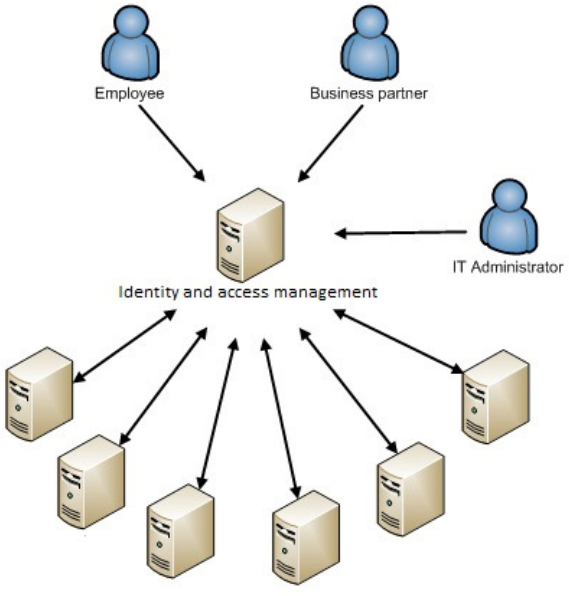
GÖTEBORGS UNIVERSITET

Rationalitet för identitet- och åtkomstlösningar i stora företag

Rationality of identity and access management solutions for large corporations



Staffan C. Gustafsson
Mikael Paradis

Kandidatuppsats i Informatik

Rapport nr. 2011:014
ISSN: 1651-476

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2011

Sammandrag

Säkerhet och användaradministration är två stora problem som alla företag måste behandla. Brandväggar och VPN-tunnlar är grundläggande delar för säker dataöverföring som hjälper företag att skydda sin infrastruktur. Men, hot i form av kvarliggande konton, inaktuella rolltilldelningar och låg spårbarhet, måste hanteras. Denna uppsats undersöker vad som motiverar företag att investera i en IAM-lösning (Identity & Access Management). Baserat på intervjuer med personal på företag, tillsammans med rapporter och uppsatser så utreder vi vad en IAM-lösning innebär för ett företag; vilka effekter den får på affärsprocesser och vilka tekniker som vanligen implementeras. Studien visar att huvudanledningen till att företag investerar i en IAM-lösning är att få ordning och reda bland sina användarkonton genom en effektiviserad administration.

Nyckelord: användaradministration, drivkrafter, IAM.

Abstract

Security and user administration are two major issues every enterprise has to deal with on an everyday basis. Fire wall solutions along with VPN tunnels for secure data transfer are forming the foundation for enterprises trying to protect their infrastructure from external threats. However, threats in the form of orphan accounts, legacy roll entitlement and low traceability are a growing concern for information security managers in large companies as enterprises grow. This essay is investigating what the motivating drivers are for an enterprise to consider investing in an IAM solution. Based on interviews with key personnel in two major companies, along with reports and essays we give a summary of what an IAM solution means for a company; what effects on business processes are expected and what different kinds of solutions are implemented to help them provide better user management. This study shows that the main reason for enterprises to consider an IAM solution is the pursuing of orderliness in user accounts through more effective administration.

Keywords: user administration, drivers, IAM.

Förord

Vi vill rikta ett stort och varmt tack till vår handledare Aida Hadzic! Hennes stora engagemang, idérikedom, feedback och entusiasmerande förmåga har varit en stor hjälp under arbetets genomförande och gjort det möjligt att leverera en högkvalitativ rapport.

Tack!

