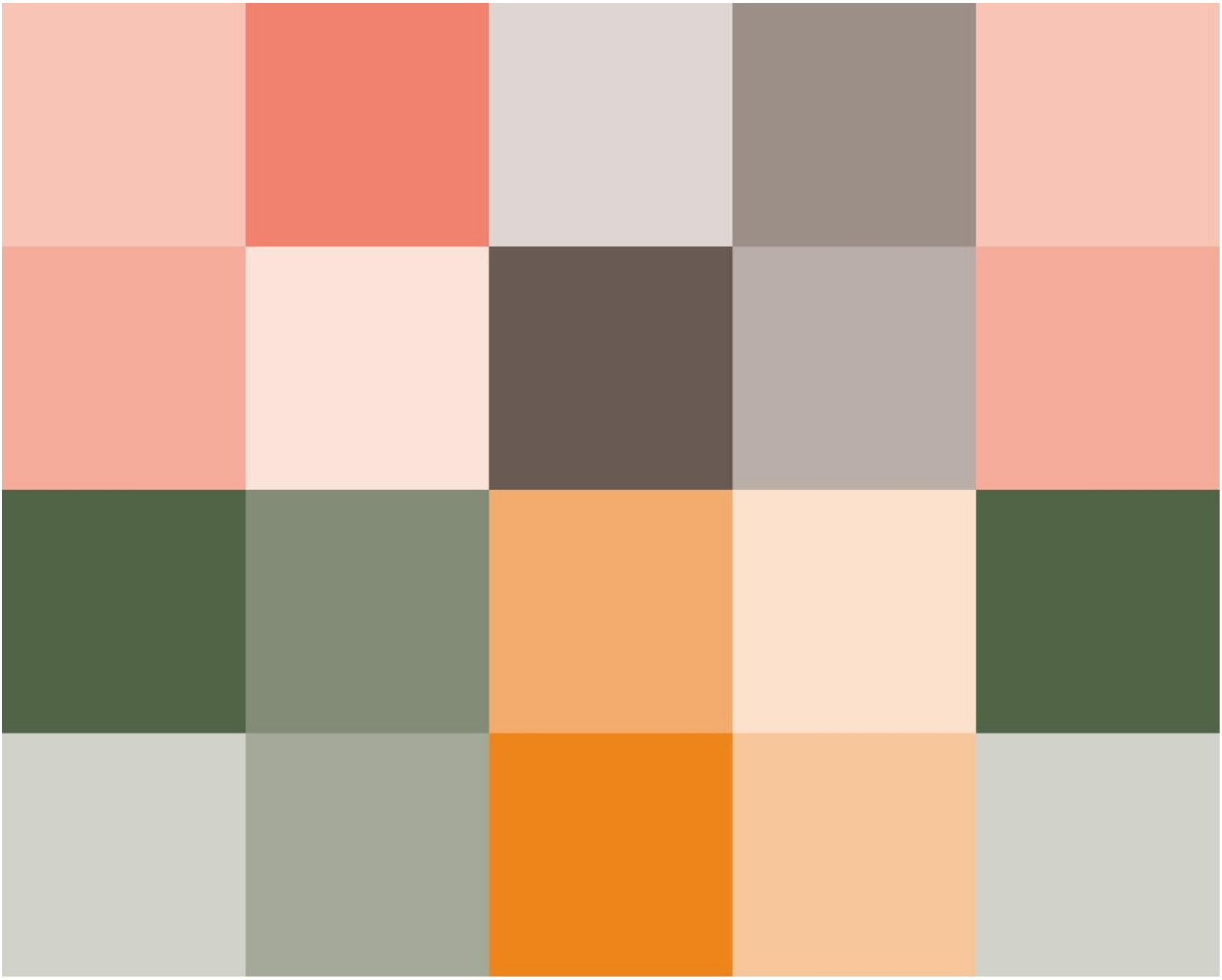


Tillitsramverk

Byggblocksbeskrivning

MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Sammanfattning

Inledning

Byggblockets arbete har initialt fokuserat på att reda ut begreppet ”tillit” och definitionen av ett ”tillitsramverk” eftersom många olika definitioner och avgränsningar förekommer vilket leder till otydlighet och missförstånd.

Tillit är en grundförutsättning för ett säkert och effektivt informationsutbyte mellan välfärdens aktörer. Inom svensk offentlig förvaltning är organisationstillit ofta praxis men allt för ofta utan en tydlig definition och modell att bygga detta på.
Ett tillitsramverk ger förutsättningar för att skapa och vidmakthålla organisationstillit inkluderat aktörernas systematiska informationssäkerhetsarbete och dess identitetshantering.

En framgångsfaktor är att hålla samman och inkludera befintliga och nya komponenter för tillit i ett gemensamt övergripande ramverk.

Grundpelare/Kuben

I mångt och mycket bygger tillitsramverket på samma grundprinciper som det trygga samhället i stort med fyra fundament;
Regler, Stöd, Uppföljning och Konsekvenser.
Till detta läggs anpassade nivåer av tillit beroende av informationens klassificering och tydligt ansvar.

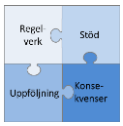
Relation till andra byggblock

Arbetet inom byggblocket har visat på mycket stora synergier och överlapp med byggblocket Identitet och med kompetensområdet Informationssäkerhet samt vikten av att förhålla sig till en övergripande arkitektur för det komplexa ekosystemet som offentlig förvaltning kännetecknas av. Detta bör hanteras i kommande arbete.

Fortsättning

Byggblocket bör snarast samordnas med överlappande block och kompetensområden för att fylla ramverkets ”delkuber” med ett väl förankrat innehåll och för att planera för ett införande och för en förvaltning.
Ett antal scenarios ska tas fram, bl.a. för SWOT-analys av olika alternativ.

