IT-forskningsstöd

En strategi att stödja forskningen genom IT

Dokumenthistorik

Version	**Datum**	**Ändrad av**	**Utförda förändringar**
0.1	2020-12-15	C. M. Wettercrantz	Initial version
0.9	2021-03-23	Arbetsgruppen	Version till referensgruppen
1.0	2021-04-07	Referensgruppen	Inga ändringar

Innehållsförteckning

1 Inledning

1.1 Uppdrag

Sveriges universitet och högskolors IT-chefsforum gav i uppdrag till IT-arkitektnätverket ATI under 2020 att närmare utreda frågan hur en lärosätesgemensam referensarkitektur kopplat till IT-forskningsstöd bör utformas. Målet med initiativet var att ge lärosäten stöd i att skapa ett effektivt IT-forskningsstöd som ger forskarna viktiga verktyg för att möjliggöra framsteg i sin forskning.

En dedikerad arbetsgrupp inom ATI skapades för att driva de olika aktiviteter som krävdes för att nå ett resultat. Arbetsgruppen bestod av:

Mikael Wettercrantz, KI
Per-Olof Andersson, UU
Ola Ljungkrona, GU
Per Hörnblad, UmU
Sören Berglund, UmU

Arbetet bedrevs under 2020 och resulterade i en referensarkitektur för IT-forskningsstöd.

1.2 Målgrupp

Målgrupp för dokumentet är ledningsnivå vid lärosäten för högre utbildning i Sverige.

1.3 Vad är en referensarkitektur?

En referensarkitektur ger traditionellt en mall för att lösa ett problem inom en specifik domän. Referensarkitekturer kan verka på olika nivåer och i olika abstraktionsnivåer. Syftet med en referensarkitektur är att ge stöd och vägledning för hur en lösning i en viss domän bör implementeras. Det är viktigt att komma ihåg att referensarkitekturer alltid är rådgivande och alltid behöver anpassas efter de förutsättningar som gäller för den specifika implementation. Referensarkitekturen måste initialt alltid analyseras och konfigureras så att den passar lokala förutsättningar och förhållanden.

I detta fall så presenteras en referensarkitektur som har till avsikt att beskriva vilka tjänster, aktörer och dess relationer i olika nivåer som behöver vara på plats på lärosätet kunna understödja forskningen med ett effektivt IT-forskningsstöd. För varje lärosäte så behöver man göra en analys av referensarkitekturen för att sedan genomföra en lokal anpassning och konfiguration utifrån de förutsättningar som lärosätet har kopplat till organisation, resurser, inriktning etc.

Referensarkitekturen för forskningsstöd skall ses som rådgivande och som ett stöd för att lokalt på lärosätet inspireras att komma vidare med planering och senare implementation av ett fungerande forskningsstöd.

2 Bakgrund

För att stödja lärosätena inom sektorn för högre utbildning att uppnå de mål som finns att vara framstående och ledande inom forskning i en rad olika områden skapades på uppdrag av ITCF ett initiativ runt IT-forskningsstöd inom ATI. Målet med initiativet var att ge forskningen det IT-stöd som på bästa möjliga sätt möjliggör framsteg och resultat samtidigt som det avlastar forskarna i deras vardag. En dedikerad arbetsgrupp inom ATI skapades där ett antal lärosäten bjöds in för att arbeta fram en referensarkitektur inom området för IT-forskningsstöd. I en första fas genomfördes en inventering, genom enkäter, vilka lärosäten som har pågående eller ännu ej startade initiativ inom IT-forskningsstöd. I en andra fas jämfördes olika initiativ och ur materialet utarbetades en referensarkitektur fram vars syfte är att stödja lärosäten i arbetet med IT-forskningsstöd.

I detta arbete har följande organisationer bidragit, Dalarnas universitet, Göteborgs universitet, Svensk Nationell Datatjänst (SND), Stockholms universitet, Sunet, SNIC, Umeå universitet, Uppsala universitet samt Örebro universitet.

Följande effektmål togs fram för arbetet:

- Förenkla samarbetet mellan forskare vid svenska lärosäten
- Göra forskning och resultat mera lättrörliga
- Främja innovation genom rätt förutsättningar

3 Definitioner

3.1.1.1 Forskningsinformation / Forskningsdata

När vi talar om forskningsinformation menar vi den information av olika slag som skapas av forskare och andra för att beskriva forskningsverksamhet. Detta görs ofta idag genom interaktion med olika tjänster och ibland med en person som stöd till forskaren som exempelvis ekonom eller forskningskoordinator. I forskningsinformation räknas många olika typer av information in, t.ex. information om forskare, organisation och projekt. Vi har utgått från hur Vetenskapsrådets (VRs)Nationella styrgrupp definierar forskningsinformation i definitionen i detta dokument. Som forskningsinformation räknas strukturerad information om:

- Forskare
- organisationer och organisationsstrukturer
- pågående forskning i form av projekt, program eller satsningar
- finansiering av forskning
- forskningsoutput (tex rapporter, publikationer, patent)
- Forskningsinfrastrukturer

Även om forskningsdata och forskningsdokumentation inte är direkt relaterat till forskningsinformation i denna definition kan även dessa typer kopplas till forskningsinformations-arbetet framöver. Forskningsinformation finns ofta spridd mellan olika aktörer i olika system.

(Definition hämtad från SUHF rapporten “Erfarenheter från forskningsinformationsarbete på lärosätena”)

3.1.1.2 RDO/RDC

RDO/RDC står för Research Data Office eller Research Data Centre. Flera lärosäten har idag inrättat denna funktion som har i uppdrag att stötta forskare i frågor om datahantering och forskningsdokumentation. Det kan t ex gälla stöd till forskarna att uppfylla formella krav på t ex datahanteringsplaner och laguppfyllnad vid hantering av personuppgifter, men också praktisk hjälp att välja rätt teknisk lösning för lagring och delning.

RDO organiseras lite olika på olika lärosäten men är ofta bemannad med personer från olika delar av organisationen, t ex IT och bibliotek.

3.1.1.3 IT-avdelning

Traditionellt är IT-avdelningens uppdrag inom en organisation att stödja den övriga verksamheten i organisationen i deras uppdrag genom att tillhandahålla IT-stöd som effektiviserar verksamheten.

3.1.1.4 IT-system

Ett IT-system är ett system som ger IT-stöd och utgörs av en eller flera tekniska komponenter som enskilt eller i samverkan samlar in, bearbetar, distribuerar samt lagrar information.

3.1.1.5 FAIR

FAIR är ett antal principer som enligt Kungliga biblioteket definieras enligt:

Syftet med principerna är att möjliggöra återanvändning av forskningsresultat, till exempel publikationer, forskningsdata och kod. Informationen ska vara tillgänglig för människor och läsbar för maskiner.

Digitaliseringen skapar nya vägar för samverkan och nya sätt att sprida forskningsresultat. Därför finns en strävan mot öppenhet i den vetenskapliga processen. Publikationer bör finnas öppet tillgängliga, vara sökbara och innehålla information om hur de kan användas.

FAIR är ett samlingsnamn på fyra ledord som ska stärka möjligheten att återanvända forskningsresultat. Principerna innebär att publikationer och forskningsdata ska vara:

- **F**indable (sökbara)
- **A**ccessible (tillgängliga)
- **I**nteroperable (kompatibla)
- **R**eusable (återanvändbara)

3.1.1.6 IaaS / PaaS /SaaS

IaaS – Infrastructure as a service är komponenter som t.ex. nätverk, datalagring, beräkningskraft

PaaS – Platform as a service är komponenter som t.ex. databaser, applikationsservrar, webhotell

SaaS – Software as a service är komponenter som t.ex. lönesystem, e-post, bokningssystem

Dessa förhåller sig till varandra i en hierarki enligt:

3.1.1.7 Molntjänster

Molntjänster, molnet eller cloudtjänster, är IT-tjänster som tillhandahålls över Internet, i synnerhet funktioner som traditionellt sköts på egna datorer men genom molnet sköts av någon annan. Det kan till exempel handla om tillämpningsprogram, serverprogram och lagring av data. I praktiken handlar detta om en industrialisering av IT.

3.1.1.8 SNIC

SNIC är en nationell forskningsinfrastuktur som tillhandahåller resurser för databehandling, datalagring samt avancerat användarstöd till svenska forskare. SNIC finansieras av Vetenskapsrådet och 10 olika lärosäten.

3.1.1.9 SUNET

Sunet (Swedish University Computer Network) är en forskningsinfrastruktur som tillgodoser behovet av datakommunikation hos svenska lärosäten och andra offentliga organisationer med koppling till forskning eller högre utbildning. Vi levererar också tjänster till anslutna organisationer.

3.1.1.10 Integration

Systemintegration innebär att två eller flera olika fristående IT-system kopplas ihop för att dela information med varandra. Integrationer är oftast tekniska och automatiserade men kan även vara manuella och bestå av rutiner och manuella handgrepp. En integration är alltid styrd av ett förutbestämt regelverk och definitioner.