Göteborg 2011-05-23
Staffan Gustafsson & Mikael Paradis

Innehållsförteckning

1 Inledning 1
1.1 Problemdiskussion 1
1.2 Studiens syfte 2
1.3 Frågeställning 2
1.4 Avgränsningar 3
1.5 Centrala begrepp 3
2 Metod 4
2.1 Vetenskapligt tillvägagångssätt 4
2.2 Praktiskt tillvägagångssätt 4
2.3 Genomförande 6
2.4 Bedömning av studiens resultat 6
2.5 Sammanfattning av studiens utredningsmetodik 7
3 Litteraturstudie 8
3.1 Informationssystem 8
3.2 IAM (identity and access management) 8
3.3 IAM's ingående delar 11
3.4 Drivkrafter som motiverar införande av IAM 14
3.5 Koppling mellan drivkrafter och IAM-funktioner 18
3.6 Förutsättningar för en lyckad IAM-satsning 18
3.7 Gartners slutsatser för IAM-satsningar 19
3.8 Sammanfattning av litteraturstudie 20
4 Empirisk undersökning 21
4.1 Leverantör 21
4.2 Företag 1 23
4.3 Företag 2 28
4.4 Sammanfattning av empiri 30
5 Analys 32
6 Diskussion 35
7 Slutsats 36
8 Vidare forskning 37
9 Källförteckning 38

1 Inledning

Säkerhetsrisken för organisationer och företag är ett problem som har ökat i storlek de senaste åren. Problem med datastöld, inbrott på servrar och cyberattacker är en vardaglig företeelse som alla organisationer måste hantera. Samtidigt ligger krav på revision och bolagskod, i form av Basel II och Sarbanes-Oxley - vars syfte är att styra upp ekonomisk rapportering, i bakgrunden som behöver tillgodoses (1). IAM (Identity and Access management) är lösningar för administration och övervakning av användare systemåkomst, rättigheter och rolltilldelning med hög spårbarhet i alla led.

Användarkonton som tillhör uppsagda medarbetare utgör ett hot för företaget då personer, förutom att stjäla data, illvilligt kan få tillgång till resurser och kan förstöra eller radera företagskritisk information. Det finns även många tekniker i en IAM-lösning som kan hjälpa företaget att bli effektivare i sin hantering av affärsprocesser, till exempel flödet av användarrättigheter när personal avskedas eller anställs, som i vissa fall kan automatiseras helt.

1.1 Problemdiskussion

Stora företag har på grund av sin storlek höga hanteringskostnader. Ju fler anställda desto mer tid och därmed kostnad krävs för att administrera dessa anställda, en större organisation är helt enkel dyrare att driva. Frågor alla organisation brottas med – vad skall organisationen göra, vem skall göra vad, hur skall arbetet delas upp, hur skall något utföras etcetera – blir mer komplexa ju fler anställda och affärsområden som finns. För att kunna hantera och driva den stora organisationen effektivt behöver den delas upp, dels i olika delar men även olika lager. Tittar man på en organisation finns ofta tre nivåer som går att urskilja – operationell, taktisk och strategisk. En större organisation är utöver detta även uppdelad i olika delar beroende på verksamhetsområde eller geografisk placering. Diskuteras de tre nivåerna i kontexten av en affärsprocess förstår vi att någon utför en process eller ett arbete (operationell), någon styr och övervakar denna process (taktisk) och någon bestämmer vilka processer som skall finnas och vilka egenskaper dessa skall ha (strategisk).

En utmaning som uppstår när det finns många affärsområden, eller många kontor på separata geografiska platser är svårigheten med central övervakning och styrning av en given rutin eller process.

Kvaliteten på informationen som är lagrad i företagets databaser är ytterligare en utmaning för det stora företaget. En fråga som IT-avdelningen i större företag ofta brottas med är hur de skall säkra kvaliteten på data. När och var skall den skapas, vem har ansvar för datan, hur skall företaget säkerställa att data som är lagrad stämmer med verkligheten, när är den inaktuell osv. Det här arbetet försvåras av mängden databaser och system som delvis innehåller likadan information. Att likadan information lagras och behandlas i flera system ökar resursbehoven i form av personal som skapar och underhåller sagda information. Kvalitetssäkring av och rapportering från dessa utspridda och isolerade system blir en tidsökande uppgift som riskerar att falla mellan stolarna. Utmaningen omfattar som synes både verksamhetens organisationstruktur, organiserandet av olika aktiviteter samt tekniken och systemen som stödjer dessa aktiviteter. För större företag kan den ansenliga och växande mängden system med

