UNIVERSITETET I OSLO
Institutt for informatikk

Suksesskriterier og fallgruver i IAM-prosjekter, 3 case-studier

Masteroppgave
(60 studiepoeng)

Nurettin Erman

7. November 2008

Sammendrag

Oppgaven har som mål å belyse problemstillingen på et overordnet nivå ved hjelp av teori og empiri. Teorien knytter seg til fagområde datasikkerhet som også kalles informasjonssikkerhet, IKT-sikkerhet og IT-sikkerhet. I denne oppgaven brukes datasikkerhet og informasjonssikkerhet om hverandre. Oppgaven starter med å definere på en overordnet nivå hva datasikkerhet er, hvilke farer og trusler som truer datasikkerheten. Videre nevnes det om at sikkerhet ikke begrenser seg til installering av et program, men heller en lang og kontinuerlig prosess der forebygging og skadebegrensning er vesentlig. Lover, forskrifter og instrukser setter grenser for hva vi kan gjøre og ikke kan, oppgaven går inn på de lovene som omhandler personvern, informasjonssikkerhet, graderings av informasjon, osv.

Deretter går oppgaven inn på den delen av datasikkerhet som har med å identifisere brukerne og styre deres tilganger til ressursene. Først ser vi på hva identitets og tilgangskontroll(Identity and Access Management(IAM)) er, og hvorfor virksomheter bør se nærmere på det, og i tillegg se på forutsetninger som må være på plass før virksomheter begir seg ut på å innføre en løsning. Videre ser oppgaven på hvilke fallgruver og suksesskriterier som blir sett på som ”beste praksis” ved innføring av IAM.

Formålet med IAM er å sikre at de som skal ha tilgang til informasjon, tjenester eller ressurser gjør, og de som ikke skal, ikke gjør det. Veien fra planlegging til ferdig innføring av en IAM-løsning er komplisert og omfatter flere hindringer på veien. Det kreves kunnskap og erfaring fra flere fagområder, og innføringsprosessen er ikke en lineær prosess som mange anskaffelsesprosjekter der hensikten er innkjøp av en programvare. Mange av de utfordringene som møtes i prosjekter skyldes ikke bare kompleksiteten IAM innehar, men mye av det skyldes manglende eller dårlige forutsetninger for å forstå hva denne kompleksiteten innbærer for ens egen virksomhet.

For mye fokus på teknologi og forståelsen om at IAM-prosjekter er som å anskaffe en programvare som kan installeres i organisasjonens IT-systemer, skaffer til veie for mange misforståelser som igjen fører til urealistiske høye forventninger. IAM-prosjekter er endringsprosjekter, det er svært viktig at i slike prosjekter vektlegges det ekstra trykk på å gjennomføre en grundig forstudie. Forstudien kan avklare forhold som antas å være viktige forutsetninger for å kunne iverksette prosjektet. ”Beste praksis” viser at i de prosjektene som lykkes med IAM, utgjør den tekniske implementeringen kun 20 % av den totale tiden.

> *” IdM is 80% business process change and 20% technology — don't start with The technology.” [1]*

Oppgavens empiri baserer seg på case-studier av 3 identitets og tilgangskontrollprosjekter. I casene ser jeg på de faktorer som kan ha vært avgjørende for prosjektets livssyklus. Suksessfaktorer og fallgruver blir sett på i lys av hva ”beste praksis” anbefaler, hva erfaringer og kunnskap fra leverandørene tilsier. Oppgaven ser nærmere på hvor langt virksomhetene har nådd i prosjektene sine, og hvor mye de har greid å oppnå av målsetningene de hadde for prosjektet.

Forord

Denne masteroppgaven er skrevet i forbindelse med mitt to års masterstudium ved Instituttet for Informatikk ved Universitetet i Oslo(UiO). Oppgaven har ett års omfang og er en selvstendig utredning som er skrevet ved **Utenriksdepartementet(UD)** på Victoria Terrasse. Oppgaven bygger på en kombinasjon av teori og empiri om temaet ”**suksesskriterier og fallgruver i IAM-prosjekter, 3 case-studier”**.

Jeg har fått betydelig hjelp i arbeidet med masteroppgaven, og vil spesielt takke min veileder ved UD, Ingvil Hovig, som har vært en god støttespiller gjennom hele prosjektet.

Tore Hemo(Jernbaneverket) og Ingrid Nordli(Norges Forskningsråd) fortjener en takk for en beundringsverdig imøtekommenhet ovenfor meg, og tusen takk for alle de erfaringene dere meddelte med meg. Jeg vil også rette en stor takk til Soner Sevin(UD), Ronny Robinsson-Stavem, Henning Gaalaas(Yamanu) og Kåre Magne Stennes, Nina Sørsdal (Steria), som bistod med teknisk hjelp og gjorde IAM mer forståelig for meg.

Til min mor…

Nurettin Erman
Oslo 7. November 2008

Innhold

Begrepsforklaringer

De fleste begrepsforklaringene er hentet fra ”Forstudierapport IdM. Innføring av Identitets- og tilgangskontroll i UD”. De som står med ”JBV” er hentet fra ”Forprosjekt:Identitetshåndtering og tilgangsstyring. Jernbaneverket”. Noe begrepene er tilpasset til denne oppgaven.

Begrep	**Forklaring**
IAM	På norsk: Identitets og tilgangskontroll. Identity and Access Management. Sammenhengen her er referansen til alle kjerneområdene av IAM, som inkluderer provisioning, tilgangskontroll, katalogtjenester, prosesser, arbeidsflyt, revisjon, autorisasjon, og rapportering.
Tilordning	Provisioning, opprettelse av noe, for eksempel brukerkonto i en applikasjon.
Adapter/Connector	Refererer til applikasjonsmoduler som kan kommunisere på en gitt applikasjons eget ”språk”/format, og som ivaretar den aktuelle applikasjonens prosesser/logikk slik at egenutvikling for integrasjon ikke skal være nødvendig i forbindelse med datautveksling mellom to applikasjoner.
Autentisering	Authentication. Verifikasjon og bekreftelse av om en person er den han/hun hevder å være. Brukerens bekreftelse kan være passord, biometri, token eller pin.
Autorisasjon	Authorisation. En tillatelse til å gjøre noe som ofte skjer etter at brukeren er verifisert gjennom en autentisering.
Katalogtjenester	Tjenester for håndtering av brukere, brukerrettigheter, og ressurskontroll som f. eks bruk av LDAP eller MS Active Directory.
Føderasjon	Federation. Tillit til ukjente brukeres tilganger til webapplikasjoner på tvers av organisasjonsgrenser.
Identitet	Refererer til aspekter ved det unike ved en bruker (eller ressurs) som antas å være mer bestandig eller uforanderlig over tid.
Metakatalog	En elektronisk katalog som inneholder informasjon om andre elektroniske kataloger.
Policy	En bevisst aksjonsplan som gir retningslinjer for hvordan ta avgjørelser og hvordan oppnå forventede resultater. En

	rettesnor.
SSO	Single Sign-On. Et system/applikasjon som er laget for at en bruker skal minimere antall ganger han/hun må logge inn/autentisere seg. Dette gir redusert antall innlogginger ved automatisering av innloggingen.
Etterlevelse	Compliance av for eksempel lover og regler eller en definert standart. Påvises gjerne ved attestering eller revisjon.
RBAC	Role Based Access Control. En standard for tilgangstyring basert på roller.
Workflow	Også kalt arbeidsflyt. Automatiserte eller delvis automatiserte prosesser, der en rekke av hendelser eller aktiviteter følger hverandre og har en bestemt start og slutt.(JBV)
Passord synkronisering	Password syncronization. Passordene synkroniseres mellom de systemer som er knyttet til identity management løsningen, slik at bruker kun forholder seg til ett passord i alle applikasjoner.(JBV)
Autoritativ kilde	Dette er kilden der initial brukerdata blir lagt inn i. Det kan være flere autoritative kilder, men det er kun en pr. Dataelement.(JBV)
Granskning/Overvåking og rapportering	Audit and reporting. ”Overvåking” av systemet, arbeidsflyter m. m Audit funksjoner medfører sporbarhet i systemet i form av logger, rapporter og lignende.(JBV)

Kapittel 1

Introduksjon

Dette kapittelet vil starte med å skissere bakgrunnen for oppgaven. Deretter blir problemstilling og omfang for oppgaven beskrevet. De avgrensningene som er gjort i oppgaven blir presentert, og til slutt blir oppgavens struktur gjennomgått.

1.1 Bakgrunn for oppgaven

Virksomhetene står ovenfor økende kompleksitet og akselererende teknologiske og økonomiske endringer. En av hovedoppgavene for IT-avdelingene har vært å holde konfidensiell informasjon og ressurser, sikker og tilgjengelig. Et antall mekanismer, prosedyrer og rutiner har blitt iverksatt for å sikre at kun autoriserte har tilgang til virksomhetens IT-ressurser og tjenester.

Ved hjelp av disse mekanismene og prosessene vil virksomheten sikrer at de som skal ha tilgang har det, og de som ikke skal ha, ikke har det. Konfidensialiteten, integriteten og tilgjengeligheten av informasjon, tjenester og ressurser ivaretas med disse mekanismene.

De fleste virksomheter har vidt forskjellige programmer kjørende på sine systemer. Og mange av programmene har sine egne autentiserings og autorisasjonsmekanismer uavhengige av vertssystemet og andre programmer. Organisasjonen vil bruke mye ressurser på å vedlikeholde dobbelt lagrede informasjonen om brukerne. Det er alltid en risiko for at informasjonen ikke stemmer, og som kan føre til at folk får tilgang til informasjon og ressurser som de i utgangspunktet ikke har autorisasjon til.

Kunder og partnere forventer og etterspør flere tilganger til virksomhetens datasystemer. I tillegg til økt etterspørsel etter datatilgang, har også nye krav fra myndighetene som pålegger virksomheter å følge regler som gjelder for kontroll av persondata og behandling av dataene. To fremtredende eksempler på disse kravene er Personopplysningsloven og IKT-forskriftene. I tillegg til disse er det også andre lover og forskrifter som sikrer integriteten og privatlivet til den enkelte. En strengere lov kjent som Datalagringsdirektivet eller EURO-SOX er ikke ferdig behandlet av norske myndigheter, og det er noe usikkert om alle punktene i direktivet vil vedtas av myndighetene.

Etter hvert som virksomhetene står overfor utfordringen med å håndtere identitet og tilganger til vidt forskjellige systemer og i tillegg følge lovverket, vil de ha behov for å innføre en teknologi som kan hjelpe dem med å styrke virksomhetens relasjoner til kundene, partnere og i tillegg oppfylle regulatoriske krav fra myndighetene.

Identitets og tilgangskontroll(Identity and Access Management(IAM)) består av moduler som kan hjelpe organisasjoner med å håndtere komplekse krav til identitet og tilgangskontroll. IAM er et området som dekker mange aspekter av sikkerhet. IAM-løsninger kan hjelpe organisasjoner med å få kontroll over alle identiteter i systemene som har behov for å få

tilgang til organisasjonens applikasjoner og ressurser. Brukere, passord, tilganger og administrasjon av dem danner kjernen i en IAM-løsning.

1.2 Problemstilling

IT-prosjekter av den komplekse typen kan by på store utfordringer, som kan undergrave motivasjonen, samarbeidet og kommunikasjonen internt i prosjektgruppen og ellers i organisasjonen. Konflikter og problemer av slik art kan utøve omfattende hærverk på prosjektet, og kan føre til at prosjektet avblåses eller sluttføres med et dårlig resultat og med store kostnadsoverskridelser.

IAM-prosjekter går på tvers av avdelings- og faggrenser, og involverer flere grupper mennesker. Del resultatene eller sluttresultatet av et prosjekt vil føre til endringer av prosesser, rutiner og i noen tilfeller endringer av organisatorisk karakter.

IAM er et endringsprosjekt som krever strategisk planlegging. Et mislykket prosjekt vil føre til langt flere problemer enn et mislykket anskaffelsesprosjekt som omhandler innkjøp av standard IT-utstyr.

I denne oppgaven vil jeg belyse de faktorer som kan være avgjørende for om et prosjekt når sine mål eller mislykkes med å nå målene og dermed feile i å innfri forventningene brukerne har til prosjektet. Oppgaven vil prøve å svare på spørsmålene om hva virksomhetene feiler eller gjør riktig mht prosjektet? Hva er det som skiller prosjekter som når sine mål fra de som ikke greier å nå målsetningene med prosjektet?

Den primære problemstillingen for denne oppgaven er å belyse de faktorer som påvirker et prosjekts livssyklus. Hva er de mest kritiske fallgruvene virksomheter bør passe seg for og helst ikke komme bort i? Og hva er faktorer som kan hjelpe organisasjoner til å nå sine mål?

Faktorene vil settes i fokus med de organisasjoner oppgaven har som ”caser”. Ved hjelp av casene vil påstanden om fallgruver og suksesskriterier bekreftes med betraktning av deres prosjekter.

Den sekundære problemstillingen er å gi en overordnet beskrivelse av hva IAM er, hvorfor virksomheter bør se nærmere på det, og tilslutt å gi en beskrivelse hvilke forutsetninger som må være på plass før en implementering kan starte. Beskrivelsene er på et overordnet nivå og tar for seg de basis komponentene i en IAM-løsning. Bedrifter er organisert i ulike strukturer, det er vanskelig å gi et fasitsvar på hvordan IAM kan innføres i en og hver. Den enkelte bedrift bør utforme sin egen prosjektmodell, men det er heller ikke så dumt å støtte seg til tilgjengelige modeller og erfaringer utviklet og erfart av andre i praksis.

1.3 Avgrensning og presisering av problemstillingen

Generelle It-prosjekter har mange fellestrekk med IAM-prosjekter. Men på noen punkter adskiller de seg fra hverandre. Prosjekter involverer flere grupper mennesker ofte med svært forskjellige bakgrunn og kunnskapsnivå enn for eksempel et prosjekt som omhandler innkjøp av IT-utstyr.
Det finnes lite informasjon og datagrunnlag mht IAM og prosjekter både i offentlig og privat sektor i Norge. Mye av informasjonen som er produsert om IAM er forstudie og

forprosjektrapporter tilhørende prosjekter virksomheter har eller har hatt. Disse rapportene inneholder konfidensiell informasjon, og er ikke alltid egnet for publikasjon.

Det finnes nesten ingen forskningsrapport som omhandler direkte IAM eller IAM-prosjekter. Mye av det som er å finne på internett, er ”white paper” som leverandørene har publisert. De fleste av disse rapportene omhandler bestemte produktspesifikasjoner, og er ikke alltid pålitelige informasjonskilder.

Det finnes også en del analyserapporter som analyseselskaper som Gartner og andre har lagt ut på internett. Noen av rapportene som omhandler IAM og prosjekter er gratisutgaver og derfor inneholder ikke detaljerte beskrivelser. Forhold som er nevnt ovenfor setter sterke rammer for kritisk datainnsamling.

Med begrenset pålitelige og kritiske informasjonskilder begrenses oppgavens rammer betraktelig, en annen faktor som også begrenser oppgaven er at IAM er ganske ny I Norge og det er få virksomheter i Norge som har innført alle moduler i en løsning.

En av de viktigste faktorene som setter sterke rammer og grenser for denne oppgaven er prosjekterfaring som kan tilegnes hvis en får lov til å komme så nær casene og føle på kroppen og komme på innsiden av organisasjonskulturen. Prosjektene som går ved Jernbaneverket(JBV), Norges Forskningsråd(NFR) og Utenriksdepartementet (UD) danner oppgavens fokusområde. Oppgaven vil fokusere på alle prosjektene med hensyn til om de har greid å hente ut gevinster og dermed oppnådd målsetningene med prosjektet, eller om de har feilet i prosjektarbeidet og har dermed ikke oppnådd de fordelene som var tiltenkt med prosjektet i første omgang.

IAM er ikke kun et program, men et konsept som innholder mange moduler som kan implementeres hver for seg og gradvis og kan samkjøres med modningsprosessen i en organisasjon. Denne oppgaven vil begrense seg til å gi en overordnet beskrivelse av basis modulene, og går ikke noe dypere inn på en spesifikk teknologi eller løsning.

1.4 Valg av Metode

Jeg har valgt å legge til grunn en kvalitativ forskningsmetode for gjennomføring av oppgaven. Undersøkelsen vil basere seg på case-studier, hvor oppgaven begrenser seg til 3 caser.

Case-studiene vil bidra til å kartlegge de erfaringer som er knyttet til prosjektene, og bidra til å undersøke og gjennomskue hva det er som skjuler seg bak kulissene. Dette vil gi meg muligheten til å tilegne meg dybde kunnskap og forståelse mht de variabler som avgjør et prosjekts sluttresultat. Ved å avdekke og fortolke de forhold og faktorer som leder til at prosjektet når sine mål, eller feiler i å dra fordeler av prosjektet, kan være en lærdom for mange virksomheter som er i ferd med å implementere eller planlegger å innføre en IAM-løsning.

Organisasjoner jeg ser på er JBV, NFR og UD. Jeg har fått kjennskap til disse organisasjonene via andre personer som enten er eller var direkte eller indirekte innblandet i IAM-prosjekter, Jeg har blitt kjent med en del mennesker i løpet av prosjektperioden og har hatt møter med og intervjuet noen av dem angående deres innsats i prosjektet, og forhold som har hatt størst påvirkning på prosjektarbeidet deres.

Under disse møtene har vi snakket og diskutert rundt IAM, løsninger, prosjektene deres og faktorer som de ser på som kritiske for et prosjekts resultat. Påliteligheten og relevansen av informasjon som har kommet ut av disse møtene har vært verdifulle og har belyst mange sider ved prosjektene.

Informasjonen som er blitt formidlet i løpet av disse møtene kan ikke tas som sannheter, men det er viktig å være klar over at det de har formidlet er erfaringer som har rot i det arbeidet de har utført og vært en del av.

1.5 Informasjonssamling

Denne delen av oppgaven har både vært lett og vanskelig. Lett fordi jeg har fått tilgang til mange forskjellige "white paper" direkte på internett. Det har vært svært vanskelig fordi informasjonen en får tak i er produsert med tanke på salg, og reklame for produkter og løsninger. De fleste leverandører har sine egne løsninger, og har fokus på det de er sterkest på. Det har ikke vært lett å grave seg gjennom all salgsargumentene, og skille sannhet fra overdrevet sannhet. ta det for gitt at det er hele sannheten om IAM, og glemmer at det er kun en av mange løsninger. Det finnes nesten ingen forskningsartikkel som

1.5.1 Primær informasjon

Dette bygger på det som er blitt formidlet til meg via informasjonsmøter jeg har hatt med fagfolk, og nøkkelpersoner i prosjektene. Informasjonen bygger på deres kompetanse, og erfaringer tilegnet i prosjektene. Primær informasjon omfatter også de bøker, og artikler som omhandler direkte eller indirekte om IAM, og IAM-løsninger og systemer.

1.5.2 Sekundær informasjon

Denne type informasjon bygger på publiserte informasjonsmaterialer produsert av leverandører, eller andre utredninger som er publisert i fagblader.

1.6 Metodekritikk

3 caser vil ikke belyse alle deler av prosjektarbeidet, og vil heller ikke være nok for å kunne avdekke alle de sider av prosjektene som trenger ekstra oppmerksomhet i løpet av prosjektperioden. Det er vanskelig å si om noen av fallgruvene eller suksessfaktorene alene har vært utslagsgivende for forskjellen i prosjektene, men det er lett å innse at de til sammen kan ha ført til svært ulike resultater. Oppgaven vil være en introduksjon for IAM-konseptet, og vil være veiledende for mange virksomheter som har planer om å innføre IAM.

1.7 Krav til leseren

Det forutsettes at leseren har en viss generell kjennskap til datamaskiner, dataterminologi og noe generell kunnskap om datanettverk.

1.8 Konvensjoner brukt i oppgaven

Denne seksjonen tar for seg de forskjellige konvensjonene brukt i denne boken.

1.8.1 Typografiske konvensjoner

> Sitater utheves særskilt og settes i 12 pkt Times New Roman. Sitatene rykker inn ett tabulatorsteg fra venstremargen.

Noe av teksten er uthevet, og er gjort for å unngå lage unødvendige overskrifter av dem.

Lovtekstene som er gjengitt i oppgaven er satt i kursiv med 12 pkt Times New Roman.

1.8.2 Uttrykk brukt i oppgaven

IAM er et fagområdet som det norske språket ikke har klart å få innpass i enda. All av litteraturene jeg har studert har vært på engelsk, og noe av dette skyldes at IAM er ganske ny i forhold til andre teknologier. Derfor er mange av uttrykkene på engelsk, og det ser vi også av alle forkortelsene som brukes i denne oppgaven. Der jeg har ment at det ikke kan misforstås, har jeg forsøkt å oversette ulike fagbetegnelser til norsk. Jeg bruker også det engelske ordet i parentes ved siden av det norske uttrykket.

Kjært barn har mange navn heter det, og det gjelder også identitets og tilgangskontrollsystemer som har mange betegnelser og forkortelser. IAM har like mange forskjellige oversettelser til norsk, Alle oversettelsene er dekkende, men ingen av dem forklarer hva IAM egenlig er. Jeg bruker ” identitets og tilgangskontroll” på norsk, mens bruker forkortelsen IAM konstant. Jeg synes denne betegnelsen er mer dekkende, og påminner om at prosjektet innebærer mye mer enn bare identitetshåndtering. Men mange bruker IAM, og IdM litt om hverandre, mens andre bruker det for å adskille identitetshåndterings del av prosjektet med tilgangskontrolls del. I litteraturen er det også stor variasjon i hvilket av uttrykkene som blir brukt. Det er fortsatt ingen enighet om definisjonen til verken IAM, IdM, IdA, eller mange andre versjoner.

1.9 Oppgavens struktur

I første kapittel har bakgrunnen for oppgaven blitt presentert, sammen med problemstillingen og omfanget. Videre belyses hvilke metoder som ble brukt og hvordan datainnsamlingen for oppgaven har foregått. Oppgaven fortsetter i neste kapittel med å ta for seg teori og bakgrunn som er relevant for oppgaven.

Kapittel 2 En introduksjon til datasikkerhet: Første del tar for seg hva datasikkerhet er, og lover som beskytter og sikrer privatpersoners integritet. Andre del tar for seg hvorfor man skal beskytte data og hvem man skal sikre det mot. Tilslutt hvordan beskytte data mot indre og ytre trusler.

Kapittel 3 Identity and Access Management: Dette kapittelet gir et teoretisk grunnlag teknologien som denne oppgaven bygger på. IAM blir introdusert med alle de basis komponentene som kan finnes i en løsning.

Kapittel 4 Forutsetninger for et IAM-prosjekt: Kapittelet beskriver hvordan organisasjoner bør tilnærme seg IAM-prosjekter, og hvilke forutsetninger som må være på plass før en implementering av IAM kan starte.

Kapittel 5 Fallgruver i et IAM-prosjekt. Hva bør organisasjoner som planlegger eller er i ferd med å innføre et IAM-system passe sg for, hva er fallgruvene som kan være avgjørende for om et prosjekt overlever, og kommer i mål som først antok.

Kapittel 6 Suksessfaktorer i et IAM-prosjekt. I dette kapittelet besvares følgende spørsmål. Hva er faktorer som påvirker et prosjekts livssyklus. Hva er de kriterier som bidrar til eller som gjør at prosjektet kan resultere i suksess, og ikke i budsjettoverskridelser og fiasko.

Kapittel 7 Case-studier. Kapittelet tar for seg de organisasjoner som oppgaven har som case. Casene gjennomgås med tanke på de faktorer som har hatt størst virkning på resultatet, og om det er erfaringer andre organisasjoner i liknende situasjoner kan ha nytte av. Prosjekterfaringene analyseres og diskuteres mht til den teoretiske bakgrunnen som er nevnt i denne oppgaven.

Kapittel 8 Avslutning. Oppgavens siste kapittel gir en oppsummering av funnene som er gjort, og noen forslag til videre forskning.

Kapittel 2

Datasikkerhet og sikkerhetstenkning

Kapittelet begynner med en innledning om blant annet hva data sikkerhet er og hvorfor det er viktig å sikre data. Videre gir kapittelet en oversikt over områder som hører under datasikkerhet, trusler som eksisterer mot datasystemer. I tillegg gis det anbefalinger som kan følges for å sikre systemene, og hindre innbrudd i systemene. Det finnes mange gode råd til dem som har ansvaret for å sikre bedriftens verdier, og begrense skadeomfanget ved innbrudd eller angrep på systemene.

2.1 Innledning

Samfunnet utvikler seg i et enormt tempo, og det skjer så raskt at det ikke er tid til å sette seg inn i den nye teknologien. Mange er bekymret for den teknologiske utviklingen som i stadig sterkere grad påvirker samfunnet og griper mer og mer inn i hverdagen vår. En annen bekymring er at utviklingen innen teknologi kan resultere i at vi blir overvåket, og fulgt med på mer enn ønskelig

Sikkerhet har alltid vært et aktuelt tema i samfunn der verdier skal beskyttes mot indre og ytre ”fiender”. Men hva som er i fokus i det store sikkerhetsbildet endrer seg ofte med tiden og i stor grad med den teknologiske utviklingen. Stadig nye trusler gir nærmest en kontinuerlig endring av trusselbildet.

Et grunnleggende prinsipp innen sikkerhetstenkning er at ikke alt er like fundamentalt å beskytte. Dette innebærer at man må utvikle prosesser for å kunne identifisere hva som har sikkerhetsmessig verdi og hvor godt det skal beskyttes.

2.2 Definisjon av datasikkerhet

> *”Security is about protecting things of value to an organization, in relation to the possible risks. This includes material and intellectual assets.”[2]*

Datasikkerhet er metoder, forholdsregler som innebærer å beskytte data i datamaskiner, kommunikasjonssystemer og beskyttelse av systemer (fysiske, systemtekniske og organisatoriske områder) der det oppbevares data og informasjon.

> *”Computer security rests on confidentiality, integrity, and availability” [3]*

Metoder og forholdsregler brukes for å bygge systemer som er pålitelige og driftssikre uansett situasjon som måtte oppstå og minimere risikoen for å miste eller skade informasjon. Disse metodene kan hjelpe og sikre mot at uautoriserte personer kan overføre, endre, slette, modifisere og offentliggjøre data de i utgangspunktet ikke har tilgang til.

> *"Informasjonssikkerhet innebærer sikkerhetstiltak innenfor både fysiske, systemtekniske og organisatoriske områder, og omfatter følgende tre begreper:*
>
> *Konfidensialitet – sikkerhet for at kun autoriserte personer får tilgang til følsom eller gradert informasjon og at det på forhånd er foretatt en gyldig identifisering og autentisering av personen*
>
> *Integritet – sikkerhet for at informasjon og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter*
>
> *Tilgjengelighet – sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov"* ***[4]***

Ut fra sitatet ovenfor kan vi forstå at **Konfidensialitet** er det som sier om informasjonen er tilgjengelig kun for de som skal ha tilgang. Dette er viktig for å kunne sikre at sensitiv informasjon er umulig/ vanskelig å få tak i for de som i utgangspunktet ikke har tilgang til det.

Vi oppfatter også at **Integritet** er det som sier at en er sikker på at informasjonen er korrekt og fullstendig eller at kilden til informasjon er den som er angitt.

Tilgjengelighet sier noe om hvem som har tilgang og hva vedkommendes rolle er i systemet for å begrense tilgjengeligheten innenfor de krav som er satt.

Ut fra sitatene ovenfor definerer boken informasjonssikkerhet som:

> *"beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles av systemet og systemet i seg selv"* *[4]*

Vi kommer også inn på begreper som "ikke-benekting" og "sporbarhet" som har en gjensidig avhengighet. "Ikke-benekting" beskriver metoder som skal dokumentere at en handling virkelig har vært gjort av en person. Slik beskrives det i "Håndbok i datasikkerhet(2006)" boken.

> *"ikke-benekting(uavviselig) – sikkerhet for at de som har sendt meldinger gjennom et informasjonssystem ikke kan benekte eller avvise at det er de som har foretatt denne handlingen" "* *[4]*

"Sporbarhet" beskriver metoder som skal knytte enhver endring av informasjon til en identitet. Og slik beskrives det i boken "Håndbok i datasikkerhet 2006".

> *"Et prinsipp som sikrer at behandling av en sak kan rekonstrueres i ettertid. Det skal være mulig å etterspore hva som har skjedd(audit trail)."* *[4]*

Ved hjelp av disse metodene kan man finne ut hva som har skjedd, hvem som står bak handlingen og hvordan det har skjedd ved hjelp av logger, elektroniske spor, osv. Metodene kan hjelpe til å kunne dokumentere kriminelle handlinger som hvitvasking av penger, narkotika og andre type kriminalitet eller avverge terrorhandlinger.

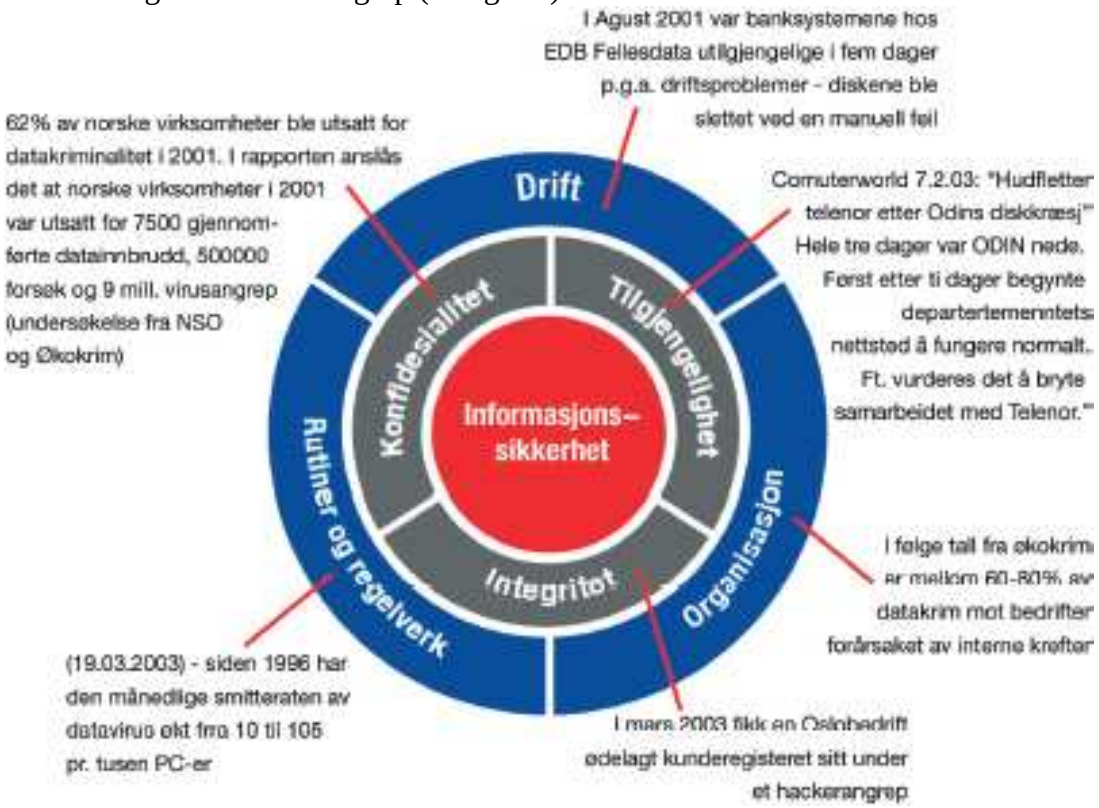
Det er vesentlig å huske på at datasikkerhet ikke bare er et fysisk- og systemteknologisk sak men heller en kontinuerlig prosess som angår hele organisasjonens data og informasjons håndtering. Denne prosessen må sørge for at forholdet til informasjonssikkerheten holdes oppdatert og at den følges fra første gang data produseres til dataene skal slettes.

2.3 Hvorfor sikre data?

Datasikkerhet ble et hett tema da datamaskiner ble koblet sammen i nettverk. Data ble flyttet fra papir til elektronisk format. Datautveksling foregår mer og mer på maskiner/systemer som er koblet sammen i nettverk. Den teknologiske utviklingen tvinger seg fram på i mange områder i samfunnet og spiller en økende rolle for utvikling og forandring av samfunnet. Samfunnet er blitt ekstra følsom for feil, tap og mislighold av data. Mange offentlige organisasjoner, private bedrifter og folk flest er blitt mer avhengig av IT. Det blir stilt ekstra krav om oppetid, sikkelige driftsrutiner, sikkerhet og stabilitet til tjenestene og systemene.

Nye verktøy og nye metoder for å løse forskjellige oppgaver gjør livet og jobben enklere for mange. Men det finnes også flere verktøy og metoder for å bryte seg inn i datasystemer, der hensikten er å sabotere, ødelegge, snylte andre for penger eller informasjon, osv. Data skal gjøres lett tilgjengelig men skal ikke være mulig å få tak i av utenforstående. Det at flere systemer blir tilgjengelig via internett utgjør en stor sikkerhetsrisiko fordi en da gjør det teknisk mulig å få tilgang til mange maskiner over internett tilkoblingen.