Innehållsförteckning



1. Introduktion

	Utveckling	Förvaltning
Färdledande myndighet	EHM	DIGG
Samverkande myndigheter	MSB, LM, Inera	DIGG

En förutsättning för att kunna skapa ett säkert och effektivt informationsutbyte är att samtliga ingående aktörer känner tillit till de övriga aktörerna, deras arbetssätt samt till den infrastruktur som används, till en sådan nivå att de kan acceptera den risk som informationsutbytet innebär för dem själva. Tillitsramverket måste därför ha acceptans hos statliga, regionala och kommunala myndigheter, samt hos offentliga och privata leverantörer av välfärdstjänster.

Till ovan nämnda parter tillkommer tekniska leverantörer.

Tillitsramverket behöver även kunna utvecklas och förvaltas över tid allt eftersom behoven förändras. Begreppet ”Tillit” bör tolkas inom kontexten ”informationsdelning mellan välfärdens aktörer”:

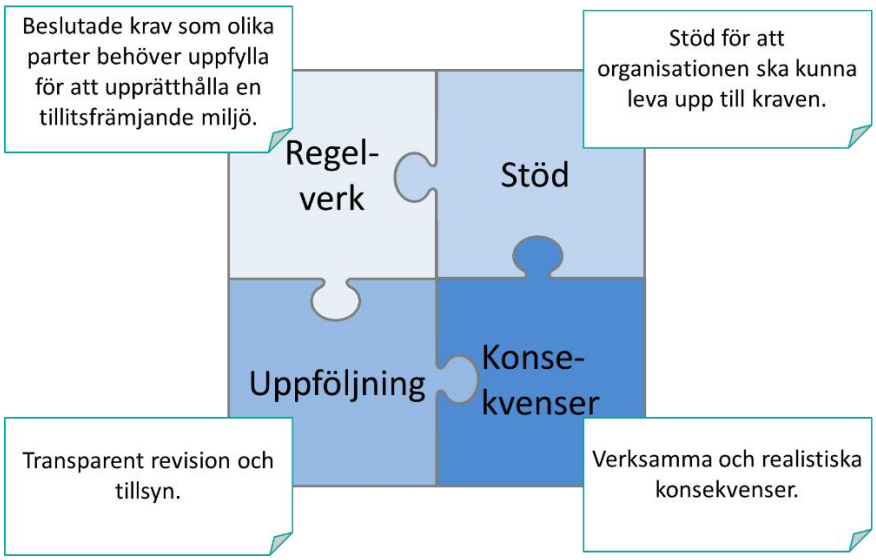
> ”Inom svensk offentlig förvaltning är organisationstillit praxis.
> Behovet av att konkretisera organisationstillit har aktualiserats vid informationsdelning mellan olika offentliga verksamheter.”
>
> ”Att lita på den samverkande partens förmåga att hantera den information som delas enligt gällande lagar och informationsklassificering möjliggör en effektiv och trygg digitalisering.”
>
> ”Inom svensk välfärd och demokratimodell finns generellt en tillitsfrämjande miljö.”

”Tillit är svårt att skapa men lätt att rasera – mänskligt beteende ”Ramverket avser att inkludera befintliga ramverk och komponenter för tillit och få dessa att agera som en helhet utifrån gällande lagar och förordningar. Ramverket ska också fylla ut det glapp som kan finnas mellan ingående delar.

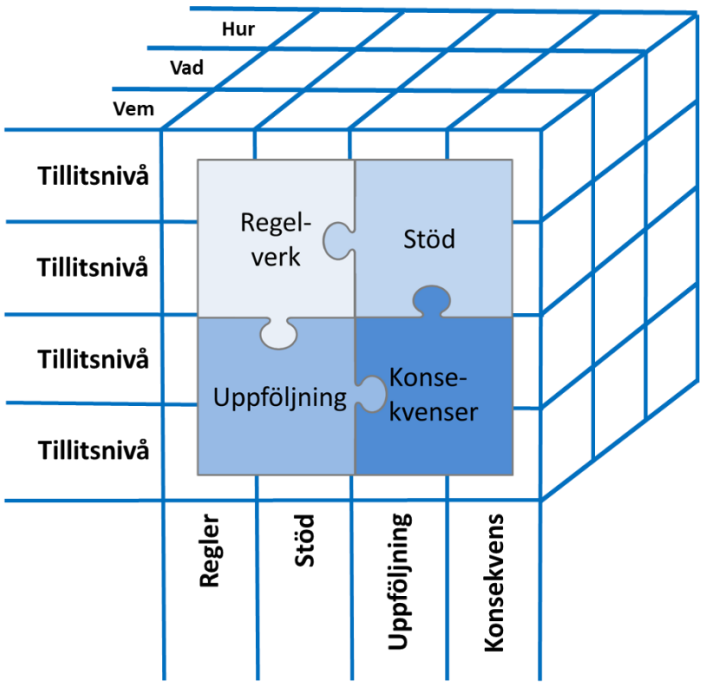

Regel-
verk
Stöd
Uppföljning
Konse-
kvenser

2. Tillitsramverkets uppbyggnad

Regeringsuppdragets tilltänkta tillitsfrämjande miljö består av ett ramverk som vilar på fyra delar över tid vilket kan visualiserats som:



Förutom de fyra fundamenten tillkommer olika nivåer av tillit, ansvar och arbetssätt. Innehållet i respektive delkub bör koordineras med övriga byggblock under nästa fas av uppdraget.



2.1 Regler

Regelverket bör vara enkelt och tydligt men verkningsfull och omfatta (integrera) andra tillitsregelverk som krävs. En förvaltad kravkatalog utgör stommen i regelverket.

2.2 Stöd

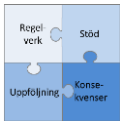
Stödet ska ge förutsättningar för alla parter att leva upp till regelverket genom tex utbildning och mallar.