egna användarkonton utvecklas till en administrativ börda med höga hanteringskostnader och bristande säkerhet som följd.
Ett exempel som illustrerar detta är Företag 1:s rutin att hantera användare i sina IT-system. De har 30000 anställda inom ett av sina affärsområden och circa 800 system. Givetvis använder ingen samtliga system, snittanvändaren använder mellan 10-30 system. För att skapa en ny användare behöver ett antal system nyttjas för att skapa behörigheter i de olika system som en anställd behöver ha tillgång till. Den anställde måste dessutom komma ihåg de uppgifter, såsom användarnamn och lösenord, som används för att logga in i respektive system. Vidare finns en säkerhetsaspekt gällande begränsning av åtkomst till känslig information och av system som den anställde inte behöver för sitt arbete. Man behöver dessutom rutiner för när en användare behöver tillgång till mer system eller data eller då användaren får en ny roll inom företaget och därför behöver en annan uppsättning rättigheter. När den anställde slutar skall dessutom rättigheterna i alla de system den anställde hade tillgång till upphöra. Utöver detta måste det finnas kontroller av informationsägare och informationsansvariga (ansvaret över information är utdelegerat) att en anställd verkligen skall få tillgång. För att få ett smidigt flöde måste den här informationen finnas tillgänglig så att inte ansvarig behöver kontaktas varje gång, med ökad ledtid som följd. Vem som har tillgång till vilka system är intressant att följa upp för den som är ansvarig för informationssäkerhet. Tiden som går åt att hantera användares digitala identiteter är kostsam, både för användare och administration.

Exemplet illustrerar behovet av att samla rutiner och processer gällande användardata i ett system och, medelst automatisering och kontroll av användardata, effektivisera och förenkla hanteringen av de anställdas digitala identitet och åtkomstregler. IAM- Identity and Access Management är system som avser lösa problematiken kring hanteringen av användarkonton och tillgång till olika IT-resurser.

1.2 Studiens syfte

Studien behandlar problemet med administration av användares tillgång till informationssystem och andra IT-resurser. Uppsatsens syfte är att utreda och sammanställa vad en IAM-lösning innebär för ett företag och förklara varför företag väljer att implementera IAM. Förståelse eftersträvas för de behov som föregår en IAM-upphandling, de drivkrafter som finns för införande av IAM samt vilka specifika IAM-tekniker som implementeras. Vidare utreds vilka effekter en IAM-lösning har på företagens verksamhet.

1.3 Frågeställning

Studiens söker besvara varför företag väljer att implementera IAM-lösningar, detta görs genom tre delfrågor:

- Vilka är drivkrafterna bakom företags satsningar på IAM?
- Vilka IAM-tekniker väljer företag att implementera?
- Vilka effekter har dessa på verksamheten?

1.4 Avgränsningar

Vi förhåller oss till IAM-lösningar på en övergripande nivå, fokus ligger på de verksamhetsspecifika frågorna. IAM som företeelse och process beskrivs, inte produkter med vars hjälp IAM kan implementeras. De företag som används i den kvalitativa undersökningen verkar i olika branscher men samtliga är relativt stora med tusentals anställda.

1.5 Centrala begrepp

AD – Active Directory
En av Microsoft producerad katalogtjänst för användardata.

Autentisering
En process genom vilken en påstådd identitet verifieras

Auktorisering
En process genom vilken en autentiserad identitets åtkomst till en specifik resurs beviljas eller nekas baserat på innehållet i en åtkomstlista.

Business case
Investeringsunderlag som bland annat innehåller drivkrafter för investering.

IAM – Identity & Access Management
System som hanterar användares identiteter och tillgång till olika system.