De fleste bedriftsnettverk inneholder mye viktig og sensitiv informasjon, slik som bedriftshemmeligheter, forretningskontrakter, produktbeskrivelser, persondata, osv. Det vil være katastrofalt dersom noe av dette blir ødelagt, slettet, endret eller kommer i hendene på konkurrentene eller folk med uærlige hensikter. Resultater fra flere undersøkelser bekrefter at truslene mot bedriftenes datasystemer er økende og at den største trusselen kommer fra bedriftens egne rekker, altså ansatte. I en undersøkelse gjort av Økokrim viser at mellom 60-80 % av datakrim mot bedrifter har vært forårsaket av interne krefter. I figur 1 under kan du se noen flere saker som har fått oppmerksomhet i norsk media. I en undersøkelse gjort av Næringslivets sikkerhetsorganisasjon (NSO) og Økokrim anslås det at i 2001 ble norske virksomheter utsatt for 7500 gjennomførte datainnbrudd. Og at det var 500000 forsøk på innbrudd og 9 mill. virusangrep (se figur 1).



Figur 1

Virksomheter har verdier, bedriftshemmeligheter, forretningskontrakter, produktbeskrivelser, persondata(ansatte, kunder), osv som de vil beskytte. Privatpersoner har navn, personnummer, kredittkortnummer, adresse, telefonnummer eller lignende som de bør være forsiktig med når de er på internett. Fremmed etterretning, terrororganisasjoner, kriminelle grupper, hackermiljøer er noen av de som kan være interessert i informasjon om akkurat deg.

Det finnes uttalige av bedrifter og folk på internett som er ute etter å få tak i personlige opplysninger og andre sensitiv informasjon. Selv om slik informasjon ikke bør innhentes uten ditt samtykke, er det ikke mange nettsider som opplyser deg om hva de sender tilbake til eierne av nettsiden. Det finnes mange webområder, nettsider og programmer som er laget kun for å stjele/innhente informasjon som kan brukes til å oppspore deg, din datamaskin. Nettsteder har flere verktøy tilgjengelig for å kunne innhente og lagre informasjon om deg og dine surfevaner slik som webskjemaer, informasjonskapsler, websignaler og webserverlogger.

Om noen av disse opplysningene havner i hendene på bedrifter eller folk med uærlige hensikter, kan opplysningene i etterkant selges til andre eller brukes i mange forskjellige sammenhenger.

Opplysningene som er stjålet eller kapret kan brukes til bestemte formål blant annet brukes til identitetstyveri, loggføre bevegelser slik som hva du har gjort, hvor du har vært og til hvilken tid, for utpressing, kartlegging av potensielle ofre. Informasjon kan sammenstilles fra forskjellige databaser/logger og kan brukes til å lage en profil som gir et bilde av en persons privatliv. Mange av oss bruker søkemotorer for å finne det vi er ute etter på internett. Men mange søkemotorene som lar deg søke via deres nettsider krever i gjengjeld de kan hente inn informasjon om hva du søkte på og igjen selge dine surfevaner på Internett til en tredje part.

2.4 Trusler

Vi har verdier som skal beskyttes mot skade, tap eller misbruk, mot indre og ytre fiender, mot tekniske feil og svikt, mot naturlige katastrofer. Det er en nødvendighet å finne ut av hvor mye er vi innstilt på å gjøre for å beskytte de verdiene og hvor mye kan vi miste eller tape før det virkelig er ille. Vi må stille spørsmålet om hvor stor risiko vi er villige til å ta sett i forhold til krav til sikkerheten. En risikovurdering kan hjelpe til å identifisere sannsynligheten og konsekvens av en sikkerhetsbrydd. Vurderingen kan hjelpe til å sette kriterier for akseptabel risiko. Akseptabelt risikonivå vil variere i forhold til verdier og hva som må gjøres for å kunne beskytte verdiene.

De virksomheter som jobber med behandling av personopplysninger som helt eller delvis med elektroniske hjelpemidler er det pålagt å gjennomføre en risikovurdering. Dette vil hjelpe virksomhetene slik at de får en vurdering som kan hjelpe dem i å kunne analysere og avdekke farer som kan true bedriftens nettverk og systemer. Analysen bør starte fra når data produseres til det skal tilintetgjøres. Det er mange farer og trusler en bedrift kan bli utsatt for, derfor er det viktig å ha tenkt og trent på situasjoner som kan oppstå. Og med dette kan man redusere sannsynligheten for at sikkerhetshendelsen inntreffer eller slik at skadeomfanget begrenses dersom sikkerhetshendelsen skulle inntreffe.

Man kan kategorisere farer og trusler som kan skade/ødelegge informasjonssystemene under 3 hovedpunkter;

Type	Trusler
Menneskelige	Innbrudd, spionasje, sabotasje, uhell.
Fysiske	Strømtilførsel, natur og menneske skapte katastrofer, etc.
Programvare	Virus, logiske bomber, malware, trojanere, orm, phishing.

Tabell 1

Før vi ser på noen av de mest aktuelle truslene som finnes for programvare, ser vi litt på den største trusselen, nemlig medarbeiderne i virksomhetene. Misfornøyde medarbeidere som har lyst til å ta igjen ved å skade systemene eller slette data, utgjør en større trussel enn hva andre utenfor kan gjøre. Skadeomfanget kan bli mye større og mer omfattende enn de som kan utføres med eksterne programmer. Det kan også være mange andre grunner til at ansatte utgjør enn større trussel enn noe annet. Under har vi nevnt noen av de punkter som kan gjøre at forsvaret faller før "fienden" har nærmet seg bymuren.

2.6.1 Menneskelige trusler

- Misfornøyde medarbeidere, medarbeidere som skal slutte
- Brukeridenter og passord som ikke endres/slettes
- Manglende kontrollrutiner
- Manglende rutiner for å håndtere e-poster
- Manglende eller feil kompetanse
- For dårlig fysisk adgangskontroll

2.6.2 Fysiske trusler

- Strømtilførsel, mangler UPS og dermed mister data som ikke er lagret,
- mulige disk krasj
- naturkatastrofer
- menneske skapte katastrofer

2.6.3 Programvaretrusler

Vi ser på noen typiske angrep som systemene kan bli utsatt for. Angrepene blir mer og mer utspekulerte og tar i bruk grunnleggende programvareutvikling for å spre ødeleggende programvare.

Type	Definisjon
Malware	Fellesbetegnelse på skadelig programvare som trojanere, datavirus og spyware.
Virus	Et lite dataprogram som kan reprodusere seg selv og henger seg på kjørbare filer. Det finnes flere tusener av slike virus.
Orm	Det er programmer som kan spre seg selv fra maskin til maskin. De skjuler seg ikke inn i andre programmer som virus gjør, men prøver å skjule sin identitet.
Trojansk hest(spionprogrammer)	Trojanske hester er som en blanding av virus og orm. De utgir seg for å være noe annet enn det de egentlig er. De ligger skjult for eieren samtidig som de spionerer på/overvåker

	maskinens aktiviteter og på informasjoner som behandles/mottas/sendes – for så misbruke disse informasjonene senere.
Automatiserte direkte angrep ved innlogging	Programmer som har spesialisert seg på å finne brukernavn og passord, programmene prøver alle ord i en bestemt ordbok.
Spam (uønsket e-post)	E-post som sendes av fiktive adresser, de reklamerer for forkjellige produkter eller tjenester. Noen av e-postene har hensikt å lure mottakeren med falske forhåpninger, slik som at de kan være med å dele på en stor sum av penger om de tar kontakt med avsenderen.
DDoS (Distributed Denial of Service attacks)	Dette går ut på at en eller flere bombarderer en server med så mange henvendelser at serveren ikke makter å svare på alle. Dette kan føre til krasj, henge seg opp eller oppføre seg rart ved å svare med feil data på henvendelser.
Phishing (identitetstyveri)	Dette går ut på å fiske etter sensitiv informasjon, som passord eller kredittkortnummer, personnummer, brukernavn, passord etc. En kjent måte den utføres på er at en person sender en e-post og utgir seg for å være fra for eksempel en stor bank. E-posten opplyser for eksempel om at det er problemer med noen kredittkort fra den banken. Problemet kan derimot, ifølge e-posten, løses lett ved å følge en vedlagt link til en fiktiv nettside.

Tabell 2

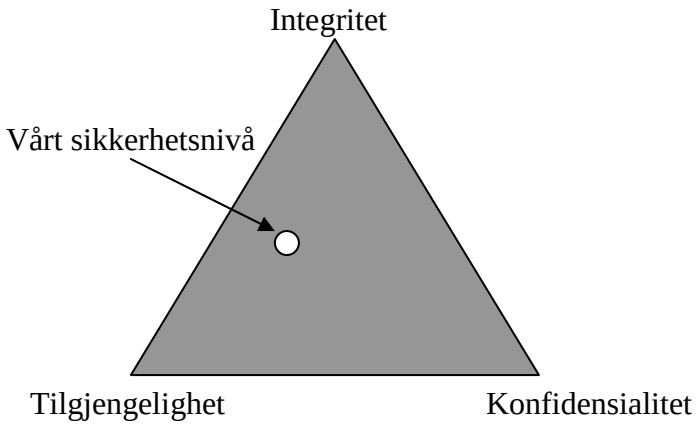
Dette går ut på å fiske etter sensitiv informasjon, som passord eller kredittkortnummer, personnummer, brukernavn, passord etc. En kjent måte den utføres på er at en person sender en e-post og utgir seg for å være fra for eksempel en stor bank. E-posten opplyser for eksempel om at det er problemer med noen kredittkort fra den banken. Problemet kan derimot, ifølge e-posten, løses lett ved å følge en vedlagt link til en fiktiv nettside.

2.5 Sikkerhetstenkning

En av de bedre metoder for å beskytte seg mot angrep på, og dermed sikre data til en viss grad er å skaffe seg kunnskap om risikofaktorene og hvordan man unngår dem. En godt utviklet sikkerhetstenkning trengs både hos ledere og ansatte. Risiko og sikkerhetsforholdene bør granskes systematisk og helst av en 3. part som har mer kunnskap og ikke er avblindet for feil og farer som kan finnes ved virksomhetens systemer. Man bør prøve å kartlegge, vurdere, sikre og fjerne feil og farer som finnes. Ved å utvikle og bruke riktig arbeidsmetoder og sikkerhetstiltak kan man minske farene som finnes. Virksomheter kan redusere muligheten for feil og uhell i betydelig grad om de investerer i god sikkerhet. God sikkerhet vil gjøre virksomheten langt bedre i stand til å håndtere feil og farlige situasjoner raskt og riktig dersom de oppstår.

Som vi også har nevnt tidligere så er sikkerhet en lang og kontinuerlig prosess, man kan ikke bare si at nå har man implementert sikkerhet. Forebygging og skadebegrensning er vesentlig her, som vi også har nevnt ovenfor så er det viktig å kunne analysere hva som skal beskyttes, finne svakheter ved systemet, hvor ligger risikoen, og hvordan begrense skader som er påført systemet. Når svakheter ved systemet er funnet og risikoområdene er dekket, bør man komme i gang med å planlegge kostnadseffektive løsninger der det er nødvendig med sikring og beskyttelse. Det er også viktig å huske på at ved å innføre strengere sikkerhetstiltak, detaljerte begrensninger vil/kan føre til systemer der brukervennlighet er ned prioritet i følge av disse sikkerhetsordningene.

Figuren illustrerer at valg av sikkerhetsnivå i en organisasjon må balanseres i forhold til de 3 punktene nemlig integritet, tilgjengelighet og konfidensialitet som vi har nevnt tidligere. Sikkerhetsnivået vil/kan variere fra organisasjon til organisasjon, spørs hva som prioriteres i virksomheten. Om en ønsker full tilgjengelighet av informasjon, så utelukker man full konfidensialitet. Dvs. at konfidensialitet ned prioriteres for ønsket tilgjengelighet.



Figur 2

Man kan håpe på at man ikke blir utsatt for datakriminalitet, bare fordi man har installert et antivirus program men dette vil ikke holde i tiden der datakriminelle blir mer proffe og flere. Data- og informasjonssikkerhet er mer enn bare passord, viruskontroll. Under følger noen tips om hvordan systemene kan beskyttes mot trusler og angrep.

Her har vi også gruppert tiltakene også i 3 hovedområder.

Trusler	Tiltak
Menneskelige	Øke kompetansen, Øke bevisstheten og ansvarsfølelse blant de ansatte. Enkle fornuftige regler, Enkle fornuftige retningslinjer og Enkle fornuftige sikringstiltak.
Fysiske	Sikring av rom, utstyr, strømtilførsel,

	sikkerhetskopi.
Programvaretrusler	Oppdatert versjon av programvare, anti-virus, anti-spyware, sikkerhetskopi.

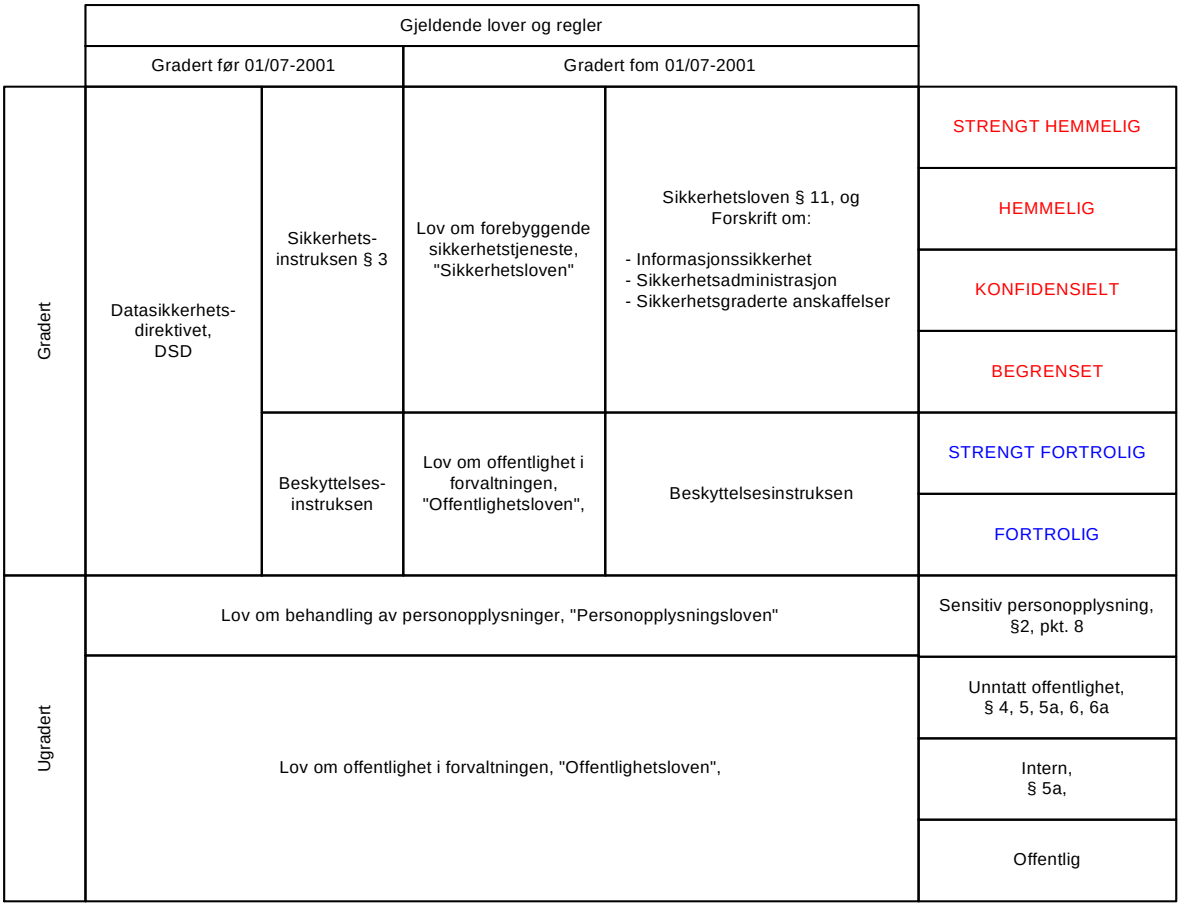
Tabell 3

2.6 Lover, forskrifter, instrukser

Et aspekt av informasjonssikkerhet er å sikre og påse at den enkelte individets integritet beskyttes, vernes og at opplysninger om personlige og intime forhold ikke bringes videre uten samtykke fra de personer opplysningene gjelder. Utenom privatlivets fred, blir også straffbare handlinger der utnyttelse av datateknologien har vært betydelig for gjerningen berørt av loveverket.

> *"For å kunne regulere bruken av databehandling slik at både etiske, moralske og ikke minst strafferettslige spilleregler i samfunnet blir fulgt, er det nødvendig med lover og forskrifter"* *[4]*

En del av forebyggende sikkerhetstiltak kan være meget inngripende overfor enkeltpersoner, og kan misbrukes mot enkeltpersoner. Flere lover og forskrifter, herunder sikkerhetsloven, personopplysningslovens sikkerhetsforskrift og Kredittilsynets IKT-forskrift pålegger virksomheter å gjennomføre sikkerhetsrevisjoner, og med dette bevise at informasjonsbehandlingen er i overensstemmelse med krav og kriterier satt i lover og forskrifter, eller i interne retningslinjer, standarder med jevne mellomrom (årlig). Under ser du en oversikt over lover, instrukser, osv. Legg merke til at lovene er delt i 2 hovedgrupper som gradert og ugradert, og helt høyre ser du graderingsnivåene.



Figur 3

2.6.1 Personopplysningsloven

Personopplysningsloven ble vedtatt i år 2000 og trådte i kraft året etter. Loven er en videreutvikling av bestemmelsene i personregisterloven. Personregisterloven fra 1978 ble avløst av denne loven.

> *"Et hovedprinsipp i personopplysningsloven er at du i større grad skal ha kontroll med opplysninger om deg selv. I mange tilfeller er det frivillig å gi fra seg slike opplysninger"* ***[4]***

Den avløste personregisterloven av 9.juni 1978.
Datatilsynets årsmelding fra 1995 s 26 framgår det slik:

> *«Ny teknologi er i utgangspunktet verken positiv eller negativ for personvernet. Det er hvordan vi anvender teknologien og hvordan vi legger premissene for utviklingen av ny teknologi som bestemmer om teknologien skal styrke eller svekke personvernet.»* ***[5]***

Lovens formål er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger, dette gjelder for enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Hver enkelt har rett til innsyn i å få vite hva virksomheter har registrert opplysninger om den enkelte og hvor de har hentet det fra, og hva de skal bruke det til. Loven omfatter både elektroniske og manuelle registrer. Ved å sette sammen sensitive personopplysninger fra registrene kan enkeltpersoners liv blottlegges for offentligheten og få svært alvorlige konsekvenser for den enkelte.

> *"Ved behandling av sensitive personopplysninger, er utgangspunktet at man må søke datatilsynet om konsesjon."* ***[4]***

Datatilsynet er en uavhengig forvaltningsorgan, som er administrativt underordnet Kongen. Datatilsynet passer på at sensitive personopplysninger om den enkelte som er lagret systematisk av offentlige og/eller private instanser ikke utveksles på tvers av registrene.

Personopplysningslovens § 13 pålegger den behandlingsansvarlige og databehandlere å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Loven pålegger ansvarlige å dokumentere informasjonssystemet og sikkerhetstiltakene for medarbeiderne for å kunne oppnå tilfredsstillende informasjonssikkerhet.

2.6.1.1 Personopplysningsforskriften

Forskrifter utfyller personopplysningsloven, og ble vedtatt 15. desember 2000.

> *"I tillegg til ansvar for sikkerheten i egen organisasjon, må den behandlingsansvarlige også forvisse seg om at informasjonssikkerheten er tilfredsstillende hos kommunikasjonspartnere og leverandører"* *[4]*

2.6.2 Kredittilsynets IKT-forskrift

Med bakgrunn i finans foretakenes økte bruk og avhengighet av IKT, utarbeidet Kredittilsynet en forskrift om bruk av informasjons og kommunikasjonsteknologi i finanssektoren (IKT-forskriften). IKT-forskriften bidrar til å sette en standard for IKT-driften i foretaket. Den fokuserer på IKT-prosessene hvor stikkord er rutiner og dokumenterte prosedyrer. IKT-forskriften er omfattende og beskriver ganske detaljert de prosesser og arbeid som må gjøres for å sikre virksomhetens datasystemer. Under § 5 er det fastsatt regler om sikkerheten i foretaket.

> *"§ 5 Sikkerhet*
>
> *Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare."[4]*

2.6.3 Sikkerhetsloven

Sikkerhetsloven trådte i kraft 1. juli 2001.
Sikkerhetsloven har som formål å redusere risiko for sikkerhetstrusler som spionasje, sabotasje og terrorhandlinger gjennom forebyggende defensive tiltak. Loven har ifølge § 1 som formål å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet, sikkerhet og andre vitale sikkerhetsinteresser, samt ivareta den enkeltes rettsikkerhet og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste.

Vi ser av paragraf 5 av sikkerhetsloven at ansvaret påhviler lederen for virksomheten.

> *"§ 5.* **Den enkelte virksomhets plikter**
>
> *Enhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av loven her.*
>
> *Virksomheten skal*
>
> *utarbeide intern instruks for å ivareta sikkerheten,*
>
> *sørge for at virksomhetens ansatte og engasjerte får tilstrekkelig opplæring i sikkerhetsspørsmål, og regelmessig kontrollere sikkerhetstilstanden i virksomheten.*
>
> *Ansvaret påhviler lederen for virksomheten. Dersom utøvende funksjoner delegeres internt i virksomheten, skal dette gjøres skriftlig.*
>
> *Alt ansatt eller engasjert personell har i sitt arbeid eller oppdrag for virksomheten ansvar for å ivareta sikkerhetsmessige hensyn, og plikter å bidra til forebyggende sikkerhetstjeneste."[4]*

Loven gjelder også for sikkerhetsgradert informasjon og eventuelle skjermingsverdige objekter virksomheten har ansvaret for. Det er fire grader som kan brukes hvis informasjon må beskyttes av sikkerhetsmessige grunner. Dokumenter som ikke trenger å beskyttes og som ikke er graderte kalles ugradert informasjon. Denne betegnelsen er ikke en grad, men de som

jobber med slike dokumenter regner det som en egen grad. Vi ser fra loven at det ikke skal brukes høyere sikkerhetsgrad enn nødvendig.

Her har vi tatt med en del av § 11. Sikkerhetsgradering fra kapittel 4 i sikkerhetsloven.

"§ 11. Sikkerhetsgradering
Når informasjon må beskyttes av sikkerhetsmessige grunner, skal en av følgende sikkerhetsgrader benyttes:

a. *STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
b. *HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
c. *KONFIDENSIELT nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
d. *BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*

Den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon, skal sørge for at informasjonen merkes med aktuell sikkerhetsgrad. Sikkerhetsgradering skal ikke skje i større utstrekning enn strengt nødvendig, og det skal ikke brukes høyere sikkerhetsgrad enn nødvendig.

Sikkerhetsgradering skal ikke gis virkning for lengre tid enn det som er strengt nødvendig, og graderingen skal senest bortfalle etter 30 år. Nærmere regler om ned- og avgradering gis av Kongen. Kongen kan for særskilte tilfeller fastsette unntak fra 30 års regelen i første punktum.

Kongen kan under forutsetning om gjensidighet treffe overenskomst med fremmed stat eller internasjonal organisasjon om sikkerhetsgradering av mottatt informasjon som er sikkerhetsgradert av vedkommende stat eller internasjonale organisasjon, og om plikt til å treffe tiltak for å sikre slik informasjon. "[4]

2.6.4 Arkivloven

Loven trådte i kraft 1. januar 1999.

Arkivloven har som formål å sikre at alt offentlig arkiv som har betydelig verdi av forksjellige art, som kulturelle, forskningmessige, rettslige og forvaltningsmessige dokumenter. Formålet med loven er å bevare og tilgjengeliggjøre informasjonen for samtiden og for ettertiden. Loven har også bestemmelser om bevaring av private arkiver, men stiller ingen konkrete krav om hvordan arkivene bør sikres.

Følgende er tatt fra lovteksten om formålet med arkivloven, og definisjon på forksjellige arkiver som er finnes i lovteksten.

”§ 1. Føremål.

Føremålet med denne lova er å tryggja arkiv som har monaleg kulturelt eller forskingsmessig verde eller som inneheld rettsleg eller viktig forvaltningsmessig dokumentasjon, slik at desse kan verta tekne vare på og gjorde tilgjengelege for ettertida.

§ 2. Definisjonar.

I denne lova vert desse omgrepa nytta slik:

a. *dokument: ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lyding, framsyning eller overføring.*
b. *Arkiv: dokument som vert til som lekk i ei verksemd.*
c. *Statleg arkiv: arkiv skapt av statleg organ.*
d. *Kommunalt arkiv: arkiv skapt av fylkeskommunalt eller kommunalt organ.*
e. *Offentleg arkiv: statleg eller kommunalt arkiv.*
f. *Privat arkiv: arkiv som ikkje er offentleg arkiv.*
g. *Offentleg organ: statleg, fylkeskommunal eller kommunal institusjon eller eining.”*[4]

2.6.5 Åndsverkloven

Åndsverkloven er en forkortelse for ”lov om opphavsrett til åndsverk m.v.”
Musikk, film, tekster og dataprogram vil ofte ha vern som åndsverk, og den som har lagt inn en innsats for å kunne skape verket vil ha opphavsrett over det verket.

Følgende er hentet ”kapittel 1 Opphavsrettens gjenstand og innhold” fra lovteksten:

”§ 1. Den som skaper et åndsverk, har opphavsrett til verket.

Med åndsverk forståes i denne lov litterære, vitenskapelige eller kunstneriske verk av enhver art og uansett uttrykksmåte og uttrykksform, så som

1) *skrifter av alle slag,*
2) *muntlige foredrag,*
3) *sceneverk, så vel dramatiske og musikkdramatiske som koreografiske verk og pantomimer, samt hørespill,*
4) *musikkverk, med eller uten tekst,*
5) *filmverk,*
6) *fotografiske verk,*
7) *malerier, tegninger, grafikk og lignende billedkunst,*
8) *skulptur av alle slag,*
9) *bygningskunst, så vel tegninger og modeller som selve byggverket,*
10) *billedvev og gjenstander av kunsthåndverk og kunstindustri, så vel forbildet som selve verket,*
11) *kart, samt tegninger og grafiske og plastiske avbildninger av vitenskapelig eller teknisk art,*
12) *datamaskinprogrammer,*
13) *oversettelser og bearbeidelser av verk som er nevnt foran.*

For fotografiske bilder som ikke er åndsverk gjelder § 43a. ”[4]

2.6.6 Forvaltningsloven (Bestemmelsene om taushetsplikt)

Regler om taushetsplikt finnes i forvaltningsloven under §§ 13 til 13f, forvaltningsloven gjelder for den virksomhet som drives av organer i stat eller kommune. Formålet med bestemmelsene er å beskytte gradert informasjon mot innsyn fra uautoriserte.

Ut fra Forvaltningsloven § 13 gjelder følgende:

"§ 13. (taushetsplikt).

Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

1) *noens personlige forhold, eller*
2) *tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.*

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre."[4]

2.6.7 Offentlighetsloven

Lov om offentlighet i forvaltningen (offentlighetsloven) trådte i kraft 1. juli 1971.

Offentlighetsloven gjelder for alle institusjoner og virksomheter som er en organisatorisk del av den statlige, kommunale eller fylkeskommunale forvaltningen.. I utgangspunktet er alle offentlige saksdokumenter tilgjengelig for innsyn, med mindre det er gjort unntak i lov eller medhold av lov. Enhver kan kreve innsyn i det offentlige innholdet i en bestemt sak i følge offentlighetsloven. Unntak fra offentlighet skal ifølge offentlighetsloven ha hjemmel i eller medhold i lov,

Formålet med innsynsretten er å gi allmennheten innsikt i de sakene som forvaltningen behandler. Et "dokument" er ikke bare papirbaserte dokumenter. Etter lovens definisjon gjelder retten all lagret informasjon uten hensyn til hvilket medium som er benyttet for lagringen.

Under følger § 2 som er hentet fra lovteksten:

"§ 2. Lovens hovedregel

Forvaltningens saksdokumenter er offentlige så langt det ikke er gjort unntak i lov eller i medhold av lov.

Enhver kan hos vedkommende forvaltningsorgan kreve å få gjøre seg kjent med det offentlige innholdet av dokumenter i en bestemt sak. Det samme gjelder journal og lignende register og møtekart til folkevalgte organer i kommuner og fylkeskommuner. Forvaltningsorganet skal føre journal etter bestemmelsene i arkivloven med forskrifter.

Forvaltningsorganet skal vurdere om dokumentet likevel bør kunne gjøres kjent helt eller delvis, selv om det etter bestemmelser i loven kan unntas fra offentlighet." *[4]*

2.6.8 Beskyttelsesinstruksen

Beskyttelsesinstruksen brukes på materiale som ikke kan graderes etter sikkerhetsloven, og trenger beskyttelse av andre grunner enn de som er gitt i loven. Den brukes på informasjon som kan skade offentlige interesser, en bedrift, institusjon eller enkeltperson om innholdet blir kjent for uvedkommende.

Beskyttelsesinstruksen er verken lov eller forskrift, men en kongelig resolusjon.

Følgende er tatt ut fra lovteksten:

"§ 1. Anvendelse.

Denne instruks kommer til anvendelse ved behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i sikkerhetsloven med forskrifter, jf. § 4.

Instruksen omfatter dokumenter uavhengig av mediet de er tilgjengelig på.

§ 4. Om bruken av beskyttelsesgrader.

Når betingelsene for gradering etter § 3 er til stede, nyttes beskyttelsesgradene slik:

STRENGT FORTROLIG nyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.

FORTROLIG nyttes dersom det vil kunne skade offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.

Det må påses at det ikke nyttes høyere beskyttelsesgrad enn strengt nødvendig." *[4]*

2.6.9 Gradert informasjon

Gradert informasjon beskriver data som er forbehold og som er betraktet høyst sensitiv. Personer som i forbindelse med sitt arbeid vil komme i kontakt med eller har behov for å behandle gradert informasjon, må sikkerhetsklareres før de kan få tilgang til den graderte informasjonen. Klarering gis på ulike nivåer, alt etter hvor strengt graderte opplysninger personen trenger tilgang til

Under ser vi et utsnitt av paragraf 11 i sikkerhetsloven. Her kan vi se de graderingsnivåene som benyttes i Norge og dets allierte(NATO).

"§ 11. Sikkerhetsgradering

Når informasjon må beskyttes av sikkerhetsmessige grunner, skal en av følgende sikkerhetsgrader benyttes:

a. *STRENGT HEMMELIG(COSMIC TOP SECRET) nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
b. *HEMMELIG(NATO SECRET) nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
c. *KONFIDENSIELT (NATO CONFIDENTIAL) nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
d. *BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende."* *[4]*

2.6.10 Datalagringsdirektivet

EU-direktivet 2006/24/EF forkortet til datalagringsdirektivet ble vedtatt 15. mars 2006 Rådet for Den europeiske union og Europaparlamentet. Direktivet handler om lagring av opplysninger fra såkalte trafikkdata fra telefoni og datakommunikasjon. Opplysningene skal kunne benyttes til å bekjempe kriminalitet og terrorisme.

Direktivet er ansett som EØS-relevant, og Samferdsels og justisdepartementet tar sikte på å fremme lovforslag til Stortinget rundt årsskiftet 2008/2009. En innføring av langtidslagring av trafikkdata vil være omstridt, særlig ut fra personvernhensyn, men også på grunn av kostnadene den vil føre med seg.

Her er en kort oversikt over det endelige innholdet i rammeverket:

"*1. De dataene som skal lagres omfatter trafikk- og lokaliseringsdata hos teleoperatørene (benyttede telefonnumre, tidspunkt og fra hvilket område), samme opplysninger for SMS, samt "Internett- trafikkdata", dvs. IP- adresser og tidspunkt for "oppetid". Operatørene skal i tillegg lagre navn og adresse på abonnenten, som nevnte opplysninger er knyttet til.*

2. Det er teleoperatørene og Internettleverandørene som pålegges plikten til å lagre. Unnlatelse av å etterkomme kravet skal kunne underlegges sanksjoner.

3. Direktivteksten viser til at de registrerte opplysningene skal kunne brukes til bekjempelse av alvorlig kriminalitet ("serious criminal offences"), og henviser til det enkelte lands lovgivning for nærmere tolkning av dette.

4. Parlamentets vedtak omfatter lagring for etterforskning og rettsforfølging av alvorlig kriminalitet. Det er imidlertid ikke endelig avklart hvilke terskler man skal ha for å ta materialet i bruk. Saken må imidlertid være konkretisert. Det gis ingen generell tilgang til opplysningene.

5. Lagringstiden ble fastsatt til å være minimum 6 måneder, og maksimum 2 år.

6. Parlamentet utrykte at medlemslandene må fastsette hvilke offentlige organer som skal gis tilgang til dataene.

7. Medlemslandene skal peke ut et uavhengig organ som skal overvåke bruken av dataene.

8. Det ble videre bestemt at tilgang til de lagrede dataene skal baseres på et "push- system", der det kun gis tilgang i enkeltsaker, og bare til spesifikt angitt formål. Det skal ikke gis tilgang etter selvforsyningsprinsippet til hele databasen hos den enkelte operatør, men kun data knyttet til en bestemt angitt mistenkt.

9. Kostnadene forbundet med lagring ble vedtatt å legges til de enkelte aktører. Parlamentet anbefaler imidlertid at medlemslandene dekker ekstrakostnader forbundet med lagringen, men dette er det etter rammeverket opp til medlemslandene selv å bestemme." **[6]**

2.7 Sikkerhetsrelaterte standarder

Defineres som et dokument som beskriver krav, retningslinjer og veiledning for styringssystemer, prosesser, produkter, tjenester, osv.