Tillit bygger bland annat på transparens, öppenhet och följsamhet kring gemensamma regelverk. Stöd vid tillämpning av ett ramverk är vital för att säkerställa att grundförutsättningar finns för ett tryggt informationsutbyte, d.v.s. att hjälpa parter att göra rätt både vid anslutning och användning, samt att få dem att känna sig trygga i sin efterlevnad av tillitsramverket. Stöd kan ges genom:

- Initial granskning för efterlevnad av tillitsramverket.
- Stöd i form av expertis och tillvägagångsätt vid nödvändiga förändringar i verksamhet och infrastruktur.
- Kontinuerlig samverkan med ingående parter.

2.3 Uppföljning

Att alla parter vet att alla är granskade och lever upp till regelverket ger en trygghet och bidrar starkt till tillit.



Grundförutsättningen för ett gemensamt tillitsramverk är förmågan att granska och följa upp regelefterlevnad. Syftet är att kunna motverka brister och avvikelser som kan påverka ingående parter negativt genom att:

- att vara stödjande inför anslutning,
- ha förmåga att utföra löpande kontroll och vara vägledande och stödjande vid förändringar

2.4 Konsekvenser

Verksamma konsekvenser om en part inte lever upp till regelverket bidrar till att förebygga avvikelser. Detta kan förebygga allvarliga incidenter vid informationsutbyte för övriga, ingående parter.

Ingående samverkansorganisationer och operatörer tillämpar tillitsramverket i syfte att upprätta och bibehålla tillit och trygghet vid informationsutbyte genom den gemensamma infrastrukturen. Avvikelser i de delar som tillitsramverket omfattar och som kan påverka ingående parter negativt vid informationsutbyte, ska motverkas genom tydliga och exekverbara konsekvenser beroende på grad av avvikelser.

2.5 Tillitsnivåer

Beroende av … kommer det att krävas olika nivåer av tillit. Dessa nivåer påverkas av externa ramverk, av parternas informationsklassning och av lagar. Vilka nivåer som ska finnas i tillitsramverket ska arbetas fram i nästa fas av uppdraget.
Exempel på dessa beskrivs närmare i kap. 8

2.6 Ansvar och arbetssätt

Informationsutbyte kräver att parterna har tillit till både ansvar, roller och arbetssätt hos övriga parter:

- **Vem**: Tillit till den andra partens identitetshantering och arbetssätt.
- **Vad**: Tillit att den andra parten har ett systematiskt informationssäkerhetsarbete.
- **Hur**: Tillit att den andra partens rutiner och tekniska lösningar hanterar informationen enligt överenskommen informationsklassning.

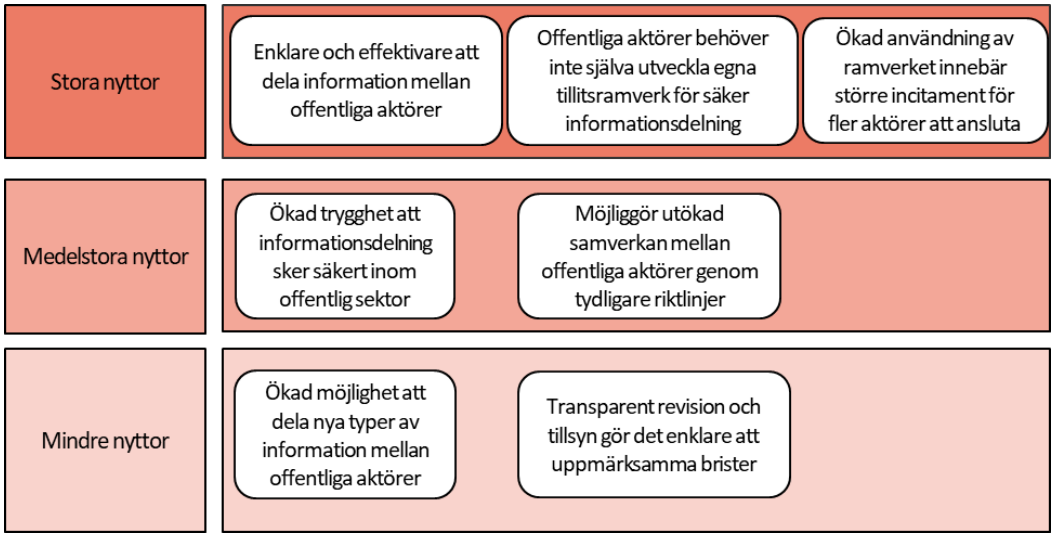
3. Nyttoanalys

3.1 Beskrivning av identifierade nyttor

Vi uppskattar att byggblocket Tillitsramverk skapar samhällsekonomiska nyttor genom att göra informationsutbytet mellan offentliga aktörer billigare, effektivare och säkrare. Byggblocket skapar nyttor genom både tids- och kostnadsbesparingar (effektivitetsvinster) och genom bättre tjänster och nya användningsområden (ökad kvalitet). Vi bedömer att nyttorna framför allt tillfaller offentlig sektor, eftersom ramverket riktar sig mot offentliga aktörer. Nyttor skapas dock även i viss utsträckning för medborgare och företag. Exempelvis skapas nyttor för dessa aktörer genom att byggblocket leder till en säkrare och tryggare informationsdelning inom offentlig sektor vilket även skapar nyttor genom ökad trygghet.

Eftersom byggblocket Tillitsramverk är i ett tidigt utvecklingsskede är det ännu inte möjligt att kvantitativt beräkna hur stora nyttorna kommer bli. Vi har därför istället beskrivit nyttorna kvalitativt och uppskattat nyttornas inbördes storleksordningen, se Figur 1. Inga beräkningar ligger i dagsläget bakom dessa uppskattningar. Nyttorna i figuren beskrivs i detalj i respektive underkapitel. För utförligare beskrivning av genomförandet hänvisas till Metodbilagan[1].