3.1.1.11 GDPR

Dataskyddsförordningen (GDPR, The General Data Protection Regulation) gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras.

(Definition hämtad från integritetsmyndighetens hemsida www.imy.se)

3.1.1.12 OSL

Offentlighets- och sekretesslagen (OSL) (2009:400) är en svensk lag som trädde i kraft den 30 juni 2009, och samtidigt ersatte sekretesslagen (1980:100). Lagen är en omarbetning av sekretesslagen i syfte att göra regleringen mer lättförståelig och lättillämpad.

Lagen, som består av sju avdelningar, innehåller bestämmelser om myndigheters och vissa andra organs handläggning vid registrering, utlämnande och övrig hantering av allmänna handlingar. Lagen innehåller också bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Förbud att röja uppgift gäller om det sker muntligen eller genom utlämnande av allmän handling eller på något annat sätt. Bestämmelserna innebär begränsningar i

- yttrandefriheten enligt regeringsformen,
- rätten att ta del av allmänna handlingar som följer av tryckfrihetsförordningen samt i vissa fall även
- rätten att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

(Definition hämtad från Wikipedia)

3.1.1.13 Artificiell Intelligens

Artificiell intelligens (AI) är egentligen ett område in om IT och inte specifika system eller lösning. Det finns ingen vedertagen definition av AI men det som kännetecknar AI är ett datorsystem som utifrån ganska vida ramar och regelverk kan fatta nya och beslut, ett beslut i detta sammanhang behöver nödvändigtvis inte vara det som i dagligt tal avses med beslut utan inom AI kan detta närmast ses som en mängd slutsatser med olika grad av sannolikhet. Typiska AI tillämpningar är mönsterigenkänning, beslutsstöd, automatisering, förstärkt verklighet (AR). AI delas typiskt in i tre nivåer:

- Snäv AI: Återfinns i inbäddade system och som delar i större lösningar, snäv AI är mycket effektiv inom ett starkt avgränsat område och dess förmåga till inlärning relativt begränsad. Typiska tillämpningar är enklare mönsterigenkänning, navigation, automation.
- Generell AI: System som till sin natur efterliknar de beslutsprocesser och förmåga till självständig inlärning baserat på tidigare erfarenheter liknande den mänskliga hjärnan. Typiska tillämpningar är avancerad mönsterigenkänning, beslutsstöd, maskininlärning (ML) baserat på stora datamängder, vissa kognitiva förmågor.
- Super AI: Ett självreproducerande system vilket genom mycket snabba generationer konstant förbättrar sina egna förmågor, ramar och regelverk långt bortom det ursprungliga. Idag finns inga tillämpningar då denna nivå fortfarande är hypotetisk.

4 Referensarkitektur

4.1 Ansats

Referensarkitekturen är som tidigare omnämnts ett stöd och föreslaget angreppsätt på en rådgivande nivå varför den behöver anpassas till egna lokala förutsättningar beroende på faktorer så som den egna organisationens indelning, grupperingar och avgränsningar. Vidare kan förhållande så som egen IT-drift eller extern sådan spela in.

Referensarkitekturen har en organisatorisk utgångspunkt där olika delar inom verksamheten samverkar med varandra men där ansatsen är att minska överlapp och dubbleringar av kompetens och leveranser.

Referensarkitekturen har också utgångpunkt i IT och en tjänstebaserad IT-leverans, den gör ingen ansats att vägleda övrig forskningsstödjande verksamhet eller forskningsinfrastruktur förutom de delar som är direkt påverkande på IT och dess förmåga att leverera ett brett och / eller specialiserat IT-forskningsstöd.

I arbetet med framtagandet av referensarkitekturen har det framkommit att ett vanligt scenario vid svenska lärosäten är att institutioner eller liknande avgränsade verksamhetsdelar mer eller mindre oberoende av centrala IT leveranser bygger en helt egen leveransorganisation för den egna verksamheten och dess behov. Denna leverans kan vara heltäckande både vad gäller personal och tekniska bastjänster där allt från klienter, licenser, support till högspecialiserad kompetens inom till exempel data-analys och praktisk datahantering ingår i den egna organisationen. Utan tvivel är ofta denna leverans mycket väl anpassad och ger ett utmärkt stöd till den egna institutionen eller verksamheten.

Detta är problematiskt på flera sätt:

- Man använder inte resurser effektivt vid lärosätet eftersom det mest troligt finns flera delar av lärosätet som har samma eller liknande behov av IT-stöd till forskningen.
- Man kan få problem att använda övriga centrala tjänster då de egna inte linjerar tekniskt och / eller logiskt med de centrala vilket skapar en fragmentering av data och tjänster där i värsta fall användare och forskare inte får det stöd de behöver fullt ut.
- Informationssäkerheten blir svårare att upprätthålla då dessa funktioner oftast placeras centralt och har en god överblick och kunskap om de centrala IT-tjänsterna men ofta har svårare att nå ut till institutioner och liknande varför det blir problematiskt om stora mängder data och hanteras och lagras mera perifert vid lärosätet. Vidare har framkommit att kunskapen och förståelsen för lagar och regelverk så som GDPR och OSL i många fall är bristfällig.
- Samarbete med forskare vid andra institutioner och lärosäten försvåras ibland då samarbete i detta perspektiv förutsätter ett bra och väl utvecklat IT-stöd där till exempel identitetshantering, verktyg för samarbete, tekniska skydd för överföring och delande av data vanligtvis finns centralt men där lokala dito visserligen passar den egna verksamheten väl men mindre väl med övrig verksamhet vid lärosätet eller nationellt.
- En mindre lokal IT-organisation blir ofta mera sårbar och har svårare att kompensera för varierande leveransbehov och påverkan av den egna leveransförmågan vid till exempel sjukdom och ledigheter.

Referensarkitekturen försöker att adressera dessa problem utan att göra avkall på förmågan att kunna leverera specialiserade IT-lösningar och expertstöd samtidigt som den drar nytta av det faktum att storskalighet alltid lönar sig inom IT. Den lägger även stort fokus vid att främja samarbete med externa parter.

I framtagandet av referensarkitekturen har en analys av vilket tekniskt stöd som finns inom olika områden gjorts i referensgruppen. Denna analys ger vid handen att det tekniska stödet vid ingående lärosäten är tämligen likartat både vad gäller faktiska tekniska lösningar och vilka områden som täcks in väl och vilka som täcks in mindre väl. Mer om denna analys längre fram.

4.2 Struktur och samverkan

Referensarkitekturen utgår från stapelprincipen där varje lager bygger på det underliggande samtidigt som komplexitet och specialisering ökar med högre lager i stapeln.

Stapelprincipen är särskilt tillämplig inom IT där de flesta moderna lösningar med tillhörande arkitektoniska principer bygger på just denna princip.

Botten av stapeln utgör en robust grund baserad på beprövade teknologier och lösningar där standardisering och storskalighet är nyckelbegrepp, det är också I detta lager den största kostnaden för leveransen hamnar varför storskalighet är viktigt då det som tidigare nämnts är något av en naturlag inom IT gällande kostnadseffektivitet.

I överliggande lager återfinns relativt kostsamma lösningar och system som var för dig är stora investeringar men som i helheten inte utgör den största kostnaden.

Återigen kan detta vara något som, beroende på lokala förutsättningar och verksamhetens art, kan vara omvänt som exempel kan nämnas ett lärosäte som har en eller flera superdatorer vilka hamnar ett lager upp från botten.