Standarder får stadig større betydning etter som internasjonal standardisering øker og flere bruker de internasjonale standardene. Standardene nevnes for å vise til at kvaliteten på produktet, tjenestene følger strenge internasjonale krav. Kjøper og selger spesifiserer ofte produktene, prosessene og tjenestene sine ved å henvise til passende standarder.

> *"Standarder er viktige kvalitetssikringsverktøy, som skal gi tilstrekkelig tiltro til at et produkt eller tjeneste vil tilfredsstille angitte krav til kvalitet"[4]*

2.7.1 Standarinserings organisasjoner

Informasjon er hentet fra **Wikipedia, den frie encyklopedi[hentedato: 27.10.2008].**

Internasjonale

- ISO(International Organization for Standardization) har utviklet tekniske standarder på de fleste sektorer siden 1947.

- IEC(International Electrotechnical Commission) utvikler og publiserer internasjonale elektrotekniske normer.

Europeiske

- CEN(**Comité Européen de Normalisation**) er en felles europeisk standardiseringsorganisasjon.

- CENELEC(European Committee for Electrotechnical Standardization) publiserer Europanormer (EN) og Harmoniseringsdokumenter (HD)

- ETSI(European Telecommunication Standard Institutte) arbeider for felles europeisk telekommunikasjonsstandarder.

Norske
- Standard Norge (SN) er en norsk privat medlemsorganisasjon, og har ansvar for standardiseringsoppgaver på alle områder unntatt elektro og post- og telestandardisering.

- Norsk elektroteknisk komité (NEK), er en selvstendig og nøytral organisasjon som har ansvaret for standardiseringen på det elektrotekniske området i Norge.

- Post og teletilsynet er en norsk statlig etat som regulerer og overvåker post- og telekommunikasjonssektoren og har ansvar for radiofrekvensforvaltning og nummerforvaltning.

2.7.2 ISO/IEC-17799:2005

" ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization." [7]

2.7.2 ISO/IEC-27001:2005

"ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof."[8]

2.7.3 COSO – rammeverket for internkontroll

"Internal Control – Integrated Framework er et faglig utgangspunkt for å sikre at de interne kontroll strukturer som er utviklet i virksomheten ivaretar alle relevante elementer og

dimensjoner knyttet til den interne kontrollen." [9]

2.7.4 COBIT – Standard for IT-revisjon

"CobiT er et IT governance rammeverk med verktøy, som har mål å hjelpe IT til å forstå virksomhetens behov og få på plass metoder og prosesser slik at behovene kan nås så effektivt som mulig." [10]

2.8 Oppsummering

Med den voksende informasjonsmengden, samt lov og krav fra myndighetene om å være oppdatert til enhver tid kan by på administrative og sikkerhetsrelaterte utfordringer.

Datasikkerhet er et tema med mange aspekter og komponenter som innehar mange forskjellige disipliner i seg. Det kreves ofte kunnskap fra mange forskjellige disipliner for å kunne utvikle systemer med høy grad av sikkerhet.

I de neste kapitelene ser vi på et konsept som har den hensikt å fjerne silo tankegang innen sikring av organisasjonenes ressurser og systemer. Mange ulike systemer som har med å administrere brukerkontoer, styring av tilganger, overvåking og logging av hendelser. Med den nye teknologien blir mange ulike systemer samlet under et nytt fellessystem.

Virksomheter som har startet med å implementere slike systemløsninger, regner med å spare store summer etter hvert som systemet innføres. Organisasjoner regner med å kunne få bedre kontroll på hvem som har tilgang på hvilken informasjon, og kunne få bedre oversikt over hvem som har endret eller hentet ut informasjon.

Kapittel 3

Identity and Access Management

Dette kapitlet starter med å gjennomgå sentrale begreper som ligger bak Identitets og tilgangskontroll, bedre kjent som Identity and Access Management. Videre beskrives IAM-konseptet med tilhørende komponenter, prosesser og teknikker.

3.1 Introduksjon

Med den teknologiske utviklingen særlig via internett, gir store muligheter for virksomheter til å komme i kontakt med nye kunder og partnere. For å kunne konkurrere på det globale markedet, må virksomheter kunne bruke teknologien til å understøtte forretningsprosessene som er nødvendig for å kunne nå nye kunder og partnere.

> *" As enterprises externalize their business processes over the Internet to customers and trading partners, they have expanded the number and types of users with which they must contend. Accordingly, more users need access to IT resources; platform environments will remain complex and heterogeneous; and Web services are driving the need to manage transactions, as well as user access to IT resources." [11]*

Med ekspandert forretningsvirksomhet, vil kunder, partnere, leverandører kreve tilgang til virksomhetens informasjons systemer, databaser, osv. Med denne utviklingen vil flere brukere få tilgang, og virksomheten vil stå overfor utfordringen med være mer åpen for samarbeid og samtidig gi bedre sikkerhet og ha bedre kontroll. Dette problemstillingen presenterer en kompleks utfordring mange virksomheter står overfor. Mange av dagens systemer og prosesser som er i bruk, ble opprinnelig utviklet for en verden som er annerledes enn det vi står overfor i dag. Mange av systemene har ikke den samme funksjonaliteten for brukeridentifisering og tilgangskontroll som finnes i moderne systemer.

> *" Thus, enterprises no longer can effectively manage user access to the heterogeneous IT environment (for example, external and internal user identity information repositories, databases, operating systems, and applications) for multiple access purposes, such as business roles, password management rules and business hours access policies." [11]*

Flere av de gamle systemene mangler moduler for å kontrollere hvem som har tilgang til hva, og loggføre alle hendelser gjort av autoriserte brukere. Å håndtere flere brukertilganger med flere forskjellige tilgangsbehov, og forskjellige standarder som kan eksistere innad i en virksomhet gjør administrering og håndtering av systemene, kompliserte og vanskelig å ha kontroll på hele tiden og til en hver tid. Kompleksiteten kan bidra til høyere kostnader, økt tidsbruk på administrering, flere betydelige sikkerhetssårbarheter.

"A multiproduct implementation is the only way to meet these enterprise requirements. Vendors are addressing this multiproduct approach by delivering identity and access

management (IAM) product suites." ***[11]***

Identitets og tilgangskontrollsystemer(IAM) kan sikre at virksomheten kan bevise hvem som har tilgang, hva de har tilgang til og hvorfor de har tilgang over for myndighetene.

3.2 Hva er Identity and Access Management?

Virksomheter har behov for å forsikre seg om at brukerne er identifiserte og at disse identitetene har de tilgangene de skal ha. Virksomheten har også behov for å forsikre seg om at brukerne har kun de tilgangene det er nødvendig for å kunne utføre jobbene sine. Virksomheten må kunne administrere brukernes tilganger og rettigheter innenfor virksomhetens datasystemer og at aktiviteter assosiert med brukertilganger er loggført med bestemte regler.

"Organizations face a proliferation of application access needs, and at the same time a greater imperative than ever to ensure that such access is only available on a controlled basis of proven user identity. " ***[12]***

Voksende behov for brukerkonto og tilgangsadministrering, krever komplekse og sammensatte produkter. Ingen produkter gjør alt, det finnes mange forskjellige produkter som har spesialisert seg på forskjellige løsninger slik som brukerkontohåndtering, håndtering av privilegier, håndtering av passord, osv. Identity and Access Management (IAM) er et av de navn som kalles for slike programvareløsninger. Det er mange definisjoner som er i bruk, avhengig av bransje, leverandører, eller konsulent. Men hoveddefinisjonen er den samme.

"Identity Management (IDM) is a broad, administrative area that deals with identifying individuals (identities) and controlling their access to resources, services and systems whereas Access Management (AM) defines the set of rules required to control and allow individual access to internal or external systems." ***[13]***

IAM kombinerer prosesser, prosedyrer, teknologier for å administrere livssyklusen og tilgangsrettigheter til brukeridentiteter, og skal sikre at riktig person har tilgang til riktig tjeneste. IAM er et kompleks system, fordi den skal fungere sammen med mange forskjellige infrastrukturer, plattformer, krypteringsmekanismer, policyer og skal integreres med mange ulike systemer og mekanismer. IAM-systemer har hensikt å forbedre tilganger til nettverket og dens ressurser, og sikre riktig håndtering av brukeridentitetenes livssyklus.

"Identitetshåndtering, IAM handler om informasjonssikkerhet, forbedre prosessene for oppretting, sletting og bruk av digitale identiteter samt å få en effektiv hverdag for brukere (ansatte) og samarbeidspartnere." ***[14]***

Identitets og tilgangskontrollssystemer spiller en avgjørende rolle fra brukerkontoen blir etablert med alle sine tilgangsrettigheter til brukeren en gang forlater virksomheten. Hver organisasjon må ha pålitelig metoder å identifisere brukerne, og effektive prosesser og prosedyrer for å regulere hvilke applikasjoner, data og andre ressurser brukerne kan få tilgang til.

3.3 Autentisering

Det hele starter med godkjenning av om brukeren er den han hevder å være ved innlogging til systemet. Virksomheten må forsikre seg om at den som logger på er hvem de sier de er, slik at vedkommende kan få tildelt de tilgangsrettigheter som han/hun skal ha.
Brukeren taster inn sitt brukernavn og passord, og systemet avgjør om brukeren er den han/hun utgir seg for å være. Brukeren har overrakt systemet noe han og systemet kjenner til, og dermed har brukeren bevist sin identitet ovenfor systemet.

> *"Autentisering er en prosess som sikrer at en bruker faktisk er den han/hun utgir seg for å være. En vanlig form for autentisering er å benytte brukernavn og passord. Dette defineres som en svak autentiseringsmetode." [15]*

Det er fullt mulig å bruke flere faktorer i en autentisering, dette sikrer at virksomheten gir tilgang og rettigheter til rett person på en sikrere måte.

> *"En mer avansert og mye sikrere metode er å benytte engangspassord og egen kode, såkalt to-faktor autentisering. Dette defineres som en sterk autentiserings metode." [15]*

Autentisering kan skje ved forskjellige mekanismer som kan inkludere andre metoder for å påvise identiteten til personen, for eksempel et smartkort, iris skanning, ansiktsgjenkjenning, stemmegjenkjenning eller fingeravtrykk.

> *"`Noe du bærer`-metoden*
>
> *Adgangskontrollsystem som er basert på `noe du bærer`-metoden, omfatter vanlige nøkler og/eller adgangskort med eller uten bilde/personligkode" [4]*

Noe man har eller bærer på kan være et smartkort, private nøkler, et sertifikat, passordkalkulatorer (tokens), cryptocards, digitale sertifikater.

> *"`Noe du vet`-metoden*
>
> *`Noe du vet` kan være en medarbeider nummer, en egen PIN-kode, et passord eller lignende (for eksempel nøkkelkort med kode)." [4]*

"Noe man vet"-metoden kan også kombineres med andre faktorer, såkalt sterk autentisering. Nettbank er et eksempel på dette. Når bankkunden logger seg på nettbanken, identifiserer kunden seg ved å skrive inn personnummeret/brukernavnet. Kunden autentiseres ved hjelp av en PIN-kode fra en passordkalkulator.

> *"`Spesielle egenskaper`-metoden*
>
> *Biometri er en teknologi som kan avlese menneskelige kjennetegn som fingeravtrykk, øye(iris), stemme, ansikt, håndgeometri eller andre personlige kjennetegn. Slik karakteristikum er stort sett unike for alle mennesker." [4]*

Noe man er/spesielle egenskaper-metoden er basert på at alle mennesker har forskjellige kjennetegn, og at de kan identifiseres ved hjelp de forskjellene.

3.3.1 Katalogtjenester (Directory Services)

Katalogtjenester tilbyr en organisasjon til å administrere og lagre informasjon om brukere og andre enheter i IT-infrastrukturen. Mange virksomheter kjører ulike systemer som igjen krever ulik organisering og ulik lagring av brukerinformasjon. Informasjon er fordelt over de forskjellige katalogtjenestene, og ofte er det snakk om dobbellagrin av data.

Med forksjellige ulike kataloger for informasjon økes vanskeligheten med å finne ut hvem som har tilgang til hva. Det er heller ikke lett å knytte en person med alle de tilgangene vedkommende har til de brukerkontoer han har i IT-systemene.

> *" Directory services provide the foundation of any identity and access management infrastructure. Directory services provide a single source of authoritative digital identity information. Such information can include security information, such as passwords and X.509 certificate mappings, as well as user profile information in the form of user attributes that include addresses, telephone numbers, office space, titles, and department names."* ***[16]***

Med spredning av brukere og enheter i en organisasjon er det større behov for et sentralt sted å lagre og behandle informasjon om brukere og deres rettigheter.

> *"Directory services and meta-directories deal with the representation, storage, and management of identity and profiling information. They provide standard Application Program Interfaces (APIs) and protocols for information access. Data repositories are often implemented as a Lightweight Directory Access Protocol (LDAP)-accessible directory, meta-directory, or virtual directory."* ***[17]***

Katalogtjenester vil integreres med IAM-løsninger, og vil kunne administrere et økende antall brukere, roller og enheter. IAM-løsninger kan inkludere andre kilder, inkludert SQL-databaser, XML-formaterte filer, flatfiler. I tillegg vil katalogtjenester kunne tilpasse seg til nyere organisatoriske sikkerhetsrutiner for eksempel to-faktor autentisering, kryptering av data og sporing.

Katalogtjenester muliggjør sentralisering og sikker håndtering av et helt nettverk, som kan utstrekke seg i en bygning, en by eller flere steder over hele verden. Lagring og håndtering av brukerinformasjon vil kunne sentraliseres, som vil føre til en bedre administrering av identitetsdata på tvers systemer og avdelinger**.**

> *"Enterprise directories are a single authoritative source for identity information throughout an enterprise. All users and directory-enabled applications rely on the identities stored in the enterprise directory. This is the ideal scenario. However, most enterprises cannot use this approach due to the presence of legacy directories."* ***[17]***

En metakatalog sørger for at brukerdata, og andre attributter synkroniseres mellom en eller flere katalogtjenester og databaser.

> *" Meta-directories provide a consolidated view of the identity data stored in different repositories. They also synchronize the data in the different repositories. A meta-directory resembles an advanced directory synchronization utility. Most meta-directory solutions come with workflow logic, and they overlap with many of today's identity provisioning solutions."* ***[17]***

Katalog synkronisering muliggjør synkronisering av brukerinformasjon på tvers av heterogene katalogstrukturer. Dette gjør det mulig å automatisere prosessen med å oppdaterebrukerinformasjon på tvers av plattformer samtidig som integriteten og eierskapet av data opprettholdes for hele virksomheten.

> *"Directory synchronization utilities are intelligent LDAP-based utilities that can synchronize identity data between different types of identity repositories—such as directories, databases, and the repositories linked to enterprise resource planning (ERP) systems."* ***[17]***

Virtuell katalog samler brukerinformasjon fra flere heterogene kilder som kataloger, databaser, flatefiler og webtjenester og gjør det tilgjengelig via LDAP.

> *" Virtual directories, unlike meta-directories, do not build a central repository. Instead, they rely on directory server or client functions to access the data stored in different directory sources. Virtual directories also allow for the creation of different application-specific views of directory data."* ***[17]***

3.3.2 Identitetshåndtering (Identity Management)

Det er veldig vanlig i dag at en som er nyansatt bruker 1-2 uker før vedkommende kommer i gang med arbeidet. Det er ikke fordi personen skal få noe tid til å bli bedre kjent med sine kollegaer men det er fordi det tar tid før IT-avdelingen får opprettet en brukerkonto til vedkommende. Det vil si at de 2 første ukene går til å vente på at det opprettes en ny digital identitet med forskjellige rettigheter som kreves for at den nyansatte kan komme i gang med jobben.

Under ser vi tall fra en studie fra 2003 gjort ved Stanford og Hong Kong universitetene med 2000 bedrifter der 200 av dem ar globale virksomheter.

> *" Q. How long does it take a new hire to get access to all the systems he/she needs?*
>
> *48% of companies take more than two days.*
>
> *10% of companies take more than two weeks"* ***[18]***

Samme problematikk gjelder også når en ansatt slutter i jobben, ansatt kan ha adgang til sensitive data og systemer i ukevis fordi systemadministrator ikke har fått oppsigelsesbrev/e-post fra HR(Human Resources). Dette gir mulighet for informasjonslekkasje, eller sikkerhetshull som kan føre til alvorlige trusler eller ødeleggelser i systemene.

> *" Q. How long does it take your company to revoke an employee's access rights?*
>
> *43 % of companies surveyed take more than two days*
>
> *15 % take more than 2 weeks"* ***[18]***

Identitetshåndtering(Identity Management) begynner med etableringen av brukerkonto og brukes til å automatisere administrative oppgaver relatert til brukeridentiteter i en virksomhet. Dette kan være å opprette, endre eller slette brukerkontoer, brukerprofiler eller kundekontoer, osv. Brukerkontoen etableres og deretter spres den til alle de systemene som den aktuelle brukeren vil få tilgang til. Endringer som brukeren opplever i henhold endringer i sin stilling, i prosjektarbeid vedkommende er med eller skal være med eller når vedkommende forlater virksomheten, vil oppdages av identitetshåndteringssystemet.
Oppgaver som er en del av identitetshåndteringssystemet i løpet av levetiden for brukerkontoen inkluderer:

- Legge til eller fjerne brukerkonto til bestemte systemer
- Tilbakestilling av passord ved mistet eller glemt passord
- Håndheving av passordregler for periodiske endring av passord for å øke nettverksikkerheten

3.3.3 Passordhåndtering (Password management)

Passordbeskyttelse er den mest vanlige måten å forhindre at uautoriserte får tilgang til systemene og ressursene. Passord er et svakt punkt når det gjelder sikkerheten ved datasystemer, med svake passord eller ingen passord gir man en åpen anledning til uautoriserte personer til å legalisere seg på systemet. Dette slipper angriperen inn som en normal bruker, eller som en administrator. Selv om angriperen får tilgang til en vanlig brukerkonto, gir dette tilgang til å kartlegge systemet slik at angriperen kan angripe systemet ytterligere og utføre alvorlige angrep på systemet og/eller på brukerkontoer.

> *"Password management is a significant part of any solution to improve security in an organization, because weak passwords are an open opportunity for anyone with access to those systems to authenticate themselves and mount an attack on other user accounts with weak passwords. "[19]*

Passord som kan finnes i en ordbok er ubrukelige i nettverk der ressurser skal beskyttes mot uautoriserte og utenforstående personer. Det finnes programmer som kan teste mange tusen passord i sekundet, til programmene følger ordlister som er mer omfattende en vanlige ordbøker med ord fra mange forskjellige språk og tallkombinasjoner.
Selv om angriperen får tilgang til en vanlig brukerkonto, gir dette tilgang til å kartlegge systemet slik at angriperen kan angripe systemet ytterligere og utføre alvorlige angrep på systemet og/eller på brukerkontoer.

> *"Attackers often gain access to sensitive data through weak or stolen passwords. Alternatively, an attacker can use accounts as a foothold within a network to launch increasingly sophisticated and dangerous intrusions into an organization's IT systems."[19]*

Passordstyring er et viktig del av IAM-løsninger der hensikten er å forbedre sikkerheten i en organisasjon. Svake passord er en åpen anledning for de som har uærlige hensikter til å legalisere seg på systemene og til å utføre angrep på andre brukerkonto med svake passord. Veldig ofte at ansatte som bruker mange programmer i løpet av en arbeidsdag, bruker programmer som krever hvert sitt brukernavn og passord. Brukere som hver har mange passord å huske og mange programmer å forholde seg til, ofte skriver ned passordene eller bruker et og samme passord på alle programmene. Mange brukere velger også enkle passord

like før de skal ta ut ferie, fordi de vil klare å huske passordet når de møter på jobben etter ferien.

> *"META Group research shows that approximately 45% of total calls to the average help desk are password reset assistance."[20]*

Antall anrop til brukerstøtte hoper seg opp etter ferier eller lengre tid med sykefravær, fordi mange da har glemt passord til systemene når de er tilbake på jobb. Dette er noe som fører til økte operative kostnader og fører til unødvendig bruk av ressursene.

> *"In a survey of over 400 large organizations automating password reset would reduce help desk calls by 30%. In a 10,000 user organization, this equates to $648,000 annually."[21]*

Løsningen på disse problemene kan være å automatisere prosessene via en IAM-løsning. Passordhåndtering inkluderer forenklet tilbakestilling av eget passord, dvs. at brukerne kan tilbakestille sine egne passord, endre passord, passordsynkronisering og passordpolicyer. Ansatte selv kan da ta seg av jobben med å tilbakestille passordet sitt, de kan identifisere seg overfor systemet med en PIN-kode, svare på et personlig spørsmål, eller via en biometrisk autentisering og kunne da tilbakestille passordet sitt. Denne prosessen kan redusere administrasjons kostnader og redusere ventetiden som oppstår mens brukeren venter på hjelp fra brukerstøtte.

> *"Twenty-five percent to 30% of help desk call volume for password management will directly affect cost reduction."[22]*

3.3.4 Passord Synkronisering

Passord synkronisering hjelper å forenkle prosessen med å opprettholde sikre passord i ulike miljøer. Når en bruker endrer passord i en domene, spres denne endringen automatisk til andre domener og systemer.

> *" Password synchronization is a process that applies both to password reset and password change. Quite a bit of confusion exists in the industry about the related terms password synchronization and password push. This series defines password synchronization as an operation in which a plaintext copy of a password is extracted from one location and then placed in one or more credential stores. Password synchronization can then occur in one of two ways:*
>
> *• One-way password synchronization (or password push). Changes to the password in one central system are intercepted and pushed to one or more additional stores.*
>
> *• One-way password synchronization (or password push). Changes to the password in one central system are intercepted and pushed to one or more additional stores.*
>
> *• One-way password synchronization (or password push). Changes to the password in one central system are intercepted and pushed to one or more additional stores.*
>
> *• Bidirectional password synchronization. Changes can be made in either store and then replicated to the other." [23]*

Passordsynkronisering kan være et problem for informasjonssikkerheten ved organisasjonen, fordi hvis passordet blir gjettet av en datasnok, da har han/hun adgang til mange flere applikasjoner enn om det kun var et enestående passord for hver applikasjon.

3.3.4 Single Sign-On

Anrop til servicedesken hoper seg opp etter ferier eller lengre tid med sykefravær, fordi mange da har glemt passordet til systemene når de er tilbake på jobb. Dette kan føre til økte operative kostnader og skape problemer innad i bedriften fordi ansatte ikke får gjort jobben sin, administrator ikke får gjort det egentlig han skulle ha jobbet med.

Løsningen på disse problemene kan være å automatisere prosessene via en identitets og tilgangskontrollssystem. Arbeidstakere kan da ta seg av jobben med å tilbakestille passordet sitt. Arbeidstakere kan da identifisere seg ved en vekslende opplysning, og kunne da tilbakestille passordet sitt. Denne automatiserte prosessen kan redusere administrasjon og support kostnader, fordi servicedesken ikke trenger å tilbakestille brukerpassrodene. Det reduserer også ventetiden som oppstår mens brukerne venter på support fra servicedesken. Et passordstyringssystem forbedrer og effektiviserer ikke bare sikkerheten, men det gjør også noe dramatisk med servicedeskanropene. Anrop til servicedesken kan gå ned med ca.75 % og dette kan hjelpe virksomhetene til å kalkulere gevinstene ved en IAM-løsning.

I de fleste virksomheter har brukere vanligvis flere systemer de må logge seg på hverdag for å utføre jobbene sine. Hvert system kan omfatte ulike brukernavn og passord, ulike regler for når og hvordan du endrer passord. Disse systemene opptrer som uavhengige domener i den forstand at en bruker må identifisere og autentisere seg på hvert av systemene uavhengig av hverandre.

> *” Q. How many passwords do you have to remember on a daily basis?*
>
> *86% have to keep track of two or more passwords*
>
> *26% of which have to keep track of four or more passwords” **[18]***

Flere logo prosedyrer med ulike brukernavn og passord kombinasjoner er også en sikkerhetsrisiko. Fordi brukere ofte skriver ned passordet, eller velger enkel passord som er lett å huske.

Fra et brukerperspektiv er det betydelig mye enklere å bli identifisert og autentisert en gang, og deretter få adgang til alle applikasjoner og databaser, heller enn å måtte logge på hvert system separat. Det er her "Single Sign-On"(SSO) kommer inn, vi ser på en definisjon av det(den er hentet fra Wikipedia, the freke Encyclopedia).

> *”Single sign-on (SO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. Single sign-off is the reverse process whereby a single action of signing out terminates access to multiple software systems. "[25]*

Ved å redusere antall loging prosedyrer med ulike brukernavn og, kan forbedre sikkerheten ytterligere. Sikkerheten øker fordi ved å redusere antall passord brukerne må huske, kan man kjøre strengere regler for passordvalg. Med denne løsningen kan brukeren bruke flere

tjenester sømløst, og man reduserer også problematikken ved at brukerne skriver ned passordene sine.

> *"META Group research demonstrates that single sign-on would result in a 33% reduction in help desk call volume as well as a 32% increase in overall security."* ***[20]***

4.3.5 Føderasjon (Federation)

Behovet for samarbeid og informasjonsdeling med samarbeidspartnere, leverandører, kunder og ansatte på tvers av organisatoriske grenser har hatt en kraftig utvikling de siste årene.

> *"Enterprises are continually extending their business processes outside their traditional boundaries to conduct electronic business with partners and suppliers."****[24]***

Virksomheter ønsker å utvide interne systemer for eksterne brukere, og gi sømløs tilgang til informasjon og ressurser, men samtidig vil de ikke gi slipp behovet for å opprettholde sikkerheten ved systemene.

De fleste av oss administrerer et antall internettprofiler på ulike nettsteder. Nettstedene kommuniserer ikke med hverandre, og dermed eksisterer det flere brukeridentiteter for samme person. Administrering av disse identiteter er bortkastet tid, men om alle dissene kontoene kan fødereres, kan brukerne få tilgang til de alle nettstedene uten å huske alle passordene.

> *"Federation is the combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries."**[24]*

Begrepet føderasjon blir stadig viktigere i en verden der virksomheter står overfor et mer komplekst sett av utfordringer, og muligheter. Føderering gjør det mulig å koble sammen digitale identiteter i på tvers av organisatoriske grenser, plattformer.

> *"Federation makes it possible for an authenticated identity to be recognized and take part in personalized services across multiple domains."* ***[24]***

Føderert identitet kan løse disse problemene, føderering gjør det mulig å koble sammen digitale identiteter i forskjellige virksomheter. I en føderert nettverden, kan personlig informasjon overføres mellom nettsteder. En bruker kan logge seg inn i nettbanken sin, og der fra navigere videre til flyselskapets hjemmeside for å kjøpe flybilletter. Informasjon om bruker bringes med fra innloggingen i nettbanken.

> *" Liberty Federation allows consumers and users of Internet-based services and e-commerce applications to authenticate and sign-on to a network or domain once from any device and then visit or take part in services from multiple Web sites. This federated approach does not require the user to reauthenticate and can support privacy controls established by the user."*
> *[25]*

Føderering mellom uavhengige virksomheter bygger på tillit, gjensidige avtaler og andre måter å etablere tillit på. Det nettstedet som tar i mot brukeren må ha tillit til at det nettstedet som autentiserte brukeren gjorde dette på en forsvarlig måte.

Security Assertion Markup Language (SAML) protokoller er det mest brukte mekanisme for å utveksle autentisering og autorisasjon av data over plattformuavhengige XML-rammeverket. SAML gir umiddelbar anerkjennelse av om den fremtidige brukeren er en person eller en maskin, og hva personen eller maskinen kan få tilgang til.

> *"By implementing federation technologies, a business can gain greater efficiency with IT expenditures, realize new revenue opportunities with its business partners, and expand its product and service offerings to its customers."* *[24]*

Mange virksomheters portaler har et behov for en tettere integrasjon med partner- og/eller kunder. Med en solid føderert identitetsstyring kan virksomheter effektivt håndtere integrasjon med kunder, partnere og føre til vesentlig kostnadsparinger, operativ effektivitet, økt sikkerhet, og samtidig sikre at virksomhetene er i samsvar med nasjonale og internasjonale reguleringer og standarder.

3.4 Administrasjon

Administrering av brukeridentiteter anses som en av de mest utfordrende aspektene ved IAM. Fremgangsmåten for å sette opp kontoer og sikre rett tilgang er tidkrevende og ofte utsatt for feil. Dette gjelder spesielt når mange systemer, programmer der unike identiteter er involvert.

3.4.1 Brukertilordningsprosess (User Provisioning)

Ved ansettelse av en ny person i organisasjonen, vil den nyansatte trenge en brukerkonto i organisasjonens nettverk, en e-postkonto, registrering i lønningssystemet, registrering i timeregistreringssystemet, etc. Å gi den nyansatte riktige ressurser blir fort en ganske omfattende og komplisert oppgave. Denne prosessen kan ta tid, og det er ikke sikkert nyansatt vil få med alle rettigheter etter flere dager i jobb.

Det kan også hende at den nye brukeren ikke er en nyansatt, men en ekstern konsulent, kunde, partner eller annen type ressurs som vil bli involvert i organisasjonen. I slike situasjoner kan det ta enda lenger tid til å identifisere de systemene en skal ha tilgang til, og opprette bruker i de respektive systemene.

> *"Tilordningsprosessen utstyrer brukerne med brukerkontoer og de tilgangsrettigheter de trenger for å få tilgang til gitt system eller en applikasjon"* ***[4]***

Bruker tilordningsprosessen omfatter brukerkontohåndtering (opprette, modifisere og slette brukerkonto og privilegier) for adgang til heterogene IT ressurser. Virksomheter bruker typisk tilordningsprosessen til å forvalte interne brukertilganger. Brukertilordningsprosessen er jobben med å gi brukerne de riktige ressursene de trenger for å kunne utføre oppgavene sine. De fleste brukertilordningsprodukter byr på passordhåndteringsfunksjonalitet, delegert administrasjon, en rollebasert tilgangskontrollsmodell og arbeidsflyt (workflow).

Tilordningsprosessen inneholder følgende aktiviteter:

"

- *klargjøring av brukeren*
- *samle inn og sjekke identifiseringsinformasjon (som identifiserer person eller objekt)*

- *identifisere de systemene en bruker skal ha tilgang til*
- *opprette brukerkonti (rettigheter) i de respektive system*
- *opprette en kopling til autentiseringsinformasjonen*
- *foreta autorisering av tilgangsrettigheter*
- *vedlikeholde autentiseringsinformasjon og tilgangsrettigheter for alle brukerne*
- *fjerning av tilgangsrettigheter ”* [4]

Brukere kan ha behov for tilgang til en rekke ressurser, slik som IT ressurser som nettverket, e-post, digitale sertifikater, databaser, servere og applikasjoner. Brukertilordningsprosessen vil identifisere de systemene en bruker skal ha tilgang til, og oppretter brukerkonti i de respektive systemene.

Når vi snakker om brukertilordningsprosessen, må vi også nevne de-provisioning som går ut på å slette brukerkontoer, og sørge for at tilgangsrettighetene til eksmedarbeider er slettet. En organisasjon ønsker ikke å gi en eksansatt tilgang til sensitiv informasjon, og heller ikke tilgang til andre deler av organisasjonen.

Når en bruker forlater organisasjonen, vedkommendes tilganger må trekkes tilbake fra alle systemene i virksomheten vedkommende har hatt tilgang til.

> *”...what (some) ex-employees do*
>
> *Worrying!*
>
> *50% continue to use corporate networks*
>
> *55% retain their laptop's if not taken back*
>
> *58% use cell phones if not taken back*
>
> *67% to steal and use proprietary information”* **[26]**

3.4.2 Automatisert brukertilordningsprosess (Automated User Provisioning)

I små foretak der brukertilordningsprosessen utføres manuelt, er det ikke en tidkrevende jobb å fikse feil man har gjort under oppretting av en bruker. Men i organisasjoner med flere tusen brukere og flere ulike systemer, er det alltid fare for menneskelige feil. Disse feilene er ikke bare veldig tidkrevende å reparere, men øker også risikoen for uautorisert tilgang til ressursene.

Automatiserte prosesser kan bidra til å beskytte sensitiv informasjon, redusere administrasjonskostnader og se til at foretakspolicyene og juridiske krav blir fulgt. I tillegg kan det redusere den ineffektiviteten i forbindelse med administrering av brukerkontoer og brukertilganger på en ad-hoc måte.

> *” The Gartner Consulting multiclient study found that at the companies surveyed lost productivity averaged 35 minutes per-user, per-month. This average included new employee or contractor setup time, password resets for enterprise IT systems, and employee role changes that required IT system changes. For a company with 10,000 employees, that equates to 2,916 lost days of employee productivity per year.”* **[27]**

Virksomheten ønsker at en nyansatt skal bli produktiv så fort som mulig. Det vil være unødvendig inneffektivitet om en nyansatt ikke får kommet i gang med jobben sin, fordi vedkommende venter på å få de tilgangene han skal ha til systemene. Automatisert brukertilordningsprosessen automatiserer tidkrevende prosessen med å håndtere brukerens

rettigheter på tvers av flere systemer umiddelbart etter at en bruker er opprettet. Brukerne får raskere tilgang til riktige IT-ressurser i henhold til forhåndsbestemte prosesser og retningslinjer.

Å automatisere brukertilordningsprosessen har noen klare fordeler, slik som:

- Reduserer kostnader ved å automatisere oppretting, sletting av brukerkontoer i sammensatte identitetsbeholdere.