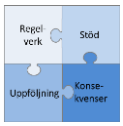
Figur 1. Uppskattat storleksintervall med rangordning av samtliga nyttor



3.2 Nyttor i form av tids- och kostnadsbesparingar

Tillitsramverket skapar nyttor till följd av tids-och kostnadsbesparingar. Nyttor skapas dels genom effektiviseringar i informationsdelningen mellan offentliga aktörer, dels

[1] Nyttoanalysens metodbilaga, Slutrapportens bilagor, https://www.digg.se/informationsutbyte-och-grunddata



genom kostnadsbesparingar då offentliga aktörer inte själva behöver utveckla egna tillitramverk. Byggblocket fungerar som ett substitut för bilaterala avtal mellan offentliga aktörer. Detta innebär att nyttorna framförallt realiseras i utvecklings- och implementeringsfasen av en ny tjänst. Vi uppskattar att nyttorna tillfaller offentlig sektor då det är för dessa aktörer som byggblocket är tänkt att skapa nyttor.

3.2.1 Effektivare informationsdelning inom offentlig sektor

Ett nationellt tillitsramverk gör det enklare och effektivare för offentliga aktörer att dela information mellan varandra. Exempelvis behöver inte offentliga aktörer hålla reda på olika regler för informationsdelning med andra aktörer inom offentlig sektor vilket sparar tid. Det blir även enklare för myndighetsanställda att veta vilka aktörer som kan ta emot olika typer av information och på vilket sätt. Detta leder till tidsbesparingar för de anställda hos samtliga offentliga aktörer som ansluter till tillitsramverket.

3.2.2 Offentliga aktörer behöver inte själva utveckla egna tillitsramverk

Utvecklingen av ett tillitsramverk innebär att offentliga aktörer inte själva behöver utveckla egna ramverk. Utan ett nationellt tillitsramverk kan aktörer tvingas ta fram bilaterala avtal om informationsdelning för varje bilateralt förhållande som ser olika ut för olika aktörer. Detta är en kostsam process för alla parter. Genom att utveckla ett nationellt tillitsramverk undviks denna kostnad. Detta leder till en direkt offentligfinansiell kostnadsbesparing för alla offentliga aktörer som annars hade tvingats ta fram egna tillitslösningar.

3.2.3 Tydligare riktlinjer möjliggör utökad samverkan

Ett gemensamt tillitsramverk möjliggör och förenklar utökad samverkan mellan offentliga aktörer. Tillitsramverket fungerar som en kvalitetsindikator på informationssäkerhet för aktörerna som ansluter. Detta gör det enklare för anslutna aktörer att avgöra vilka andra inom offentlig sektor som de kan dela information med. Tillitsramverket gör det på så sätt enklare att så väl identifiera som inleda samarbeten i informationsdelningssyfte med nya aktörer. Dessa nyttor, som framförallt består av effektivitetsvinster, tillfaller primärt offentliga aktörer. Ett effektivare informationsutbyte leder till indirekta offentligfinansiella effekter genom tidsbesparingar för myndighetsanställda. Beroende på vilka nya typer av samarbeten som kan påbörjas kan även direkta offentligfinansiella besparingar uppstå. I och med att nya samarbeten uppstår inom offentlig sektor skapas även effektivitetsvinster för medborgare och företag som nyttjar offentlig sektors tjänster.

3.3 Nyttor skapas av fler tjänster och nya användningsområden

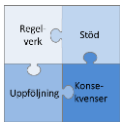
Ett nationellt tillitsramverk skapar nyttor genom att göra informationsdelning mellan offentliga aktörer säkrare och genom att det blir enklare att uppmärksamma misstag eller brister. Risker som finns med separata tillitsramverk mellan olika aktörer kan minskas drastiskt genom framtagandet av ett gemensamt nationellt regelverk. Att information kan delas säkrare mellan offentliga aktörer skapar kvalitativa nyttor på flera olika sätt. Exempelvis genom att alla aktörer i samhället känner en ökad trygghet med informationsdelningen inom offentlig sektor. Eller genom att det blir enklare att upptäcka eventuella brister. Nyttorna inom denna kategori tillfaller offentlig sektor, medborgare och företag.

3.3.1 Ökad trygghet att informationsdelning sker säkert inom offentlig sektor

Ett nationellt tillitramverk med tydliga regler för informationsdelning mellan aktörer innebär att information kan delas på ett säkrare sätt inom offentlig sektor. Exempelvis minskar tydliga riktlinjer risken att en myndighetsanställd delar information med fel aktör till följd av flera, förvirrande riktlinjer för informationsdelning med olika aktörer. Ett gemensamt ramverk med transparent uppföljning gör det även enklare för mottagare och avsändare att verifiera att respektive part följer alla riktlinjer. Detta leder till kvalitativa nyttor för medborgare och företag som känner sig tryggare med att information om dem hanteras på ett säkert och korrekt sätt inom offentlig sektor. Det innebär även en kvalitativ nytta för offentliga aktörer genom en ökad trygghet att den information de delar med andra aktörer hanteras på ett säkert sätt.

3.3.2 Underlättar delning av nya informationsmängder mellan offentliga aktörer

Ju säkrare informationsdelningen kan göras mellan offentliga aktörer, desto större är chansen att ny typ av information kan delas mellan aktörer inom offentlig sektor. Genom att tillitramverket fungerar som en garanti för att parter som ingår i ramverket uppfyller vissa krav på informationssäkerhet möjliggörs potentiellt nya typer av informationsdelning mellan aktörer. En offentlig aktör som exempelvis saknat resurserna för att verifiera vilka aktörer som uppfyller vissa säkerhetskrav kan nu använda tillitsramverket för att göra den verifieringen. Och detta kan i sin tur göra det möjligt för aktörer att dela ny information med varandra – information som inte hade delats om inte tillitsramverket funnits. Dessa nyttor, som består av både effektivitetsvinster och ökad kvalitet, tillfaller primärt offentliga aktörer.