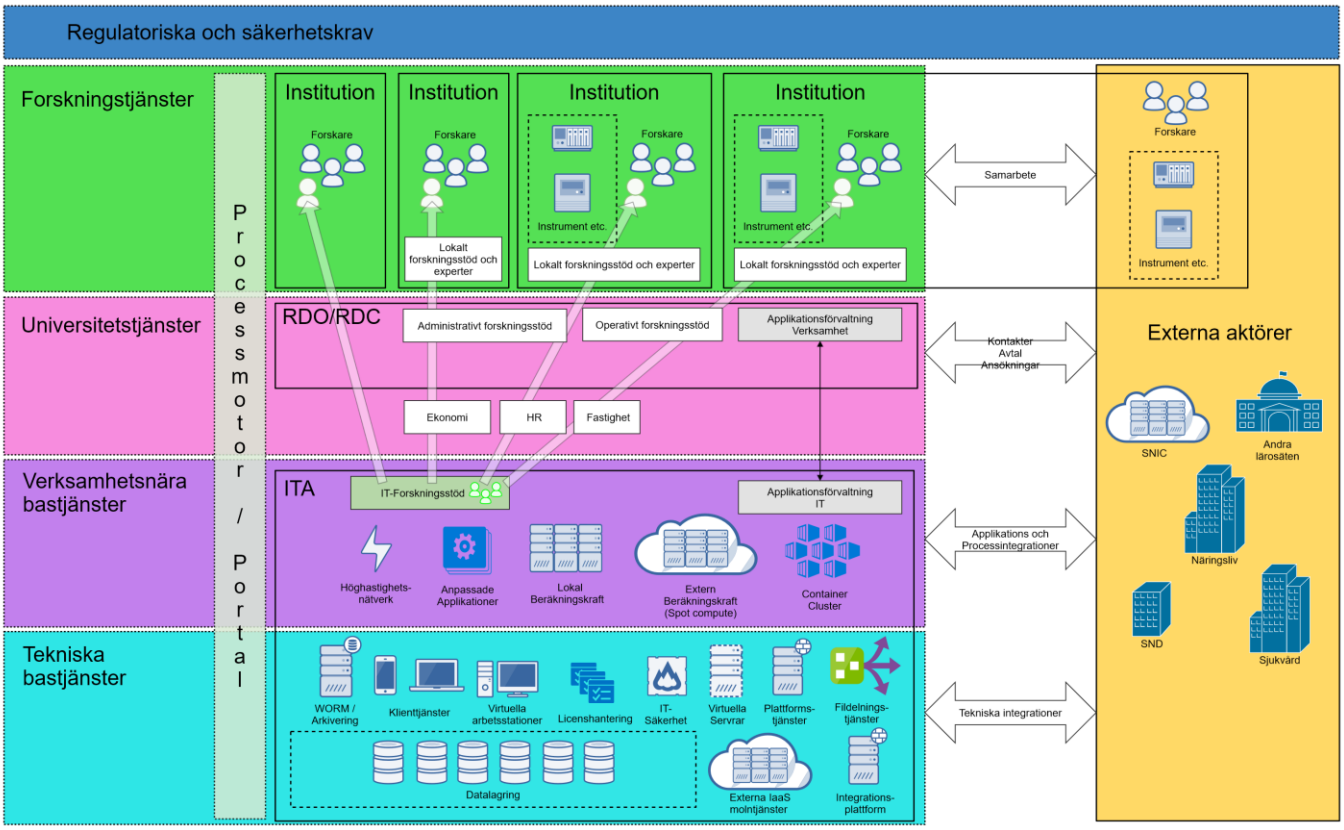
Specialisering är också något som ökar ju högre upp i stapeln man kommer och i och med specialisering grenar även områdena ut sig till fler och smalare varför mer och mer spetskompetens behöver tillföras.

Problemet som idag finns inom många verksamheter är att spetskompetensen visserligen behövs men inte till en heltid. Genom att samla denna spetskompetens centralt och tillgängliggöra densamma för fler uppnår man en bättre effektivitet samtidigt som flera forskargrupper, institutioner och liknande får tillgång till dessa vilka i många fall varit låsta till några få där de grupper med mindre behov av spetskompetens helt enkelt inte har kunnat motivera kostnaden i en heltidsanställning vilken inte kan nyttjas fullt ut.

Samverkan med externa parter sker också i enlighet med stapelprincipen där, precis som i den interna organisationen och leveransen, varje lager ansvarar för och levererar inom sitt respektive område och bör i möjligaste mån sträva efter att hitta en motsvarande part hos den externa parten.

4.3 Referensarkitektur

Nedan beskrivs referensarkitekturen i huvudsak nerifrån och upp samt grafiskt.



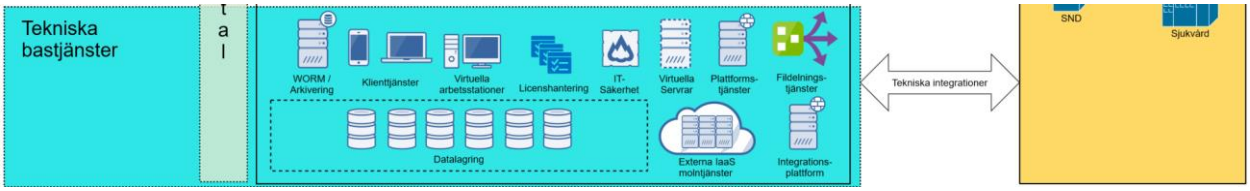
4.3.1 Tekniska bastjänster

I detta lager återfinns det som i mångt och mycket förknippas med traditionell IT-drift.

Nedan avsnitt (4.3.1.X) är inte på något vis att se som vare sig heltäckande eller exkluderande utan är resultatet av arbetet och arbetsgruppens erfarenheter över vilka delar som bör ingå i detta lager.

Inom tekniska bastjänster arbetar man med beprövad teknik, och standarder i så stor utsträckning som möjligt, det är också här storskaliga lösningar återfinns där dess komponenter används och återanvänds i de flesta överliggande tjänsteleveranser. Tekniska bastjänster bemannas och supporteras av den befintliga klassiska IT-avdelningen med dess förmågor och processer.

Många nödvändiga delar finns inte med I referensarkitekturen då dessa ses som förutsättningar snarare än ingående komponenter, dessa kan vara delar som nätverk, datacenter, backup och så vidare.



Interaktion och integration i detta lager handlar främst om tekniska integrationer för överföring och spridning av data men också tillgång till externa tjänster och system via t.ex. APIer eller federationer.

4.3.1.1 Datalagring

Förmågan att lagra data är att se som något av grundfundamentet i IT-forskningsstödet, det är här alla informationstillgångar samlas centralt för att uppnå just den storskalighet som krävs för kostnadseffektivitet och kontroll. Lösningen behöver kunna skala både i prestanda och kapacitet i tämligen små steg för att inte orsaka allt för stora fluktuationer i kostnader. Lösningen behöver inte nödvändigtvis vara helt sammanhållen i ett och samma system, till exempel kan de klassiska begreppen SAN och NAS separeras i olika lösningar beroende på vilka de lokala förutsättningarna är. Viktigt är dock att väga uppdelning mot stordriftsfördelar. Datalagringen behöver stödja alla större och vanligt förekommande protokoll för åtkomst så som CIFS, NFS, S3, iSCSI och således behöver lösningen kunna hantera både fil-, block- och objekt-lagring. Behörigheter och annan åtkomststyrning behöver också vara väl integrerade med befintliga centrala IAM-system.

4.3.1.2 Klienttjänster

Här återfinns den klassiska centralt administrerade och supporterade Windows- och Mac-klienten. Ur perspektivet IT-forskningsstöd behöver klienttjänsten stödja de inom forskningen vanligt förekommande applikationerna för dataanalys, databearbetning, samarbete etc. Klienttjänsten bör också innehålla en tillräcklig bredd av hårdvara för att tillgodose både mobilitet och relativt höga krav på prestanda.

4.3.1.3 WORM / Arkivering

För att uppfylla kraven som ställs gällande bevarande och tillgängliggörande av forskningsdata behöver tjänster för arkivering och I vissa fall även WORM (Write Once Read Many) finnas. Dessa tjänster använder normalt underliggande tjänster för datalagring som omnämns ovan. Det är också dessa tjänster som svarar upp för kraven som ställs inom EU-direktivet FAIR och man bör om möjligt göra integrationerna från metadatasystem för detta mot just de egna tjänsterna för arkivering och WORM. Exempel på metadatasystem för FAIR är SNDs DORIS.

4.3.1.4 Licenshantering

Ett problem som identifierats hos många lärosäten är licenshantering där det finns en osäkerhet i vilka licenser som finns, hur många och vilka villkor som gäller för användande. Ofta kostar applikationer för dataanalys, datainsamling och databearbetning stora summor och i många fall är alternativen få eller obefintliga varför det i mångt och mycket är en leverantörernas marknad. Det finns mycket stora vinster I att hantera licenser centralt då det vanliga är att lärosätet är en och samma juridiska person varför inköpta licenser avtalsmässigt normalt sett kan användas över hela lärosätet och inte bara hos den institution som gjort inköpet. Lärosätet som helhet har också ofta större möjligheter att förhandla med leverantörer om priser och villkor vid större inköp än om dessa sker i mindre skala. Man bör här också sträva efter licensmodeller baserade på antal samtidiga användare för att på så sätt effektivast möjligt utnyttja gjorda investeringar. Lika viktigt som att inte vara underlicensierad är att inte vara överlicensierad vilket kan uppnås med en central hantering av licenser. En central hantering av licenser är också en stor fördel i tjänsterna virtuella arbetsstationer och klienter.

4.3.1.5 Virtuella servrar (IaaS)

En grundläggande komponent i de flesta system och lösningar är virtuella servrar vilka erbjuder en mycket kostnadseffektiv och flexibel plattform att bygga tjänster på. Tekniken är välbeprövad och mogen varför den lämpar sig mycket väl som tjänst till forskargrupper och institutioner. IaaS lämpar sig för de behov där andra redan befintliga SaaS tjänster inte är tillräckliga eller där en lösning baserad på container och plattformstjänster inte passar. IaaS innebär ett större ansvar och kunskap hos användaren varför andra lösningar bör övervägas först.