- Øker produktiviteten ved å redusere tiden som trengs for å opprette brukerkonto, passord, og tilgangsrettigheter for en nyansatt.

- Øker sikkerheten ved å forsikre om at ansatte som slutter i virksomheten fratas alle de tilgangsrettigheter vedkommende har.

Automatisert brukertilordningsprosess kan støtte fullt ut livssyklusen til brukeridentiteter og deres tilgangsrettigheter, fra registrering, godkjenning, tilordningsprosessen, løpende vedlikehold, revisjon og til oppsigelse. Revisjon av roller og rettigheter er en viktig del av automatiseringsløsningen, som manuelle prosesser nesten aldri har noe tilsvarende.

3.4.3 Policybasert brukertilordningsprosess

> *"Policyer er spesielle regler laget med det formål å regulere forhold ved en organisasjon eller ved et system innenfor en organisasjon."* ***[28]***

Organisasjoner kan definere og bruke policyer til å administrere og spore brukerkontoer, tilgangsrettigheter, osv. Policyer kan brukes for å sikre at prosesser for brukertilordning overholdes, og brukeren ikke har fått flere rettigheter enn det han skal ha. For eksempel brukes for å angi at alle som har fått tilordnet administratorrollen får automatisk tilgang til admin-mappene, og får opprettet brukerkonto i ulike respektive systemer.

> *"Once an entity such as a user is defined to the central identity manager, it is likely that the same entity will require creation of accounts o none or more of the managed services and systems."* ***[29]***

Policyer kan også ha bestemmelser om hvilke handlinger brukerne kan utføre, skal vikarer ha alle de tilgangene en de vikarier for har? Hva med en som har tatt permisjon fra jobben, skal vedkommendes brukerkonto fortsatt være aktiv, og hvor lang tid skal brukerkonto og e-postkonto til en som har sluttet i firmaet oppbevares og hvilke handlinger utføres med mapper og filer vedkommende står oppført som eier. Policyer kan gjøre det enklere til å overholde firmaets interne prosesser, og å overholde juridiske bestemmelser.

> *"Policy-based account provisioning refers to setting up provisioning policies to perform this automation process. Such policies can be based on various conditions such as role, prostion within the organization, or possession of particular attributt."* ***[29]***

Virksomheter endrer seg etter hvert som omgivelsene, markedet, teknologi endrer seg. En policy vil også oppdateres etter hvert, og vil gjennomgå endringer i forhold til omgivelsene over tid.

"They should be easy to develop, be flexible enough, and allow for coarse and fine granularity." ***[29]***

4.4.4 Revisjon.

Virksomheter kan ha vanskeligheter med å i møte komme myndighetenes krav om revisjon, og kunne identifisere brukere, deres roller og tilknyttete ressurser. Det er ofte vankelig å gjengi nøyaktig hvor mange brukere som virkelig eksisterer i systemene. Og om de brukerne som finnes i systemet virkelig tilhører en eksisterende ansatt i virksomheten eller en ekstern partner. Et annet problem som eksisterer i mange virksomheter, er rettigheter og tilganger som brukeridentitetene har. Foreldreløse brukeridentiteter som ikke er oppdaget og fjernet, vil være et sikkerhetshull for systemene. Virksomheter som har erfart og er klare over problematikken, har ikke alltid teknologien og prosessene for å kunne fjerne foreldreløse identiteter.

IAM-løsningen kan samle inn informasjon, analysere og rapportere på bakgrunn av tilganger, aktiviteter, svakheter og revisjon som kan dekke de fleste behov for rapportering. Løsningene kan også ha muligheten til å ta ut rapporter, som viser roller og deres medlemmer, oppgaver og roller som er assosiert med dem, brukerprofiler og deres tilganger. Med enkle operasjoner kan man få ut rapporter som kan hjelpe oss til å få bedre kontroll på systemene og forbedre sikkerheten ytterligere.

Det er viktig å kunne dokumentere svakheter ved systemene og kunne overvåke. Ved innbrudd kunne undersøke og dokumentere innbruddet, det vil være avgjørende for å ta tyven, og som også kan hjelpe oss videre i arbeidet med å sikre systemene. En svikt i systemene kan ha negative vikninger på selskapets navn utad og kan forhindre forretningsekspansjoner. Ofte er det slik at før to selskaper velger å slå seg sammen at de ber om en uavhengig gjennomgang av det andre selskapets systemer.

Det er av stor nødvendighet å kunne dokumentere hvem brukere vi har i systemene, og hva de kan gjøre i systemene. Men å kunne dokumentere hva som er blitt gjort i systemene, hvem som har gjort og når han/hun har gjort det, er verdifull informasjon for organisasjonen. En solid IAM-løsning vil kunne hjelpe oss med å loggføre alle hendelser relatert til hver aktivitet, inkludert bruker oppretting, rollestyring, provisioning aktiviteter, osv.

3.5 Autorisering

Autorisering er prosessen for å fastslå om en bruker har de privilegier som må være tilstedet for å kunne nå en ressurs. Dette bestemmes vanligvis ved å finne ut om personen er en del av en bestemt gruppe, eller om personen har betalt medlemskontingent, eller om brukeren har et bestemt nivå av sikkerhetsklarering. I datasystemer, defineres autorisering som prosedyren med å avgjøre om en bruker har tilgang til systemet (for eksempel tilgang til hvilke filer, kataloger, disker, og så videre).

I sikkerhetslovens § 3 er autorisasjon under pkt. 17 definert som:

"Avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenestelig

behov samt avlagt taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad."[30]

Autorisering er nær knytt til autentisering. Du må kunne styre hva brukerne faktisk kan gjøre etter at vedkommende er identifisert og godkjent.

"However, more precise usage describes authentication as the process of verifying a claim made by a person (or a computer, smart card etc.), while authorization is the process of verifying that an authenticated person has the authority to perform a certain operation. Authentication, therefore, must precede authorization." [31]

Har du gitt bilnøklene dine til en person som har skjulte hensikter, hjelper det lite om du har alarm i bilen.

"Total sett er autorisering en kompleks og sammensatt oppgave. Korrekt autorisering er imidlertid fundamentalt for hele sikkerhetssystemet. Kryptering hjelper ikke hvis feil person er autorisert til å motta meldingen" [4]

3.5.1 Tilgangskontroll(Access management)

Store virksomheter med tusenvis av brukere, har systemer og infrastruktur som bygges opp hele tiden. Virksomheter har mange interne og eksterne brukere, med forskjellige tilgangsbehov som kan omfatte mange ulike systemer, kataloger og programmer. Organisasjoner har behov for å regulere ansattes tilgang til bedriftens data, og holde orden på hvem som har tilgang til hva. Hvis brukerne og applikasjonene gis flere privilegier enn nødvendig, utsettes systemet for farer som virus, datatyveri, osv.

"Gartner estimates that more than 70 percent of unauthorized access to information systems is committed by employees, as are more than 95 percent of intrusions that result in significant financial losses." [32]

Tilgangskontrollprosessens oppgave er å gi autoriserte brukere tilgang til de ressurser og systemer de har behov for å kunne utføre jobben sin. Prosessen skal også sperre tilgangen til ressursene for uautoriserte brukere. Før legitime brukere får tilgang, må de først identifiseres og godkjennes, så sjekkes det om brukeren kan få tillatelse til å få tilgang til de ønskede ressurser.

"*Prosessen inneholder følgende hovedtrekk:*

- *sjekking av brukerens identitet*
- *autentisering av brukeren*
- *å ta stilling til brukerens behov for tilgang (nivå av rettigheter)*
- *å gi brukeren formålstjenlig tilgang til et system" [4]*

Ressurser og tjenester kan være et hvilket som helst objekt som tilgangen skal kontrolleres, dette kan være for eksempel maskinvare, programvare, bygninger, dører og så videre.

Tilgangskontrollløsninger kan gi omfattende tilgangskontroll over alle kritiske ressurser, systemer, databaser, og webapplikasjoner. Løsningene omfatter autentisering, autorisasjon og sikkerhetsrevisjon. Tiltak som digitale signaturer, kryptering, biometrisk skannere og overvåking systemer er også inkludert i de fleste løsninger.

Tilgangskontrollsløsningene har mekanismer for å begrense tilgangene til systemene basert på prinsippet om det minste privilegium ”the principel of least priviligum”, og ved hjelp av etablerte roller, regler og policyer. Prinsippet om det minste privilegium, er målet å gi brukerne bare tilgang og rettigheter de trenger for å fullføre arbeidsoppgavene de har.

> *”The principle of least privilege states that a subject should be given only those privileges that it need in order to complete its task.”[3]*

Tilgangskontrollsløsningene gir organisasjonene mulighet til å kunne styre tilgangskontroll fra et sted, for å gi brukerne tilgang til flere systemer og applikasjoner på tvers av organisasjonen.
Dette kan forbedre sikkerheten, virksomheten vil få full kontroll over hva brukerne kan få tilgang til og beskytte ressursene fra uautorisert tilgang.

Når en ny ansatt starter i virksomheten, får han opprettet en brukerkonto med noen standard rettigheter og tilganger. Men det kan ta enda lenger tid, før han får de tilganger og rettigheter til kataloger og filer han trenger for å kunne utføre jobben sin. Og når den ansatte flytter på seg innad i virksomheten, kan det ta nesten like lang tid før han får de rettigheter og tilganger som kommer med den nye arbeidssituasjonen. Med IAM kan virksomheter aktivere brukerkontoer for alle de systemer som vedkommende skal ha tilgang til i en enkel handling.

Enda viktigere er det motsatte tilfellet, altså når en ansatt slutter i jobben. Ansatt som har sluttet i jobben, kan eksistere lenge i systemene før brukeren hans fjernes med de rettighetene og tilgangene han/hun har. I de fleste tilfeller vil ikke vedkommende fjernes fra systemene, vedkommende vil da ha full adgang til systemene, og kan bruke, modifisere ressurser han har tilgang til(filer, e-post, osv).

Tilgangskontroll i en IAM-løsning skal kunne garantere at brukerne får de rettighetene når de trenger det, og at tilgangene endrer seg med de endringene som følger med jobben, og at tilgangene fjernes når brukerne ikke har behov for dem lenger.

3.5.2 Rollebasert tilgangskontroll (Role-based Access Control (RBAC))

RBAC er en metode for håndtering av tilgang til data og ressurser i informasjonssystemer. En bruker har tilgang til de nødvendige deler av informasjonssystemet som en funksjon av sin rolle i organisasjonen. Dette betyr at en brukers tilgang til data og ressurser er begrenset av brukerens legitime roller i organisasjonen. En bruker kan ha flere roller, en rolle kan ha flere brukere, en rolle kan ha mange tilganger; en tilgang kan tildeles mange roller. Roller er faktisk forhåndspakkede ressurser og tjenester. Disse rollene har fått tilknyttet rettigheter som gir tilgang til operasjoner på data og ressurser.

> *”RBAC is a technology that offers an alternative to traditional discretionary access control (DAC) and mandatory access control (MAC) policies. RBAC allows companies to specify and enforce security policies that map naturally to the organization’s structure.” **[NIST,2002]***

Ofte en ansatte kan risikere å spille flere roller i løpet av en arbeidsdag, han kan utføre flere ulike arbeidsoppgaver. Tillatelse til å utføre visse operasjoner, er tildelt spesifikke roller.

Styring av enkelte bruker rettighetene blir en enkel sak for å tilordne de riktige rollene til brukeren.

> *"This technology decreases the cost of network administration while improving the enforcement of network security policies"* ***[33]***

Fleksibiliteten som ligger i en rollebasert tilgangskontroll, gir store fordeler når endringene gjør seg gjeldende ved forandringer i arbeidsroller, tilganger for ansatte og partnere. For eksempel, hvis en bruker skifter jobb til en ny funksjon i organisasjonen, kan brukeren ganske enkelt tilordnes den nye rollen og den gamle rollen fjernes.

> *"some firms or organizations are very dynamic, and user roles and permissions change quickly. In these environments, RBAC is more efficient in moving users in and out of given roles and changing the permissions of given roles than competing access control systems"* ***[33]***

Men i et system uten RBAC innført, ville gamle tilganger bli individuelt tilbakekalt før nye tilganger kunne tilordnes brukeren.

> *"Traditionally, the prevalent approach to granting access to information within a particular database or access to a particular application is to establish specific permissions for each user within an organization. If the user must have access to multiple applications and databases, the user must be assigned permissions for each resource."* ***[33]***

En bivirkning av en implementert IAM-løsning er at roller kan effektivt kartlegge organisasjonens struktur og dokumentere systemet med tanke på en revisjonskontroll.

> *"To comply, companies are required to use access control policies that will safeguard data. RBAC is one such policy that may be best suited for this purpose"* *[33]*

3.6 Etterlevelse (Compliance)

I dag er drivkraften bak mange IAM-investeringer, en rekke lover og forskrifter som setter klare føringer for hvordan virksomheten forvalter og styrer IT-systemet sitt.

Organisasjonen må kunne redegjøre for at virksomheten etterlever juridiske, forskriftsmessige forpliktelser og tilfredsstiller regulativer som kan komme fra myndighetene, bransjer, interne retningslinjer og standarder.

Virksomhetene har plikt til å bevise overfor myndighetene om at de har etablerte rutiner for å sikre etterlevelse av lovverket og segregering av roller. Gjennom effektiv revisjon og rapportering av autentisering, autorisasjon og administrasjons aktiviteter, skal virksomheten kunne dokumentere informasjonssikkerheten ved organisasjonens systemer.

> *"Kravene til hvordan informasjon og dokumenter skal forvaltes i en virksomhet, kommer til å øke i tiden fremover. Allerede legger Bokføringsloven, IKT-forskriftene for finansforetak, og Hvitvaskingsloven strenge føringer. Dertil kommer særlige lover og forskrifter for bestemte industrier og bransjer."* ***[34]***

3.6.1 Gransking (Audit)

Ofte er det slik at det ikke finnes noe dokumentasjon på hvilke privilegier og tilganger en bruker har fått. Brukeren får de rettigheter og tilganger de skal ha til ressursene, men å kunne dokumentere dette i ettertid om hvem brukerne er og hva de har tilgang til er vanskelig. Dokumentering blir sjeldent utført i ettertid, fordi det er ressurs krevende og det kan være mange krysskoblinger i systemene.

Granskingsrapporter viser hvem som har visse rettigheter, og når, hvordan og hvorfor de har dem, er svært verdifullt særlig hvis de kan leveres raskt og enkelt. Å vite hvem som har tilgang til systemressurser, holde orden på hvem som gjorde hva, og når er en av de største utfordringene komplekse heterogene organisasjoner har. Det er ikke lett å svare på, og spesielt ikke når du må hente slik informasjon gjennom manuelle prosesser.

> *"to reduce organizational risk to the level that comes as a result of being compliant requires an identity audit solution that can provide state-based reporting and real-time monitoring of an organization's identity systems."[35]*

Dagens IAM-løsninger tilbyr automatisering av prosesser for å styre hvem som har tilgang til hva og hvem kan gjøre hva, og åpne veien for en kostnadseffektiv, bærekraftig tilnærming for å forbedre tilsyn av aktivitetene og oppnå etterlevelse av regulativene.

IAM-løsninger automatiserer fangst av historiske brukerdata og deres tilganger, og det gjennom integrerte automatiserte prosesser for rapportering og revisjon (det vil si sporing) av godkjente arbeidsflyter og fullmakter knyttet til tilgang.

"An effective identity auditing solution delivers an automated, proactive approach to meeting enterprise audit and compliance requirements, providing functionalities that move organizations from manual, fragmented processes to a monitored, optimized state. Such a solution specifically:

- *Provides continuous insight into access, privileges, and violations*
- *Enables real-time visibility into access status*
- *Automatically defines why access is granted on any given occasion*
- *Detects not only violations but also potential violations of audit policy*
- *Takes steps for remediation and mitigation in the event of a violation*
- *Creates a trail of accountability with auditable evidence of controls*
- *Automates processes, reducing staffing and services requirements."[36]*

IAM bruker automatisering til å eliminere de tidkrevende og kostbare manuelle prosesser som brukes til å kontrollere hvem som har tilgang til hvilke opplysninger, applikasjoner og tjenester, og rapportering av disse opplysningene.

> *"identity audit solutions can reduce the time, effort and cost required to achieve compliance. Identity audit solutions eliminate the need to manually attempt to collect information from various systems and cross-reference that information with policies and regulations." [35]*

3.6.2 Separation of Duty

> *"Segregation of Duties: deliver access based on policy, roles, and rules to ensure that no single individual is given the "keys to the kingdom"." [37]*

"Separation of Duty" er prinsippet om å spre ansvar og myndighet for en handling eller oppgave over flere personer. Funksjoner bør deles slik at en enkel person ikke har kontroll over alle deler av en transaksjon. Et eksempel her kan være at den som har som oppgave å foreta utbetalinger i en bank skal ikke være den samme som overvåker alle utbetalingene.

> *"The most common example of separation of duties is the separate subtasks involved in authorizing a payment for a particular transaction. By separating submission for payment and authorization for payment into separate roles, no individual can accomplish both tasks." [33]*

For å sikre tilstrekkelig internkontroll, og bekjempe svindel har bedrifter en regel om at: "En person kan ikke godkjenne sin egen bestilling. Det vil si at en bruker som tildeles rollen for å opprette bestillinger skal ikke kunne tildeles rolle til å godkjenne bestillingen sin. En annen regel kan være at "en sjekk krever to forskjellige signaturer."

Flere av IAM-leverandører har dette prinsippet inkludert i sine produkter. Ved bruk av "Separation of Duty" utelukker man at en person kan inneha to motstridende roller, og samarbeid med en annen person er nødvendig for å fullføre oppgaven. Dette kan ha en avskrekkende effekt mot svindel eller skjult agenda, og gjør sikkerhetsrevisjon oversiktlig og forståelig.

3.7 Oppsummering

IAM-løsninger har prosessene og komponentene til å identifisere hver enkelt bruker, applikasjon eller enhet på tvers av organisatoriske grenser. IAM kan gi fleksible autentiseringsmetoder, tilgangskontrollsystemer, etterlevelsessystemer og sikkerhetsrevisjonssystemer. Disse verktøyene lar forvaltning av store grupper med brukere, applikasjoner og systemer raskt og enkelt. Løsningene har verktøy som kan tildele roller og rettigheter, noe som gjør det enklere å være i samsvar med regelverket og gir mulighet for å kunne dokumentere alle tilgangene brukere har, og loggføre og rapportere alle hendelser.

IAM kan hjelpe virksomheter til å forbedre sikkerheten, effektivisere forretningsprosesser, redusere kostnader som er tilknyttet programvarelisenser, osv. IAM vil også forenkle hverdagen for mange, systemadministrator kan få flere automatiserte prosesser for oppretting, endring og sletting av brukerkontoer og deres rettigheter, vanlige brukere kan slippe å huske flere brukernavn og passord for å få tilgang til ulike systemer og applikasjoner.

Under følger andre fordeler som kan rettferdiggjøre investering i en IAM-løsning.

- Bedre kvalitet på identitetsdata
- Bedre informasjonssikkerhet med en helhetlig sikkerhetsløsning for alle ansatte
- Etterlevelse og revisjon av lover, regler og regulatoriske krav blir automatisert
- Effektivisering av driften
- Betydelig større fleksibilitet og endringsevne for virksomheten
- Single Sign On (samme brukernavn / passord og lik tidsvarighet) - for brukerne.

Kapittel 4

Forutsetninger for et IAM-prosjekt

Kapitlet starter med å beskrive forutsetninger som må være på plass før en implementering av IAM kan starte.

4.1 Innledning

IAMs appellerende fordeler både når det gjelder økonomiske innsparinger og en enklere hverdag, frister mange organisasjoner til å ta fatt på den enorme oppgaven med å initiere et IAM-prosjekt. Hver organisasjon vil ha en unik kombinasjon av mål og prioriteringer for å vurdere implementeringen. Mange organisasjoner starter arbeidet før de har fullt vurdert implikasjonene den kan ha for deres eksisterende systemer.

Initiering av et IAM-prosjekt er ressurskrevende, og er et omfattende prosjekt som krever et godt grunnarbeid. Før innføring av en IAM-løsning, bør det utvikles en plan og strategi som inkluderer en rimelig tidsperiode for gjennomføringen. En slik plan bør inkludere en skisse av IT-arkitekturen, systemene, prosessene og et beskrivende veikart for gjennomføring av prosjektet. Forarbeid er den mest kritiske delen av prosjektplanen, mange organisasjoner tar det for lett. og må betale overpris for prosjektet i tapt tid og ressurser.

4.2 Visjon, Hvorfor IAM?

Virksomheter bør ha det klart for seg hva de spesifikke fordeler som oppnås ved å forbedre eller innføre en ny IAM løsning. Uten å ha klar for seg denne visjonen vil det endelige resultatet ikke gi konkrete forbedringer og kan til og med føre til enda mer innviklede og upraktiske systemer. Virksomheten må kunne stille seg det spørsmålet om hvilke fordeler en vil få ved en implementering av en IAM-løsning. Et annet viktig spørsmål er hvilke hindringer og utfordringer som vil dukke opp underveis i prosjektet, slik at disse barrierene kan adresseres tidlig i prosjektfasen.

> *"The needs analysis should identify the problems associated with existing business processes. The resulting set of requirements should be mapped to technical specifications, to be fed into subsequent technology selection and implementation design."* *[38]*

En omfattende IAM-løsning vil kunne påvirke ansattes hverdag i stort omfang og dermed er det viktig at de organisatoriske faktorene er definerte og at ansatte er informert om de endringer som vil komme med en IAM løsning.

4.3 Planlegging av prosjektet

Det er viktig å foreta en god og grundig analyse av bedriftens behov, ønsker og nåværende situasjon. Noen ganger er en investering av denne størrelsen en altfor stor kostnad i forhold til

det behovet bedriften egentlig har. En av nøklene til suksess i ethvert IT-prosjekt er planlegging av det, og om det ikke planlegges riktig og realistisk, kan det være en kostbar affære. En god plan vil inneholde en grundig undersøkelse av alle aktiviteter som må skje før, under og etter prosjektet.

> *"Det er ofte mange av de samme årsakene som ligger til grunn for "problemprosjektene", og de kan som regel spores tilbake til mangel på tilstrekkelig planlegging og styring."*[39]

Organisasjonen bør definere hva IAM-løsningen vil utrette, og om behovet virkelig vil løses med det nye systemet. Spør de vanskelige spørsmålene og ikke utsett dem unødvendig ellers vil de komme tilbake igjen og igjen. Innføring av en IAM-løsning i en organisasjon er et omfattende prosjekt som berører store deler av virksomheten og har ofte store konsekvenser for den enkelte brukeren av systemene og dets tjenester. Leverandører tilbyr en mengde av automatiserte løsninger, men p.g.a. begrensinger og utfordringer vil de fleste ikke passe til enhver organisasjon. Ressurser må brukes for å tilpasse det til virksomhetens struktur, og prosesser.

> *"Det er selvfølgelig ikke en enkeltårsak til feilskjærene, men svarene er ganske enige: Suksessen eller havari skyldes god eller dårlig planlegging. Årsakene ligger ikke i problemer med gjennomføring."*[40]

Mange er enig i at i de fleste tilfeller der IAM prosjekter har feilet, viser seg å være at virksomheter har bagatellisert design og planlegging og har startet med teknologi ganske tidlig i prosjektfasen. Å starte med tekniske løsninger tidlig i prosjektfasen, kan føre til problemer og utfordringer som ikke oppdages i planleggingsfasen og dermed kan føre til ikke så godt gjennomtenkte løsninger.

> *"The Analysis and Planning of Identity & Access Management solution can help reduce implementation risks, identify key requirements, define the scope which can maximize ROI and provide accurate elements for the estimation of the implementation effort."*[41]

Det er av stor viktighet å kunne adressere tidlig de problemer som kan oppstå, utfordringer som kan møtes, prosesser som bør forbedres, prosesser som kan automatiseres og antall roller som kan økes eller minkes i forhold til funksjonene som eksisterer i organisasjonen. Det er viktig å ha dokumentert og definert virksomhetens datasystemer, forretningssystemer, organisasjonens struktur, osv.

4.4 Prosjektorganisasjon

Prosjektorganisasjonen skal gjennomføre nødvendige aktiviteter for å innføre IAM i virksomheten. Ved etablering av en prosjektorganisasjon er det viktig å ha avklart at brukermedvirkning finner sted i prosjektet. Brukermedvirkning kan f eks skje gjennom deltakelse i referansegrupper eller gjennom en brukergruppe.

Omfanget av IAM-prosjekter er betydelig større enn mange andre anskaffelsesprosjekter av programvare. Prosjektet vil påvirke en stor del av organisasjonen, og vil gå på tvers av avdelinger og vil ha behov for ressurser og kompetanse fra forskjellige fagområder.

Prosjektet vil medføre kostnader, samt endringer i større utstrekning enn vanlige IT-prosjekter. Virksomheten må sette av nødvendige personressurser, og bør avdekke hvem som har beslutningsmyndighet og hvem som kan godkjenne den nødvendige ressursbruken i prosjektet.

En prosjektorganisasjon må opprettes for å begynne med å utvikle en mer detaljert konseptuel modell, og en overordnet fremdriftsplan med oversikt over alle fasene i prosjektet. Tidlig involvering av alle interesserte parter i en organisasjon, og andre berørte i prosjektet, sikrer at deres behov blir møtt på design stadiet og at den endelige utformingen gjenspeiler alle behov.

"The following groups are typically involved in an identity management project:

• Security administration:
Must understand how to use the system and its impact on their work.

• Enterprise security and/or audit:
Must define security policy and audit requirements that the system will enforce. Will likely use the system to monitor policy compliance, access rights and change history.

• Systems administrators:
Must understand the impact of an identity management solution on the systems they manage.

• IT security:
Must understand the impact on overall security policy and design.

• Human resources:
Must agree to provide authoritative input information to the system, at least for employees, and ideally for contractors as well." [38]

Roller, ansvar og organisering må avklares før prosjektorganisasjonen etableres. Avklaring av prosjekteier, prosjektleder, prosjektdeltakere og gruppene som skal opprettes er meget viktig.

> *" It is crucial for an identity management project to include the system's long-term owner, as early as possible." [38]*

Hver virksomhet har en egen måte å organisere prosjekter på, men de fleste vil oppnevne en styringsgruppe, en referansegruppe og en arbeidsgruppe.

4.5 Begynn med prosessene, og ikke teknologien

Det er mange som tror at IAM-prosjekter kun består av å kjøpe en programpakke og dermed får virksomheten de fordeler som følger en IAM implementering, men dette stemmer ikke med virkeligheten. Den tilnærmingen om at IAM er et teknisk prosjekt, gir ikke et godt fundament for et kompleks og omfattende system som IAM er. IAM-prosjekter er langt mer enn bare et sett av teknologier, men står for det mest av forbedringer, endringer, automatiseringer av prosesser, policyer og teknologi som understøttende funksjon i virksomheten.

Det er av størst nødvendighet at IAM-prosjekter blir vurdert som et prosessbasert, og ikke utelukkende som et teknisk prosjekt.

> *"Identity and access management is not only a set of technologies but also a set of processes that address fundamental issues about handling the strategic asset of identity in any enterprise. Establishing a long-term solution for managing identity requires understanding these basic processes."[42]*

Det er tre viktige aspekter virksomheter bør vurdere før innføring av en IAM-løsning: prosesser, mennesker og teknologi. Det er ofte teknologien som får mest av oppmerksomheten, men det er prosessene som bør få mer fokus for å kunne nå målene med IAM.

> *" While I&AM solutions require a technology implementation, this is only a part of the solution. Understanding the transformational nature of the processes and aligning the solution with the people in the organization is critical to the success of the I&AM solution."[41]*

Arbeidsflyten som gjelder ved registrering, oppretting, endring, deaktivering og sletting av brukerkontoer, osv. bør dokumenteres med alle unntak som kan gjelde for ulike situasjoner. For eksempel når prosessen med å rekruttere en ny person til virksomheten starter til denne personene er i jobb, kjøres en rekke prosesser. Flere forretningsprosesser involveres i rekrutteringen, til denne personen får tilordnet tilganger og rettigheter i IT-systemet.

> *"Each company has a unique set of processes that affect the management of identities throughout the identity lifecycle."[43]*

Andre forretningsprosesser bør dokumenteres, slik at virkeligheten som gjelder for sluttbrukerne kan beskrives så godt som mulig. Informasjonsflyten i organisasjonen må også dokumenteres nøyaktig, slik at potensielle eller faktiske flaskehalser identifiseres og forbedringer eller endringer kan innføres.

"*The approach for developing the functional solution*
Activities
- Analyze HR data, procedures and existing role mapping rules (inter-application)
- Analyze existing permissions/roles per application (intra-application)
- Analyze existing approval processes, and escalation paths

- Re-design processes, roles and responsibilities for Permission Management
- Re-design intra-application and inter-application roles and rules
- Re-design processes, roles and responsibilities for Roles, Rules and Requests Maintenance"
[41]

Med beslutningen om å innføre en IAM-løsning, har virksomheten fått en gyllen mulighet til å gå gjennom sine forretningsprosesser med den hensikt å kartlegge og dokumentere dem. Denne kartleggingen gir organisasjonen muligheten til å gå gjennom prosessene, og der det er mulig designe nye måter å utføre prosessene på. Automatisering er en metode, men før det må prosessene først kartlegges som de faktisk er, og deretter kan man se på alternative måter å gjøre ting på.

4.6 Kartlegging av ståsted

Det er av stor betydning at en organisasjon iverksetter en komplett vurdering av systemene, sjekker kompatibiliteten en IAM-løsningen vil ha med nåværende datasystemer, applikasjoner og videre utvidelser av nettverket.

En kartlegging bør gjennomføres, gjennom intervjuer av nøkkelpersoner fra ledelse, personal og IT, kan status kartlegges i forhold til virksomhetens datainfrastruktur, systemer, sikkerhetsnivå, osv. Kartleggingen kan anses som en intern-kontroll der fagpersoner benyttes for å få en helhetlig og riktig bilde av infrastrukturen, systemene, applikasjonene, prosessene og rollene som finnes ved virksomheten. Gjennom denne kartleggingsfasen kan virksomheten få et helhetlig og detaljert bilde av datasystemet og nettverket (lokalt og eksternt), beskrive programvare som er i bruk, eksisterende sikkerhetstiltak (brannmurer, passordrutiner, fysisk sikring, sikkerhetskopirutiner, etc.), akseptabelt risikonivå, og lovpålagte krav om informasjonssikkerhet.

En fullstendig revisjon kan gi svar på hva organisasjonen har - og hvordan alt fungerer sammen, og skissere statusen på systemene. Denne prosessen vil gjøre det noe enklere å velge de produkter og tjenester som vil kunne dekke virksomhetens egentlige behov.

Virksomheter har flere registre og tjenester som inneholder forkjellige informasjon. Å kartlegge og få oversikt over alle registrene, tjenestene og applikasjonene er en av de store oppgavene ved implementering av en IAM-løsning. En slik kartleggingsprosess kan sørge for at i den planlagte løsningen, informasjonen ikke legges inn og behandles overflødig mange steder.

”*Kartlegging bør være så grundig som mulig. Og bør inkludere alle personregistre og tjenester. Kartleggingen vil avsløre at informasjon blir behandlet på langt flere steder enn antatt.*

Kartlegging skal avdekke

- *Hvor ulike personopplysninger legges inn og oppdateres*
- *Hvor det finnes dupliserte data i flere registre og tjenester*
- *Hvor og hvordan informasjon brukes i forksjellige tjenester*
- *Hvor informasjon flyter(sørge for kontrollert flyt av data)*” **[44]**

Denne prosessen kan hjelpe til å lage en oversikt over hvor, hvordan informasjonen lagres, oppdateres og hvilke tjenester som benytter informasjon fra de forskjellige registrene og tjenestene. Kartleggingen vil også sørge for at informasjon og data som det vil være behov for under innføring av en ny IAM-løsning, gjøres tilgjengelig for prosjektet.

I etterkant kan en rapport skrives, og grunnlaget for omfanget av prosjektet. Rapporten kan inneholde konkrete tiltak og anbefalinger til forbedring av datasystemene og prosessene som eksisterer i organisasjonen. Rapporten bør inneholde de krav som kan stilles til en IAM-løsning, slike som om organisasjonen vokser i størrelse, om det opprettes flere avdelinger, eller eksisterende organisasjonen vokser betraktelig i størrelse.

4.7 Datavask

Et hvert datasett inneholder noen feil, og det er ikke sikkert at feilene blir oppdaget i det hele tatt. Å analysere datasettene og prøve å finne disse feilene er ikke alltid like lett, og noen ganger en umulig oppgave. Korrigering av feil i data og eliminere feilene kan være en tidkrevende og langtekkelig prosess, men kan heller ikke ignoreres og utsettes for alltid.

> *"An identity data quality assessment helps identify areas of concern within the enterprise and provides a roadmap to begin implementing controls that help improve IAM data quality."* **[43]**

Datavask kan hjelpe oss til å fastslå unøyaktige, ufullstendige eller urimelig data og sjekking av dupliserte data, sjekking av foreldreløse data. Blir feilene oppdaget kan man forbedre eller rette de oppdagede feilene.

Behovet for datavask er sentrert rundt å forbedre kvaliteten på informasjon som benyttes av systemer, tjenester og applikasjoner i en organisasjon. De tjenester som benytter informasjonen, skal kunne stole på at informasjonen kommer fra autoritative kilder som har kontrollert informasjonen for feil, inkonsistens og at dataene følger et visst format. Prosessen med å rydde opp i systemene og skissere hvordan data behandles, lagres bør starte så tidlig som mulig i prosjektfasen.