3.3.3 Transparent revision och tillsyn gör det enklare att uppmärksamma brister

Ett gemensamt tillitsramverk med en tydlig tillsynsprocess gör det enklare att uppmärksamma om brister i informationshanteringen hos aktörer som ingår i ramverket. Det finns idag inget enhetligt sätt att utvärdera myndigheters informationshantering utifrån ett tillitsperspektiv. Framtagandet av ett enhetligt ramverk med tydliga riktlinjer och krav möjliggör sådan typ av utvärdering. Detta innebär att informationshanteringen på den enskilda myndigheten som ingår i avtalet blir säkrare. Det innebär även att informationsdelningen mellan aktörerna blir tryggare. Detta leder till kvalitativa nyttor för medborgare och företag som känner sig tryggare med att information om dem hanteras på ett säkert och korrekt sätt inom offentlig sektor. Det innebär även en kvalitativ nytta för offentliga aktörer genom en ökad trygghet att den information de delar med andra aktörer hanteras på ett säkert sätt.

3.4 Ökad nytta av att fler använder tillitsramverket

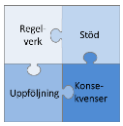
Ju fler som är anslutna till tillitsramverket, desto större blir incitamenten för en enskild aktör att ansluta eftersom det gör att det standardiserade tillitsramverket kan ersätta fler bilaterala avtal och lokala anpassningar. Och desto större blir nyttorna som byggblocket realiserar. Det är enklare för aktörer som är anslutna till tillitsramverket att dela information med varandra än med aktörer som står utanför ramverket. Om antalet anslutna aktörer är stort är även nyttan av att ansluta stor för en enskild aktör som enkelt vill dela information med andra aktörer. Detta är ett exempel på en direkt nätverkseffekt där en ökning i antalet anslutna aktörer (offentliga aktörer i detta fall) ökar nyttan för redan anslutna, och därmed också positivt påverkar antalet aktörer som vill ansluta. Och detta leder i sin tur till ökad nytta.

3.5 Potentiellt stora nyttor genom framtida utveckling

Tillitsramverk skapar potential för fler nyttor än de som är beskrivna ovan. Tillitsramverket fungerar som en byggsten i funktionaliteten i alla andra byggblock och således kan närmast alla potentialer som andra byggblock realiserar förbättras med hjälp av utvecklandet av tillitsramverket. Eftersom dessa typer av nyttor huvudsakligen realiseras och beskrivs inom andra byggblock kommer de inte beskrivas här. I tillägg till detta möjliggör tillitsramverket en ökad digitaliseringstakt. Nyttan kategoriseras som en potential eftersom dess realisering till stor del är utanför byggblockets kontroll. Andra aktörer behöver vidareutveckla eller använda funktioner som finns inom tillitsramverket för att nyttorna ska realiseras.

3.5.1 Ökad digitaliseringstakt

Tillitsramverket möjliggör en förbättrad samverkan inom offentlig sektor vad gäller informationsdelning, och bidrar på så sätt till en mer integrerad digital infrastruktur mellan offentliga aktörer. En mer enhetlig och mer integrerad digital infrastruktur är i sig viktig för det fortsatta arbetet med att digitalisera olika offentliga processer. Således bidrar realiseringen av tillitramverket potentiellt till att digitaliseringstakten inom hela offentlig sektor kommer att öka.



4. Finansieringsanalys

I nedanstående tabell anges endast tilldelat anslag för arbetet med Tillitsramverket.

I föreslagen, långsiktig plan anges ett antal aktiviteter och milstolpar baserat det som anges tidigare i detta dokument. Beräkningar utifrån dessa aktiveter och de estimerade timmar som vi uppskattat visar på ca 7 MSEK sammanlagt för år 2 och år 3. Med föreslaget anslag på 2 MSEK år 2 uppstår en differens motsvarande 1,5 MSEK. För år 3 skulle då den totala kostnaden bli 3,5 MSEK exkluderat anslag som fn. är okänt.

[TSEK]	Anslag	Lån	Avgift	Bidrag	Totalt
År 1					? MSEK
År 2	2 MSEK				3,5 MSEK
År 3					3,5 MSEK
År 4					
År 5					
Totalt	> 2 MSEK				7 MSEK

5. Rättslig analys

5.1 Inledning

En förutsättning för att kunna skapa ett säkert och effektivt informationsutbyte är som beskrivits mer utförligt ovan att samtliga ingående aktörer känner tillit till de övriga aktörerna, deras arbetssätt samt till den infrastruktur som används, till en sådan nivå att de kan acceptera den risk som informationsutbytet innebär för dem själva.

Frågan är på vilket sätt ett effektivt och fungerande ramverk för tillit skapas?

Räcker det med överenskommelser eller avtal mellan deltagande aktörer eller behövs författningsreglering i någon omfattning?

Kan befintligt regelverk i sig utgöra ett tillitsskapande ramverk?

5.2 Kortfattat om befintlig reglering

Det finns i gällande rätt redan en mängd författningar som reglerar dataskydd och informationssäkerhet som aktörerna är bundna av.[2]

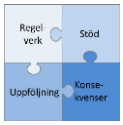
Aktörernas ansvar för behandling av personuppgifter regleras i EU:s dataskyddsförordning[3], lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och särskilda registerlagar som till exempel patientdatalagen (2008:355). Gällande rätt avseende behandling av personuppgifter reglerar såväl villkor för behandling av uppgifterna som krav på säkerhet vid behandlingen. Av artikel 24.3 dataskyddsförordningen framgår att tillämpningen av godkända uppförandekoder är ett sätt för den personuppgiftsansvarige att visa hur denne fullgör sina skyldigheter enligt förordningen.