4.3.1.6 Virtuella arbetsstationer

Behovet av beräkningskraft för analys och databehandling upp till medelnivå blir allt större inom de allra flesta forskningsområden samtidigt som kraven på informationssäkerhet ökar. Klassiskt har man löst behovet av beräkningskraft av medelnivå genom investeringar i arbetsstationer, en typisk arbetsstation renderar i en investering om mellan 100–200 tusen kronor och har en typisk livslängd om ca. 4 år. Vid många lärosäten finns heller inga tjänster från central IT inom området arbetsstationer varför forskargrupper och institutioner måste tillgodose dessa behov på egen hand där ofta kompetens såväl som resurser brister.

En virtuell arbetsstation bygger i grund och botten på samma tekniska komponenter, teknik och miljöer som IaaS med adderade lager för att tillgängliggöra en skrivbordsupplevelse genom så kallad VDI (Virtual Desktop Infrastructure). De primära fördelarna är:

- Enklare handhavande för forskargrupper och institutioner.
- Sänkta kostnader för forskargrupper och institutioner då man inte behöver hantera en stor investering med en avskrivningstid om minst 4 år samt administration och support under denna tid.
- Möjlighet att nyttja tjänsten bara under den tid man behöver vid till exempel gästforskare, kortare projekt, projekt med varierande behov.
- Möjlighet att snabbt kunna ändra hårdvarubestyckningen efter behov.
- Stora möjligheter att bygga säkra och avgränsade miljöer där kontroll av både in och utförsel av data kan göras på flera nivåer.
- Mycket större flexibilitet i vilka applikationer som erbjuds där ny eller ominstallation inte är nödvändig.
- Åtkomst till beräkningsresurser via Internet med bibehållen säkerhet.

4.3.1.7 Plattformstjänster

Plattformstjänster utgör byggstenarna för att bygga specialiserade och unikt anpassade lösningar utan behovet att ansvara för och administrera alla underliggande lager vilket medför sänkta kostnader och snabbare utveckling. Typiska plattformstjänster är webhotell, databashotell, applikationsservrar, objektlagring.

4.3.1.8 Fildelningstjänster

Behovet att samarbeta runt data och utbyta data mellan forskargrupper och / eller andra externa parter ökar i och med ökade datamängder inom forskningen. Att kunna göra detta på ett enkelt och samtidigt säkert sätt är en förutsättning för att upprätthålla god informationssäkerhet och i förlängningen förtroendet för den egna forskningen och lärosätet i stort. Fildelningstjänster bör kunna hantera känsliga personuppgifter och vara byggda på ett sätt som kräver att endast den ena parten behöver affileras eller på annat sätt anknytas till lärosätet. Viktigt är att tydliga regler och riktlinjer för användande av fildelningstjänster finns och tillämpas då det i stort ankommer på den enskildes ansvar att data delas rätt. Enkelheten i fildelningstjänsterna är inte obetydlig då allt för svåranvända tjänster tenderar till ett användande av andra icke säkra metoder för datadelning.

4.3.1.9 Integrationsplattform

Ofta finns behovet att koppla samman olika system vid till exempel automation, återanvändning dynamiska datakällor, berikande av data, datakontroll, datavalidering etc.

Genom att tillhandahålla en integrationsplattform kan detta göras enkelt och med stor grad av återanvändning vilken ökar i och med antalet system och lösningar som använder plattformen. En integrationsplattform bör stödja integrationer mot centrala datakällor så som IAM och egna datakällor samt i vissa fall även externa datakällor, integrationsplattformen bör således också stödja identitetshantering och åtkomstkontroll till integrationer. Med en integrationsplattform följer också ett behov av strategi och principer hur systemintegration skall genomföras.

4.3.1.10 IT-säkerhet

Med IT-säkerhet avses här, innefattande men inte uteslutande, tekniska lösningar som brandväggar, MFA (multifaktorautentisering) skydd mot skadlig kod, IPS (Intrusion Prevention System). Dessa delar ingår normalt i alla standardtjänster men ur detta perspektiv finns de med som tillgängliga komponenter att använda i forskningstjänster. En viktig princip är att varje tjänst var för sig skall bära sin egen säkerhet och inte till fullo förlita sig på externa lager så som generella brandväggar, VPN, LAN etc.

4.3.1.11 Externa IaaS och PaaS molntjänster

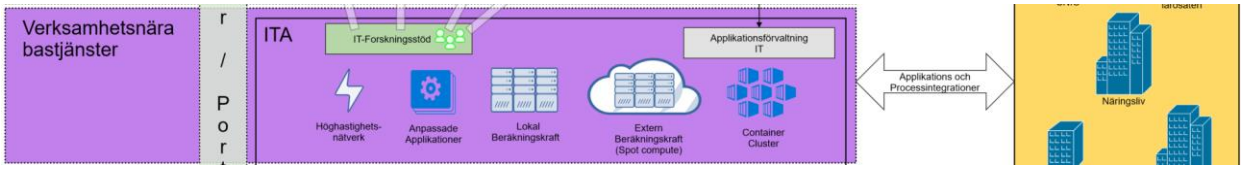
Genom att centralt avtala och möjliggöra användande av externa IaaS-tjänster skapar man en möjlighet till flexibilitet i lösningar. Privata externa aktörer har en större möjlighet att erbjuda kostnadseffektiva lösningar med hjälp av storskalighet än vad som normalt kan göras vid i den egna organisationen. En viktig del vid användande av externa IaaS och PaaS tjänster är den juridiska där men behöver ha klara processer och riktlinjer för vilken typ av data som kan behandlas och lagras i dessa.

Möjliga områden kan vara.

- Samarbete med externa aktörer både andra lärosäten och privata aktörer där man arbetar med och i samma lösning.
- Användande av IaaS och / eller PaaS tjänster som inte finns i den egna organisationen.
- Initiala skeden av utveckling av lösningar eller test där inte känsligt data hanteras.
- Möjlighet att snabbt skala upp och skala ner lösningar beroende på behov.
- En kombination där vissa delar av en lösning ligger externt och andra delar internt.
- Vid framtagande av lösningar som skall användas av många externa aktörer, antingen i den framtagna lösningen eller en kopia av den samma.

4.3.2 Verksamhetsnära bastjänster

Det som definierar detta lager är att tjänsterna i mångt och mycket står för sig själv och oftast inte verkar som komponenter i större lösningar, tjänsterna i detta lager använder dig dock i stor utsträckning av underliggande tjänster i lagret “tekniska bastjänster”.



Interaktion och integration i detta lager avser att möjliggöra samarbete och tillgång till olika former av slutanvändarsystem eller där processer automatiserat interagerar med sina externa motsvarigheter. Även saker som standardiserad flytt av analysmodeller inom AI och ML till och från externa parter sker i detta lager där parterna gemensamt skapar rätt förutsättningar för detta.

4.3.2.1 Höghastighetsnätverk

Många instrument och enheter för datainsamling och analys kräver antingen hög bandbredd för att överföra data till andra system eller har behov av extremt korta svarstider, i vissa fall både och. För att möta det behovet behöver lärosätet ha en väl definierad metod att tillgängliggöra denna typ av nätverk ute i verksamheten jämte en tydlig och transparent modell för finansiering av densamma. Ett problem som identifierats är att ofta drar leveranser av specialiserade nätverkstjänster ut på tiden just på grund av en otydlighet i hur dessa skall levereras och finansieras.

Exempel på teknik inom detta område är:

- 10/25/100Gb/s LAN
- InfiniBand
- 5G
- Olika proprietära trådlösa tekniker för IoT / övervakning

4.3.2.2 Lokal beräkningskraft

Till skillnad från arbetsstationer (klassisk eller VDI-Workstation) och SNIC eller motsvarande High Performance Compute (HPC) finns ofta ett behov av återkommande beräkningskraft av kraft och volym som ingen av de två förstnämnda kan tillhandahålla. En annan begränsning med SNIC eller motsvarande HPC är att tillgång oftast baseras på tilldelade tider kopplade till forskningsprojekt varför ett mera dagligt användande blir svårt.

Beroende på lärosätets och dess forsknings behov kan det vara nödvändigt att investera i en central egen Mid Performance Compute (MPC) eller HPC-lösning.

Erfarenheter från förstudien har visat att vissa institutioner vid lärosäten i vissa fall investerar i och själva administrerar en MPC- eller HPC-lösning som i de fallen väl fyller institutionens behov men ofta har svårt att användas av andra vid lärosätet. I de fall flera institutioner gör investeringar i MPC och / eller HPC får det även till följd att lärosätets totala möjliga nyttjande minskar i det att en större central lösning blir mera effektiv är flera mindre.

Lokal beräkningskraft skall inte ses som en konkurrent till SNIC eller motsvarande utan som ett komplement och en resurs som kan användas inom det område som faller mellan arbetsstationer och HPC.