> *"Datavaskingen må inkludere en gjennomgang og kvalitetssjekk av alle data i de ulike systemene:*
>
> *• Fjern utdatert og fyll inn manglende informasjon. Husk også å korrigere feil informasjon*
>
> *• Fjern duplisert informasjon: Ulike registre kan ofte overlappe hverandre. Slike overlapp er uheldige, og må unngås i størst mulig grad."* **[44]**

Kvalitetssjekke for feil og ufullstendig data bør også rydde opp i roller og identiteter i multiple datakilder, fjerne eller deaktivere foreldreløse kontoer eller systemkontoer som ikke er i bruk lenger. Opprydding av eksterne brukerkontoer som ikke lenger er i bruk, eller ikke har en godkjent eier lenger bør enten deaktiveres eller slettes. Datavask er ikke en engangs jobb, men heller en kontinuerlig prosess, som må sjekke dataene for feil, holde dem oppdatert og fjerne dem når det ikke lenger er krav eller behov for det.

4.8 Autoritativ datakilde

Hvem eier dataene er et evig spørsmål som dukker opp ganske ofte i IT sammenheng, men informasjon og data er noe som er dynamisk og alltid i endring. Det endrer seg med tiden, etter hvert som teknologi og systemene videreutvikles eller endres. Og ikke bare med det finnes det samme data som er lagret på mange ulike steder, og ofte har hver av dem helt forskjellige forvaltere og eiere.

> *" If HR isn't centralized or at least standardized, you'll most likely have a difficult--if not impossible--task ahead of you,"* [45]

En IAM-løsning handler om å sikre at riktig person får tilgang til riktig informasjon til rett tid. En organisasjon må bestemme hvilke data virksomheten vil beskytte, hvem som eier dataene,

hvem er den autoritative kilden og hvordan det passer inn i organisasjonens overordnet dataklassifikasjonspolitikk, dette bør komme på plass før implementering av noe IAM-løsning kan starte.

> *"I Feide kaller vi et system hvor data om personer vedlikeholdes, og hvor man finner det som til en hver tid er de korrekte dataene om tilknyttede personer, for en autoritativ datakilde."* ***[44]***

IAM-løsninger krever autoritative kildesystemer, for å kunne bestemme hvilket kildesystem som skal være overordnet andre kilder som behandler samme data. Ved synkronisering eller konflikt vet systemet at det er dette kildesystemet som har det siste og korrekte data.

> *"Dersom organisasjonen har flere kildesystemer, er det svært viktig å vite hvilket kildesystem som er autoritativt. Det vil si hvilken kilde som til enhver tid er primærkilden for et visst dataelement. Autoritative data er de opplysningene som regnes som mest riktige – de som kommer fra den mest pålitelige kilden."****[44]***

Det må defineres autoritative kilder som garanterer at informasjonen er oppdatert og korrekt. Tjenester som henter informasjon kildesystemene, skal være sikre på hvor de alltid kan hente de riktige dataene.

> *"You need an 'authoritative source' of people information, and HR is usually the right place to find that."[45]*

Ofte er HR-databaser en god og fullverdig autoritativ datakilden for brukerdata. Men mange organisasjonene har også databaser som enten er utdaterte eller inneholder manglende informasjon. Noen av databasene mangler informasjon om samarbeidspartnere, kunder og andre ikke-ansatt personell. Utdatert informasjon om organisatoriske tilknytninger, roller, jobbtitler, osv.

> *"Without quality information from an authoritative source, IAM projects cannot be very successful. As a result, an initial effort to establish data integrity in an authoritative source is often required."* ***[43]***

4.9 Katalogtjenester

En katalog kan sammenlignes med en svært strukturert database, hvor Informasjonen er organisert på en bestemt, strukturert måte. Eksempler på slike tjenester er telefonkatalogen som lar brukere lete opp informasjon om abonnenters fast- og mobiltelefonnummer samt adresse.

> *"Formål: Gi tilgang til strukturerte data på en standardisert måte. "[46]*

Katalogtjenester brukes til å lagre informasjon om brukere, maskinvare, systemer og applikasjoner, og gjør deling og administrasjon av informasjon om nettverksressurser effektivt og enkelt.

”Noen eksempler på innhold:

- *personopplysninger/hvite sider*
- *brukerkontoopplysninger*
- *soner i DNS*
- *autentiseringsinformasjon/passord*
- *digitale sertifikater*
- *binære data som f.eks. bilder og dokumenter ”**[46]***

Mange organisasjoner mener de trenger en felles katalog som vil inneholde identiteter over alle brukere og enheter. Men dett er ingen lett oppgave, et problem de fleste organisasjoner møter er det mangfoldet av systemer og applikasjoner som må støttes, med flere ulike brukere som er registrert på forskjellige måter og på ulike steder med ulike autentiseringsmekanismer.

> *” Enterprises today must make critical business information and applications available to a constantly growing and changing universe of users that includes not only internal employees but also external users such as customers, vendors, and other business partners.”[47]*

Virksomheter må vurdere ulike tilnærmingsmetoder for å finne gode løsninger som kan håndtere framtidige endringer. Etablering av katalogtjenester er en kompleks oppgave, men det ligger svært mange fordeler i å bruke tid og ressurser på etableringen.

> *“As an essential element in the overall identity management infrastructure, the directory service adds value by enhancing the availability, security, interoperability, and manageability of key identity data across the organization.”**[48]***

Katalogtjenester øker sikkerheten ved å sikre at informasjonen blir riktig brukt og delt, og at sensitiv informasjon blir beskyttet.

> *” Data protection can also be important for well-intended but poorly designed or written identity-consuming applications. An outage caused by “friendly fire” is no more acceptable than one resulting from an external attack“[48]*

Det tekniske aspektet er viktig ved etablering av en katalogtjeneste, men med å kun fokusere på teknologi kommer man ikke langt. Det andre aspektet som skal ha like fokus er å sikre at informasjonen som ligger i katalogen er korrekt, og i samsvar med pålitelige datakilder. Det er nødvendig å gjennomgå rutinene, for å sikre at fullstendig og konsistent data hentes inn til katalogtjenestene. Når rutinene er gjennomgått, og de nødvendige endringer er avdekket, kan den tekniske delen av etableringen starte.

> *” The directory service must be able to scale from thousands to tens of millions (if not hundreds of millions) of users, process tens of thousands of requests per second for information, and handle hundreds of updates per second**.”** **[48]***

Ofte i virksomheter er det nødvendig med mer enn en katalogtjeneste. Fusjoner, oppkjøp, samarbeid kan innføre to, tre eller flere katalogtjenester i en organisasjon.

4.10 Etablering av IT-policy

En policy beskriver krav til hvordan systemene skal brukes og hvordan informasjon håndteres, distribueres og beskyttes innad i en organisasjon og dets datasystemer.

> *"Hovedformålet med en IT-policy er å lage et konkret regelverk de ansatte kan rette seg etter, og forenkle administrasjonen av nett som vokser seg større og mer kompliserte i takt med virksomhetens vekst."[49]*

Policyene kan bidra til å definere virksomhetens forutsetninger, regler, normer og begrensninger som styrer hvordan teknologi og prosesser skal brukes til å dekke virksomhetens mål.

> *"Når prosesser og policyer er basert på gode fremgangsmåter og er automatiske og konsekvente, kan organisasjoner fokusere flere IT-ressurser på å oppnå strategiske forretningsmål."[50]*

En sikkerhets og tilgangspolicy med utgangspunkt i standarder, forskrifter, og lover bør utarbeides og dokumenteres. Om det allerede eksisterer slike policyer i virksomheten, bør de revideres og oppdateres i forhold til de nye krav og regler som gjelder. Dokumentet bør illustrere virksomhetens tilnærming til administrasjon av informasjonssikkerhet og rettlede i samsvar med krav, lover og forkskrifter.

Policyene bør offentliggjøres og formidles til alle ansatte i en form som er forståelig og relevant for de det gjelder. Policyene vil være bruksveiledninger, og vil skissere prosedyrene som vil holde systemene sikre, og synliggjøre ansvarsforhold som gjelder for datasystemene. En stor fordel ved å etablere sikkerhet og tilgangspolicy er økt sikkerhet på tvers av organisasjonen.

Policyene kan inneholde retningslinjer for ekstern kommunikasjon. Regler for passord, som kan angi at passord må endres på regelmessig basis og at passord må være av et visst minimum lengde og kompleksitet. VPN tilganger som kan kreve et smart kort, biometrisk bekreftelse eller annen form for bekreftelse. Dataforbindelser til høyverdisystemer som krever bruk av forskjellige krypteringsalgoritmer.

Policyene kan regulere hva er det som skal til for å kunne registrere en bruker i virksomhetens datasystemer, og når er skal denne personen registreres i systemene. Skal personen registreres før han har begynt i jobben, skal brukerkontoen aktiveres før første dag på jobb? Og flere andre spørsmål som gjelder ved registrering av en person i virksomhetens datasystemer.

Hva med endringer, hvordan kan de meldes, og hvem har ansvar for å ta imot, og utføre endringene? Eller hva med ansatte som tar permisjon, langferie, langtidssyke, eller de som slutter i bedriften, når og hvordan skal identiteten deres deaktiveres? Hvem har ansvar for slettingen? Hvor lenge etter at en person har sluttet, slettes personopplysningene og dataene? Det må være avklart hvem som gir beskjed om slike hendelser.

For å sikre seg at registrert informasjon er korrekt og oppdatert, bør det innføres rutiner som sjekker og verifiserer all registrert informasjon. Slike rutiner kan beskrives i policyene, og kan endres etter hvert som endringene kommer. En ting er å opprette policyer, men enda viktigere er å forsikre seg om at policyer overholdes, og faktisk blir oppfylt i praksis.

4.10.1Sikkerhetspolicy

En sikkerhetspolicy definerer sikkerheten i en virksomhet og dets system eller et sett av dets systemer.

> *" Security policies are dynamic, too, so identity management solutions should include tools that streamline policy creation and allow administrators to assess the potential impact of policy changes without introducing them to a production environment."*[43]

En sikkerhetspolicy skal være fleksibel og skal være mulig å revideres, endres eller oppdateres etter hvert som det blir behov for det, eller at det er nye krav fra myndighetene som må inn. Sikkerhetspolicyen bør være plattform og maskinvare uavhengig, slik at den ikke endres etter hver utskifting av maskinvare.

4.10.2 Tilgangspolicy

En tilgangspolicy definerer aksessrettigheter for å beskytte viktige data fra tap eller at uautoriserte får tilgang til dataene. Regler for tilgangskontroll og rettigheter bør dokumenteres, og bør beskrive de rettigheter som gjelder for hver bruker, brukergrupper eller andre ressurser. Dokumentasjonen bør også kunne skissere om behandlingen av data følger de eksisterende retningslinjer og rutiner.

4.10.3 Passordspolicy

Enhver organisasjon trenger regler om hvordan passordene kan opprettes, brukes, tilbakestilles, og så videre. Virksomheter må opprette en policy som vil beskytte passordene fra å bli stjålet eller gjettet av utenforstående, men som samtidig ikke overbelaster brukere med vanskelige krav. En automatisert policy-håndterer vil håndheve reglene for passord, for eksempel ved å ikke tillate en bruker til å sette sitt brukernavn som passord, eller lage et passord på mindre enn syv bokstaver, eller bruke vanlige ord og navn.

4.11 Automatisering av prosesser

Manuelle driftsoppgaver i forbindelse med å opprette, endringer, deaktivering eller sletting av brukerkonto og deres tilgangsrettigheter kan medføre at mye av tiden til ressurspersoner blir bundet. Disse manuelle driftsoppgaver utføres gjentatte ganger og kan også føre til mange feil som må rettes i ettertid og noen ganger medfører feilretting med seg nye feil som må rettes opp igjen.

> *"For most companies, the drivers behind an IAM implementation are to automate manual processes, reduce costs and increase security."*[43]

Virksomheter bør gjennomgå sine forretningsprosesser, analysere dem og sjekke mulighetene for å forenkle og automatisere dem. Dette innebærer automatisering av bruker tilordningsprosesser på tvers av flere systemer og plattformer. Det kreves omfattende arbeid, fordi det er i dette trinnet at du definerer konvensjoner for brukernavn, roller og hvilke tilgangsnivåer roller skal ha til de forskjellige systemene. Fordelene med å automatisere tilgangsnivåene er betydelige, fordi når du har definert rollene, slipper du å tilordne rettigheter manuelt til hver ny medarbeider. Du kan bare tilordne dem en rolle eller stilling og programvaren vil håndtere resten.

> *" When considering whether to automate, organizations need to conduct a clear cost-benefit analysis that considers the number of IDs being managed as well as the cost of current identity-related processes."* ***[43]***

Ved hjelp av strukturert metodikk og gode modelleringsverktøy kan man kartlegge de forskjellige prosessene som finnes ved virksomheten, og skissere hvordan de fungerer i dag. hvilke prosesser kan være riktig å fokusere på, hvilke forbedringsområder eller muligheter som finnes og om det går an å optimalisere prosessene, eller at prosessene må lages fra bunnen av for å kunne understøtte overordnede forretningsmål.

Ved hjelp av automatisering kan IT-løsninger gi forbedret effektivisering, optimalisering og kvalitetssikring av prosesser og arbeidsoppgaver som finnes ved virksomheten. Systemene kan optimaliseres og konfigureres i henhold til definerte rutiner, og automatisk sørge for at riktige oppgaver utføres i riktig rekkefølge. Automatisering av store, ressurskrevende og kompliserte oppgaver kan deles opp i mindre oppgaver, og kan utføres systematisk etter hverandre.

> *"Når oppgaver automatiseres, kan feilraten forårsaket av menneskelige inngrep reduseres; når minst 40 prosent av alle feil som skjer i driften skyldes feilkonfigureringer og feilaktige kommandoer, er det klart at automatisering har et stort potensial."* *[51]*

4.12 Integrering

Applikasjonene og systemene i virksomhetens IT-miljø vil før eller senere integreres med IAM-løsningen i bedriften.

> *"An identity management system should integrate seamlessly with existing IT infrastructure,"* *[38]*

Organisasjoner har vanligvis en del programmer som de har utviklet selv, og som er av kritisk type og må inkluderes i den sentraliserte tilordningsprosessen. En del koding måtte til for å lage grensesnitt til disse programmene. Men med noen av IAM-løsningene slipper man å kode noe som helst, alt gjøres via grafiske grensesnitt.

> *"The biggest challenge with most IAM projects is creating a consistent approach toward application integration. To overcome this hurdle, organizations can leverage IAM architectural principles—a prescriptive set of best practices that help establish a standardized approach for application integration"* ***[43]***

Virksomheter bør gjennomgå alle de applikasjonene og systemene de har i sin IT-infrastruktur, og dokumentere de med tanke på hvordan de er konfigurert, hvilke servere de er tilkoblet til, hvor mange brukere som er registrert og hvem som er systemeiere.

4.13 Oppsummering

Implementering av en IAM-løsning kan være vanskelig fordi det krever at organisasjonen endrer spillereglene og arbeidsmetode både for IT og forretningsprosesser.

Det mange gjør feil i er å bevege seg mot IAM uten forståelse for sin IT-infrastruktur, og uten å ha avdekket det faktiske behovet ved virksomheten. Den beste tilnærming er å foreta en fullstendig oversiktsliste, få en inngående kunnskap om eksisterende applikasjoner, modernisering av eldre applikasjoner. Hva har du hjemme, og hva er det du mangler for å forbedre, effektivisere produktiviteten og sikkerheten? Og hva kan du finne ut i markedet, kan det som tilbys dekke behovene virksomheten har? Mange spørsmål skal stilles, og mange av dem skal besvares før en går ut og sjekker markedet.

Vurder med et kritisk blikk på fordelene ved enhver ny teknologi og velg riktig tilnærming til behovene, og tiltakene. Problemene en vil møte i første omgang, vil ikke ha noe å gjøre med teknologien, men med prosesser som ikke er riktig definerte eller som ikke er definert i det hele tatt. Hvis prosjektet ikke er planlagt riktig kan du være nesten sikker på at du får en kostbar katastrofe. Det grunnleggende og mest verdifulle er at man hører på de som allerede har vært bort i det, og henter mest mulig erfaringer, kunnskaper av de som har gjort flere slike prosjekter. Det er viktig å ikke undervurdere kompleksiteten, og de utfordringer man kan møte underveis både når det gjelder teknologiske og organisatoriske.

Et annet viktig punkt er å ikke undervurdere kostnadene som kan dukke opp med innføring av IAM. En kostnadsanalyse må til for å kunne fastslå kostnadene i forhold til den utpekte strategien for implementeringen. Identitet og tilgangskontrollssystemer genererer ikke direkte inntekter, som igjen lager det vanskelig å måle suksessen. Enkle og forklarende figurer bør produseres, figurer kan vise hvordan virksomheten kan spare penger ved implementering av IAM. Og det er viktig å huske at de fleste virksomheter er mer interessert i noe som er forenelig med det eksisterende systemet, enn noe som må bygges fra bunnen av.

Kapittel 5

Fallgruver i et IAM-prosjekt

Dette kapitlet omhandler fallgruver i IAM-prosjekter. Kapitlet skisserer fallgruvene og utfordringene i et prosjekt og sier litt om hvorfor virksomheter feiler i å nå målsetningene i prosjektet.

5.1 Innledning

Virksomheter som planlegger eller er i ferd med å gjennomføre identitets og tilgangskontrollsystemer, får det påvist ganske fort at IAM-prosjekter ikke er som de først antok det. For noen virksomheter er det selvlært erfaring gjennom kostbar investering i feil teknologi, mens andre har lært av hva andre har feilet i og lært noe av det.

Som i mange andre prosjekter, er det også mange fallgruver i et IAM-prosjekt. IAM er vanskelig, komplisert og gjør det meget viktig å kjenne til og være klar over risikoer og utfordringer en kan komme bort i under prosjektperioden, og sannsynligvis også etter at prosjektet er ferdig.

> *" The project team, the suppliers, the customers and other stakeholders can all provide a source of failure, but the most common reasons for project failure are rooted in the project management process itself and the aligning of IT with organizational cultures"[52]*

Virksomheter er organisert på en eller annen måte, og har en struktur og organisering vidt forskjellige fra hverandre. Videre, hver organisasjon har sine tekniske løsninger, forretningsprosesser, prioriteringer og forretningsmål. Det finnes ikke raske og enkle løsninger for å få til en vellykket implementering av et IAM-system. Det finnes heller ingen fast system og struktur på hvordan, og hvilke moduler i et IAM-system bør innføres i en organisasjon.

Snarveier kan ofte føre til utfordringer og problemer som kan undergrave forventninger organisasjonen har til et IAM-system. Hver virksomhet bør vurdere sine egne fremgangsmetoder, og evne til å følge og realisere dem.

5.2 Begrenset forståelse av IAM

IAM er fortsatt i en tidlig fase i Norge, det norske markedet er fortsatt ung i forhold til andre land som USA. Men markedet er i vekst, og både leverandørene og kundene opplever en gradvis økende modenhet. I virksomheter som har etablert bekjentskap med IAM, men ikke kjenner det så godt råder det en forvirring rundt begrepsbruken. Det at mange ikke er så nøye med begrepsbruken, kan blant annet skyldes hva forskjellige leverandører kaller sine moduler/programpakker, eller fordi folk har lite kunnskap på området.

Lite kunnskap om IAM-systemer fører ofte til at omfanget av implementeringsprosjekter undervurderes, og som kan føre til forsinkelser og problemer innad i organisasjonen. Ofte oppfattes IAM-prosjekter som vanlig IT-prosjekter med anskaffelse av programvare og innføring av det i organisasjonens IT-systemer. Prosjektet starter ambisiøst og oppfattes som vidundermiddelet som vil løse mange IT-problemer som organisasjonen har.

Mange prosjekter motbeviser at IAM-prosjekter er 3 månedsprosjekter, og at det bare er å velge seg leverandør og få det implementert i organisasjonen.

> *" IdM implementations can be complex and take years to complete." [53]*

5.3 Fravær av definerte behov

Det å kartlegge nå situasjonen for å kunne legge planer, slik at en vet hvor en ønsker å gå med den nye teknologien er en avgjørende aktivitet i prosjektarbeid.

Mange prosjekter har fått unødvendig avbrudd, fordi man ikke har en god beskrivelse av nåsituasjonen og et godt grunnlag for å bygge systemet på. Virksomheter som ikke har vurdert sine forutsetninger, men i stor grad baserer seg på at det har gått bra for andre organisasjoner vil ikke klare å synliggjøre behovet som finnes ved sin egen organisasjon.

> *"That entails understanding your current posture, known as your "as-is" state, and coming up with a realistic plan for bridging the gap between the two. It also requires that you understand the business drivers behind the IAM initiative, to ensure IT strategy aligns with business strategy."[54]*

Organisasjoner er sammensatte og komplekse og det er derfor viktig at man forstår denne kompleksiteten og kan anvende ulike strategier for å synliggjøre behovet som finnes. Vet man ikke hva nåsituasjonen er, vil gapet mellom ønsket situasjon være for stor og utfordrende for mange. Å forstå organisasjonen både på den tekniske siden og på forretningssiden, krever kunnskap, åpenhet og ydmykhet.

> *"The goal of the definition stage of an IdM project is to document the established, or "as is" status of your overall IdM practices."[53]*

5.4 Mangel på visjon og strategi

De virksomheter som ikke har en klar visjon og en overordnet strategi for IAM-prosjekter vil tidlig eller senere i prosjektperioden komme i en situasjon hvor de ikke vet eller husker hensikten og målet med IAM-systemet. Prosjektet og teknologien vil igjen oppfattes noe større og komplisert en den egentlig er, og involverte i prosjektet mister oversikten og interessen for videre arbeid. Strategien for prosjektet må være godt forankret i ledelsen, og må formidles til alle involverte. Deltakerne må ikke oppfatte strategien som et nødvendig påfunn, men heller en viktig veiviser som de har tro og tillit til.

> *" A vision in writing for the desired end state of your IAM strategy, which is a subset of your overall security and IT strategy."**[54]***

Det er viktig å huske på at oppgaver og prioritering vil endre seg etter hvert som prosjektet utvikles, men visjonen bør bestå og være målet som prosjektgruppen strever etter å nå. I vanskelige tider i prosjektperioden skal visjonen og strategien gi retning og energi til prosjektarbeidet.

5.5 Mangel på målbare suksesskriterier

En av årsakene til at IAM-prosjekter skaper så sterk hodepine under hele prosjektperioden, og som også kan føre til at prosjektet mislykkes er at man ikke fokuserer på de små seierne man har i prosjektet. Vet vi ikke når vi når et viktig stadium i prosjektet og som også kan brukes til å motivere prosjektdeltakerne, kan vi ha det ekstra vrient for å nå de målene som er lenger unna.

> *"A definition of success metrics, so it's clear when you've achieved your IAM goals. These definitions must be measurable and quantifiable."[54]*

Ledelsen er interessert i å få noe igjen for de investeringer som de har gjort, men det er ikke alltid like lett å synliggjøre resultater i slike prosjekter. Noen virksomheter velger å fokusere for mye på de vanskeliste oppgavene, og går for å løse dem først. Det tar ikke lange tiden før de blir utmattet og blir overmannet av oppgavene, og må kaste inn håndkleet. Og suksessen som ledelsen ønsker å innhøste ganske kjapt, kan ha fått en risikabel og usikker fremtid.

> *"Go for the low hanging fruit, without losing sight on the long term goals. Short term success gives IAM more visibility throughout the organization, paving the way for the more difficult aspects of the project."[55]*

Mange utsetter unødvendig lenge gevinstrealiseringen som medfølger innføringen av en IAM-løsning. Å vente for lenge med å ta ut gevinster eller vente lenge med å presentere oppnådde resultater kan ha en demotiverende effekt på alle involverte og som igjen kan fører til usikkerhet og dårlig inne klima i organisasjonen.

5.6 Uklart Eierskap

En av hovedgrunnene til at IAM-prosjekter oppfattes som noe teknisk, er ofte det at det er IT-avdelingen som kommer med ideen om et nytt IAM-system. De bruker da en teknisk beskrivelse for å selge ideen, og ledelsen tar det for gitt at det er et teknisk-prosjekt som vil løses med teknologi. Dermed starter prosjektet som et IT-prosjekt, men som endrer identitet og status etter hvert som kompetansen i organisasjonen øker parallelt med kostnadene. I denne utilfredse perioden oppstår konflikten om eierskap til prosjektet. Forvirringen om hvem som egentlig har eierskap til prosjektet kan ofte føre til forsømmelser av ansvar og dårlig oppfølging med tanke på fremdriften i prosjektet. Utfordringen ligger i forståelsen av hva IAM egentlig er for noe. Uklarheten som kan råde kan ha negative impulser på framdriften, og gjøre det vanskelig å ta kloke og ansvarsfulle beslutninger.

> *" IdM is 80% business process change and 20% technology — don't start with the technology."[53]*

I store og kostelige prosjekter er det alltid flere interessenter som følger med prosjektets fremdrift og ser fram til at deres interesser blir ivaretatt og dekket. Om eierskapet ikke blir klarert tidlig i prosjektet, vil prosjektet havne i en situasjon der beslutninger tas for å unngå konflikter og prøve å gjøre alle interessenter fornøyde.

> *"Gartner advises that the biggest gains from an IdM implementation are achieved when the IdM project is viewed as a business process change project rather than a technology-only project."[53]*

5.7 Dårlig samarbeid innad i organisasjonen

Mangel på teoretiske kunnskaper og mangel på en helhetlig forståelse av prosjektet skaper usikkerhet og utsetter de involverte for ubehagelige situasjoner. IAM er stor og vanskelig, spesielt fordi den berør så stor del av en virksomhet. Det berør og involverer mange med tanke på de endringer og krav som er forbundet med implementering av det i en virksomhet.

> *" IAM touches virtually everyone in an organization, so it's only natural that you need to involve representatives from your end user community as well as IT, executive management and others."[54]*

En annen faktor som kan være tyngende for samarbeidet er den interne motstanden mot endringer av arbeidsoppgaver og rutiner som medfølger ny og ukjent teknologi. Motstanden kan også skyldes angsten og frykten for ikke å lykkes eller at automatiserte prosesser vil etter hvert ta fra dem jobben. Et unødvendig opphold i prosjektet som skyldes dårlig kommunikasjon mellom ledelsen og prosjektgruppen kan få mange uheldige ettervirkninger i stor omfang.

> *" Ultimately, it's the end users who will be most effected by an IAM system, so they should be well-represented as you scope out your project."[54]*

5.8 Manglende lederstøtte

I IAM-prosjekter er ledelsens nærvær og tilgjengelighet en av faktorene som svikter hos mange virksomheter, og omfanget av problemet blir bare større etter hvert som avklaringer og uoverensstemmelser må håndteres og utfordringene blir mer kompliserte.

> *"The research companies and academic institution has focused on the lack of executive support and user involvement as two main difficulties in managing IT projects" [56]*

Om involverte i prosjektet opplever mangel på lederstøtte og i tillegg møter mange utfordringer i prosjektet, kan de bruke opp energien og engasjementet tidligere i prosjektperioden enn antatt. Det er her ledelsen har en sentral rolle i forhold til å motivere og gi inspirasjon, og legge til rett for at alle involverte i prosjektet yter sitt beste hele tiden.

5.9 Utilstrekkelig forståelse av egne forretningsprosesser

Ikke alle virksomheter har enkle og vel dokumenterte rutiner og prosesser. Noen har kompliserte prosesser, andre har igjen avhengige prosesser som venter på hverandre.

Ved innføring av et IAM-system, har virksomheter ønsket om å automatisere flest mulig av sine rutiner og prosesser. En gjennomgåelse på tvers av avdelinger og systemer av prosessene gjør seg gjeldende her. Kartleggingen av prosessene vil være til hjelp ved automatisering, forbedring og endring av rutinene som eksisterer i organisasjonen.

> *" FAILURE TO CONSIDER PROCESS*
>
> *Implementing new IAM technology without addressing underlying processes means you may be doing nothing more than automating a flawed process"[54]*

Om organisasjonene har ingen eller mangelfull forståelse og kunnskap om sine forretningsprosesser, kan det bli tungvindt å ta innsiktsfulle og målbevisste beslutninger i forhold til å automatisere arbeidsoppgavene. Mangelfull forståelse kan medføre komplekse prosesser som skaper forvirring og mer arbeid for brukerne, og kan føre til at de ikke tas i bruk i det hele tatt.

5.10 Oppsummering

Virksomheter investerer store summer og beløp i produkter og prosjekter med det mål å forbedre deres produktivitet og effektivitet, gjennom endringer og effektiviseringer av arbeidsprosesser, arbeidsoppgaver og rutiner. Disse prosjektene skal igjen gjøre det mulig for virksomheter å vokse i størrelse og i kapital ved å få tilgang til nye markeder og nye partnere.

Men virkeligheten viser seg å være noe annet enn det mange først antok, virksomheter har store utfordringer med å fullføre komplekse IT-prosjekter i tide eller innenfor budsjettrammene. Prosjektene mislykkes på en rekke ulike måter, og årsakene varier fra store feil til noe mer generelle feil.

IAM-prosjekter kommer under prosjekter som er av den store og komplekse typen, som berør og påvirker mange i organisasjonen. Virksomheter som har sluttført sine prosjekter har ingen garanti for at de vil dermed klare å hente ut alle fordelene med et system. Mange opplever en stor skuffelse å kun oppnå en begrenset suksess med de systemene som ble anskaffet etter en lang, krevende prosjekttid.

Kapittel 6

Suksessfaktorer i et IAM-prosjekt

I dette kapitlet vil jeg gå nærmere inn på de faktorer som er viktige og avgjørende for et prosjekts livssyklus. Faktorene som nevnes her kan være utslagsgivende for om et prosjekt lykkes eller ender med fiasko.

6.1 Innledning

Det finnes nok av prosjekter som har blitt avsluttet før det i det hele tatt kom i gang, eller andre prosjekter som har blitt kansellert midt i prosjektperioden fordi man ser ikke nytteverdien av å forsette eller at kostnadene blir for store i forhold til gevinstene ved å sluttføre prosjektet. Ikke alle organisasjoner som sluttfører prosjektet klarer å ta i bruk alle de fordelene som ligger i implementeringen av en IAM-løsning.
Det eksisterer ingen kokebok som passer like godt til alle typer virksomheter, og til alle omstendigheter. Det som er riktig og fungerer for andre virksomheter, kan være feil for en annen.

Å bedømme om en virksomhet har oppnådd suksess med sitt IAM-prosjekt, må man finne fram til forhold og variabler som er av betydning for at prosjektet kan oppfattes som vellykket. En fast definisjon på suksess er vanskelig å gi da det er en relativ måling av forskjellige variabler, men ofte har virksomheter en oppfatning av hva suksess er for dem.

> *"Successful projects were completed on time and on budget, with all the features and functions that initially specified" [57]*

Det finnes imidlertid noen kritiske suksessfaktorer som kan gjelde for de fleste virksomheter, og som må ivaretas for å komme i mål med prosjektet.

6.2 Strategisk tilnærming

Å gjennomgå en organisasjon med tanke på å endre og forbedre prosesser, rutiner, og forbedre effektiviteten, produktiviteten og sikkerheten er ikke gjort på noen få måneder. Det er en kontinuerlig prosess som ikke kan begrenses til en kort periode av gangen for å tette sikkerhetshull eller for å avverge katastrofer. Et slikt endringsprosjekt er krevende, og kunnskap om hvordan slike prosesser styres og gjennomføres er viktige og avgjørende for prosjektets utfall. Analyse selskapet Gartner påstår at virksomheter bør utvikle en strategisk og langsiktig plan for innføringen av IAM, men at leveransen av resultatene settes i kortsiktige tidsplaner.

> *"IdM requires a tactical, pragmatic approach to a strategic end" [53]*

Endringsprosesser vil berøre mange og derfor krever full fokus fra ledelsen. Slike prosesser kan ikke alltid planlegges til minste detaljer, og uforutsette situasjoner og utfordringer vil dukke opp. Og det er da ledelsen skal komme på banen og ta viktige beslutninger, og styre prosjektet mot målsetningene og sluttføre det med suksess.

Det er helt avgjørende at det finnes en strategisk tilnærming til prosjektet bestående av en helhetlig forståelse av de behov og prosesser prosjektet skal dekke og understøtte.
Med en strategisk tilnærming vil det ta lenger tid å implementere, men virksomheten vil være mer fleksibel for endringer som kan komme med teknologisk utvikling og bedre rustet til å møte fremtidens utfordringer i forhold nye regulatoriske krav og lover.

6.3 Forarbeid

Mange virksomheter kaster seg ut i prosjekter uten å ha gjort nødvendige analyser av hva deres behov tilsier og hva markedet kan levere, og dermed er ikke alltid like forbredt på de oppgaver og utfrodringer som dukker opp med implementeringen. Å investere store summer på å få produktet til å tilpasses til organisasjonens behov eller bruke masse tid og energi på å få tilpasset prosesser og rutiner til produktet, er metoder som bør hardt unngås for å spare virksomheten for tid og penger. Dårlig og ikke gjennomtenkt forarbeid kan føre til at prosjektet tar lenger tid, gir dårligere datakvalitet og føre med seg ekstra kostnader.

Prosjekter som gjennomføres og betegnes som suksessfulle, kan ofte spores tilbake til startfasen. Nøkkelen ligger i å gjøre et grundig og gjennomtenkt forarbeid, og avverge at prosjektet går i vasken. Erfaring viser at prosjekter som har hatt dårlig tid til forarbeid og mindre involvering av interessenter ofte fører med seg store og noen ganger uhåndterlige utfordringer.