Information hos deltagande myndigheter utgör allmänna handlingar och omfattas av bestämmelserna i offentlighets- och sekretesslagen (2009:400). En myndighet får inte röja sådana uppgifter i strid med lagens bestämmelser.

---

[2] En mer utförlig genomgång av gällande rätt finns t.ex. i *Juridik som stöd för förvaltningens digitalisering*, betänkande av Digitaliseringsmyndigheten (SOU 2018:25), avsnitt 9.5. Jämför även avsnitt 4.2 i *Säkert och effektivt elektroniskt informationsutbyte inom den offentliga sektorn* Slutrapport i regeringsuppdraget Fi2018/02150/DF, FI2018/03037/DF och I2019/01061/DF (DIGG Dnr: 2019-100).

[3] 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).



De olika aktörer som ska använda en gemensam infrastruktur är också bundna av olika författningar som reglerar informationssäkerhetskrav, som gäller oavsett om uppgifterna som behandlas utgör personuppgifter eller inte. I lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster finns bestämmelser som syftar till att uppnå en hög nivå på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom utpekade sektorer. Vissa av dessa sektorer ansvarar kommuner och regioner för. I Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter regleras att myndigheter ska bedriva ett systematiskt och riskbaserat informations-säkerhetsarbete med stöd av vissa standarder. Även i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap finns krav på statliga myndigheters informationssäkerhet. Därtill finns inom hälso- och sjukvårdens område krav på informationssäkerhet i Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.

Den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd bedriver säkerhetskänslig verksamhet. Sådan verksamhet omfattas av säkerhetsskyddslagen (2018:545). Det innebär enligt 2 kap. 1 § att verksamheten har en skyldighet att utreda behovet av säkerhetsskyddsåtgärder. Om verksamheten till exempel hanterar säkerhetsskyddsklassificerade uppgifter ställs särskilda krav på informationssäkerhet (2 kap 2 §).

Europaparlamentets- och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93 EG (eIDAS-förordningen) reglerar dels erkännande av utländska e-legitimationer, dels s.k. betrodda tjänster. Med betrodda tjänster avses en elektronisk tjänst som vanligen tillhandahålls mot ekonomisk ersättning och som utgör elektroniska underskrifter och stämplar, validering och bevarande av elektroniska underskrifter och stämplar, tjänster för rekommenderad elektronisk leverans och utfärdande av certifikat för autentisering av webbplatser. Tillhandahållare av betrodda tjänster ska enligt artikel 19 i eIDAS-förordningen vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller. Denna förordning utgör ett tillitsramverk inom sitt tillämpningsområde.

5.3 Utblick till Norge – uppförandekod som tillitsramverk?

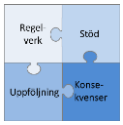
Exempel på hur man kan arbeta med uppförandekoder kan hämtas från ett av våra grannländer. I Norge har man i 14 år arbetat med en uppförandekod för informationssäkerhet för vård- och omsorgssektorn. Den norska normen för informationssäkerhet och integritet (Normen)[4] är en samling krav och riktlinjer som ska bidra till att skapa en tillfredsställande informationssäkerhet i verksamheterna och i hela sektorn. Direktoratet for e-helse är sekretariat för Normen. Vård- och omsorgsgivare i Norge är enligt lag skyldiga att använda Helsenettet (motsvarande Sjunet i Sverige) för informationsutbyte. Alla verksamheter som vill ha ett sådant informationsutbyte och vara anslutna till Helsenettet är genom anslutningsavtalet förpliktade att också följa Normen. Den som genom avtalet med Helsenettet har en juridisk förpliktelse att följa Normen ska kunna lita på att andra verksamheter, som också har ett sådant avtal, har tillfredsställande informationssäkerhet för sin behandling av personuppgifter. På så sätt skapas mekanismer så att verksamheterna kan ha ömsesidig tillit till att behandlingen av personuppgifter görs på en god säkerhetsnivå. Normen är indelad i tre delar; en styrande, en genomförande och en kontrollerande del. Den styrande delen beskriver krav på verksamhetens ledning att till exempel ta fram ett ledningssystem för informationssäkerhet och arbeta med riskbedömningar. I den delen som avser genomförande av Normen finns krav som handlar om tillgångsstyrning, autentisering, etablering och drift av informationssystem, avtal och utbildning med mera. Den kontrollerande delen handlar bland annat om säkerhetsrevisioner, avvikelsehantering och åtkomstkontroll. Normen består förutom av kravdokumentet av vägledningar, mallar, faktaark och utbildningsmaterial.

De aktörer som ska använda den gemensamma infrastrukturen i Sverige skulle således kunna ta fram och enas om en uppförandekod för detta samarbete. En myndighet skulle, enligt norsk modell, kunna utgöra sekretariat åt en sådan uppförandekod. Arbetet med att ta fram en gemensam uppförandekod skulle kunna påbörjas utan författningsändringar. Men resultatet av ett sådant arbete skulle därutöver kunna kombineras och förstärkas med hjälp av olika regelförändringar.

5.4 Finns det behov av att reglera ett tillitsramverk?

Det framgår av avsnitt 2 ovan att ett fungerande tillitsramverk bör bestå av fyra komponenter; regler, stöd, uppföljning och konsekvenser. Vi utgår i denna rapport

[4] Normen.no



således från att det är en grundförutsättning för ett gemensamt tillitsramverk att det ingår strukturer för att granska och följa upp regelefterlevnaden.

Det finns som vi konstaterade ovan befintlig reglering som ställer krav på informationssäkerhet, men det finns inte någon heltäckande reglering som samma krav till samtliga deltagande aktörer. Det finns heller inte författningar som reglerar strukturerna för samverkan i en gemensam infrastruktur eller någon gemensam tillitsnivå.