4.3.2.3 Extern beräkningskraft

Detta är i princip samma sak som lokal beräkningskraft med skillnaden att denna köps som tjänst hos externa så kallade molnleverantörer. Beroende på användande kan den ena, andra eller båda nyttjas.

Fördelarna med extern beräkningskraft är att det är lätt att skala upp och ned efter behov samt att lärosätet inte behöver göra stora investeringar. Nackdelarna är att vissa typer av data inte alltid kan hanteras av externa parter samt att man är begränsad de tjänster och dess utformning som de externa leverantörerna erbjuder.

4.3.2.4 Container cluster

Enkelt uttryckt är detta efterföljande teknik till servervirtualisering även om container-teknik inte i alla tillämpningar kan ersätta den tidigare. Fördelarna är att olika delar av en lösning skiktas och återanvänds i underliggande lager varför effektiviteten ökar avsevärt. En annan fördel är att implementation av nya lösningar är väsentligt mycket snabbare än i en traditionell servervirtualisering.

Ur ett forskningsperspektiv finns flera fördelar med en containerbaserad infrastruktur.

- Fler och fler verktyg för dataanalys levereras idag som så kallade Docker-images och kan på kort tid implementeras om infrastrukturen finns på plats.
- Om forskargrupper eller lärosätet har ett tätt samarbete med externa parter som har en motsvarande containerinfrastruktur kan verktyg och modeller snabbt och lätt flyttas mellan olika parter.
- Området AI som inom många områden växer oerhört starkt är ofta tekniskt byggt med hjälp av containerbaserad teknik.
- Den lokala expertisen i en forskargrupp behöver inte spänna över alla mjukvarulager på samma sätt som i en klassisk servervirtualisering där istället experter kan fokusera på de faktiska verktygen som ligger närmast forskningen och dess resultat.

4.3.2.5 Applikationsförvaltning IT

Detta är en gruppering som verkar som motpart till *Applikationsförvaltning verksamhet.* Här återfinns administrativa applikationer som är forskningsstödjande, exempel kan vara elektroniska labböcker, bokningssystem, publikationstjänster, datakataloger etc. Denna gruppering behandlas närmare i avsnittet *Universitetstjänster*.

4.3.2.6 Anpassade applikationer

Till skillnad från applikationsförvaltning och dess administrativa applikationer återfinns här applikationer som används direkt i den konkreta forskningen och starkt bidrar till resultaten.

Problem som ofta uppkommer med applikationer av denna typ som är specialiserade, ofta unika och med få användare är att dessa passar dåligt in i befintliga modeller för förvaltning. Applikationsförvaltning syftar generellt till att under lång tid förvalta applikationer med många användare där stabilitet och långsam strukturerad förändring prioriteras. Dessa begrepp passa dåligt när det kommer till aktiv forskning som ofta är beroende av snabba, små iterativa förändringar med möjlighet att prova olika vägar för att utvärdera resultat och framtida utveckling. Vidare är ofta forskningens finansiering ett problem sett från den klassiska applikationsförvaltningens perspektiv där en långsiktig och stabil finansiering är nödvändig i det att förvaltningsplaner beslutas på årsbasis och sedan ligger mer eller mindre fast.

För att bemöta dessa svårigheter med att förvalta forskningsnära applikationer i en klassisk modell läggs dessa helt enkelt utanför denna och hanteras var för sig i tätt samarbete med forskargrupper. Den klassiska modellens begrepp får följande motsvarigheter.

Applikationsförvaltning verksamhet – Forskare och forskargrupp

Applikationsförvaltning IT – IT-forskningsstöd (gruppering, se nedan) och utpekade resurser

Anpassade applikationer byggs av de standardkomponenter och tjänster som återfinns i *Tekniska bastjänster* och *Verksamhetsnära bastjänster* och varför dessa i sig inte behöver förvaltas av IT-forskningsstödgruppen eller forskarna själva.

En viktig komponent för anpassade applikationer är återanvändbarheten genom Configuration as Code och Infrastructure as Code vilka är metoder att snabbt starta upp och konfigurera basen i de system och anpassade applikationer men avser att leverera mer om detta i avsnitt 4.3.4.

4.3.2.7 IT-forskningsstöd

IT-forskningsstöd är en gruppering bestående av personal med en tydlig forskarbakgrund eller motsvarande. Vika kompetenser som behövs är starkt beroende av lärosätets forskning men typiska profiler kan vara;

- Dataanalytiker
- Informatiker
- DBA med bakgrund inom utveckling
- Linux / Unix expert
- Specialkunskap inom HPC

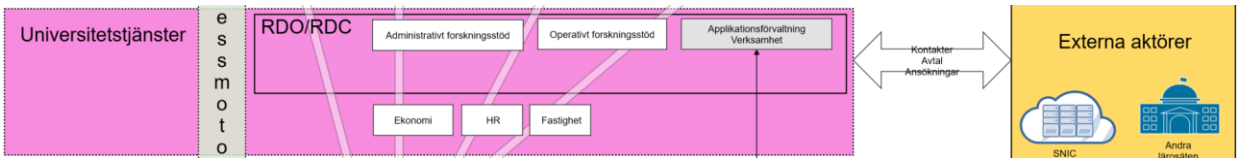
Denna gruppering finns normalt inte hos en IT-avdelning vid svenska lärosäten, i de fall den finns har det visat sig vara en mycket bra lösning och komplement för att stödja forskningen med IT.

Styrkan i detta kommer av att;

- Guppens personal skall kunna lånas/hyras-ut till forskningsprojekt på hel eller visstid där personen sitter tillsammans med forskare och arbetar i deras verksamhet och aktuella projekt.
- Gruppens breda kompetens gör att forskargrupper på så sätt har tillgång till den kompetens som behövs i olika skeden av projekten.
- Gruppen tillhör IT-avdelningen vilket innebär detta att det finns en närhet till alla resurser och kompetenser som kan behövas inom samt att det genom detta blir en upplevd större närhet till IT-avdelningen.
- Guppens erfarenheter kommer över tid att spänna över hela lärosätet och alla dess verksamheter och områden varför många lösningar och mönster kommer att kunna återanvändas på samma eller nya sätt inom olika områden.
- Gruppen kommer att bidra till att “bryta gamla mönster”, effektivisera och underlätta genom att med sin erfarenhet kunna råda och bistå forskare med rätt verktyg och lösningar som inte allt för sällan ligger utanför forskarens egen horisont.
- Genom att gruppens personal inte anställs av institution eller forskargruppen själv skapar detta en större flexibilitet att över tid ska upp och ned resurser samt använda olika kompetenser vid behov.

4.3.3 Universitetstjänster

Universitetstjänster ligger helt utanför IT-avdelningen och denna referensarkitektur har inte som ansats att definiera vilka dessa är eller hur de bör organiseras. De tjänster som har en direkt koppling till IT-avdelningen och forskningsstöd omnämns dock för att sättas i sitt sammanhang ur perspektivet att dessa är ett viktigt stöd för ett komplett IT-forskningsstöd. Dessa återfinns inom Research Data Office/Center (RDO/RDC). Övriga tjänster som Ekonomi, HR och Fastighet behandlas i avsnittet *Processmotor*.



Interaktion och integration i detta lager är av mera kontaktskapande och avtalsmässig karaktär där forskare och även IT-avdelningen får stöd och hjälp med detta genom RDO/RDC. Fördelen är att en gruppering har den övergripande kunskapen om det mesta av externa relationer och på så sätt man hjälpa andra i liknande situation.

4.3.3.1 Applikationsförvaltning verksamhet

Tillsammans med Applikationsförvaltning IT förvaltar denna gruppering administrativa forskningsstödjande applikationer så som elektroniska labblöcker, bokningssystem, publikationstjänster, datakataloger, Current Research Information System (CRIS) etc.

Gemensamt för dessa är att de inte kan sägas ha en ägare i en forskargrupp eller institution utan snarare betjänar hela lärosätet och har en långsiktig förvaltning.

Tre applikationer inom denna förvaltning och som hamnar inom ramen för referensarkitekturen är;

- **Processmotor** vilken behandlas i ett eget avsnitt
- **Datakatalog (Intern)** är den interna sammanställning över vilken data som finns tillgänglig vid lärosätet och som fritt eller under vissa förutsättningar kan användas av andra forskargrupper. Denna interna datakatalog i kombination med externa sådana t. ex. SNDs DORIS ger forskargrupper en större möjlighet att återanvända data i sin egen forskning.
- **Datakatalog (Extern)** kan vara en eller flera för olika ändamål. Det ändamål som här lyfts fram är den eller de kataloger som är nödvändiga för at uppfylla FAIR direktivet, de tekniska integrationer som behöver göras mot denna eller dessa kataloger förvaltas inom denna gruppering.