Skal prosjektet gjennomføres med suksess og få varig betydning for virksomheten, må uenigheter og konflikter avdekkes på et tidlig stadium. IAM prosjekter tar tid å gjennomføre, og 2-3 år til implementeringen er ikke uhørt. Det er viktig å være på vakt og ha det klart for seg at, ofte når prosjektet starter med konflikter, har det en lei tendens til å vedvare.

7.4 Målbare kriterier/milepæler

Prosjektet som helhet må ha klare definerte mål av suksess. Så tidlig som mulig må prosjektgruppen finne ut hva som får ledelsen til å mene at prosjektet er vellykket. Etter at gruppen har definert kravene til suksess, må de følges opp for å sikre at de overholdes. Ved å holde fokuset på resultater og feire framskritt, prestasjoner gjort i prosjektet kan gi drivkraft, begeistring og engasjement for prosjektet.

6.5 Trinnvis innføring

Ledelsen er interessert i å se fordeler og gevinster av prosjektet tidlig. Få vil akseptere og ha kjørende prosjekter som strekker seg over måneder uten å vise til oppnådde resultater. Prosjektplaner bør utvikles med tanke på korte og kontinuerlige leveringssykluser, slik at resultater og fordeler som medfølger systemet synliggjøres. Å fremheve og kassere inn de raske gevinstene virksomheten vil oppnå og oppnår, kan spre glede og begeistring hos ledelsen og andre interessenter.

Den beste praksisen er å plukke de lavt hengende fruktene først, altså utføre de oppgaver som leverer raske fordeler. Begynn alltid med de enkle funksjonene og oppgavene først, følg de ekspertenes råd og hør på hva andre virksomheter sier om løsningen og problemene som de har møt underveis i prosjektet. Med denne praksisen kan man bygge videre på det man har lært i de foregående oppgavene, og ta fatt i de ventende oppgavene med ekstra energi og glede.

Oppnådde gode resultater vil vise at det går riktig vei for prosjektet, og muligheten for å lykkes og overleve budsjettkutt vil øke betraktelig. Resultatene vil også gi god grunn for ledelsen å forsette med støtten, slik at neste fase i utrullingen er innen rekkevidde. Levering av resultater i intervaller vil fastholde presset og forventningene til prosjektgruppen. I stedet for å vente på resultater i flere måneder, gjør fasedelt tilnærming mulig å kassere inn investerte verdier tidlig i prosjektet.

6.6 Bruk av eksterne eksperter

Ofte er det slik at prosjektdeltakerne ikke har jobbet med slike oppgaver før. Og folk blir trukket inn i prosjektet på tvers av organisasjonen. Prosjektgruppen vil bestå av folk som kommer fra forskjellige fagområder, og av folk som vanligvis ikke arbeider sammen. Dette kan medføre at de ikke klarer eller har vankeligheter med å dimensjonere oppgavene og klarer å se de potensielle problemene som kan komme. Det er ikke innlysende for mange hva et IAM-system vil bidra med i virksomheten, og hvilke fordeler som vil medfølge. Eksterne konsulenter og leverandører som kan faget vil besvare flere spørsmål, og kan forklare vanskelige saker enkelt, slik at omgivelsene begriper bedre hva som foregår.

Overvei om du vil bruke eksterne konsulenter som har spesialisert seg på IAM med gode referanser. Konsulentene som besitter ferdigheter og kunnskaper på fagområdet kan være nøkkelpersonene som kan forenkle det store og komplekse bildet. Dette kan øke farten for prosjektet og oppdage flere risikoer og utfordringer og raskere gevinstrealisering i prosjektet.

6.7 Ferdigheter

IAM-prosjekter vil trenge folk med forskjellige ferdigheter. Det er ikke alltid like enkelt å finne dyktige folk som kan bidra til prosjektet inert i virksomheten. Og om man har er det ikke dermed sagt at personen kan bare tas inn i prosjektet, ofte er de allerede med i et eller annet prosjekt og ikke har tid til andre oppgaver.

Store IT-prosjekter krever folk med en rekke ulike ferdigheter, og den kontinuerlige utviklingen og endringer innen teknologi gjør det vanskelig å forutse hva slags folk det vil være behov for. IAM-prosjekter er store og komplekse, og det vil være nødvendig med folk som er gode til å planlegge, å ha oversikt og dyktig til å organisere og kommunisere.

”Erfarne folk med tekniske ferdigheter har ikke nødvendigvis disse mulighetene”[58]

6.8 Samarbeid

En vellykket implementering av IAM krever samarbeid mellom applikasjonseire, forretningsledere, IT-personell og sluttbrukere. Samarbeid vil finne sted mellom avdelinger

og ulike nivåer i organisasjonen for å oppnå et felles mål. Samarbeid mellom personer på ulike nivåer og på tvers av organisasjonen viser seg å gi store fordeler i prosjektarbeidet.

For å holde engasjementet oppe hos sluttbrukerne og andre involverte er det viktig at de involveres mest mulig i gjennomgåelser av prosjektplaner, framdriften, milepæler, osv.

6.9 Involvering av interessenter

Involverer man flere folk fra forskjellige avdelinger og nivåer i virksomheten, vil problemene og utfordringene belyses fra ulike perspektiver. Løsningen man kommer fram til vil få bred oppslutning og støtte, som igjen kan gjøre det enklere å sette det ut i livet. Besørger man for å involvere mange medarbeidere på et tidligere stadium, er det enklere å skape mer vilje, engasjement og energi til å få unnagjort oppgavene.

Prosjektgruppen bør tas med på alle viktige beslutninger, og bør få så mye innflytelse som mulig. Med en effektiv og god kommunikasjon kan man lære opp både sluttbrukerne og ledelsen angående fordeler med prosjektet, slik at du sikrer fundamentet du trenger for å realisere den strategiske visjonen.

6.10 Involvering av ledelsen

Organisasjoner har mange ulike typer prosjekter løpende samtidig. Ledelsen vil ha fokuset på de prosjekter som vil koste mest og som har større risiko for å mislykkes. En viktig oppgave for prosjektlederen er å opprettholde ledelsens interesse for prosjektet. Ledelsen må informeres og holdes oppdatert slik at de får de rette forventningene til leveransen.
Ved å holde ledelsen informert om hva som foregår og hvilken rolle de spiller i sammenhengen kan være viktig for den støtten prosjektgruppen forventer av ledelsen.

Ledelsen og prosjektdeltakerne må forstå prosjektet riktig og fullt ut for å kunne styre prosjektet i riktig retning, og kunne ta bevisste beslutninger. For å nå målene, er det høyst nødvendig at ledelsen følger med og har en faglig innsikt og dyktighet for å kunne få prosjektet i boks.

Ledelsen er viktig for at en organisasjon skal klare å tilpasse seg og endre seg i forhold til endringer og bevegelser som skjer i omgivelsene. Av mange prosjektdeltakere blir ledelsens rolle og engasjement sett på som den mest kritiske risikoen forbundet med et prosjekts suksess.

> *"Project manager is the interface between the business and technology sides of the company" [57]*

Vellykkede prosjekter handler ikke bare om å fullføre prosjektet innenfor tiden og budsjettet. Kvalitet, tilfredse sluttbrukere, enklere prosesser og effektiv ressursforvaltning bidrar sterk til prosjektets suksess. Det er katastrofalt for prosjektet å ha ledere som ikke interesser seg for å nå målene og oppnå gode resultater. Lederen har ansvaret for å virkeliggjøre prosjektets mål, og skal overvåke og kontrollere at prosjektets mål nås, og etterkontrollere kvaliteten på det som sluttføres.

6.11 Blottlegging av eksisterende systemer

Virksomheten må starte en prosess som kan kartlegge eksiterende forretnings og sikkerhetsprosesser og studere de avhengigheter som foreligger. Og samt beskrive hva IAM vil spille i virksomhetens infrastruktur, og steg som må tas for å komme til ønsket sted. Kartlegging og utforskning av ulike alternativer på et tidligere stadium, kan gjøre det tydeligere oppfatningen av hva virksomheten faktisk ønsker å oppnå med prosjektet.

En praksis som anbefales av mange, og mange virksomheter har klart fått fordeler av det er å bruke eksterne konsulenter som har kompetanse og kunnskap på fagområdet. Konsulentene kan bidra med å kartlegge eksisterende systemer og prosesser, og tilslutt komme med en anbefaling om hva de bør foreta seg for å oppnå sine mål med et IAM-system. En sluttrapport kan skrives i ettertid med beskrivelser, planlegging og anbefalinger forbundet med en implementering av et IAM-system.

6.12 Kommunikasjon

Implementering av IAM i en organisasjon er en viktig avgjørelse, og må gjennomdiskuteres med alle berørte parter. Utfordringene og problemer i prosjektet må diskuteres i felleskap, slik at problemene blir belyst fra flere perspektiver. Dette forutsetter at alle deltakerne er fortrolig med og har en faglig innsikt i prosjektet. De må ha en felles forståelse som gjør dem i stand til å kommunisere med hverandre.

Denne måten å kommunisere på har vist seg å være meget vellykket i praksis. En vellykket innføring krever samarbeid og kontakt på tvers av grupper og avdelinger i organisasjonen. Om kommunikasjonen ikke fungerer mellom interessegruppene, kan forventninger, krav og ønsker ikke bli innfridd fordi man vet ikke hva den andre prøver å formidle. Det er viktig at kommunikasjons veier er full fremkommelige, og at det er en kort og enkel vei til overordnede slik at beslutninger kan tas raskere.

I IAM-prosjekter er det samarbeid på tvers av avdelinger og de fleste bransjer har et eget fagspråk og begrepsapparat som utenforstående ikke lett skjønner seg på. Når folk skal samarbeide for å løse et problem, må de bli enig om et begrepsapparat som setter folk i stand til å samarbeide om de samme målene. Er ikke kommunikasjonen godt nok, kan det bli vanskelig å løse de foreliggende problemer.

> *” Because complex IT projects often involve large amount of analysis and work, the project teams are busy and the executive management sees no progress. IT project managers do not communicate progress regularly because they believe that progress will not be seen by the executive management” [58]*

Ledelsen og involverte i prosjektet må finne måter å forbedre kommunikasjonen på innad i prosjektgruppen. Og legge til rette for at folk kan møtes og kan ha uformelle samtaler om prosjektet og ting rund det. Uformell kommunikasjon kan bidra til en vennlig og munter stemning og kan gi folk muligheten til å stille dumme spørsmål, og bli kjent med hverandre. Kommunikasjon innad i prosjektgruppen er svært viktig for lagåndet, og kan gjøre det lettere for folk å oppføre seg som et lag og møte utfordringene sammen.

6.13 Klare mål og forventninger

Å sette gode mål for et prosjekt er ikke alltid like enkel oppgave, men det er en avgjørende faktor for et prosjekts livssyklus. Det er ikke nok å definere noen mål, men at de definerte målene er de riktige å arbeide etter for prosjektet. Ved å få frem hensikt og mål tydelig kan føre til at man klarer å skape en riktig motivert prosjektgruppe.

Målet med IAM må være definert, og godt forankret hos ledelsen og andre involverte i prosjektet. Målene må ikke være for ambisiøse, men heller skape et bilde som kan gi realistiske forventninger. For høye og urealistiske forventninger til systemet kan ha vanskeligheter med å tilfredsstille sluttbrukerne, selv om systemet skulle fungere alle tiders.

Virksomhetens forutsetninger må gjennomgås en grundig og nøye vurdering, slik at behovet som eksisterer i organisasjonen synliggjøres mest mulig. Ved hjelp av denne diagnosesettingen kan man sette seg mål som vil dekke behov i organisasjonen.
Ved å involvere flere i prosjektet kan målene vurderes og eventuelt omformuleres av forskjellige medarbeidere med vidt forskjellige synsvinkler.

Et IAM-prosjekt er en endringsprosess, virksomheter må derfor sette opp strategiske mål for hvordan organisasjonen skal ta over seg de endringer som følger med prosjektet. Er målene konkrete, er det en stor fordel for hele prosjektet fordi resultatene er lett målbare. Med målbare resultater kan man sikre en tilfredsstillende produktivitet i prosjektet.

Med uklare mål kan involverte i prosjektet komme opp i en situasjon der de ikke lenger ser sammenhengen mellom arbeidet de utfører og det endelig resultatet. Dette kan føre til skuffelse, maktesløshet og en følelse av at arbeidet de utfører er meningsløst.

6.14 Leverandørvalg

Det er viktig å ta en hel vurdering av alle de leverandører som klarer å levere en løsning som dekker organisasjonens behov og innfrir alle eller meste parten av virksomhetens krav til et IAM-system. Det er viktig å huske på at det er flere variabler å vurdere før man går inn for å kjøpe en løsning. Teknologi kan sette sterke rammer, og kan være en hindrer i å endre forretningsprosesser.

Ved leverandør valg bør virksomheten være sikker på at leverandøren vil være tilgjengelig i lang fremtid, og kan bistå ved utfordringer og problemer som kan dukke opp etter implementeringen.

6.15 Oppfølging

De fleste organisasjoner befinner seg i dag i skiftende omgivelser. Produkter og markeder er i hurtig utvikling, og vi får stadig nye teknologiske løsninger og vinninger.
Organisasjonen må hele tiden være oppmerksom på hva som skjer i omgivelsen og holde seg orientert på nye utgivelser og funksjoner som kan komme med en ny versjon av programvaren. Virksomheter må følge med i den teknologiske utviklingen, og endre og forbedre sine forretningsprosesser i takt med markedet og regulatoriske krav.

Et viktig element i oppfølgingsarbeidet av store prosjekter som IAM som ikke får nok oppmerksomhet, er opplæring av sluttbrukere og IT-personell som har fått endret

arbeidsoppgaver og arbeidsrutiner. Vet ikke brukerne hvordan de skal ta i bruk det nye systemet, er det vanskelig å snakke om en vellykket implementering. Opplæring er ikke et engangs tilfelle, men en kontinuerlig arbeid som må oppfølges og tilpasses til brukernes behov. Innlæring av nye funksjoner og nye arbeidsmetoder som følger med nye produktoppdateringer, er en viktig del av det kontinuerlige oppfølgingsarbeidet.

Jobben er aldri sluttført, det er alltid noen prosesser og prosedyrer som kan forbedres eller endres. For å kunne hente ut alltid det beste i IAM-løsninger krever det at man viser oppmerksomhet og holder seg oppdatert på nye funksjoner og produkter. Et IAM-system må holdes oppdatert, og tilpasses til endringer i forretningsprosesser, IT-miljøet og optimalisering som kan effektivisere prosesser og forbedre sikring av ressursene.

Det er viktig å ha kontinuerlige sjekk av IAM-løsningen for å forstå endringer som kan komme med en ny versjon av produktpakken. Og virksomheten må alltid forsikre seg om at IAM-løsningen alltid leverer det den skal av funksjonalitet, og forsetter med å forbedre prosesser.

6.16 Oppsummering

IAM prosjekter er innviklede og kan være vanskelig for mange, spesielt for ledelsen og andre prosjektdeltagere som kommer fra andre avdelinger og er ikke vant med å jobbe med IT-folk. Alle som involveres i prosjektet bør få muligheten til å tilegne seg nødvendig kunnskap for å kunne bidra til prosjektet. God kommunikasjon i ethvert endringsprosjekt er en av grunnpilarene for å bygge tillit, samarbeid og for å oppnå best mulig resultat.

Det er viktig å stoppe opp og reflekter over hvor langt prosjektet har kommet, og hvor mye som gjenstår igjen. Det er viktig å legge inn tid til å reflektere over prosjektet, få oversikt over situasjonen, og framfor alt vurdere gruppens innsats. Dette kan gi mange nye synspunkter og aha-opplevelser om organisasjonen har prioritert feil.

Kapittel 7

Casestudier

Mye har blitt skrevet og sagt om hvor mange IT-prosjekter som feiler og dermed ikke kommer i mål. Det er mange faktorer som fører til uforutsette utfordringer og problemer i prosjektarbeid. I løpet av de siste årene har svært mange virksomheter, både offentlige og private har hatt omfattende endringsprosjekter med tanke på å forbedre og effektivisere forretningsprosesser og effektivisering av IT-systemene. Endringsprosjekter blir ofte omtalt som ”organisasjonsutvikling”, fordi organisasjonen skal endre måten den gjør ting på, og effektene av prosjektet oppnås som resultat av organisatoriske endringer. Det er virksomheten selv som har ansvar for å utføre og sette endringer ut i livet

Sammenlignet med privat sektor har offentlig sektor en del spesielle utfordringer som gjør livet noe vanskeligere for de involverte. En viktig forskjell mellom offentlig og privat sektor er, mens private bedrifter selv i større eller mindre grad bestemmer at det skal gjennomføres en endring, er offentlige virksomheter underlagt nasjonale og internasjonale direktiver og bestemmelser.

Offentlige organisasjoner er ikke nødvendigvis dårligere på IT-prosjekter enn privat sektor, men mislykkede prosjekter i offentlig sektor får større media oppmerksomhet enn privat sektor. Vi skal ikke gå inn på hvordan prosjektarbeid utføres i de forskjellige sektorene, men de 3 casene som skildres her er offentlige organisasjoner, men mye av det som gjengis av erfaringer vil også være overførbare til privat sektor.

I dette kapittelet presenteres 3 caser som omhandler innføring av IAM-systemer og utfordringer som medfølger innføring av slik teknologi i organisasjonen. Organisasjonene som er med i denne case-studien befinner seg i forskjellige faser av prosjektarbeidet, og ligger litt forskjellige i forhold til hvor langt de har kommet i prosjektet og hvilke moduler de har innført i virksomheten. Casene vil presenteres hver for seg, men å vurdere disse i forhold til hverandre og måle hvem som har lykkes best med prosjektet og hvilke mål og endringer de har nådd vil ikke være rimelig.

7.1 Case 1: Jernbaneverket

Jernbaneverket er statens fagorgan for jernbanevirksomhet i Norge, og underlagt Samferdsels departementet. JBV tilbyr tog selskapene i Norge et sikkert og effektiv trafikksystem. I tillegg har JBV også ansvaret for den daglige styringen av togtrafikken, og ansvaret for å vedlikeholde jernbanenettet, inkludert stasjoner og terminaler.

- Over 800 tog er innom Oslo s i løpet av et døgn.
- Ca. 600 tog passerer Oslo tunnelen hvert døgn.

Jernbaneverket(JBV) forvalter en omfattende teknologi infrastruktur for å støtte transport av et bredt spekter av produkter og tjenester på kryss og tvers av landet. Et bredt utvalg av

systemplattformer, forretningskritiske systemer og applikasjoner inkludert servere og arbeidsstasjoner utgjør JBVs IT-infrastruktur.

I tillegg har JBV en mangfoldig arbeidsstyrke som består av ca. 3000 ansatte, som jobber med svært forskjellig arbeidsoppgaver på mange steder langs det 4000 km lange jernbanenettet. Mangfoldet spenner seg fra arbeidsgrupper som IT, drift, administrasjon, vedlikehold(utstyr, terminaler og infrastrukturen), signalbehandlere, m.m. Alle disse personene har behov for informasjon for å kunne utføre jobben sin, og krever forskjellige tilgangsrettigheter til et variert sett av systemer som omfatter mange forskjellige plattformer.

JBV blir mer og mer en høyteknologisk bedrift, og er på mange områder langt fremme med teknologiske systemer og løsninger. I et stadig mer kompleks IT-miljø, og stadige teknologiske endringer medfølgende protokoller, applikasjoner, lisenser og ikke minst gamle systemer som ikke blir faset ut, gjør administreringen og styringen til en stor belastning for IT-avdelingen og organisasjonen.

7.1.1 Problemområde

Her beskrives situasjonen som gjaldt før hovedprosjektet kom i gang hos JBV. Beskrivelsen som gjengis her, er på ingen måte detaljert og utfyllende. Situasjonen beskrivelse med tanke på å gi leseren en viss forståelse, slik at han/hun kan danne seg et bilde av IT-miljøet og systemene som brukes hos JBV.

Det er en rekke sentrale problemstillinger knyttet til identitets og tilgangskontroll innen JBVs IT-systemer. Administrering av brukeridentiteter og deres tilganger til IT-systemene blir behandlet manuelt ved hjelp av ulike verktøy og prosesser. Administrering av brukernavn, passord, tilganger og annen brukerinformasjonen til et bredt spekter av ansatte, hver med et sett med tilganger er en kostbar, og tidskrevende prosess.

Jernbaneverket
Katalogtjeneste
Active Directory (AD) brukes til autentisering av maskiner og brukere mot Windows-domenet og oppretting av e-postkontoer i Exchange. Gjennom AD administreres også katalogtilganger basert på organisasjons og kostnadstilhørighet.
Brukertyper som eksisterer i systemet er;

- Vanlig brukere, dvs. alle i JVB.
- System administratorer.

Plattform

- Windows
- Linux
- Oracle
- IBM

Applikasjoner

- Agresso(HR)
- MS SQL Database
- Aris, er et fagsystem med begrenset antall brukere
- Banedata, et program som brukes av banearbeidere via PDA for å registrere feil og lese rapporter.
- Banenett, JVBs intranett.
- Citrix, gir tilgang til Microsoft Office applikasjoner, intranett, samt andre styringsapplikasjoner.

En direkte betydning på hvor lønnsom og verdi skapende en medarbeider kan være når vedkommende begynner i JBV, er den tiden det tar å få satt vedkommende opp på alle relevante systemer med riktig tilgang. I enkelte tilfeller kan det ta dager eller uker, før vedkommende er i full produksjon.

I JBV er det systemadministrator som gir og endrer tilganger. Tilgangsrettigheter bestilles ved å sende en e-post til ansvarlige systemadministrator. Den som bestiller må inneha bestillingsrettighet for det systemet det søkes tilgang til.

Ved endringer og deaktiveringer av brukeridentiteter og deres tilganger, meldes det til systemadministrator som har ansvaret for det aktuelle systemet det søkes om endring eller deaktivering av bruker. Men de gangene manuelle prosesser ikke følges, medfører dette sikkerhetstrusler som ikke er så lette å avdekke som det er med datavirus.

Konsekvensene av dette er at brukere som skulle slettes fra systemet forsetter å eksistere med de tilgangene vedkommende har, brukere som skulle fratas sine tilganger fordi de har fått en annen stilling i virksomheten, forsetter å ha de tilgangene. Når uautoriserte har tilganger de ikke skal ha, og autoriserte får ikke de tilgangene de skal ha, vil dette undergraver selskapets navn og ry ved et angrep på systemene.

Noen av systemadministratorene har egne rutiner for å rydde opp i gamle inaktive brukerkontoer i sine systemer en gang i året. Men det er ikke alltid denne jobben huskes, og det er ikke sikkert at alle inaktive brukere blir identifisert, slik at de kan deaktiveres i forhold til prosedyrene.

JBV har i dag 15-20 applikasjoner og systemer som er tiltenkt å integreres med en fremtidig IAM-løsning. Noen av systemene har egne brukerdatabaser, mens andre systemer lar brukerne autentisere seg mot en sentral katalogtjener. Brukerne har forskjellige brukernavn og passord som er spredd på tvers av flere systemer, og som gjør det vanskelig å huske alle. Ved endring av passord i et system, blir ikke denne endringen registrert av de andre systemene, og fører ofte til inkonsistent brukerdata i flere av systemene.

7.1.2 Løsningen

Det er opplagt at løsningen ligger i verktøy som kan automatisere flest mulig av de manuelle oppgavene som tar tid og ressurser. Ved hjelp av automatisering kan svikt i rutinene unngås, og oppgavene kan utføres i forhold til en bestemt tidsplan.

JVB ønsket å gjøre det så enkelt og effektivt som mulig for personell til å få tilgang til den informasjonen de trenger for å gjøre jobben sin. JVB gjennomførte et forprosjekt med den hensikt å kartlegge selskapets nå situasjon, og for å kunne ha noen retningslinjer og anbefalinger når den går til anskaffelse og innføring av et IAM-system. Hensikten med hovedprosjektet er å hel eller delvis automatisere de fleste manuelle prosesser i JVB, som er forbundet med identitets- og tilgangshåndtering. Og i tillegg å integrere passordsynkronisering mellom de fleste systemer, slik at "Singel Sign-On" kan virkeliggjøres.

Forprosjektet avdekket flere tilfeller av dobbellagring av brukerdata, manglende oppfølging av sikkerhetsregler som er ført i JBVs sikkerhetsbok, og innføring av tvungen passordskifte i flere av systemene.

Den raske utviklingen i et stadig mer kompleks IT-miljø, og fleksibiliteten organisasjoner må inneha brer seg i alle IT-miljøer. Med denne utviklingen vil ikke JBV med dagens løsninger klare å takle den betydelig innsatsen som trengs for å videreutvikle systemene og i tillegg administrere brukeridentiteter og deres tilganger på en effektiv og tilfredsstillende måte. JVB erkjenner behovet for å innføre et IAM-system, som vil optimalisere, forenkle og effektivisere arbeidet med identitets og tilgangskontroll i JVB.

7.1.3 Etter innføring av IAM-løsningen

IAM-løsningen vil overta mange av operasjonene forbundet med å håndtere brukerkontoer og deres tilgangsrettigheter til de ulike systemene. Når målet for prosjektet er innen rekkevidde vil man kunne se klare forbedringer med tanke på sikkerheten samtidig som man vil kunne se dramatiske forbedringer i håndteringen av tilgangsrettigheter til ansatte, partnere og kundene. Når IAM er fullstendig innført vil de fleste prosesser bli automatisert, og vil styres gjennom IAM-systemet. Forprosjektet anbefaler å etablere et elektronisk bestillingsskjema som styres av IAM. Endringer i rutiner og prosesser med tanke på bestilling av nye brukere, endringer av tilganger eller det å fjerne en bruker som har sluttet i virksomheten vil sannsynligvis komme raskt.

7.1.4 Ny ansettelse

Når en ny medarbeider blir registrert i systemene av personalavdelingen, vil IAM-systemet kunne se denne oppdateringen og hente ut nødvendige data for å kunne igangsette prosessen for å opprette bruker og gi tilganger til de ulike systemene. IAM-systemet vil deretter opprette brukere i AD, og etablering av tilganger basert på rollene vil settes i gang.

7.1.5 Endringer

IAM-systemet vil motta bestillinger for endringer, og sender en e-post til aktuelle systemadministratorer for godkjenning.

7.1.6 Deaktivering

Når en ansatt slutter i virksomheten, skal dette kunne oppdages av IAM-systemet. Når sluttdato som er registrert i systemet har kommet vil IAM sette i gang prosessen med å slette brukeren og deaktivere alle hans/hennes tilganger til de ulike systemene. Det kan også være aktuelt med at en systemadministrator godkjenner slettingen før det settes i gang.
På sikt ønskes det å integrere samtlige systemer i den fremtidige IAM-løsningen.

7.1.7 Oppnådde mål eller feilet i å nå målene?

Under har vil valgt å legge ved en tabell med noen av de høyst viktige suksessfaktorer som vil gjelde for de fleste virksomheter. Her skisseres de punkter som gjelder for IAM-prosjektet som kjøres hos JBV. Prosjektet er ikke ferdig enda, og derfor gjelder disse faktorene for den delen av prosjektet som er rapportert som utført. Disse faktorene kan være avgjørende karakter for virksomheter som enten planlegger å innføre en IAM-løsning, eller er i ferd med å innføre en løsning. Under ser du tabellen med ulike fargekode for status.

	Bra **Delvis/middels** **Dårlig** **Vet ikke/ikke aktuelt** **Suksessfaktorer** **I hvor stor grad opplevde du at:**	**Status**
1	**organisasjonen hadde en strategisk tilnærming til prosjektet?**	

	JBV har en strategisk tilnærming til IAM-prosjektet. JVB gjennomførte et forprosjekt i samarbeid med et rådgivningsfirma, med den hensikt å starte et endringsprosjekt med en klar mandat til å løse de spesifikke tekniske og organisatoriske utfordringer og oppgaver JBV sto overfor forbundet med identitets og tilgangskontroll.	
2	**organisasjonen hadde det nødvendige forarbeidet til prosjektet, og kartlegging av eksiterende systemer ble utført?**	
	Organisasjonen hadde det nødvendige forarbeidet til prosjektet, som ga mersmak for å forsette. Forprosjektet bidro til modningsprosessen som er høyst viktig for å kunne vite hva som kommer, slik at prosjektet kan planlegges mht utfordringene.	
3	**prosjektet hadde klare mål og realistiske forventninger?**	
	JBV har realistiske forventninger som kan dempe ideen om at IAM er vidundermiddelet som vil løse alle teknologiske problemene JBV. Organisasjonen har definert klare mål for å holde fokuset på hva JBV vil med prosjektet.	
4	**organisasjonen hadde klar definerte variabler for å kunne måle suksess. Organisasjonen hadde en trinnvis innføring av løsningen?**	
	JBV hadde klare definerte variabler for å kunne måle status i forhold til fremdriftsplanen. JBV har valgt en trinnvis innføring av løsningen. Enkle oppgaver blir løst først, deretter de litt vanskeligere, og så videre.	
5	**det var behov for å leie inn eksterne spesialister til prosjektet?**	
	JBV leide inn eksterne eksperter på fagområder der egne ansatte manglet kompetanse.	
6	**prosjektet hadde et klart eierskap, og ansatte som ble berørt av prosjektet var flinke til å samarbeide?**	
	JBV var tidlig ute med å informere om hensikten og konsekvensene av de endringer prosjektet vil medføre for den enkelte. I forprosjektet konstateres det, at det er systemets egentlige brukere som vil jobbe med det nye systemet, og det er de som vil ha en tett dialog med leverandøren. Og ser derfor nødvendigheten med opplæring og motivasjonstiltak som kan frembringe eierskapsfølelse overfor løsningen, og legge til rette for at samarbeid kan skje på tvers av avdelingene.	
7	**sluttbrukerne, berørte og interessenter ble tidlig involvert i prosjektet?**	
	I JBVs forprosjektsrapport settes det fokus på hvor viktig det er å inkludere virksomhetens IT-personell tidlig i planleggingsfasen. Og i tillegg til de som blir direkte berørt av prosjektet, vil det også være andre interne og eksterne brukere som vil berøres og må dermed informeres tidlig i planleggingsfasen.	
8	**ledelsen vær med og støttet prosjektet?**	
	I forprosjektrapporten konstateres det at tiltaket må i første rekke forankres hos ledelsen, og at fokus på endringsledelse er en kritisk suksessfaktor i prosjektet. Dernest er det nødvendig med en god forankring hos ledelsen for å sikre at ledelsen er med hele veien til sluttresultatet leveres.	
9	**kommunikasjon blant deltakerne i prosjektet?**	
	Det var jevnlige møter, som gjorde det lettere med kommunikasjonen innad i prosjektgruppen. Ledelsen var tilstedet under disse møtene, slik at det var kort vei til beslutningene. Ledelsen ble ansvarliggjort tidlig og gevinstrealiseringen ble formidlet på en forståelig måte, slik ble støtte til prosjektet sikret. Informasjonsdelingen og informasjonsmøtene førte til bedre samarbeid innad i	

	organisasjonen og lettere involvering av sluttbrukerne og berørte i prosjektet.	
10	**organisasjonen hadde flere evalueringsrunder før valg av leverandør?**	
	JVB har vurdert flere leverandører med tanke på hvem av dem som kan levere en løsning som kan dekke JBVs behov. Leverandørene er vurdert med hensyn til noen viktige kriterier, slik som kostnader, kompetanse, leveringsvilkår, kompleksitet og arkitektur.	

Tabell 4

7.1.8 Konklusjon

Å ha en definisjon på hva suksess er og være klar over hva det betyr for prosjektet er første skritt for å oppnå målsetningene i prosjektet. Men å avgjøre om et prosjekt er vellykket eller ikke, er ikke så lett som det kan virke. Det er flere perspektiver, variabler og vurderinger på hva det er som gjør at prosjektet kan betraktes som suksessfull. I IAM-prosjekter det ikke så lett å vise fram målbare resultater i tall. Men det går likevel an å vise fram hvor mye virksomheten vil spare av ressurser når selvbetjening av passord, automatisk oppretting, sletting av brukerkontoer innføres i organisasjonen. Og ikke minst forbedring av nettverkssikkerheten, og forbedret brukerstøtte.

Det er mange grunner til at IAM-prosjektet hos JBV kan defineres som vellykket, men før vi nevner dem må vi opplyse om at oppgaven tar for seg den delen av prosjektet som er meldt som ferdig innført. Det er forsatt for tidlig å si om prosjektet har oppnådd målsetningene den hadde ved begynnelsen prosjektet. Så langt ser det ut som prosjektet er innenfor det budsjetterte beløp, og er i rute i henhold til fremdriftsplanen. JBV har en klar oppfatning at de er på riktig vei, og at arbeidet som er gjort så langt tilfredsstiller prosjektets målsetting og hensikt.

JVB en klar visjon om hva de ønsket med det nye systemet, og hva de måtte foreta seg for å komme i mål med systemet. De startet prosjektet med et forprosjekt der de ville kartlegge systemene, og avdekke behovene JVB hadde. De gikk til konsulentmarkedet og hentet inn eksperter på området. Konsulentene foretok seg en behovsanalyse, kartla datasystemene, prosessene og foretok også en vurdering av leverandører som finnes på markedet, og deres løsninger mht krav JBV har til et nytt IAM-system.