Identitet
Något som unikt identifierar en viss användare eller resurs. En fysisk person representeras av digital identitet i form av en användarpost i någon databas.

Identity life-cycle management
Att över tid och genom en identitets livslängd hantera alla ingående faser. Skapande (provisioning), uppdaterande (reprovisioning) och inaktivering (deprovisioning)

IDM – Identity Management
Ingående del i IAM som administrerar processer kring identitet.

Provisioning
Att förse ett annat system med data.

ROI – Return on investment
En ekonomisk term som uttrycker vilken vinst som görs på en investering.

SIEM - Security Incident and Event Manager
Ett övervakningsverktyg för resurser och händelser på flera olika system.

SSO – Single sign-on
En användare behöver enbart autentisera sig mot ett system för att få tillgång till övriga.

2 Metod

Kapitlet avser återge hur studien har genomförts.

2.1 Vetenskapligt tillvägagångssätt

De vetenskapliga metoder och ansatser som använts för den här studien redovisas kort.

2.1.1 Kvalitativ ansats

Vi har valt en kvalitativ ansats i vårt arbete. Detta är för att få ut kärnan och underliggande mening av intervjuerna. En kvalitativ analys av ett textmaterial vill hitta det som står mellan raderna, fånga upp känslor om ämnen och att inse att vissa delar av en text är mer betydelsefull än andra (2). Då intervjufrågorna är ordnade i fyra kategorier så kan vi lätt sammanställa materialet i en tabell där kärnorna i materialet finns representerade. Vidare har vi gjort en diskursanalys på de transkriberade intervjuerna och sammanställt resultatet.

2.1.2 Deduktiv/induktiv ansats

Vi har arbetat enligt en kombination av deduktiv och induktiv ansats. Deduktiv i det avseendet att intervjumaterialet är grundat i teorier som vi sökt fram i litteratur. Induktiv då materialet är grundat i den förstudien som gjordes med en säljare (2), se figur 1. Förstudien låg till grund för kategorierna som frågorna är uppdelade i och den fokus på kärnämnena vi sökte svar på (2).

Figur 1. Modell för induktiv ansats.

2.1.3 Deskriptiv ansats

Vi har utgått från en deskriptiv ansats i denna uppsats då vi inte har några förutfattade meningar om hur resultatet bör se ut, utan grundar alla slutsatser på vår analys och på teorin (2).

2.2 Praktiskt tillvägagångssätt

Under detta avsnitt redovisas hur data har samlats in och behandlats.

2.2.1 Urvalsmetod

Vårt urval av intervjupersoner är baserat på centralitet; kravet är att de ska ha arbetat ingående med implementationen av IAM-lösningen. Personerna innehar rollerna informationssäkerhetschef och förvaltningsansvarig/projektledare och har alla nära anknytning till IAM-lösningen.

Företagen som intervjurespondenterna arbetar på är ett entreprenörföretag samt en mekanikproducent vars namn anonymiserats.

2.2.2 Kvalitativa intervjuer
Vi genomförde strukturerade telefonintervjuer med anställda på två företag. Anledningen till att vi inte fick fler intervjuer var för att det var svårt att få tag på folk som hade så specifika positioner och roller som vi var ute efter. En strukturerad intervju kännetecknas av att inga av frågorna är ledande och ingen utveckling av svaren är med. Fördelen med det är att det är enkelt att göra en jämförande tabell med frågor och svar. Förstudien med en säljare (här efter, Säljaren) av IAM-lösningar skedde med en ostrukturerad intervju ansikte mot ansikte. Detta för att få ut mer av den underliggande meningen i respondentens svar (2).

2.2.4 Kategorisering
Vi har delat upp intervjufrågorna i olika underkategorier för att enklare kunna strukturera upp resultatet.

Bakgrund
Dessa frågor syftar till att utröna vilken position respondenten har i företaget. Vi vill få ut hur många anställda/användare och hur många system som används. Viktigt här är vilken relation respondenten har till IAM-implementationen.