4.3.3.2 Administrativt forskningsstöd

Ur referensarkitekturens perspektiv ansvarar det administrativa forskningsstödet för;

- Regler och riktlinjer gällande datahantering inom forskningen
- Utformning av mallar t. ex. Datahanteringsplaner, juridiska avtal, ansökningar, generella beskrivningar
- Kontakter och avtal med externa parter som används av direkt forskare och mot vilka IT-avdelningen har tekniska integrationer antingen genom *anpassade applikationer* eller som tjänster som kan användas av IT-forskningsstödgruppen för forskares räkning t. ex. SNIC.

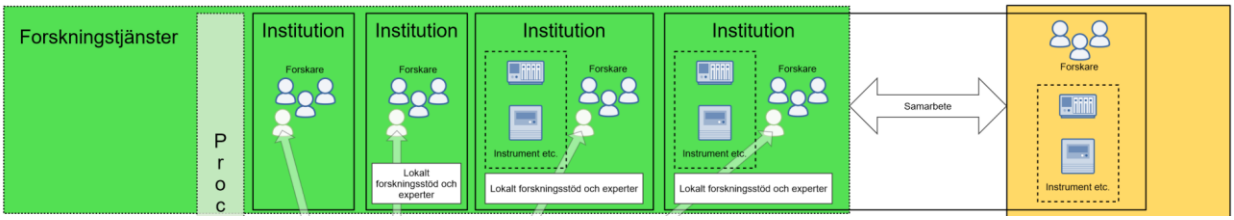
4.3.3.3 Operativt forskningsstöd

Det operativa forskningsstödet stödjer på ett mera konkret sätt forskningen och IT-forskningsstödsgruppen i frågor som;

- Etikansökningar
- Datahanteringsplaner
- Datautbyte med externa parter
- Praktisk regelefterlevnad
- Skapa och initiera rätt kontakter med parter utanför den egna forskargruppen

4.3.4 Forskningstjänster

I det översta lagret återfinns specifika forskningstjänster som aktivt och konkret bidrar till forskningens resultat och mål till skillnad från de tjänster som förvaltas och ägs av lagren *verksamhetsnära bastjänster* och *universitetstjänster* som är administrativt och / eller processmässigt stödjande till forskningen men inte i sig bidrar till resultaten av forskningen.



Forskningstjänster är de applikationer, system, verktyg etc. som ägs av forskarna själva och där forskningsprojektet själv ansvarar för och kravställer förvaltning och utveckling. Dock är det helt upp till forskningsprojektet att själv avgöra vilken typ av förvaltningsmodell, om någon alla man vill ha, det är också helt upp till forskningsprojektet att avgöra vilka tekniska åtgärder som behöver genomföras.

Till stöd och hjälp finns här IT-forskningsstödsgruppen inom IT-avdelningen som kan ha en eller flera personer som arbetar viss eller heltid i forskningsprojektet tillsammans med forskarna och avlönas därmed indirekt av forskningsprojektet helt eller till viss del. Då personerna som ingår i IT-forskningsstödsgruppen är personal anställt på IT-avdelningen har dessa samtidigt tillgång till hela IT-avdelningens resurser och processer för att tillsammans med forskargruppen skapa ändamålsenliga och specialiserade lösningar.

Dessa lösningar kan sedan genom IT-forskningsstödsgruppen återanvändas helt eller delvis inom andra forskningsprojekt i vilka gruppen är inblandade. Detta kommer över tid att ge en mycket högre grad av återanvändbarhet och gemensam nytta för hela lärosätets forskning så nya lösningar i mindre grad behöver skapas från grunden och saker som programkod, arkitektur, lösningsmönster etc. kan återanvändas.

Vidare föreslås IT-forskningsstödsgruppen att äga ett eller flera typer av repositorier för ändamålet att helt eller delvis kunna återanvända tidigare lösningar vid senare tillfällen. Här är det dock viktigt att vara medveten om att vissa delar av olika anledningar kan vara juridiskt eller av andra orsaker omöjliga att återanvända.

Ytterligare en fördel med att centralisera de mera tekniska och IT-nära delarna av forskningstjänsterna är att IT-forskningsstödsgruppen i synnerhet men även IT-avdelningen generellt bygger en kollektiv erfarenhet och förståelse för forskningens behov och samtidigt kan arbeta mer proaktivt med att tillsammans med forskare hitta moderna och kraftfulla lösningar.

4.3.5 Processmotor

Processmotorer används när olika typer av processer skall digitaliseras och hanterar både manuella och automatiska steg. Till begreppet kopplas ofta processcentriska applikationsplattformar, kända under benämningen Business Process Management Software (PBMS). Dessa adresserar två tillkortakommanden i våra traditionella applikationsplattformar - bristen på processtöd och låg produktivitet. BPM-plattformar är avsedda för att utveckla applikationer som driver processer. Med en BPM-plattform kan man snabbt implementera stöd för komplexa applikations- och organisationsöverskridande processer. Detta kontrasterar mot t.ex. en webbplattform där fokuset är på användarens interaktion med en datamängd och inte själva verksamhetsprocessen. BPM-plattformar tillåter applikationsutveckling utan traditionell programmering (“Low Code”), vilket för många typer av applikationer ger extremt mycket snabbare applikationsutveckling utan behov av traditionell programmerarkompetens.

Genom processmotorer/BPM-plattformar så är det möjligt att tydliggöra och digitalisera relevanta delar av stödet till forskningsprocessen. Detta kan exempelvis handla om hantering inom ekonomi för att kunna följa medel och transaktioner som rör forskningsprojekt. HR-processen kan också komma in i detta på olika sätt för exempelvis placeringar, hantera av doktorander och postdoc. Andra exempel kan vara inom fastighetshantering som beställning av möbler, passerkort, felanmälningar etc.

4.3.6 Regulatoriska och säkerhetskrav

För att kunna använda referensmodellen finns det antal skyddsåtgärder både teknisk och organisatoriskt som går att härleda till regulatoriska krav. Det betyder inte att det går att garantera att en tillsyn inte ger ett föreliggande men det går att hitta indikationer i gjorda tillsyner i sektorn framför allt av DI, numera IMY.

Det finns några författningar, vägledningar och rekommendationer som är aktuella:

- MSB 2020:6
- MSB 2020:7
- MSB 2020:8
- Offentlighet och sekretesslagstiftningen, OSL
- GDPR
- Patientdatalagen, PDL
- Dataskyddslagen
- Arkivlagen

Det finns en hel del material att inhämta från olika offentliga aktörer* som går att använda som inspiration och nedan görs en snabb överblick över några aspekter som kanske inte normalt tas med i dessa.

* Örebro kommun:
Riktlinjer för informationssäkerhet (orebro.se)

Denna rapport kommer inte att i detalj beskriva varje enskild författnings krav utan varje myndighet har egna policys och riktlinjer som behöver beaktas. Syftet med detta kapitel är att förmedla en förståelse för att det är viktigt att dessa styrdokument och författning måste kunna härledas till de tekniska skyddsåtgärder som myndigheten avser att implementera. Ett av de viktigaste styrande dokumenten är att det finns en tydlig informationsklassningspolicy på plats. Utifrån informationsklass kan ett antal tekniska skyddsåtgärder gälla – se vidare nedan 4.3.6.1.1 och framåt.

Andra stödramverk

4.3.6.1 Informationsklass - MSBFS 2020:6

En grundförutsättning för att kunna sortera vilka åtgärder som är lämpliga för ett system/tillämpning är att ha en informationsklassningspolicy på plats med riktlinjer för hur de skall användas i olika system/tillämpningar. I MSB rekommendationer, MSB 0040-09, utgår MSB från att det finns tre olika säkerhetsaspekter och en konsekvensnivå enligt tabell nedan:

Säkerhetsaspekt Konsekvensnivå	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
Allvarlig	Information där förlust av konfidentialitet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **allvarlig/katastrofal** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande	Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig	Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ingen eller försumbar*	Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	Information där det inte föreligger krav på riktighet, eller där förlust av riktighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ. **	Information där det inte föreligger krav på tillgänglighet, eller där förlust av tillgänglighet inte medför någon eller endast **försumbar** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild. **

Det finns också mer förklaringar och hjälp i ett verktyg som SKR tillhandahåller, som tyvärr inte än är tillgängligt för statliga myndigheter. Beslut om detta kommer eventuellt i mars 2021. Verktyget finns på KLASSA - Start (skl.se) och heter Klassa. I Klassa är ingen eller försumbar konsekvensnivå 0 och allvarlig 3. Det finns en nivå till som är 4 och som motsvara rikets säkerhet. För den sista klassen gäller den enbart konfidentialitet.

Säkerhetsaspekterna enligt tabellen tar inte hänsyn hur exempelvis känsliga personuppgifter skall klassas eftersom just detta är ett rörligt mål där det kan uppstå en kritisk massa av information som enskilt inte direkt är känslig men tillsammans blir det känsligt. Det kan därför vara rimligt att klassa ett system som hanterar viss information som en viss klass som anses kunna motsvara säkerhetsaspekterna i beskrivningen ovan. Exempelvis ett personalsystem borde nog klassas som att den kan hantera känsliga personuppgifter och därför skall ha ett antal olika tekniska och organisatoriska skyddsåtgärder kopplat till tillämpningen.

