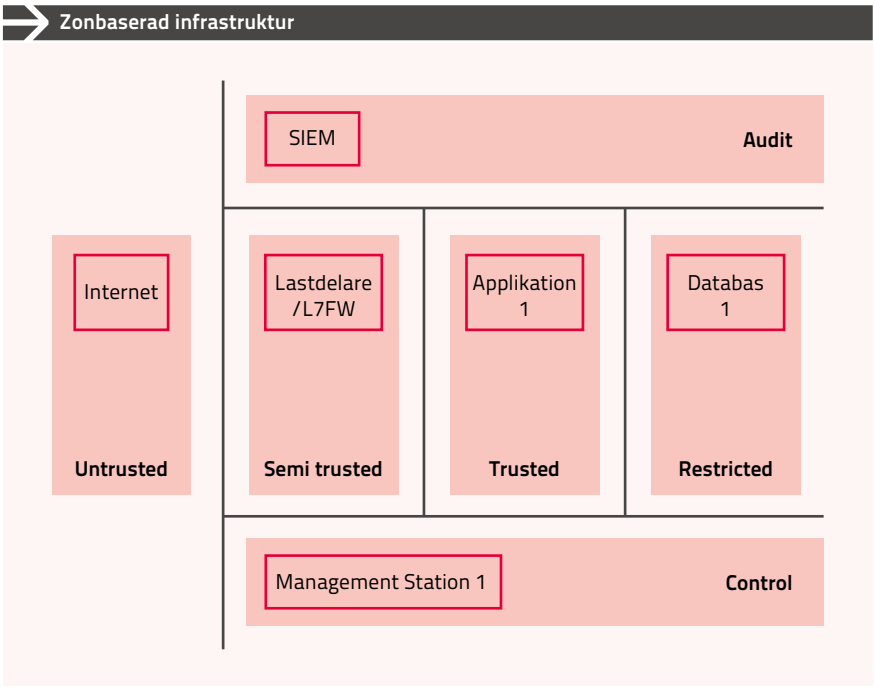
Omständigheter att beakta vid klassning av sekretessreglerade uppgifter är vilken skada som kan uppstå om uppgifterna röjs för obehörig samt om det gått lång tid sedan uppgifterna sekretessbelades och det är kort tid kvar på den skyddstid för vilken sekretessen gäller. Det innebär att konsekvensnivån kan variera från **måttlig (1)**, **betydande (2)**, **allvarlig (3)** eller **synnerligen allvarlig (4)** för säkerhetsaspekten konfidentialitet.

Arkivlagen (1990:782)

Av arkivlagen (1990:782) framgår bland annat att i arkivvården ingår att myndigheten ska organisera arkivet så att rätten att ta del av allmänna handlingar underlättas samt skydda arkivet mot förstörelse, skada, tillgrepp och obehörig åtkomst. I skydd mot förstörelse ingår såväl krav på tillgänglighet men också att ingen obehörigen ändrar i en arkiverad handling. Kravet på skydd mot obehörig åtkomst tar sikte på skyddsmålet konfidentialitet. Arkivmaterial kan bestå av en mängd olika uppgifter vilket innebär att hela skalan av konsekvensnivåer måste kunna tillämpas på de arkiverade informationstillgångarna vad gäller samtliga skyddsmål.

Bilaga 3 – Förslag till zonbaserad infrastruktur

Detta är ett förslag till modell för segmentering och zonindelning av nätverk. Förslaget till zonmodell inspireras av en modell framtagen av Burton group (numera en del av Gartner group) som är vedertagen i sammanhang där information med höga skyddsvärden förekommer.



FIGUR 17 ▪ Förslag till modell för segmentering och zonindelning av nätverk.

Modellen beskriver logisk uppdelning av olika nätverk och använder sig av zoner i vilka man sedan skapar subzoner. Zoner representeras i skissen ovan av de rektangulära fälten. Subzoner representeras av rektanglar inom respektive zon. De tjocka svarta strecken mellan zonerna representerar fysiska eller virtuella brandväggar.