Drivkrafter
Dessa frågor ska ge svar på de drivfaktorer som spelade in i investeringen av IAM-lösningen. Vi vill undersöka om det finns bakomliggande problem i affärsprocesser som lösningen kan minska/eliminera. Vi undersöker också om företaget hade/gjorde en processkartläggning innan upphandlingen. Vi ville även undersöka vem som framförde förslaget samt om det gjordes ett business case.
Utifrån intervjun med säljaren kom vi fram till att vi ville ha ett mer processinriktat tänk och, ännu viktigare, att få respondenten att tänka i processer, inte i teknik. De tekniska delarna delade vi därför in i en egen kategori.

Implementering
Denna kategori med frågor syftar till att undersöka vilka tekniska delar som företaget implementerade. Vi ville undersöka hur de gör för att välja bland dessa och hur de är kopplade till deras affärsprocesser. Vi undersöker hur företagen valde bland leverantörer och om det dykt upp något problem under implementeringen. Var det fler tekniker som implementerades i efterhand, efter att upphandlingen och kravspecifikationen hade skapats?

Systemeffekter / verksamhetseffekter
Denna kategori skapades för att få fram om implementeringen av IAM-lösningen gav de resultat som hade förväntats. Vi ville få reda på om affärsprocesserna hade påverkats och hur de hade förbättrats/försämras. Vi ville ha reda på om kostnader för personal, administration eller någon process hade minskat eller ökat. Vi ville även belysa säkerhetsfrågan och om företaget har räknat på en Return of Investment.

Utvärdering
Vi ville undersöka om en utvärdering av projektet har gjorts och i så fall hur det gick till. Resultatet om IAM-lösningen har lyckats bli implementerad är också intressant.

2.3 Genomförande

Förstudien genomfördes personligen och spelades in och transkriberades. Intervjuerna med representanterna på företagen genomfördes över Skype och spelades in på datorn. Båda författarna intervjuade. Intervjumaterialet transkriberades med InqScribe.

Begrepp som saknar ekvivalent svensk översättning är skrivna på engelska då mycket av kontexten i begreppen går förlorade i översättningen.

2.4 Bedömning av studiens resultat

Följande asvnitt avser bedöma studiens vetanskapliga validitet.

2.4.1 Begreppsvaliditet

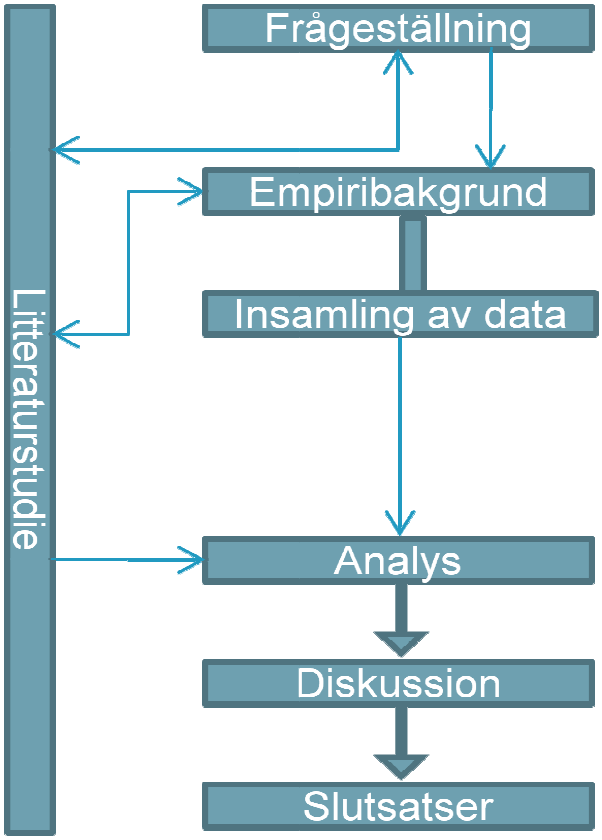
Begreppsvaliditet menar på hur väl teorins operationalisering överensstämmer med den empiriska operationaliseringen. Alltså hur väl de teoretiska begreppen och resonemangen överensstämmer med det som vi faktiskt undersökt (2). Begreppsvaliditeten för denna studie är hög eftersom vi bland annat undersöker vad som ligger bakom och driver en upphandling av en IAM-lösning och våra frågor och vår teori överensstämmer begreppsmässigt.