En tuff erfarenhet för Göteborgs universitet är e-posthaveriet där det blev uppenbart att konsekvensen inom säkerhetsaspekten tillgänglighet var allvarlig och att ytterligare skyddsåtgärder hade kunnat behövas.

För att en verksamhet skall kunna göra åtgärder behöver vi tydliga klassningar av informationen och i vilka tillämpningar informationen finns.

Nedan följer ett antal tekniska områden som är relevanta för olika säkerhetsaspekter. Det är tydligt att enbart organisatoriska skyddsåtgärder inte är tillräckligt för att säkerställa att data hanteras korrekt så att konsekvenserna uteblir – utan det krävs både tekniska och organisatoriska skyddsåtgärder för att uppfylla kraven.

4.3.6.1.1 Tillitskrav – Riktighet

Tillitsnivåer och hur de uppnås beskrivs i s.k. tillitsramverk. I tillitsramverken finns både tekniska och organisatoriska mekanismer för att uppnå en viss tillitsnivå.

Syftet med de krav som ställs på de högre tillitsnivåerna är för att vara säker på att rätt person har tillgång till en resurs. Resurstilldelningen sker med hjälp av behörighetshantering. I de tillsyner som gjorts anser DI att kravet för att hantera känsliga personuppgifter, klass 2[1], skall access ske med s.k. stark autentisering, vilket sägs motsvara e-legitimation eller liknade.

Kravet på stark autentisering gäller även när den registrerade lämnar uppgifter om sig själv.

Det tillitsnivåer som DIGG har är tillitsnivå 1-4, vilket motsvarar SWAMID AL1-AL4. SWAMID har inte AL4.

Det går att läsa mer om tillitsnivåer på: Tillitsnivåer för e-legitimering | DIGG

4.3.6.1.2 Kryptering – Konfidentialitet och riktighet

Primärt kopplas konfidentialitet till kryptering men även riktighet måste tas in här, eftersom en krypterad fil inte skall kunna ändras till exempel. Kryptering avser både transportprotokoll och filkryptering samt kryptering av lagringsvolymer. Krypteringsnycklar bör hanteras av myndigheten om det är höga[2] krav på konfidentialitet.

[1] Enligt Klassa
[2] Klass 2 eller högre

4.3.6.1.3 Loggning – Riktighet

För att kunna ha spårbarhet i vad som hänt behövs loggning av händelser i systemen. Detta för att kunna följa upp och göra revisioner på IT-system.

Viss loggning kan trigga övervakning.

4.3.6.1.4 Behörighetshantering – Konfidentialitet

I ett stort antal tillsynsärenden gjorda inom vårdsektorn är det tydligt att kontroll på behörigheter är extremt viktigt för att säkerställa åtkomst till journaluppgifter. Ett flertal av de vårdaktörer som granskats, både privata och offentliga aktörer, har sanktionsavgifter utdelats till sju av 8 samt att den 8:e fick föreliggande.

4.3.6.1.5 Övervakning – Tillgänglighet

Övervakning av infrastruktur och tjänster är nödvändig för att kunna införa preventiva åtgärder för att informera tekniker men och också support så att tidiga åtgärder kan sättas in för att lösa användarnas incidenter, eller skademinimerande aktiviteter. Exempel på aktiviteter:

- Dashboard med status
- Meddelanden till tekniker och support
- Automatiska röstmeddelanden
- Underlag för uppföljning och mätning
- Nedstängning av nätsegment
- Isolering av hackade klienter
- mm

En bra övervakning kommer också leda till kännedom om hur bra tjänsterna fungerar och att även samband kan upptäckas som leder till att hur tjänsternas tillgänglighet påverkas.

4.3.6.1.6 Redundans – Tillgänglighet

Redundans kan skapas på flera lager i teknikstacken och är många gånger kända tekniker att hantera. Det som däremot är väldigt svårt att göra en korrekt analys på vilken typ av redundans som krävs för att säkerställa verkasamhetes behov. Det är inte helt ovanligt att verksamheten ställer för höga krav på fel system. En analys av hur processen ser ut när det kommer till vilka typer av avbrott som kan hanteras och hur allvarliga de är och hur står påverkan de faktiskt har. Exempelvis kan det ett fåtal gånger per år vara väldigt hög belastning och skall då systemet dimensioneras för den absolut största piken kommer alla system att driva stora kostnader. Även egenskapen på tillgängligheten är viktig och på vilket sätt verksamheten eller användaren påverkas av att prestandan går ner eller att systemet helt drabbas av avbrott.

Ett sätta att minska påfrestningen är att minska synkrona beroenden mellan system om inte det är nödvändigt att all information i systemet måste vara uppdaterad i samma stund som användaren frågar. Det kanske är tillräckligt att en registrering av kursdeltagande kanske kommer 30 minuter senare i en annan kanal än det interface som användaren sitter i. Under bokslut brukar kraven på tillgänglighet i ekonomisystemet vara extremt höga men egenskapen på vilket avbrott som är sämst i denna period måste beaktas. Är det små avbrott eller helt bortfall under en dag eller en vecka – vad kan vi klara om systemet är borta en vecka och vilka konsekvenser kommer det bli och framförallt måste kostnaderna jämföras för de olika avbrottsfallen.

Redundans är inte bara ”mer hårdvara” utan en fråga för hela verksamheten att analysera och vilka konsekvenser avbrott eller minskad prestanda påverkar så att rätt åtgärder kan sättas in för att skapa ett kostnadseffektivt stöd. Olika metoder som kan behövas är:

- R&S
- Processkartläggning
- Informationsflöden
- Kritiska tidpunkter
- Typ av avbrott

4.3.6.1.7 Backup – Tillgänglighet och riktighet

Backup kan påverka både tillgänglighet och riktighet. För spårbarhet och kunna säkerställa tidigare versioner av data krävs olika typer av backup än för återställande vilket mer är en tillgänglighetsaspekt. Otroligt viktigt att förmedla vilken typ av klass informationen har för att kunna välja rätt typ av backup och vilka avbrottsscenarier som skall avhjälpas.

Med tanke på den mängd av data som produceras idag är det omöjligt att göra fullbackup utan tekniker som inkrementell, snapshot, sitereplikering används som backup. Dock behöver en noggrannare riskbedömning göras på olika delar av information för att kunna veta hur data skall separeras så rätt backupteknik används för vilken typ av avbrott som skall avhjälpas.

4.3.6.2 GDPR

Det finns ett antal exempel framtagna på vad som anses vara ytterligare tekniska åtgärder för att säkerställa skyddet av personuppgifter. Dessa åtgärder gäller främst för överföring av uppgifter till tredje land. EDPB har tagit fram scenarios där kompletterande åtgärder finns och där det inte fungerar[3].

Exempel på scenarios där kompletterande åtgärder finns:

Exempel 1: Datalagringför backup mm som inte kräver access till läsbardata (”data in the clear”)
- Universitetet är kryptonyckel

Exempel 2: Överföring av pseudonymiserad data
- Pseudonymisering av data där nyckeln hanteras lokalt på säker plats

Exempel 3: Krypterad data som enbart transporteras via tredjeland
- Kryptering av data och inte enbart transport

Exempel 4: Skyddad mottagare
- Godkända rutiner för identifiering av mottagare, kan vara lokala rutiner eller godkända tillitsramverk som SWAMID AL3, svensk e-legitimation, eIDAS Foreign ID, mm

Exempel 5: Split or multi-party processing
- Data splittrad över flera ställen där data inte är läsbart på ett ställe

Exempel på scenarios där inga kompletterande åtgärder finns_

Exempel 6: Överföring till molntjänstleverantörer eller annan som behöver access till läsbar data (”data in the clear”)

Exempel 7: Fjärråtkomst för affärsändamål

I artikel 25 GDPR – Privacy by Design står inga direkta tekniska åtgärder men ett arbete[4] författat av tidigare informations och sekretesskommissionär i *Ontario Ann Cavoukian* tar fram ett antal principer. Dessa ger er information, förtydligande och vägledning om de sju grundläggande principerna. Denna vägledning är avsedd att fungera som referensram och kan användas för att utveckla mer detaljerade kriterier för tillämpning och revision/verifiering.

Principerna är:

1. Proactive not Reactive. Privacy by Design comes before-the-fact, not after.
2. Privacy as the Default Setting, an individual need to do nothing,
3. Privacy by Design is embedded into the design without diminishing functionality.
4. Full Functionality – Privacy by Design is not privacy vs. security, it is possible to have both.
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open. Remember, trust but verify.
7. Respect for User[5] Privacy – Keep it User-Centric[6].