Zoner i Burtonmodellen

- **Untrusted** används för osäkra nät som exempelvis Internet.
- **Semitrusted** används för publika tjänster och innehåller system som har anslutningar till *Untrusted* zonen, exempelvis webbservrar, spärrtjänster och lastbalanserare. *Semitrusted* motsvarar det som ofta brukar kallas DMZ.
- **Trusted** är till för system som inte har direkta kopplingar till osäkra nät eller lagrar känsligt data. I *Trusted* hamnar normalt flertalet applikationsservrar.
- **Restricted** är till för känsligt data och känsliga miljöer. I denna zon skapas subzoner för att isolera informationstillgångar från varandra. Endast godkända noder i applikationsnät i zonen *Trusted* tillåts kommunicera in mot en subzon i *Restricted* zonen, dvs. åtkomst till information måste gå via auktoriserad applikationsserver. Enda undantaget till detta är den/de subzoner i zonen *Control* som används för att administrera innehåll i subzoner i zonen *Restricted*.
- **Audit** används för loggning. I denna zon skapas subzoner för exempelvis övervakningssystem som SIEM-system inklusive dess datalager. En anledning till flera subzoner är om det exempelvis finns behov av avser att isolera flera SOC från varandra. All trafik in mot subzoner i *Auditzonen* ska passera diod, enda undantaget är trafik till/från loggstation i dedikerad subzon i zonen *Control* som används för logg/eventadministration. Logg/eventadministrationsklienter ska enbart kunna kommunicera med SIEM-systemets frontend. SIEM frontend ska placeras i dedikerad subzon i Auditzonen.
- **Control** används för systemadministration och drift. I denna zon skapas subzoner för administrationsklienter och eventuella jumpservrar som används av administratörer. I *Controlzonen* skapas även en dedikerad zon för logg/eventadministratörer, vilken i sin tur tillåts kommunicera med SIEM frontend. Subzoner i Control får inte kommunicera med subzoner i mer än en zon.

Trafik mellan zoner

All trafik mellan zoner passerar en brandvägg eller motsvarande som filtrerar trafiken. Trafik som passerar fler än två zongränser är inte tillåten. Exempelvis måste trafik mellan Untrusted och Trusted termineras i zonen Semitrusted.

Subzoner

I varje zon finns en eller flera subzoner. En subzon är ett eget nätsegment (subnät) till vilket åtkomst styrs av ett regelverk. För varje subzon finns en zonägare som ansvarar för vilken trafik som är tillåten till/från zonen.

Kommunikation mellan nätsegment (subzoner) ska gå via en policy-motor. Policymotorn är oftast en brandvägg men kan även vara annan filtrerande funktion, exempelvis policy-based routing (PBR).