2.4.2 Empirisk validitet

Denna validitet syftar på dels kriterievaliditet, som förutsätter att man har flera kriterier på samma teoretiska begrepp, och dels samvariationsvaliditet som syftar på att teoretiska begrepp ifrån teorin har ett starkt samband med de teoretiska begreppen i empirin (2). Då de teoretiska begreppen finns representerade i flera olika rapporter och uppsatser och vi i intervjun har definierat begreppen tillsammans med respondenterna tyder detta på hög empirisk validitet

2.5 Sammanfattning av studiens utredningsmetodik

Vi har grundat vår litteraturstudie på den frågeställning vi har. Utifrån detta, samt förstudien med Säljaren av IAM så har vi skapat bakgrunden till insamlingen av data. Materialet är sedan transkriberat och analyserat utifrån olika kategorier. Den är sedan sammanställd i en tabell för lättare översikt. Tillslut så har vi diskuterat resultatet och dragit slutsatser. Figur 2, nedan, visar hur vi har gått till väga.



Figur 2. Modell för vårt arbetssätt

3 Litteraturstudie

3.1 Informationssystem

Informationssystem (IS) definierar vi som en tankemässig konstruktion implementerad i mjukvara avsedd att stödja vissa processer i en organisation. Enterprise-system gjorda för större organisationer har större krav på sig att vara funktionsrika och väl utvecklade än de för mindre företag. Ofta är de nischade mot specifika problem som existerar i större företag men inte i mindre. Rutiner och processer som stöds av IS kan visserligen finnas i det mindre företaget, däremot har det större företaget en stor hanteringskostnad på grund av dess storlek och skalan i vilken rutinen eller processen utförs i.
Mjukvarustödet för verksamhetsprocesser kräver alltid anpassning, antingen måste verksamheten anpassa sig efter systemets modell eller så kräver verksamheten att systemet anpassas för att passa mot dess rutiner och processer. IS gjorda för större företag är i regel mycket anpassningsbara, ibland till den nivån att de mer eller mindre enbart är en motor med stöd för olika indata, omvandling och utdata. De måste då byggas i eller med hjälp av motorn genom att definiera flöden och processer som skall utföras.

IS syftar till att ge en effektivare process eller rutin genom att automatisera något som tidigare utfördes i flera steg, kontrollera att data följer vissa regler, ge stöd för lagring av data i databas istället för i huvudet eller på papper samt minska kravet av manuell hantering.