JBV hadde noen fordeler framfor mange andre virksomheter som har den omfattende jobben med å dokumentere prosessene som finnes ved virksomheten. Mange av forretningsprosessene som finnes ved JBV var allerede dokumentert og digitaliserte. Dette gjorde at virksomheten kunne fokusere mer på de andre avgjørende områder innefor prosjektet.

Ledelsen var tidlig involvert i prosjektet, og når det var nødvendig korrigerte kurset mot det endelige målet. En viktig suksessfaktor som ble nevnt ofte under intervjuet, var den korte veien til ledelsen. Med denne tette kontakten, ble det også kortere vei til beslutningene, og mye tid ble spart fordi man trengte ikke lange møter for å ta en rask avklarering. En annen faktor som hjalp ledelsen til å forsette med støtten, var leveransen prosjektet hadde av inkrementelle og målbare resultater gjennomgående under hele planleggings- og implementeringsfasen. JBV har erfart at teknologien er den minst kompliserte delen av

prosjektet, mens prosessene, rutinene og organisatoriske endringer er det som krever mye av ressursforbruket.

Fremtids perspektive for prosjektet er at i fase 2 blir 10-15 systemer til som inkluderes i prosjektet, og disse vil bli forsøkt å integreres i løsningen. I fase 3, eller det kan også hende at JBV starter et eget prosjekt for å innføre rollebasert tilgangskontroll. Leverandøren anbefaler at JBV ikke stresser med denne modulen enda, fordi teknologi er snart moden, men forsatt for komplisert. Og det er få virksomheter som har klart å innføre det helt, og det er forsatt lite erfaring og lite best praksis på markedet.

7.2 Case 2: Norges Forskningsråd

Norges forskningsråd er et strategisk organ for norsk forskning og er underlagt Kunnskapsdepartementet. Forskningsrådet ble opprettet i 1993 og er en sammenslåing av 5 ulike forskningsråd.

Rådet er myndighetenes sentrale rådgiver i forskningspolitiske spørsmål og fordeler årlig flere milliarder kroner til forskningsformål. Norges forskningsråd forvalter og fordeler offentlige midler til norsk forskning gjennom mer enn 130 forskningsprogrammer og andre aktiviteter, samt via selvstendige prosjekter og grunnleggende finansieringen til forskningsinstitusjoner.

Rådet midler forskningsprogrammer innen bioteknologi, humaniora, landbruk, marin, medisin/helse, miljø, samfunnsvitenskap, teknologi/ naturvitenskap/matematikk, utvikling/bistand, næringsrettet forskning, grunnforskning, forskning for offentlig sektor, internasjonalisering.

I 2007 forvaltet Forskningsrådet nærmere 6 milliarder kroner og finansierte 5162 prosjekter.

Forskningsrådet er inndelt i fire divisjoner: Vitenskap, store satsinger, innovasjon og administrasjon. De fire divisjonene har til sammen rundt 350 tilsatte.

Norges Forskningsrådet har til enhver tid ett sett med brukersystemer og applikasjoner med varierende alder, plattformer og opphav (standardsystem, spesialsystem utviklet for Forskningsrådet og tilgang til eksterne løsninger via web), som understøtter det arbeidet som utføres hos NFR i ulike forskningsprogrammer. NFR har bygget opp et bredt spekter av plattformer og applikasjoner i sin IT-infrastruktur som et resultat av endringer i politiske og teknologiske krav i omgivelsene. Disse systemene inkluderer alt fra katalogtjenester, økonomiske systemer og egenutviklede applikasjoner, samt nettsteder for ansatte, kunder og partnere.

NFR har mange manuelle prosesser som er komplekse og tidkrevende, og som ofte fører til forsinkelser og stort ressurs forbruk. Arbeidsprosessene som kjøres ved en nyansettelse, og som omfatter autentisering og autorisasjon av brukere i Forskningsrådets IT-systemer kan være tidkrevende. For eksempel så kan det ta lang tid å få satt opp en datamaskin til den nyansatte og til vedkommende har alle rettigheter og tilganger for å kunne utføre sin jobb. Det kan ofte ta mellom en dag og en uke å få PC-en satt opp og til fleste parten av de viktigste rettighetene er på plass. Enda flere dager kan det ta eller i verste fall uker før alt av tilganger og rettigheter er på plass. Og like lang tid, om ikke mer kan det ta for å kunne fjerne folk fra systemene når de går over til en ny stilling, et nytt prosjekt eller at de slutter i jobben.

NFR har mange programmer og systemer kjørende i sitt IT-infrastruktur, men mangler standarder for lagring og administrering av brukerkonto. Mange av systemene jobber uavhengig av hverandre og har derfor egne brukerdatabaser, der informasjon om brukere oppdateres uavhengig av hverandre. De komplikasjoner som følge av å ha flere brukerdatabaser og ingen definerte autoritative kilder genererer mange feil, bidrar til inkonsistente data, høye kostnader, og kompleksiteten øker samt sikkerhetstruslene øker i antall.

Organisasjonen ønsket å forbedre og forenkle prosesser knyttet til ansettelse av nyansatte, endringer som medfølger jobb, prosjekter, permisjoner og oppsigelser, samt innleie av vikarer, eksterne konsulenter mm. Behovet for å sentralisere administrasjon av brukeridentiteter og deres tilganger på tvers av ulike systemer, gjorde seg framtredende for organisasjonen.

På bakgrunn av de åpenbare forbedringsområder ble prosjektet "Identitetshåndtering hos Norges Forskningsråd" satt i gang av IT-avdelingen våren 2005.

7.2.1 Beskrivelse av dagens prosesser og rutiner

Her beskrives situasjonen som gjaldt før hovedprosjektet kom i gang hos NFR. Beskrivelsen som gjengis her, er på ingen måte detaljert og utfyllende. Gjennom intervju og dokumenter jeg har fått tilsendt, forsøkes det å gi en viss forståelse og beskrivelse av dagens prosesser, slik at leseren kan danne seg et bilde av IT-miljøet og systemene som brukes hos NFR.

Beskrivelsen er på et overordnet nivå, og ser på de manuelle prosessenes aktiviteter, arbeidsflyt og andre applikasjoner som brukes ved NFR.

Et forprosjekt ble gjennomført av Forskningsrådets IT-avdeling i slutten av 2005 og en forprosjektrapport ble ferdigstilt i mars 2006. Rapporten gir en beskrivelse av nåsituasjonen, peker på en del sentrale problemstillinger med tanke på vei valg knyttet til IAM og gir noen anbefalinger om videre arbeid med innføringen.

Ansettelsesprosessen gjennomføres ved hjelp av manuelle rutiner som er nært knyttet til personalbevegelsesskjemaet. Dette skjemaet brukes ved alle personalbevegelser for ansatte (tiltredelse, permisjoner, flytting, stillingsendring, fratredelse).

Personalavdelingen registrerer først data om ny medarbeider manuelt fra rekrutteringssystemet som brukes ved NFR inn i Agresso HR. Informasjon som er tilgjengelig påføres, og bevegelsesskjemaet sendes på e-post til neste ledd i prosessen, slik at personalavdelingen, IT-avdelingen og avdelingsledere legger inn nødvendig data, og registrerer vedkommende i de systemene han/hun skal ligge i.

I dagens systemer blir ikke innleide personressurser registrert i Agresso HR. Personalavdelingen har et EXCEL-ark der personressursene som ikke registreres i Agresso blir registrert.

Brukernavn og tilgang til noen av applikasjonene i IT-systemet skjer ved hjelp av personalbevegelsesskjema som sendes til ansvarlig person for applikasjonene. I noen av systemene blir opprettelse av brukere skjer etter en forespørsel fra nærmeste leder:

7.2.2 Registrering av brukerkonto ved tiltredelse

IT-avdelingen mottar personalbevegelsesskjema med info om ny personalressurs. Den nye brukeren opprettes manuelt i Access-basen. Det utføres en sjekkmetode for å avverge at et brukernavn som eksisterer i systemene registreres enda en gang. Om personnavnet ikke eksisterer blir følgende informasjon om bruker registrert: Brukernavn/Id, navn (fornavn og etternavn), romnummer, telefonnummer og datamaskinnummer.

Ved hjelp av Novell ConsoleOne opprettes bruker deretter i eDir. Brukernavn og et passord registreres etter gjeldende regler. Ved første gangs pålogging må brukeren endre passordet.
Deretter brukes et templat til å opprette hjemmeområde og e-postkontoer til personalressursen. For brukere med tidsbegrenset ansettelse (engasjement, innleide og lignende), registreres også utløpsdato.

Deretter blir denne informasjonen som er registrert, synkronisert automatisk til Active Directory (AD) innen 15 minutter.

7.2.3 Avregistrering av brukerkonto ved fratredelse

Personalbevegelsesskjema med info om opphør av personalressurs oversendes til IT-avdelingen. Ved opphør av innleide vikarer eller konsulenter oversendes det ingen melding, men etter passert utløpsdato vil ikke deres tilganger fungere lenger.

Brukerkonto blir deaktivert, og flyttes manuelt over til mappen Sluttet. Det skjer ingenting med brukerkonto før det har gått 3 måneder. Dette er et krav fra myndighetene, og har hjemmel i arkivloven. Om brukeren skulle komme tilbake innen de 3 månedene, kan brukerkontoen gjenåpnes igjen, men brukerens overordnede eller personalavdeling må bekrefte dette. Etter de 3 månedene slettes all informasjon om brukeren fra AD og eDir.

7.2.4 Endring av brukerkonto ved endringer

Personalbevegelsesskjema med info om endringer av personalressurs oversendes til IT-avdelingen. Blir endringer registrert i AD, blir denne informasjonen synkronisert automatisk til eDir. Endringene legges også inn i Access-databasen.

NFR
Active Directory
Forklaring: Katalogtjeneste for Windows-miljøet med brukere, arbeidsstasjoner og servere)

eDir
Forklaring: Katalogtjeneste for Novell-miljøet med brukere, arbeidsstasjoner, applikasjoner og servere). LDAP-server for portalsystemene (eSak og ePort)

PC-er
Stasjonære, bærbare. Dell, Fujitsu Siemens og Compaq/HP

Operativtsystem
HP-UX, Linux, Windows 2000/2003, Novell Netware 6.5

Database
Server 2000 / 2005 og Sybase

E-postsystem
Exchange 2003

Applikasjoner

- Agresso(HR)
- Netwise: Støttesystem for sentralbordet.
- Content Server: Publiseringssystem.
- eAdmin: Søknadsbehandlingssystem.
- C-Cure: Nøkkelkort – og Adgangskontrollsystem.
- Fast: Søke- og indekseringssystem.

7.2.5 Effektmål/Gevinstmål med prosjektet

NFR ønsker å automatisere og forenkle manuelle prosesser i den grad det er mulig med mer strukturerte automatiserte prosesser rundt oppretting, endring og fjerning av brukerkontoer.

Overordnet mål for å innføre en ny identitets og tilgangskontrollssystem er å styrke organisasjonens IT-systemer med tanke på sikkerhet, effektivitet og en effektiv håndtering av brukeridentiteter på tvers av alle systemer og plattformer.

En tiltenkt fremtidig IAM-løsning i NFR forventes å kunne gi langt bedre oversikt over alle brukerne både fast ansatte og innleide som er registrert i forskningsrådets datasystemer. For de IT-systemer som vil integreres i IAM-løsningen vil det kunne bli mindre manuelt arbeid og vesentlig tid og kostnadsbesparelser og gi bedret kvalitet på registrerte data.

Personalavdelingen vil kunne spare tid i forhold til dagens rutiner med utsendelse av skjema om personalbevegelse ved innregistrering av nye brukere og senere vedlikehold endringer og sletting av slike opplysninger.

Kravene til datakvalitet er økende, betydningen av god datakvalitet i grunnsystemene er viktig for alle systemer og i alle ledd av organisasjonen som gjør nytte av disse dataene. Med færre brukerbaser å vedlikeholde oppnår du bedre kvalitet og konsistente brukerdata på tvers av systemene i organisasjonen. Ved å sentralisere hvor brukerdata registreres og holdes oppdatert vil man kunne klare å sikre at der data opprettes første gangen og formidles til andre systemer er riktig, slik at andre systemer kan ha tillit til denne datakilden

IAM-løsningen vil videre kunne gi økt effektivitet for IT-brukerne selv gjennom raskere opprettelse som bruker eller ved senere endringer av tilgangsrettigheter til IT-system. En vesentlig utbytte som vil kunne oppnås med løsningen, er å frigjøre viktig tid på IT-avdelingen og redusere trykket på brukersupporten som følge av at registrering av brukere, endringer og sletting av dette og brukerrettigheter til nettverksressursene, samt passord som glemmes, osv. integreres i IAM-løsningen.

Antall brukernavn og passord som en gjennomsnittlig IT-bruker må huske er 10-15 ulike til forskjellige applikasjoner. IT-brukeren må ofte gjennom like mange påloggінger i løpet av en arbeidsdag for å få utført jobben sin. I tiltenkt IAM-løsning kan brukernavn og passord synkroniseres på tvers av ulike systemer og applikasjoner i NFR, slik at det holder med ett brukernavn og en enkelt pålogging. Antall brukernavn og passord som brukeren må huske kan reduseres, og sluttbrukerne kan huske brukernavn og passord uten å måtte skrive det ned.

NFR ønsker å iverksette ”Single Sign-On” (SSO) mot alle IT-systemer der dette er mulig. Brukeren blir autentisert mot SSO-systemet ved pålogging på datamaskinen, og autentisering til de andre systemene trenger ikke brukeren å skrive inn brukernavn og passord. Innføring av Single Sign-On vil gjøre det enda mer nødvendig med sikre løsninger for autentisering. NFR vil løpende vurdere hvordan autentiseringen best kan ivareta organisasjonens informasjon sikker.

7.2.6 Ønsket situasjon etter innføringen

En innføring av en IAM-løsning er ikke gjort på noen få uker, heller måneder. Som det er blitt nevnt tidligere, er innføring av IAM-system et strategisk, langsiktig og kontinuerlig arbeid. NFR har valgt å dele prosjektet i flere faser, der hver fase har målsetninger som prosjektet

skal etterstrebe å nå. Fasene kan ha som mål å implementere en eller flere moduler av en IAM-løsning. Jeg har tatt for meg de modulene som vil automatisere og i noen tilfeller endre de manuelle prosessene som har med å opprette en brukerkonto, endringer som kan komme etter opprettelsen av kontoen og stenge alle tilgangene og deaktivere brukerkontoen når vedkommende slutter i bedriften.

Forskningsrådet ønsker seg en ”policy uavhengig” løsningen, som kan integrere i løsningen de endringer som kan komme med tanke på hvem som kan registreres i IT-systemene, og hva slags rolle de kan få i systemene.

All persondata som registreres skal ha et autoritativt kildesystem for grunnleggende persondata. Automatisk generering og tilordning av brukernavn som unik identifiserende attributt. Innleid personressurs, dvs. vikar eller ekstern konsulent, skal kunne innregistreres i Agresso HR-modul på lik linje med ansatte.

Oppretting av brukerkontoer både for ansatte og innleide, vil først skje i Agresso HR og deretter i Active Directory(AD) og i andre systemer.

Ved registrering av en ny personressurser, skal Agresso HR automatisk generere Brukernavn for vedkommende. På grunnlag av den nye identitet som er opprettet i Agresso HR skal AD automatisk oppdateres med samme identitet. Hvis det brukernavnet som lages for den nye personressursen finnes i AD fra før, må det finnes prosedyrer som kan håndtere slike situasjoner.

Brukerkontoen som blir opprettet i Agresso HR og AD skal det automatisk lages et startpassord i samsvar med reglene som gjelder for passordvalg i Forskningsrådet. Det genererte passordet skal lagres i AD, og ved første gangs pålogging skal brukeren tvinges til å endre passordet.

Etter at Personressurs er opprettet med sin unike brukernavn skal vedkommende bruker av IT-systemer i Forskningsrådet også automatisk få en standard sett av tilgangsrettigheter til filer/mapper og IT-systemer. Slike filer/mapper og IT-systemer kan baseres på gruppe/rolle som følger av stillingstype, eller prosjekter som vedkommende er med. Det skal være mulig å endre og oppdatere med hensyn til de regler som gjelder for NFR. En e-post sendes automatisk om den nye personressursen er som opprettet og etablert til et utvalg forhåndsdefinerte e-postadresser.

En nyansatt som registreres i IT-systemet skal ved tiltredelse automatisk knyttes til den gruppe/rolle som følger av stillingstype og organisasjonstilhørighet eller en kombinasjon av disse. Brukeren vil da automatisk få tilgang til de mapper/filer som tilhører den aktuelle organisasjonsenheten.

Ved endringer i stillingstype eller organisasjonstilhørighet skal endringene automatisk iverksettes med tanke på de grupper/roller som følger av stillingstype og organisasjonstilhørighet. Når en ansatt slutter i NFR skal vedkommende fra og med 1. dag etter fratredelse automatisk miste sitt medlemskap i grupper/roller som følger av stillingstype og organisasjonstilhørighet.

7.2.7 Endringer og oppdateringer av brukerkonto

Det skal være mulig å endre data knyttet til personressurs med minimale behov for manuelle prosesser, og deretter spre det automatisk og umiddelbart til de systemer som trenger denne informasjonen. Det er viktig at løsningen ivaretar prinsippet om oppretting og synkronisering av persondata fra autoritativ kilde. Ved at hvert dataelement endres og oppdateres ett og bare ett sted og endringer spres automatisk oppnår virksomheten en vesentlig besparelser av tid og kostnader.

Ved endringer er det mange i Forskningsrådet som skal ha en melding om de endringer som er utført. Løsningen skal automatisk kunne generere og sende slike meldinger via e-post til forhåndsdefinerte e-postadresser.

Endringer som gjøres i ett IT-system som fungerer som autoritativ kilde for passord, skal dette passordet automatisk synkroniseres mot et spesifisert sett av andre IT-systemer. Ved passordendringer kan virksomheten oppnå bedre sikkerhet, forenkling, og en vesentlig besparelser av tid og kostnader.

Brukernavnet til en ansatt som slutter i Forskningsrådet blir ikke slettet, men oppbevares, slik at samme brukernavn ikke kan benyttes av andre ved nye tiltredelser eller engasjementer i fremtiden.

7.2.8 Portal for tilgangsadministrasjon

NFR ønsker å effektivisere arbeidsprosessene knyttet til tilgangsadministrasjon i størst mulig grad gjennom arbeidsflyt og selvbetjening.

Forespørsel om tilgang til et angitt IT-system med spesifikasjon av ønskede tilgangs-rettigheter eller ved korreksjoner i tilgangsrettigheter, skal brukeren sende forespørselen til nærmeste leder. En forespørsel kan gjøres via e-post til nærmeste leder, med en beskrivelse av det aktuelle angitt brukersystemet. En leder mottar denne meldingen om ønsket tilgang til et angitt IT-system med spesifikasjon av ønskede tilgangsrettigheter. Lederen kan godkjenne eller nekte behovet, ved godkjennelse sendes en e-post med godkjennelsen videre til systemeier for angitt IT-system.

Portalen for tilgangsadministrasjon skal kunne gi oversikt over alle brukere og deres tilgangsrettigheter for det enkelte IT-system som er inkludert i IAM-løsningen.
Det er også ønskelig å ta vare på historikk for endringer i brukerens tilgangsrettigheter til IT-system. Logging av hendelser utføres mht sikkerhet og sporbarhet, slik at dato for endring, brukernavn for vedkommende, hva slags tilgangsrettighet som er gitt og info om hvem som utførte endringen kan dokumenteres.

Løsningen skal gi standardrapport med oversikt over navngitte brukere og de tilgangsrettigheter som hver enkelt har til IT-systemene. IAM-løsningen skal gi standardrapport med oversikt over endringer i brukeres tilgangsrettigheter (historikk), herunder hvem som har gitt ulike brukere tilgang til hvilke IT-system og når (sporbarhet).

7.2.7 Oppnådde mål eller feilet i å nå målene?

Under har vil valgt å legge ved en tabell med noen av de høyst viktige suksessfaktorer som kan gjelde for de fleste virksomheter. Under ser du tabellen med de ulike fargekode forskjellige status typer.

	Bra Delvis/middels Dårlig Vet ikke/ikke aktuelt **Suksessfaktorer** **I hvor stor grad opplevde du at:**	**Status**
1	**organisasjonen hadde en strategisk tilnærming til prosjektet?** NFR gjennomførte et forprosjekt i samarbeid med et rådgivningsfirma, på bakgrunn av de åpenbare forbedringsområder knyttet til nyansettelse, endringer i tilsettingsforhold ble "Identitetshåndtering hos Norges Forskningsråd" initiert høsten 2005. Prosjektet vil ha nyttegevinster både på kort og lang sikt.	
2	**organisasjonen hadde det nødvendige forarbeidet til prosjektet, og kartlegging av eksiterende systemer ble utført?** Et forprosjekt som var ferdig v06, og et omfattende arbeid i fm med kravspesifikasjonen som ble ferdig vår 2007. Det siste runden kartla alle mulige IT-systemer som var aktuelle og skapte stor bevissthet i organisasjonen og var tilfredsstillende, selv om detaljprosessarbeidet ikke ble helt ferdigstilt.	
3	**prosjektet hadde klare mål og realistiske forventninger?** NFR har klare mål med prosjektet, og vet hvor de er på vei mot. Når det gjelder forventninger, er NFR blitt noe usikker på ambisjonene de har til prosjektet. Uventete utfordringer har satt en demper på deres forventninger, de er blitt mer forsiktige og realistiske til prosjektet.	
4	**organisasjonen hadde klar definerte variabler for å kunne måle suksess. Organisasjonen hadde en trinnvis innføring av løsningen?** NFR har valgt en trinnvis innføring av løsningen, og har satt opp milepæler for alle fasene i prosjektet.	
5	**det var behov for å leie inn eksterne spesialister til prosjektet?** Der det var mangel på kompetanse internt, ble spesialister hentet inn.	
6	**prosjektet hadde et klart eierskap, og ansatte som ble berørt av prosjektet var flinke til å samarbeide?** Prosjektorganisasjonen ble etablert tidlig i prosjektet, og samarbeidet fungerte utmerket. Men etter at prosjektet stoppet opp og det ikke skjedde noe videre, ble det vanskeligere å motivere folk.	
7	**sluttbrukerne, berørte og interessenter ble tidlig involvert i prosjektet?** Alle berørte og interessenter ble tidlig inkludert i prosjektet, men p.g.a. forsinkelsen som oppstod skjedde involveringen litt for tidlig.	
8	**ledelsen vær med og støttet prosjektet?** Ledelsen var med og støttet prosjektet, men i ettertid ser man at en bedre sammensetning av styregruppe og referansegruppe burde vært bedre planlagt.	

9	**kommunikasjon blant deltakerne i prosjektet?**	
	Det meste var lagt til rette for å ha en god kommunikasjon I prosjektet.	
10	**organisasjonen hadde flere evalueringsrunder før valg av leverandør?**	
	Leverandørene er vurdert med hensyn til viktige kriterier, slik som kostnader, kompetanse, leveringsvilkår, kompleksitet og arkitektur.	

Tabell 5

7.2.8 Konklusjon

En god start og godt forarbeid er trolig den viktigste faktoren for å komme vellykket i mål, men det utsagnet stemmer ikke alltid i kompliserte prosjekter som IAM. Teknologien og markedet er i stadige endringer, og det kan inntreffe situasjoner en ikke kunne forutse i starten. Ikke på grunn av dårlig planlegging, men fordi det var ikke mulig å forutse inntruffet situasjon. IAM-prosjekter er høyrisiko prosjekter, og om man virkelig er uheldig slik at leverandøren går konkurs eller mister nøkkelpersoner er det nesten sikkert at prosjektet vil få et uheldig opphold.

Mange virksomheter er flinke til å beskytte sine rettigheter og inngår grundige kontrakter med leverandører og partnere. De definerer ansvar og premisser for gjennomføringen av prosjektet, og ansvarliggjør den som vil ha ansvaret for ulike risikoer/situasjoner som kan oppstå under prosjektet. Men alle prosjekter innebærer en viss risiko, og det er ikke mulig å sikre seg 100 prosent mot alle typer problemer som kan oppstå. Selv om prosjektgruppen har vurdert risikoen og tatt de nødvendige tiltak, kan det likevel oppstå uforutsette utfordringer som kan skape store og omfattende problemer for leverandøren og spesielt for kunden.

Virksomheter som initierer IAM-prosjekter er i stor grad avhengig av at leverandøren har kompetansen på plass, og har tatt høyde for risikoer mht. utfordringer som kan komme med kompleksiteten som store prosjekter innehar. Organisasjoner kan gjøre alt riktig og ta alle hensyn og tiltak for å sikre framskritt i prosjektarbeidet, men kan likevel feile i å følge planene og dermed feile i å innføre løsninger.

Etter at et forprosjekt ble gjennomført på oppdrag fra Forskningsrådets IT-avdeling, lå det ferdig en forprosjektrapport ferdig mars 2006. NFR utførte kravspesifikasjonsarbeidet som ble sendt til leverandør slik at de kunne gi tilbud. Etter forhandlinger ble det underskrevet kontrakt (Statens standardavtale – Tilpasningsavtalen). Det ble skrevet et avrop som omhandlet Fase 1 med opsjon på implementasjon av flere faser.

Så langt gikk prosjektet etter planen, og det så ut som NFR hadde gjort et godt forarbeid til prosjektet. Forprosjektrapporten innholder god beskrivelser av prosesser som har med oppretting, endring og sletting av brukerkontoer. Videre inneholder den en detaljert oversikt over alle programvarer som brukes ved NFR, og beskrivelser av passordpolicy, retningslinjer for brukernavn, beskrivelse av IT-systemer, oversikt over dataelementer med autoritative kilder, osv. Brukergruppene ble delt og intervjuet for å få et riktig og detaljert prosessevaluering. NFR brukte halvt år på å kartlegge prosessene, men i ettertid ser de at de burde ha brukt enda mer tid på dokumentasjonen. Dette fordi nesten alle prosesser har unntak,

og hvert unntak har et særskilt håndteringsmetode. Og det er ikke sikkert at slike unntak lar seg automatiseres, og må derfor stå utenom IAM-løsningen.

Prosjektet startet tidlig med å involvere interessenter i prosjektet, og fikk også opprettet prosjektorganisasjon med styregruppe, referansegruppe, arbeidsgruppe. Men det de opplevde som vanskelig var å ha med ikke-tekniske folk med i styregruppen, de snakket ikke et teknisk språk og hadde problemer med å oppfatte den tekniske diskusjonen. Det NFR ser i ettertid er at det er greit å ha ikke-tekniske folk i referansegruppen, men om de ikke er tekniske kan det være problematisk å ha dem i styregruppen. Det å involvere flest mulig er greit, men hva om prosjektet får et nødvendig opphold? Det kan bli vankelig å holde folk motivasjon og interesse oppe når det ikke skjer noe videre i prosjektet på lenge. Folk vil kanskje etterspørre 2-3 ganger om hvorfor det ikke skjer noe i prosjektet. Men når det ikke kommer noe nytt vil de gå lei og vil avskrive seg alt ansvar som skulle ligge på deres skulder.
NFR hadde gjort mye av leksa og hadde definert hva forbedringer og endringer de ønsket med IAM-løsningen. De hadde valgt ut systemer som skulle tidlig integreres i IAM-løsningen, og disse er systemer som brukes av mange og omfatter flere. For å få støtte fra personellavdelingen, og skaffe noen støttespillere der, ble det valgt å automatisere utsending av e-post til bestemte e-postadresser ved nyansettelse, endring og avgang. Content manager, som er publiseringsverktøyet ble valgt som testapplikasjon. Men alle applikasjoner kan ikke integreres, fordi de ikke er designet for det eller det krever masse ressurser for å tilpasse det til IAM-løsningen. NFR møtte utfordringer med å tilpasse og utvikle publiseringsverktøyet sikkelig.

Prosjektet kom så langt at arbeid på noen av prosjektområdene startet, men NFR hadde en større utfordring i vente. Men det er ikke alltid at planene slår til, 2 nøkkelpersoner sluttet hos leverandør og trakk seg fra prosjektet. Dette gjorde prosjektet og innføringsprosessen sårbar, fordi mye av kunnskapen og erfaringen lå hos disse personene. Leverandøren og underleverandøren mistet viktig kompetanse, og hadde ikke flere kompetente folk her i Norge. Det var mangel på teknologi kompetanse, og ferdigheter i å takle uforutsette problemer som kunne drive prosjektet videre. Kunnskapsoverføringen hadde også vært et problem. En lang prosess med opplæring, kompetanse oppbygging og rekruttering av fagfolk ble satt i gang.

En evaluering av prosjektet, og i gangsetting av et testmiljø nærmer seg. Resultatet og gevinstrealisering av denne perioden vil være avgjørende faktorer for om prosjektet klarer å komme på riktig kurs, og klarer å levere resultater igjen.

Ikke alt går som planlagt alltid, men det som er viktig, er at organisasjonen har en plan for hvordan uforutsette situasjoner, endringer og kriser kan håndteres og løses.

7.3 Case 3: Utenriksdepartementet

Norsk utenrikstjeneste består av Utenriksdepartementet (UD) og 104 utenriksstasjoner. Hovedoppgavene er å ivareta og fremme norske interesser i forholdet til utlandet, inkludert interesser Norge har felles med andre land, samt å gi bistand til norske borgere i utlandet. Det Kgl. Utenriksdepartement og de 104 utenriksstasjonene, som inkluderer ambassader, representasjoner, delegasjoner og generalkonsulater, utgjør til sammen utenrikstjenesten. Utenrikstjenesten omfatter om lag 100 stasjoner med utsendt personell fra Norge. Med åtte avdelinger er UD det personellmessig største departement i norsk statsadministrasjon.

Antall ansatte
Om lag 1.450, hvorav cirka halvparten er utsendte tjenestemenn ved norske utenriksstasjoner. I tillegg kommer om lag 800 lokalansatte ved stasjonene.

I kunnskapssamfunnet er medarbeiderne den viktigste ressursen, og deres produktivitet har direkte innvirkning på bedriftens ytelse, og evne til å tilpasse seg endringer i markedet og omgivelsene. Tiden det tar å få en nyansatt satt på alle relevante systemer har en direkte innvirkning på hvor produktiv og effektiv en medarbeider kan være når vedkommende begynner i jobben. I noen tilfeller kan denne prosessen ta flere timer eller dager, ut i fra de ulike godkjenningskrav som må dekkes. Tiden det tar å opprette deres brukerkontoer med riktige tilganger og applikasjoner raskt og presist er avgjørende for hvor fort nyansatte får gjort det de skal.

UD opplever det som problematisk at det tar så langt tid(3-4 uker) til ansatte er operative ved nyansettelse, flytting og endringer. UD ønsker å forbedre og forenkle prosessene som gjelder ved nyansettelse, og endringer som medfølger flyttinger og endringer i ansettelsesforhold og arbeidssituasjoner.

I april 2008 innhentet UD til Identitets og tilgangskontrollprosjektet ekstern hjelp for å bistå med innkjøpsprosessen, forankring og bygging av prosjektorganisasjonen. Prosjektets overordnede mål er en effektiv og sikker tilgangskontroll til alle virksomhetskritiske applikasjoner og ressurser i UD. Dette betyr også at alle fagapplikasjoner skal benytte en felles kilde for basis personopplysninger. Prosjektet har som mål å automatisere prosesser for oppretting, vedlikehold og administrasjon av brukerkonto og deres tilganger. Prosjektet vil forbedre de prosessene som bidrar til at det tar lang tid å få nyansatte aktive, og registrere de endringer som medfølger flyttinger intern og avslutning av arbeidsforhold. Prosjektet vil bidra til å sikre at alle brukere, interne og eksterne, får tilgang kun til de systemene som er nødvendig basert på deres rolle og funksjon i UD. Med innføring av en IAM-løsning vil ansatte føle at de blir bedre ivaretatt og tiden det tar til de har de riktige tilgangene til de riktige systemene reduseres betydelig.

7.3.1 Beskrivelse av dagens situasjon

Beskrivelsen er på et overordnet nivå, og ser på de manuelle prosessenes aktiviteter, arbeidsflyt og andre applikasjoner som brukes ved UD.

Departementet med alle sine ulike brukere og ulike tilgangsnivå, har mange systemer som håndterer persondata og styrer brukernes tilganger til de mange forksjellige systemene som eksisterer i departementets IT-infrastruktur.

Mange av dagens prosesser som har med oppretting, endring og sletting av persondata gjøres manuelt av respektive systemansvarlige. Dagens løsning er basert på SAP-HR og blir driftet av Senter for statlig økonomistyring(SSØ). Data registreres av SSØ, og blir deretter overført til UD. SSØ har laget ferdigdefinerte script som generer flatfil som brukes til å spre dataene manuelt til de ulike systemene som brukes ved UD. Datasynkroniseringsprosessen legger ikke data inn i HR-systemet.

I dagens IT-systemer hos UD er det svært vanskelig å gjøre rede for hvem som har tilgang til hva, og hvor mange av de brukerkontoene som eksisterer i systemet er foreldreløse. Et problemområde er å følge opp og ha fullstendig kontroll over alle brukere ved IT-systemene til enhver tid. Det eksisterer ingen automatisert prosesser som fjerner alle tilgangene til en ansatt som slutter i jobben. Det er ingen garanti for at de manuelle prosessene som skal deaktivere brukerkonto og tilganger blir kjørt, og dermed blir ikke vedkommendes brukerkonto fjernet fra systemene, og utstyr som gir vedkommende ekstern tilgang tas heller ikke inn.