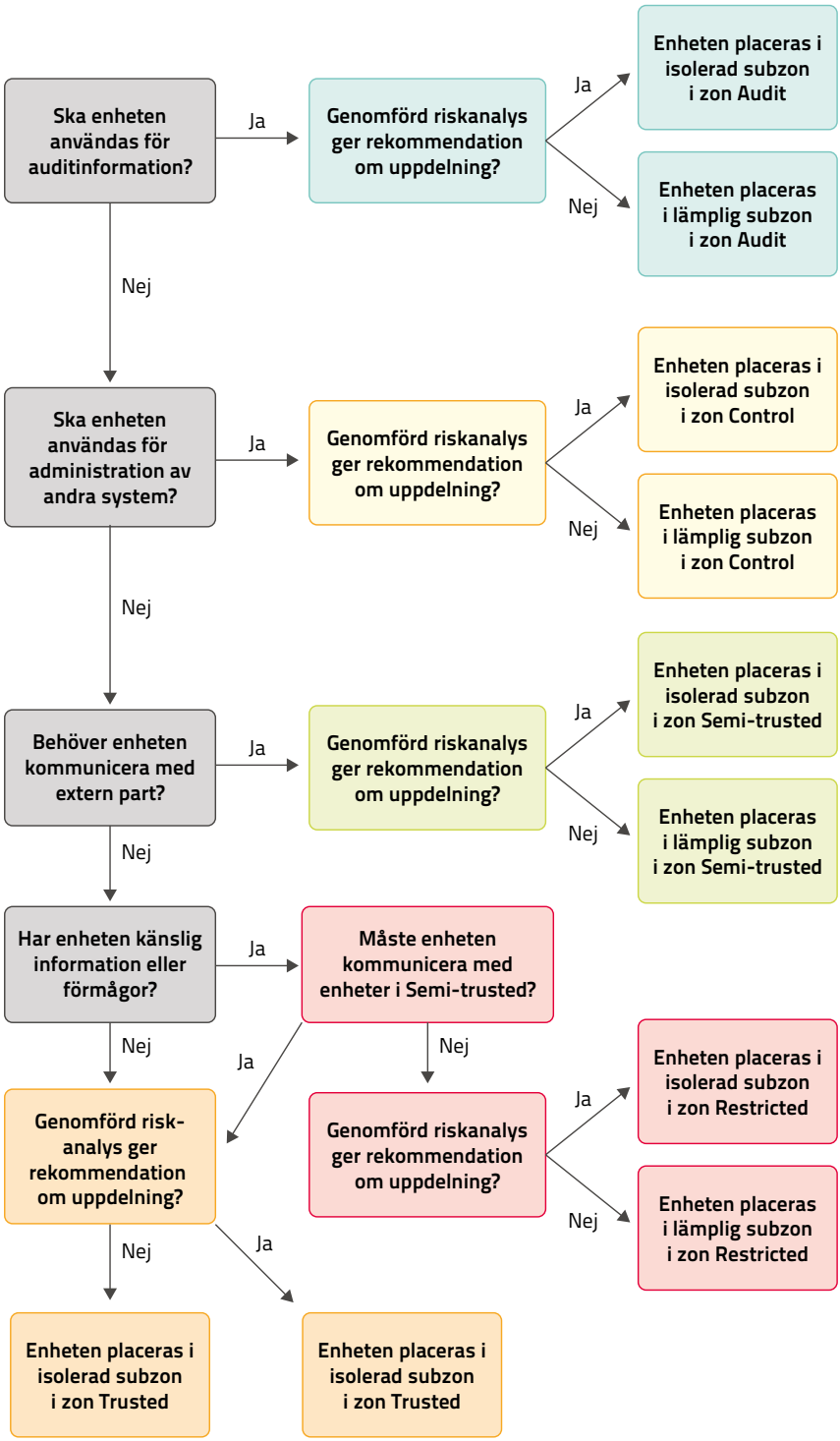
Öppningar för trafik görs i första hand mellan nätsegment på protokoll/portnivå. Exempel på en öppning kan vara SQLnet mellan två subzoner. Undantag från öppning nät/nät är all kommunikation till/från okända nät i zonen Untrusted som ska öppnas på hostnivå.