I betänkandet Reboot – en omstart för den digitala förvaltningen (SOU 2017:114) finns förslag på ett lagreglerat tillitsramverk för elektroniska identitetshandlingar. En elektronisk identitetshandling ska enligt utredningen vara utformad, skyddas och användas enligt en viss tillitsnivå. Utfärdare av elektroniska identitetshandlingar ska tillämpa sådana regler och rutiner att det utifrån tillämplig tillitsnivå finns fog för att lita på de elektroniska identitetshandlingar som tillhandahålls. Tillitsramverket och de tekniska specifikationerna bör enligt utredningen utformas med beaktande av internationellt framtagna standarder. Det bör ankomma på digitaliseringsmyndigheten att säkerställa att det finns ett tillitsramverk samt att detta är följsamt med de standarder och utvecklingen i övrigt samt de hot och risker som kan uppkomma på området. Utredningen bedömer att förekomsten av ett tillitsramverk ska regleras i lag. Utredningens förslag i denna del kan vara av intresse att beakta i vårt arbete med ett tillitsramverk för en gemensam infrastruktur.

Den gemensamma infrastrukturen kommer att på sikt att omfatta inte bara statliga myndigheter, utan även kommunala myndigheter och privata aktörer. Vår inledande bedömning i detta skede av analysarbetet är att det skulle kunna tydliggöra vilka säkerhetskrav som ska gälla vid informationsutbytet, om de gemensamma kraven uttrycks i ett lagreglerat tillitsramverk, som är tillämpligt på samtliga deltagande aktörer. Ett sådant reglerat tillitsramverk borde också innehålla regler om uppföljning av regelefterlevnaden och om konsekvenser för de aktörer som inte uppfyller kraven. I lagen bör finnas bemyndigande till regeringen eller den myndighet som regeringen bestämmer att föreskriva om mer detaljerade krav än vad som är lämpligt att reglera på lagnivå. Vår bedömning är att det i systemet bör finnas utrymme för en aktiv förvaltning av tillitsramverket och de regler som behövs för lämplig säkerhetsnivå.

6. Färdplan

6.1 Nyckelaktiviteter

6.1.1 Definiera och kommunicera

Att definiera begreppet ”Tillit” och hur detta uppnås är en förutsättning för att kunna definiera målet med byggblocket. Andra begrepp som till exempel ”organisationstillit” behöver förtydligas.

Att skyndsamt och kontinuerligt informera och kommunicera till byggblock om förutsättningarna att bygga tillit minskar risken att dessa gör felaktiga antaganden med stor påverkan av deras resultat och tidplan.

6.1.2 Identifiera tillitsnivåer

Förbereda identifiering av tillitsnivåer och verksamheter med olika krav på tillit ger förutsättningar till ett skalbart tillitsramverk där informationens klassificering styr hanteringen. Avgränsningar för skyddsklassad information ska beaktas.

6.1.3 Omvärldsanalys

Initiera dialog om befintliga tillitsramverk, såsom Sweden Connect. Detta förbättrar möjligheten till integration av dessa befintliga tillitsramverk samt återanvändning av redan förankrade ramverk.

6.1.4 Förslag till ramverk

Sammanfattning av huvudleveransen som bygger på aktiviteterna ovan och på fundamenten Regler-Stöd-Uppföljning-Konsekvens.

6.1.5 Förslag till förvaltning

Ett ramverk som lever över tid kräver en effektiv förvaltning.
Ett förslag kommer att tas fram. Att hålla tillitsramverket aktuellt är en förutsättning för acceptans och följsamhet.

6.1.6 Förslag till realiseringsplan

Implementering av tillitsramverk i samverkan med realiserande byggblock.

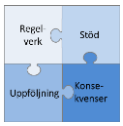
6.2 Identifierade milstolpar

Inriktningen på arbetet bygger på att analysera och komplettera befintliga tillitsramverk såsom exempelvis Sweden Connect.

- **Kort perspektiv**: Förslag på ramverk, införande och förvaltning
- **Långt perspektiv**: Införa och förvalta föreslaget tillitsramverk.

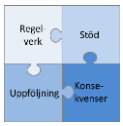
Nr	Beskrivning av delleveranser i kort perspektiv	Klart datum	Klartkriterier	Uppskattade Timmar	Ansvar
1	Begreppet ”Tillit” definierat i kontexten ”samverkan mellan aktörer inom välfärden” inklusive ”organisationstillit”	2020-10-16	Textuell beskrivet som underlag till förankring.	14 (Förarbete: 4 tim, GRP 10 tim)	AM
2	Riskanalys genomförd	2020-10-23	Fördel om vi kan ta del av tidigare riskanalys	35 (Inläsning 5 tim, GRP 25 tim, efterarbete 5 tim)	KJ + Alla
3	Förslag på resurs- och kompetenssäkring klar	2020-10-23	Förutsättning för fortsatt leverans	5 (GRP)	All
4	Initierat identifiering av tillitsnivåer ”Level of trust”	2020-11-13	Arbetet initierat	10	Alla

5	Omvärldsanalys uppstartad	2020-11-27	Tillitsramverk hos leverantörer av välfärdstjänster	20 (GRP)	Alla
6	Rättslig analys	2020-11-27	Övergripande analys genomförd	20	Extern
7	Förslag till konceptuellt ramverk	2020-11-27	Principer framtagna	80	Alla
8	Förslag på regelverk på konceptuell nivå	2021-01-31		20 (GRP)	Alla
9	Operativt samarbete med kompetensområdet Informationssäkerhet etablerat	2021-01-31		8	RÅE & LC