Denne situasjonen medfører en stor risiko for misbruk og uautorisert bruk i departementets IT-systemer, og kan medføre til uønskede hendelser som ikke er så lett å oppdage.

7.3.2 Effektmål/gevinstmål med prosjektet

Effektmål for prosjektet beskriver hva UD vil oppnå med å kjøre IAM-prosjektet. Effektmålene er tett knyttet til organisasjonens strategiske planer om å forbedre IT-sikkerheten, oppnå større fleksibilitet og endringsevne som kan følge dynamikken i omgivelsene, sikrere etterlevelse av forskrifter og lover.

UD ønsker å automatisere flest mulig av manuelle prosesser som kjøres ved nyansettelse, registrering av endringer i arbeidsforhold eller endringer som kommer med nye prosjekter. For å kunne automatisere synkroniseringen av grunnlegende persondata, og hindre at en feil ved registrering sprer seg videre til neste ledd i systemene og videre til andre brukerdatabaser, skal løsningen knyttes til autoritative kilder for alle ansatte og innleide i UD. Opplysningene som hentes fra disse autoritative kildene, vil regnes som den mest riktige i systemene. Det er penger å spare på at alle tjenester bruker de samme personopplysningene, og det forbedrer informasjonssikkerheten og personvernet.

I prosjektmandatet går det fram av delmål som er satt opp for prosjektet, at UD vil vurdere å etablere en felles metakatalog som kan innholde unike brukeridentiteter og brukerattributter for alle i UD. Metakatalogen vil sørge for flyten av data mellom en eller flere katalogtjenester og databaser. Dataene som vil veksles vil vanligvis være samlinger av oppføringer som innholder brukerprofiler av alle brukere i UD.
Videre har prosjektet mål om å etablere "Singel Sign-On" og "Single Sign-Off", slik at brukerne ikke trenger å huske mange brukernavn og passord til de systemene som de bruker ofte. Med Single Sign-On behøver ikke brukeren å registrere brukernavn og passord flere ganger etter at vedkommende har gjort det om morgenen når han/hun logget seg på første gang. "Single Sign-Off "er den omvendte prosessen som logger ut brukeren fra flere systemer med en enkel utlogging.

Et annet delmål som belyses er å gi sluttbrukerne selv muligheten til å oppdatere informasjon om seg selv, og kunne tilbakestille passordet sitt om vedkommende skulle glemme det. Med selvbetjeningstjenester vil brukerstøtte oppleve færre henvendelser. Brukerne trenger ikke å

vente på at IT-avdelingen skal tilbakestille deres passord, brukeren kan fort komme i gang med jobbingen. Brukerstøtte vil ha tid til å fokusere på andre viktige oppgaver, og de brukerne som virkelig trenger hjelp kan få det raskt.

Noen taktiske planer er også satt opp for å kunne understøtte den strategiske planen, og dermed sikre at prosjektet skrider fram og oppnår noen raske fordeler og som kan samle interessenter rundt prosjektets suksess og gevinster.

Under effektmål nevnes det flere mål som tenkes å nås etter innføring av en IAM-løsning. Innføringen vil bidra til forbedret sikkerhet ved at automatiserte prosesser vil gjøre det de er programmert til og med dette sikres det at de som skal ha tilgang har det og de som ikke skal ha det ikke har det. Med løsningen vil UD ha bedre kontroll på alle foreldreløse brukerkontoer som ikke ble slettet i sin tid. Automatiserte prosesser vil også hindre at slike foreldreløse kontoer blir liggende igjen etter at en bruker forlater virksomheten. Videre er det også tenkt på alternative autentiseringsmekanismer enn brukernavn og passord, slike mekanismer kan forbedre sikkerheten et hakk bedre. Videre er det nevnt flere mål UD vil strebe etter å nå i prosjektfasene, prosjektet vil implementeres i flere faser og basisfunksjonaliteten planlegges å være ferdigstilt innen 1. juni 2010.

8.3.3 Basisfunksjonalitet

I kompliserte systemer som IAM, er det helt naturlig å holde kompliserende momenter unna til man har fått på plass enkle systemer som virker som det skal.
Basisfunksjonalitet er det som er viktigst, og som virksomheten må bruke mye tid og ressurser på for at det ferdige prosjektresultatet skal bli bra. Det er disse funksjonene som anses som grunnmuren, eller fundamentet for hele prosjektet og som må på plass før man går i gang med å bygge videre på.

I de fleste IAM-prosjekter vil prosjektutvikling gå gjennom flere faser, der prosjektet videreutvikles etter hvert som resultater og erfaringer fra én fase gir viktig læring til hvordan en kan løse den neste. Hensikten er å ta et skritt om gangen, i riktig retning og utføre gjøremålene på en best mulig måte slik at målsetningene for prosjektet ser oppnåelig ut.

Om virksomheten vil at resultatet og kvaliteten på prosjektet skal stå godt og holde seg i mange år, er det arbeidet som gjøres i første fase helt avgjørende for om prosjektet kan overleve til neste fase. Det er viktig å beregne godt med tid for å få kunnskapen, erfaringen og modningen på plass før organisasjonen bygger ut løsningen ytterligere med ønskede tjenester og funksjoner. Ved å starte med å implementere tjenester som vil forenkle hverdagen noe for de fleste brukere, og dette uten bruk av masse tid og ressurser vil man klare å skaffe mange støttespillere til prosjektet og som kan være motivasjonen for videre arbeid.

Under følger noen anbefalinger gjort i forstudierapporten i forbindelse med innføring av IAM, fokuset er på prosessene som gjelder ved oppretting, endring og sletting av brukerkontoer:

"Anbefalingen er å implementere tjenester som vil omfatte flest brukere og som vil gi en rask gevinst før mer omfattende og avanserte tjenester implementeres. Basisfunksjonalitet som anbefales:

- *Datasynkronisering mellom autoritativ kilde (SAP HR) og AD*
- *Automatisk opprettelse av brukernavn i AD basert på policy*

- *Automatisk opprettelse av e-mail basert på policy*
- *Automatisk opprettelse av hjemmeområde i filsystem*
- *Automatisering av endringer og slettinger av brukere*

Tjenester som vil bli en del av basisfunksjonaliteten
- *Sentralisert brukeradministrasjon*
- *Selvbetjeningsside for bytte av passord"* **[59]**

7.3.4 Oppnådde mål eller feilet i å nå målene

Disse faktorene kan være avgjørende karakter for virksomheter som enten planlegger å innføre en IAM-løsning, eller er i ferd med å innføre en løsning. Under ser du tabellen med ulike fargekoder for status.

	Bra Delvis/middels Dårlig Vet ikke/ikke aktuelt **Suksessfaktorer** **I hvor stor grad opplevde du at:**	**Status**
1	**organisasjonen hadde en strategisk tilnærming til prosjektet?** UD har en strategisk tilnærming til prosjektet, men mangler en bred forankring, en felles forståelse og deltagelse på tvers av avdelinger.	
2	**organisasjonen hadde det nødvendige forarbeidet til prosjektet, og kartlegging av eksiterende systemer ble utført?** UD har behov for en grundigere analyse og dokumentasjon av nåsituasjonen. Kartlegging og dokumentering av prosessene, rutinene, og behov samt krav som er nødvendig for å iverksette en IAM-løsning.	
3	**prosjektet hadde klare mål og realistiske forventninger?** UD har definert klare mål for å holde fokuset på hva organisasjonen vil med prosjektet. Virksomheten har hatt for høye forventninger til prosjektet, og undervurdert nåsituasjonen.	
4	**organisasjonen hadde klar definerte variabler for å kunne måle suksess. Organisasjonen hadde en trinnvis innføring av løsningen?** UD har fått anbefaling om å implementere løsingen i mindre iterasjoner, tjenester som vil omfatte flest brukere og som vil gi en rask gevinst før mer omfattende og avanserte tjenester implementeres.	
5	**det var behov for å leie inn eksterne spesialister til prosjektet?** UD leide inn rådgivere for å bistå med innkjøpsprosessen, forankring og bygging av prosjektorganisasjon. Og vil helt sikkert	
6	**prosjektet hadde et klart eierskap, og ansatte som ble berørt av prosjektet var flinke til å samarbeide?**	

7	**sluttbrukerne, berørte og interessenter ble tidlig involvert i prosjektet?**	●
8	**ledelsen vær med og støttet prosjektet?**	●
9	**kommunikasjon blant deltakerne i prosjektet?**	●
10	**organisasjonen hadde flere evalueringsrunder før valg av leverandør?**	●

Tabell 6

7.3.4 Konklusjon

Meget store beløp investeres i IAM-prosjekter med håp om at det skal gi forbedret sikkerhet, enklere administrasjon, forbedrede kunderelasjoner og økt lønnsomhet. Analyser viser at mange virksomheter har problemer med å innføre et IAM-system i virksomhetens IT-systemer. I de fleste tilfeller handler det om at organisasjonen og ledelsen ikke forstår rekkevidden eller kompleksiteten som ligger i problemområdet IAM-systemet skal operere i.

Det kan være mange årsaker til at prosjektet stopper opp eller mislykkes totalt. Det mange ikke forstår er at det ikke går an å kjøpe en bestemt programvare for å dekke behov som ikke eksisterer eller ikke er avdekket enda. Det er nødvendig med en gjennomtenkt strategi og en gjennomarbeidet prosessbeskrivelse. Det er også viktig at organisasjonen har den forståelsen om at prosjektet er et endringsprosjekt, og har strategiske leveranser som ikke kan tas for lett. Det er også behov for ledere som kan ta et skritt tilbake og betrakte det hele fra et annet perspektiv og forsøke å forstå årsaken til behovet og hva som skal til for å dekke det.

I april 2008 innhentet UD ekstern hjelp for å bistå med innkjøpsprosessen, og bygging av prosjektorganisasjonen. UD følte at de hadde kommet så langt i prosjektet at de kunne gå ut i markedet og få hjelp til innkjøpsprosessen. Prosjektet endret karakter da det viste seg at UD ikke hadde god nok forankring og forståelse av prosjektet internt i organisasjonen. Etter oppstart av intervjurunden for å kartlegge behovet som er nødvendig for å iverksette en innkjøpsprosess, viste det seg at UD ikke har gode og detaljerte beskrivelser av nåsituasjonen, og at det er omfattende mangler bl.a. innenfor sikkerhetspolicyer, IKT-strategien, manglende dokumentasjon av prosesser og rutiner.

I forstudierapporten som ble skrevet etter delprosjektet, går det fram at det er uklarheter og udokumenterte forhold, mangelfull og lite dokumenterte prosesser. Virksomheten har heller ikke fullt kontroll med kvaliteten av data som legges inn i systemene.

Prosjekt lå an til å mislykkes og organisasjonen holdt på å kaste seg ut i en kostbar oppdagelses reise, men dette var ikke synlig for prosjektgruppen. Prosjektet fikk en nødvendig pause, og fikk en høyst nødvendig kurs korrigering med hjelp fra innleide

rådgivere. Rådgiverne konkluderer med i forstudierapporten at det er vanskelig å bistå med innkjøp av en løsning om virksomheten ikke vet hvorfor de skal ha det og hvilke problemer den skal løse. UD kan bygge opp kompetansen i organisasjonen, og sakte men sikkert bevege seg mot å innføre en IAM-løsning.

Under følger noen anbefalinger gjort i forstudierapporten i forbindelse med innføring av IAM, legg merke til at fokuset er på prosessene:

***"Vi** ønsker her å liste opp konkrete saker vi anbefaler UD å gjøre i forbindelse med en IdM innføring. Disse anbefalingene er:*

- *Etablere Sikkerhetsstrategi og tilhørende styrende policy dokumenter*
- *Fortsette med forankringsarbeid, spesielt på ledernivå*
- *Få på plass en visjon og målbilde av IdM i UD*
- *Inkluder systemeierne fra starten av*
- *Finne en "IdM-helt" i organisasjonen*
- *Ta lærdom av andre organisasjoners feil- og suksesskriterier*
- *Ikke la IdM bli teknologidrevet*
- *Følge en "best-practice" metodikk for IdM prosjekter*
- *Dokumentere HR prosessene inkludert tverrfaglige oppgaver i prosessen*
- *Det bør gjennomføres en prosessmodellering, (Nåsituasjon / Ønsket situasjon) som omfatter ovenfor beskrevne områder og innhold.*
- *Vurdere nye / endrede IT verktøy, som støtte til arbeidsflyten "Ønsket situasjon".(herunder IDM og Rolle verktøy)*
- *Vurdere innføringen av et eget prosessmodelleringsverktøy og metode for videreutvikling og forvaltning av organisasjonens arbeidsmetodikk."*
  [Forstudierapport IdM, Innføring av Identitets- og tilgangskontroll i UD]

Kapittel 8

Avslutning

I arbeidet med masteroppgaven fikk jeg mulighet til å stiftet bekjentskap med et spennende, og ganske omfattende fagområde med navnet Identity og Access Management. IAM er et relativt nytt begrep som betyr forskjellige ting for forskjellige folk. Forsatt er mange uenig om hvilke forkortelse man skal bruke. Men de fleste er enig om at IAM har blitt synonym med ”Single Sign-On”, automatisering av prosesser, synkronisering av passord, rollebasert tilgangskontroll.

IAM er komplisert og alt-inngripende på flere måter, og byr på tøffe utfordringer for alle som blir involvert i innføring av komponentene. Hver bedrift har sine særegne behov og et IT-miljø bestående av forskjellige applikasjoner, plattformer og tilkoblinger, dette bidrar til at prosjekter blir noe mer kompliserte enn først antatt. Det gjør ikke noe lettere at de fleste av leverandørene bruker forskjellige begreper og betegnelser for å beskrive og selge inn sine løsninger.

I denne oppgaven har jeg forsøkt å gjøre IAM mer forståelig både for meg selv, og for andre som har interesse for det. Det eksister et kaos av begreper og betegnelser innen IAM, og noe av dette gjør IAM vanskeligere enn det egentlig er.

Vi startet i kapittel 2 med å se på teori for hva datasikkerhet er, hvilke farer og trusler som truer datasikkerheten. I kapittelet konkluderes det med at sikkerhet er en lang og kontinuerlig prosess. Videre i kapittelet beskrives de lover, forskrifter og instrukser som skal beskytte, begrense eller straffefølge ved overtramp av personvern, informasjonssikkerhet, og nedgradering av gradert informasjon, osv.

I kapittel 3 så vi på hva identitets og tilgangskontroll er, og hvilke basis komponenter den består av. Det blir konkludert med at IAM kan forenkle hverdagen for mange, og hjelpe virksomheter til å effektivisere forretningsprosesser, samt forbedre sikkerheten ved IT-systemene.

I kapittel 4 blir forutsetninger for et slikt prosjekt gjennomgått. Mange gjør feil i å snakke om implementering av en IAM-løsning før de faktisk har avdekket det faktiske behovet ved virksomheten. I kapittelet anbefales det om å vurdere med et kritisk blikk på fordelene ved teknologien og velge riktig tilnærming etter å ha kartlagt behov virksomheten har. IAM er dyrt, og derfor er det viktig å kunne fastslå kostnadene relatert til alle stadier av prosjektet.

I kapittel 5 blir noen av de vanligste fallgruvene de fleste kan komme bort i ved et innføringsprosjekt av IAM. I kapitlet blir det enda en gang konkludert med at det ikke finnes noen raske og enkle veier for å få til en vellykket implementering av IAM.

I kapittel 6 blir noen av faktorene som kan hjelpe virksomheter til å ha en formening om hva det er som må være på plass for å oppnå målene i et IAM-prosjekt. Det er viktig å stoppe opp

og reflektere over de delene av prosjektet som skaper ekstra trøbbel. Og være modig nok til å stille seg vanskelige spørsmål, og søke hjelp til å besvare dem.

I kapittel 7 ser vi på de tre case-studien vi har, og vurderer prosjektene deres ut i fra de forutsetninger de hadde. Casene gjennomgås hver for seg, og ingen av dem blir stilt mot hverandre for å undersøke om hvem av dem som har vær mest suksessfull med sitt prosjekt.

8.1 Konklusjon

Mye kan skrives om IAM-prosjekter som feiler i å nå målsetningene, og like mye kan skrives om andre prosjekter som ender med suksess. Det er vanskelig å skille prosjektene i denne oppgaven på suksess og fiasko. Prosjektene har forskjellige utgangspunkt, og har ulike forutsetninger for innføringen. Det er også forskjell på hva virksomheten velger å prioritere i forhold til kravene de har til prosjektet. En virksomhet vil kanskje prioritere å starte med SSO mens den andre vil starte med roller. Men det er noen punkter som viser seg å gi en pekepinn hvor prosjektene ikke har gjort nok for å unngå unødvendige opphold, eller har gjort et godt arbeid og kommet til neste fase i prosjektet. De faktorene som trenger ekstra fokus, nevnes her med punkter organisasjoner bør være obs på.

Mange IAM-prosjekter har blitt uhensiktsmessig dyre, og endt med kostnadsoverskridelser, tapte arbeidstimer, forsømte tidsfrister, og arbeid som måtte gjøres om igjen. Store prosjekter følger ofte veier og retninger en ikke hadde forutsett tidlig i prosjektfasen. Dette kan skyldes mange ting, men det kan også hende at om man hadde foretatt en mer bevisst vurdering av konsekvenser forbundet med strategivalg, teknologivalg og leverandørvalg, kunne man ha unngått noen fallgruver.

En av bedre metoder for å lære seg teknologi på er ”test og feile”-metoden, men denne måten å lære seg IAM på kan være både dyrt, komplisert og tidtagende. En annen læringsmetode er å se og lære av andres feil. Man unngår å gjøre de samme feilene og forhåpentligvis sparer man også store summer ved å se hva ”beste praksis” anbefaler.

IAM-prosjekter er ofte vanskelige, komplekse og krevende, og ofte forlanger en strategisk og fleksibel tilnærming. Innføring av IAM i en virksomhet er et endringsprosjekt som involverer IT-systemer, det vil si prosjektet kan oppnå målsetningene først og fremst når organisatoriske endringer settes ut i livet. Prosjektet involverer ofte store deler av organisasjonen løsningen skal innføres i, og griper inn i flere områder og prosesser som ikke er vanlig for andre type IT-prosjekter. Prosjektet vil fører ofte med seg organisatoriske endringer, effektivisering og automatisering av arbeidsprosesser og rutiner. Det er ofte teknologien som får mest av oppmerksomheten, men IT er verktøyet som skal legge til rette for å få til organisatoriske endringer, og det er forretningssiden som bør styre verktøyene for å oppnå målsetningene med prosjektet.

Et godt utført forprosjekt er fundamentet for å bygge prosjektet videre på, og en forutsetning for å kunne oppnå målsetningene. Det er i forprosjektet man definerer hvorfor prosjektet igangsettes samt hva som ønskes oppnådd. Det er her man spør de vanskelige spørsmålene og forsøker å finne gode svar på dem. Det er av stor viktighet å kunne adressere tidlig de utfordringer og problemer som kan oppstå i de neste fasene av prosjektet. Virksomheter som har hatt god tid til forprosjektet og hatt muligheten til å analysere og dokumentere sine arbeidsprosesser, vil ha mye bedre forutsetning for å lykkes med IAM enn den som ikke har klar definisjon på hvordan oppgaver løses hos dem. Har ikke virksomheten brukt tid til å

analysere og dokumentere prosessene, datasystemene, forretningssystemene, kan man med nesten sikkerhet si at utfordringer vil hindre dem i å forsette med prosjektet. Forprosjekt kan også kalles for en modningsprosess, der organisasjonen opplever en modning av tankevirksomhet etter hvert som folk begynner å definere og dokumentere prosessene, og teknologien som ligger bak disse prosessene. Spørsmål om forbedrings potensialer for de manuelle prosessene vil stadig vekk dukke opp. Klarer prosjektgruppen å definere prosessene med alle unntak, vil dokumentasjonen forenkle mye av arbeidet med implementering og organisasjonen vil kunne spare tid, ressurser, og løsningen kan raskere implementeres som igjen vil realisere gevinstene tidligere enn antatt.

"Å spise hele elefanten på en gang" er et kjent uttrykk som brukes i IAM sammenheng. Det betyr at organisasjoner bør unngå å implementere alle komponenter i en IAM-løsning i en fei. Innføringen bør skje i en faseinndelt tilnærming, der prosjektet skrider frem gjennom flere faser. Hver fase kan behandles hver for seg og det kan tas en vurdering om prosjektet har greid å innfri forventningene, slik at neste fase i prosjektet kan initieres. Fasene kan deles i forhold til de funksjoner som organisasjonen vil implementere. Funksjoner som vil påvirke og omfatte flest brukere, og som vil gi en rask gevinstrealisering bør velges framfor mer avanserte og ressurskrevende.

IAM-prosjekter er en strategisk og vidtfavnende beslutning, og må derfor være en beslutning understøttet av ledelsen. Forankring på høyt plan er en av de faktorene som er en av de avgjørende i et IAM-prosjekt. Som det er også nevnt ovenfor, er IAM et endringsprosjekt med mange komplikasjoner. Ledelsen må involvere seg tidlig, og korrigere kurset når det er nødvendig. Er det kort veil til beslutningene vil mye tid og ressurser spares, man trenger ikke vente til neste uke for å ta en beslutning om f. Eks. ressursforbruk.

Alle tre casene i denne oppgaven er i offentlig sektor, men stort sett har privat sektor de samme utfordringene. Organisasjonene har hatt ulike forutsetninger for prosjektet, og ligger derfor litt forskjellig i innføringen av IAM. Alle har forsatt mye arbeid foran seg, og flere utfordringer og hindringer lurer seg bak neste sving.

Etter at de tiltenkte IAM-modulene er på plass, må ikke oppmerksomheten bli mindre av den grunn. IAM-løsninger må få utført servicer for å kunne holde seg oppdatert med produktoppdateringer, endringer i IT-miljøet og optimaliseringer som kan øke effektiviteten innad i organisasjonen. IAM er som mange andre IT-prosjekter som egentlig aldri når et sluttpunkt, det er kontinuerlige forbedringer, nye måter å gjøre ting på som gjør at utviklingen forsetter.

9.2 Forslag til videre forskning

Prosjektet har hatt relativt begrensende rammer i forhold til fagområdet, og IAM er et nytt forskningsområde hvor ytterligere forskning må utføres. Med dette arbeidet håper at jeg kan få folk til å forstå og oppfatte hvor kompleks et IAM-prosjekt er, og hvor i stor grad den involverer store deler av organisasjonen den skal innføres i. Jeg håper oppgaven kan være en introduksjon av IAM, og den bidrar til at virksomheter gjør et godt forarbeid før de går i gang med å anskaffe av en IAM-løsning.

Alle casene i denne oppgaven er offentlige organisasjoner, en interessant problemstilling i forhold til dette kan være å kartlegge hvordan prosjekter blir organisert og utarbeidet i privat sektor.

En annen problemstilling som gjør seg gjelden her, er å spørre seg om privat sektor gjør det bedre i IAM-prosjekter i forhold til offentlig sektor.

Vi sier ofte at IAM er kompleks, men hva er det som skal til for å gjøre den oversiktlig og spiselig?
Finnes det alternative tilnærminger til Identity and Access Management?

Det er mange problemstillinger som dukker opp, f. eks.;

1- Sammenligning av IAM-prosjekter med andre type IT-prosjekter.

2- IAM består av flere moduler og komponenter, hvilke(n) komponent(er) er best å implementere i forhold til de andre?

3- Implementering av rollebasert tilgangskontroll, og komplikasjoner som kan oppstå.

4- IAM-produkter, hvilken leverandør har det beste produktet med hensyn til fleksibilitet, effektivitet, sikkerhet?

5- SOA + IAM= Sant?

6- Hva med IAM og Software as a Service (SaaS)?

Det at IAM er et nytt og relativt lite forsket fagområde, gjør den til en upløyd jord som kan undersøkes på flere måter. Mange utfordringer og løsninger kan problematiseres, og nye problemstillinger kan utformes for denne upløyde jord.

Kapittel 9

Bibliografi

1- Roberta J. Witty: Identity Management Best Practices: Why They Aren't Three-Month Implementations. Identity & Access Management Summit. June 25-26, 2007

2- Burgess, Mark: Principles of Network and system administration, Wiley

3- Bishop, Matt: Computer Security: Arts and Science, Addison Wesley.2003

4- Håndbok i datasikkerhet: Håndbok i datasikkerhet – informasjonsteknologi og risikostyring. 2006

5- Datatilsynets årsmelding (1995): http://www.datatilsynet.no/templates/Page____720.aspx [Hentet 07.11.08]

6- Christian With / Gunnel Helmers (2005): http://www.datatilsynet.no/templates/Page____1290.aspx [Hentet 07.11.08]

7- http://www.iso.org/iso/catalogue_detail?csnumber=39612, [Hentet 27.10.2008]

8- http://www.iso.org/iso/catalogue_detail?csnumber=42103, [Hentet 27.10.2008]

9- www.ey.com/Global/Assets.nsf/Norway/Eierstyring_og_selskapsledelse/$file/Eierstyring og selskapsledelse.pdf

10- http://www.ciber.no/courses/hvaerCOBIT.cfm, [Hentet 27.10.2008]

11- Roberta J. Witty, Ant Allan, John Enck, Ray Wagner. Gartner, 4 November 2003: Identity and Access Management Defined, http://www85.homepage.villanova.edu/timothy.ay/DIT2160/IdMgt/118281.pdf [Hentet 27.10.2008]

12- Butlergroup, 2006: Customer Priorities in a Competitive Identity and Access Management Marketplace. Present and future enterprise needs in an increasingly identity-driven world. http://www.oracle.com/corporate/analyst/reports/infrastructure/sec/butler-iam.pdf

13- Dale Young, 2004: Human Resources have a vital role to play within employee identity and access management. Dale Young, Senior Consultant, Insight Consulting. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG-4DW87HN-6&_user=10&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_version=1&_urlVersion=0&_userid=10&md5=f96ee7981dec1071f88d041fb9a76f62

14- Prosjektmandat, JBV: Prosjektnavn: IAM (Identity and Access Management). (Konfidensielt)

15- Ementor Autentiseringspakke: www.ementor.no/upload/Campaigns/NO/NextStep løsning/Autentiseringspakke.pdf

16- Microsoft IAM: Microsoft Identity and Access Management Series, Fundamental Concepts, Chapter 3: Microsoft Identity and Access Management Technologies. http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx?mfr=true

17- HP Security: HP Security Handbook Identity Management. www.homeandoffice.hp.com/enterprise/downloads/HP Security Handbook Identity Management

18- Stanford, Hong Kong University 2003: Exploring Secure Identity Management in Global Enterprises, Stanford University and Hong Kong University of Science and Technology, March 2003. http://www.novell.com/collateral/sim_stanford.pdf

19-Microsoft IAM, 1: Microsoft Identity and Access Management Series, Password Management, Chapter 1: Introduction to the Password Management Paper. http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx?mfr=true

20- META Group: The Value of Identity Management: How securing identity management provides value to the enterprise, August 2002. http://cro.alienpants.com/identity/Value%20Of%20Identity%20Management.pdf

21- Gartner, 2002: Password Reset: Self-Service That You Will Love (Gartner Research Note T-15-6454), Study Publisher: Gartner Group - Roberta J. Witty & Kris Brittain
Study Date: April 15 2002,
http://www.gartner.com/DisplayDocument?ref=g_search&id=354760

22- Gartner, 2007: Identity & Access Management Summit. http://www.gartner.com/it/page.jsp?id=633107

23- Microsoft IAM Series, 2: Microsoft Identity and Access Management Series, Password Management, Chapter 2: Approaches to Password Management. http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx?mfr=true

24- Federation—the enabler for electronic business.White paper. 2004. http://managementsoftware.hp.com/products/slctfed/swp/slctfed_swp_electronic_business.pdf

25- The Liberty Alliance. http://en.wikipedia.org/wiki/Liberty_Alliance

26- Rosario, Craig 2007: Understand Why SUN Identity & Access Management is good for business. 7th November 2007, Ramsey Rosario, Jim Craig. http://projects.exeter.ac.uk/iam/Sun/IdMUnderstand.pdf

27- Netegrity, 2003: Identity and Access Management: The Promise and the Payoff. How an Identity and Access Management Solution Can Generate Triple-digit ROI. http://www.hillwriter.com/NetegrityWhitePaper.pdf

28- Stølen, 2006:Hva er vitsen med sikkerhetspolicies? SINTEF. Ketil Stølen Oslo 23. november 2006

29- Benantar, Messaoud: Access Control Systems, Springer. 2006

30- Sikkerhetslovens § 3: www.lovdata.no/all/nl-19980320-010.html

31- The free encyclopedia] http://en.wikipedia.org/wiki/Authentication

32- Gartner, February 2002: Security in a World Without Secrets, R. Hunter, Gartner, February 2002.

33- NIST, 2002: National Institute of Standards and Technology.The Economic Impact of Role-Based Access Control march 2002. http://www.nist.gov/director/prog-ofc/report02-1.pdf

34- kunnskapsgartnerne :http://kunnskapsgartnerne.no/index_b.html

35- www.netvision.com: White Paper.2007.Surviving an Identity Audit. What small and midsize organizations need to know about the identity portion of an IT compliance audit? http://www.netvision.com/downloads/wp_surviving_1007.pdf

36- Identity Auditing: Taking Compliance. Beyond the Baseline. White Paper.April 2005] Sun Microsystems, Inc.
http://www.sun.com/software/products/identity/wp_id_auditing_tcbb.pdf

37- www.quest.com:Simplifying Identity and Access Management.
http://www.quest.com/company/pdfs/Quest_IDM_Brochure.pdf

38- Identity Management Project Roadmap. 2008 Hitachi ID Systems.
http://idsynch.com/docs/identity-management-project-roadmap.pdf

39- Malm,2007:Oktober 2007, Av Carl Christian Malm, nordisk ansvarlig for systemintegrasjon innen telekommunikasjon, media og høyteknologi i Accenture.
http://www.accenture.com/Countries/Norway/Research_and_Insights/prosjekterfor45mrd.htm

40- Einar Ryvarden : Derfor feiler eller lykkes IT-prosjekter, tirsdag 2. okt 2007[Digi.no]
http://www.digi.no/php/art.php?id=490841

41- Identity Management strategy and business approach: it is not just about technology 20 September 2006.Andrea Multari.
http://fr.sun.com/sunnews/events/2006/sep/identite/presentations/Presentation_Accenture.pdf

42- Consider Identity and Access Management as a Process, Not a Technology. 2 September 2005 Earl Perkins, Ant Allan. http://www.gartner.com/DisplayDocument?doc_cd=129998

43- Identity and access management: uncovering the secrets to successful implementations. December 2007.IBM] http://www-935.ibm.com/services/us/gts/pdf/sp_wp_identity-and-access-management-uncovering-the-secrets.pdf

44- UNINETT ABC: Datavask og rutiner - beste praksis Temahefte. http://www.uninettabc.no/attachment.ap?id=219

45- Brooke Paul (uttaleleser til IT Automation): http://www.networkcomputing.com/channels/security/showArticle.jhtml?articleID=199901451&pgno=3&queryText=. Special Issue -- IT Automation: Identity Management. jun 11, 2007 - By Greg Shipley

46- Personinformasjon og LDAP i Feide Feide for IdM-leverandører, Gardermoen 2008-06-10 Anders Lund. http://www.uninettabc.no/multimedia.ap?id=366

47- Directory Services: Critical to Effective Identity Management. White Paper March 2005. http://www.sun.com/software/products/identity/wp_directory_services_id_mgmt.pdf

48- Directory Services: Critical to Effective Identity Management. White Paper March 2005. http://www.sun.com/software/products/identity/wp_directory_services_id_mgmt.pdf

49- Niklas Lundin: Nettverk & Kommunikasjon. 04.06.2006 kl 20:32. http://www.idg.no/cio/article12139.ece

50- IT-prosess og –policy: http://www.microsoft.com/norge/business/peopleready/coreinfra/capability_it.mspx

51- Rolf Frydenberg: administrerende direktør i Manag-E Nordic.[(www.digi). http://www.digi.no/php/art.php?id=530301]

52- Tilmann and Weinberger, 2004: Tilmann, George and Weinberger, Joshua (2004) Technology never fails, but project can. http://www.baselinemag.com/c/a/Projects-Management/Technology-Never-Fails-But-Projects-Can/

53- Identity Management Best Practices: Why They Aren't Three-Month Implementations. Roberta J. Witty. IAME1_893, 6/07, AE. http://www.gartner.com/it/content/500300/500380/iame1brochure.pdf

54- 5 Keys to a Successful Identity and Access Management Implementation DECEMBER 2007 Paul Engelbert. CA] http://www.ca.com/files/WhitePapers/iam_services_implementation_whitepaper.pdf

55- INFORMATION SECURITY INDUSTRY REPORT: February 2008.Identity & Access Management Evolutions according to the experts http://www.lsec.be/upload_directories/documents/LSEC%20Information%20Security%20Industry%20Report%20Nr.%201.pdf

56-Jenster and Hussy, 2005: Jenster, P and Hussey, D (2005) Create a common culture between IT and business people to reduce project failures. Computer Weekly, March 22

57- The Standish Group International (1999) CHAOS: A Recipe for Success the Standish Group International.

58- Glaser, J (2004) Management's role in IT project failures Healthcare Financial Management, October

59- Prosjektmandat IDM:Identitetshåndtering.Innføring av Identitets- og tilgangskontroll i UD

60- Bilag 1. bakgrunn, formål og rammebetingelser: Forespørsel om tilbud på systemløsning for identitetshåndtering i Norges forskningsråd - Mars 2007

Figurer

Tabeller