[3] edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)
[4] https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
[5] Med ”user” avses den registrerade
[6] Med ”user-centric” avses att det skall vara lätt för användaren att tillämpa ”privacy”

Dessa principer ger ett bra underlag om varför säkerhet behövs implementeras i våra lösningar utan att det blir svårare för användaren att använda sig av dessa. Dvs. det ”skall vara lätt att göra rätt”. Det är alltså inte upp till den enskilda användaren eller projektet att ta fram lösningar som uppfyller kraven utan dessa tjänster borde redan finnas eller vara tydliga som en del av arkitekturen.

4.3.6.3 OSL och begreppet röjt

I utredningen SOU 2021:1 går det att läsa på sid 25:

Vi bedömer att en myndighet som utkontrakterar it-drift har lämnat ut de uppgifter som omfattas av utkontrakteringen till tjänsteleverantören. Detta gäller oavsett om omständigheterna när uppgifterna tillgängliggjordes tjänsteleverantören var sådana att man – t.ex. pga. kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. Uppgifterna är röjda enligt offentlighets- och sekretesslagen (2009:400) eftersom ett utlämnande är en form av röjande.

På sid 235 kap 8.9 och framåt förs ett utförligt resonemang runt röjandebegreppet. Denna rapport har inte för syfte att gå igenom alla detaljer utan förklara vad röjt betyder i lagtexten. Med röjt anses att sekretessen är bruten och inte att innehållet är tillgängliggjort. För att SSC skall kunna låta Ewry drifta SSC:s system och inte anse att sekretessen är bruten togs en lag fram för att reglera detta; ”Tystnadsplikt för privata tjänsteleverantörer”. Den 1 januari 2021 trädde lagen (2020:914) i kraft. Lagen avser dock bara svenska företag och alltså inte utländska företag. Därför föreslås en ändring i OSL som ger myndigheter att göra sekretessbrytande bestämmelser istället för att försöka definiera begreppet röjt entydigt och i princip låta myndigheten själva bedöma om de kan anse att sekretessen är bruten när en utkontraktering sker utanför Sverige. Vidare skall tilläggas att detta inte påverkar kraven som GDPR ställer på skyddsåtgärder för att skydda känsliga personuppgifter.

Synpunkter på delbetänkandet:

(41) Några synpunkter på it-driftsutredningens betänkande SOU 2021:1 | LinkedIn

4.3.6.4 Tillsynsrapporter

Det finns flera tillsynsrapporter från DI/IMY som tillsammans ger ett bra underlag vilka åtgärder som har saknats. Den tillsyn som gjordes mot NAIS kan vara svår att hitta på IMY och istället hänvisas denna till sunet wiki, DI dnr 2407-2016[7]

Prenumerera på IMY pressmeddelanden görs här:

Prenumerera på pressmeddelanden - Integritetsskyddsmyndigheten (imy.se)

Tillsynsbeslut finns här:

Tillsynsbeslut Integritetsskyddsmyndigheten - Integritetsskyddsmyndigheten (imy.se)

[7] MFA i Nais - Sunet Wiki

5 Nästa steg

Detta kapitel beskriver ett förslag till arbetsgång för lärosäten som vill implementera IT-forskningsstöd med bas i referensarkitekturen.

5.1 Nulägesanalys

Ett lärosäte som vill implementera nytt eller förändra sitt befintliga IT-forskningsstöd bör inleda arbetet med att göra en nulägesanalys. Vi rekommenderar att först studera hela referensarkitekturen för att få en övergripande förståelse av områdets omfattning, även om den i sig inte alls matchar verkligheten vid lärosätet.

Nulägesanalysen ska ge svar på bl a:

- vilka aktörer ni har inom området idag, var de organisatoriskt hör hemma, hur ser relationerna mellan dem ut
- vilka forskningsstödjande IT-tjänster finns idag, hur förvaltas de, vilka arkitekturprinciper bygger de på, tänk på alla lager från nätverk till applikation
- vilka stödfunktioner, t ex RDO, finns vid lärosätet
- finns det relevanta strategier vid lärosätet att ta hänsyn till, t ex för sourcing, digitalisering, samverkan, kompetensförsörjning

5.2 Skapa en målbild

Utifrån referensarkitekturen så bör lärosätet genomföra ett arbete lokalt för att utreda vilka delar som är aktuellt att implementera utifrån lärosätes verksamhet, behov och förutsättningar. Beroende på lärosätets förutsättningar, behov och inriktning så behöver man välja ut vilka delar av referensarkitekturen som är lämplig att genomföra. Målbilden specificerar vad som skall uppnås inom olika tidshorisonter. Målbilden skall i detta läge vara oberoende av rådande resurser och ekonomiska faktorer.

Följande aktiviteter kan vara lämpliga vid skapande av en målbild.

- Analysera de olika delarna i referensarkitekturen och avgör vilka som är lämpliga att analysera närmare på utifrån lärosätets verksamhet och behov.
- Utifrån nulägesanalysen dvs. aktörer, forskningsstödjande IT-tjänster, förvaltning, principer, stödfunktioner samt strategier och för lärosätets relevanta delar i referensarkitekturen så identifieras målbilder inom de olika områdena.
- Målbild för lärosätet specificeras i olika tidshorisonter exempelvis kort, medel och lång sikt inom de olika områdena i referensarkitekturen.

5.3 Gap-analys

Efter genomförd nulägesanalys så vet man var lärosätet står idag och utifrån den målbild som togs fram i ovanstående steg så får man göra en gap-analys, dvs kartlägga skillnaderna mellan nuläge och målbild och identifiera de åtgärder som behöver **göras** för att nå målbilden. Gap-analysen ge en plan som indikerar vad som behöver göras, kostnad samt vilka resurser som krävs samt när i tiden olika steg i målbilden kan vara uppfylld. Gap-analysen ger också en bild av vilka förmågor som saknas för att kunna uppfylla ett visst mål.

5.4 Implementationsplan

Implementationsplanen är en konkretisering av gap-analysens resultat. Den visar när i tiden åtgärder ska göras och av vem samt vilka ekonomiska ramar som gäller. Målbilden kan i detta läge behöva justeras utifrån t.ex. ekonomiska faktorer. Initialt skapas en målarkitektur som stöd för att kunna nå målbilden dvs vilka förmågor, processer, tjänster, information och infrastruktur som krävs för att realisera målbilden.

Det är troligt att målbilden nås stegvis varför ett antal transitionsarkitekturer kan behöva tas fram, förutom den målarkitektur som också skapas. Detta görs att målbilden kan uppnås stegvis där en detaljerad plan tas fram för de steg som ligger närmast.

Beroende på vad som skall uppnås i målbilden så kan implementationsplanen bli omfattande och därför är hantering av prioritering en viktig del av implementationsplanen.

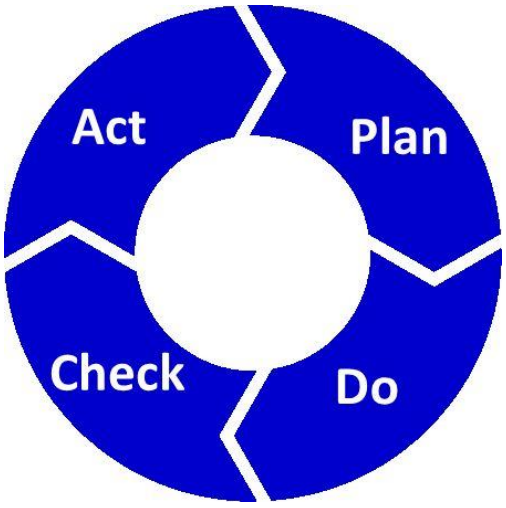
5.5 PDCA-metoden

PDCA-metoden är en av flera metoder att strukturerat arbeta med en avgränsad uppgift mot ett förutbestämt mål. Uppgiften kan vara avgränsad antingen genom sin storlek eller genom perspektiv.

PDCA-metoden ersätter inte en projektmodell eller förvaltningsmodell utan är en metod med vilken man kan arbeta mot mål inom ett t.ex. projekt.

Referensarkitekturen tar inte upp eller föreslår vare sig projektmodeller eller förvaltningsmodeller då detta är helt och hållet en lokal och organisatorisk fråga vid respektive lärosäte.

Däremot föreslås PDCA-metoden som ett verktyg att på ett pragmatiskt och strukturerat sätt arbeta mot mål som sätts upp av de/den tidigare.



Metoden har fyra steg som sker i tur och ordning, varv efter varv enligt:

1. Plan – Planera ett mindre antal förändringar som var och en har mätbara mål och kriterier för när de andes som klara
2. Do - Genomför de planerade förändringarna
3. Check – Kontrollera om de genomförda förändringarna har uppnått de mål och kriterier man tidigare planerat
4. Act - Genomför korrigeringar och ytterligare förändringar för att uppnå en uppnådda mål från steg tre.

Ett vanligt fel som görs vid användande av PDCA-metoden är att man låter steg fyra “Act” övergå och flyta ihop med steg ett “Plan” vilket gör att man riskerar att hamna i en målglidning eller arbeta mot ett så kallat “rörligt mål”.