Nr	Beskrivning av delleveranser i ett långt perspektiv, realiseringsplan	Klart datum	Klartkriterier	Uppskattade Timmar	Ansvar
1	Förslag till förvaltning	2021-Q1	Konceptuellt	80	Alla
2	Utformning av ramverk utifrån omvärldsanalys och konceptuellt tillitsramverk. Sker agilt med en hög grad av involvering av verksamheterna	2021-Q1-Q2	Omhändertagna och inarbetade synpunkter från berörda parter, byggblock och juridik	1000 Team på 5 pers. Referens-grupp	Block
3	Redaktionellt färdigställande av tillitsramverk för fastställning.	2021-Q3	Fastställt och förankrat ramverk	80	Block
4	Realisering - Kommunikation - Utbildning - Pilotanslutningar - Servicedesk Koordinerat med övrig realisering av RU	6 - 12 mån efter att finansiering och kompetensförsörjning är klar	Genomförande och implementering av tillitsramverket	3000 8 pers 20%	Block eller ingå i ”Masterplan”?
5	Etablera förvaltning (uppdrag, finansiering, personal etc.)	Bör utföras parallellt med realiseringen	Organisation och processer etablerat	3000 8 pers 20%	DIGG

6	Avslut - Arkivera - Avsluta arbetsgrupper etc.	22Q4 Enligt övergripande mål och prioritering inom regering suppdraget	Förvaltning självgående för vidare arbete	40	?



6.3 Identifierade beroenden

Block	Förslag på hantering	Ansvarig
Identitet, tidplan	- Ta in expertis från nuvarande nationella tillitsramverk och samverka med berörda byggblock.	
Auktorisation, arkitektur	- Skyndsam och kontinuerlig information om vårt arbete. Öka förståelsen för vårt resultat i andra berörda block	
Spårbarhet, arkitektur	- Deltagande vid uppstart av blocket.	
Styrning och struktur, informationssäkerhet	- Samordning av blocken och kompetensområden	
Styrning och struktur, arkitektur	- Avsaknad av övergripande arkitektur för hela ekosystemet	

7. Risk- och konsekvensanalys

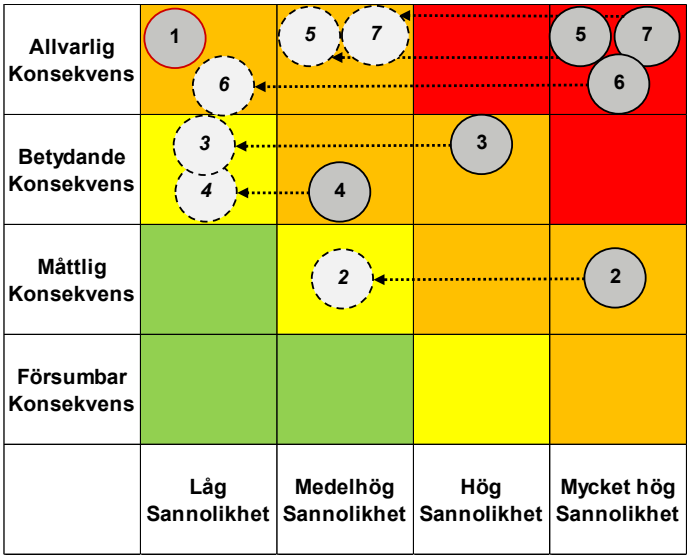
En övergripande risk- och konsekvensanalys har genomförts inom byggblocket. De identifierade riskerna och förslag på åtgärder finns dokumenterat på en skyddad lagringsyta hos DIGG.

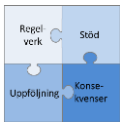
Byggblocket påverkar och påverkas av den förvaltningsgemensamma digitala infrastrukturen vilket visas i den dokumenterade riskanalysen. Dokumenterade risker, sårbarheter och hot bedöms i beskrivna scenarion kunna ge konsekvenser för hela den digitala infrastrukturen och behöver analyseras vidare. Förslag till åtgärder och hantering av risker, hot och sårbarheter i riskarbete har visat sig kunna minska sannolikheten och sänka konsekvenser om risken ändå inträffar på både kort och lång sikt.

Nettorisker, dvs de risker som inte hanterats visas som mörkare gråa ringar och bruttoriskerna visas som ljusare ringar med streckad kant.

Ett tillitsramverk påverkar stora delar av den förvaltningsgemsamma digitala infrastrukturen vilket visas i analysen. **Flera risker bedöms kunna ge allvarliga konsekvenser för hela det digitala ekosystemet och bör analyseras och hanteras i det fortsatta arbetet.**

Förslagen på hanteringen av bruttoriskerna visade sig reducera sannolikheten för att risken skulle inträffa men inte dess konsekvens om den ändå inträffar. Detta bör analyseras djupare.





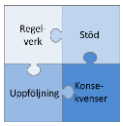
Ett fortsatt systematiskt informationssäkerhetsarbete kommer ske genom att löpande och kontinuerligt värdera sårbarheter, risker och hot inom byggblocket utifrån vilken etapp/fas byggblocket befinner sig i. Vi har även påbörjat riskarbetet av beroenden mellan byggblock inom den digitala infrastrukturen och mot grunddatadomänerna för att riskanalysera och fastställa robusthet och säkerhetsskydd för helheten i den digitala infrastrukturen.

8. Bilaga. Tillitsmatriser (fortsatt arbete)

KRAV			
Tillitsnivå	**VEM**	**VAD**	**HUR**
Mycket Hög			
Hög			
Basnivå			
Låg			

STÖD			
Tillitsnivå	**VEM**	**VAD**	**HUR**
Mycket Hög			
Hög			
Basnivå			
Låg			

UPPFÖLJNING			
Tillitsnivå	**VEM**	**VAD**	**HUR**
Mycket Hög			
Hög			
Basnivå			
Låg			



KONSEKVENS			
Tillitsnivå	**VEM**	**VAD**	**HUR**
Mycket Hög			
Hög			
Basnivå			
Låg			