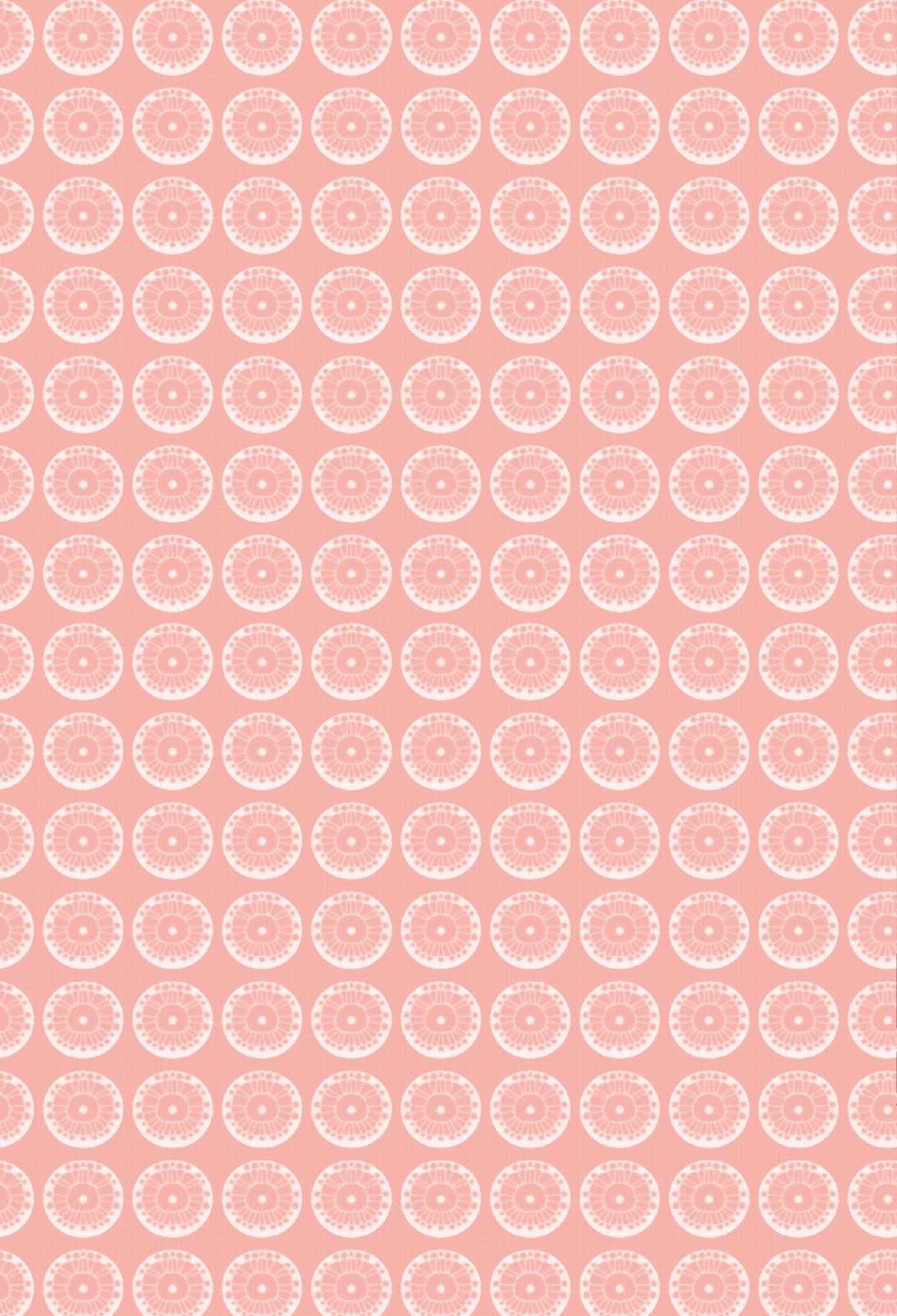
Kriterier som styr uppdelning i subzoner består i:

- Informationsklassning samt risk- och sårbarhetsanalys.
- Separation av olika applikations och databasplattformar (ex Windows/Linux, Oracle/SQLserver, Jboss/.NET).
- Separation av system som hanteras av olika driftorganisationer och/eller grupperingar.
- Separation och isolation av system som ej kommunicerar med eller delar data med varandra.
- Separation av system som utgör en risk för andra system
- Trafikmönster (t.ex. externa kopplingar eller ej)

Placering av tjänster/servrar

Flödesschemat nedan används som stöd för processen. Observera att risk- och sårbarhetsanalys alltid ska föregå zonplacering.


Ska enheten användas för auditinformation?
Ja
Genomförd riskanalys ger rekommendation om uppdelning?
Ja
Enheten placeras i isolerad subzon i zon Audit
Nej
Enheten placeras i lämplig subzon i zon Audit
Nej
Ska enheten användas för administration av andra system?
Ja
Genomförd riskanalys ger rekommendation om uppdelning?
Ja
Enheten placeras i isolerad subzon i zon Control
Nej
Enheten placeras i lämplig subzon i zon Control
Nej
Behöver enheten kommunicera med extern part?
Ja
Genomförd riskanalys ger rekommendation om uppdelning?
Ja
Enheten placeras i isolerad subzon i zon Semi-trusted
Nej
Enheten placeras i lämplig subzon i zon Semi-trusted
Nej
Har enheten känslig information eller förmågor?
Ja
Måste enheten kommunicera med enheter i Semi-trusted?
Nej
Ja
Nej
Genomförd risk-analys ger rekommendation om uppdelning?
Genomförd riskanalys ger rekommendation om uppdelning?
Ja
Enheten placeras i isolerad subzon i zon Restricted
Nej
Enheten placeras i lämplig subzon i zon Restricted
Nej
Ja
Enheten placeras i isolerad subzon i zon Trusted
Enheten placeras i isolerad subzon i zon Trusted



OFFENTLIGA FASTIGHETER

Informations-säkerhet i fastighets-organisationen

www.offentligafastigheter.se

Skriften har finansierats genom organisationen Offentliga fastigheter

ISBN: 978-91-8047-066-7
www.offentligafastigheter.se