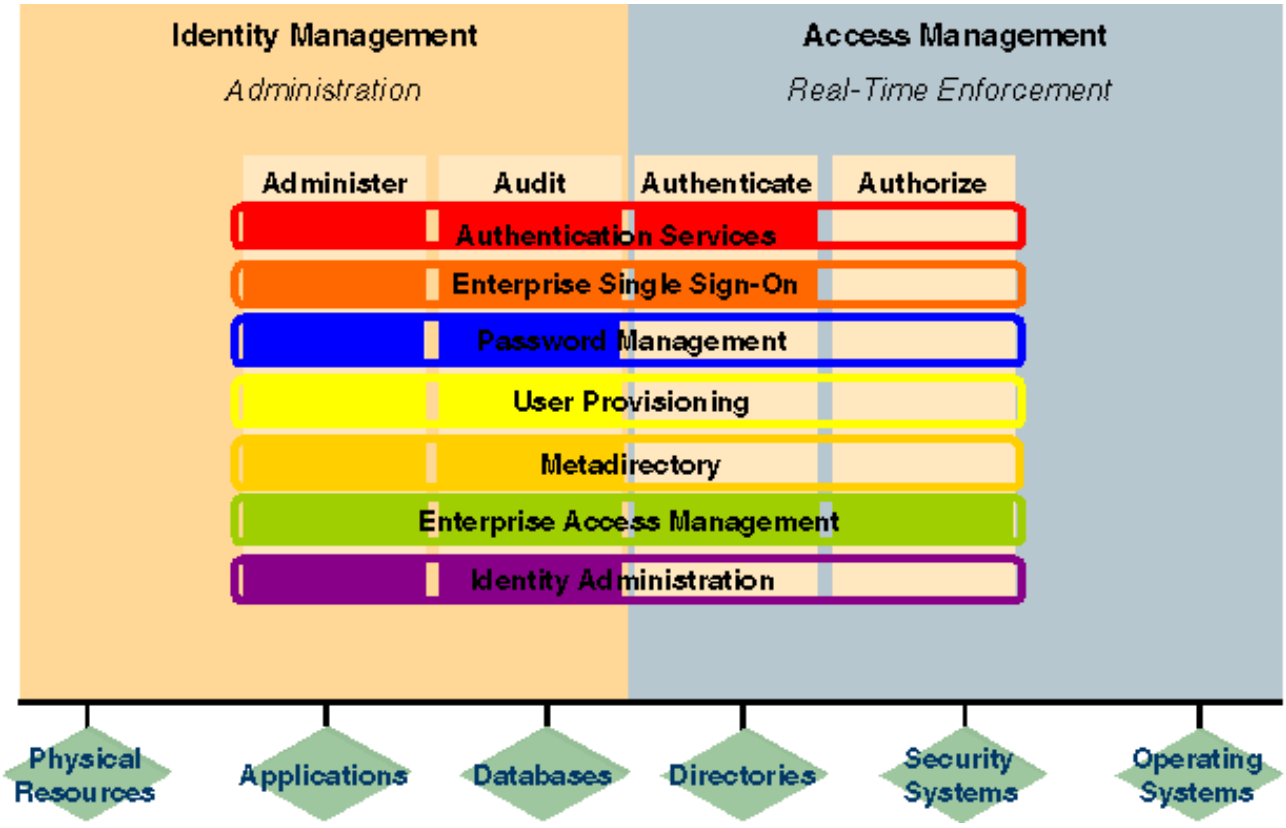
Ofta kräver ett systeminförande också någon slags omarbetning och formalisering av en process - hur och i vilken ordning saker utförs, vilket ytterligare ökar effektiviteten. Andra orsaker till införandet av verksamhetsstödjande mjukvara kan vara att få tillgång till best-practice; i större koncerner kan ledningens krav på gemensam och standardiserad rapportering kräva systeminförande i separata affärsområden eller dotterbolag.

Regler och lagar från myndigheter och kontrollorganisationer kan också vara en drivande faktor. I Sverige krävs att alla svenska bolag sköter bokföring enligt vissa regler, sjukvården har krav på sig gällande journalsystem, kreditkortbolagen har krav på säkerhet enligt standarden PCI-DSS för att tillåta företag att handla elektroniskt med kreditkort, USA kräver att alla ickeprivata bolag uppfyller SOX med mera.
En speciell sorts IS som syftar till att stödja hanteringen av användares rättigheter är IAM – identity and access management. Drivkraften för införandet av IAM är att ge verksamhetsstöd som syftar till att effektivisera rutiner kring systemåtkomst eller uppfyllandet av olika regelverk. Nästa avsnitt ger en introduktion kring IAM, vad det är, dess ingående delar och vilka drivkrafter som motiverar företag att införa IAM.

3.2 IAM (identity and access management)

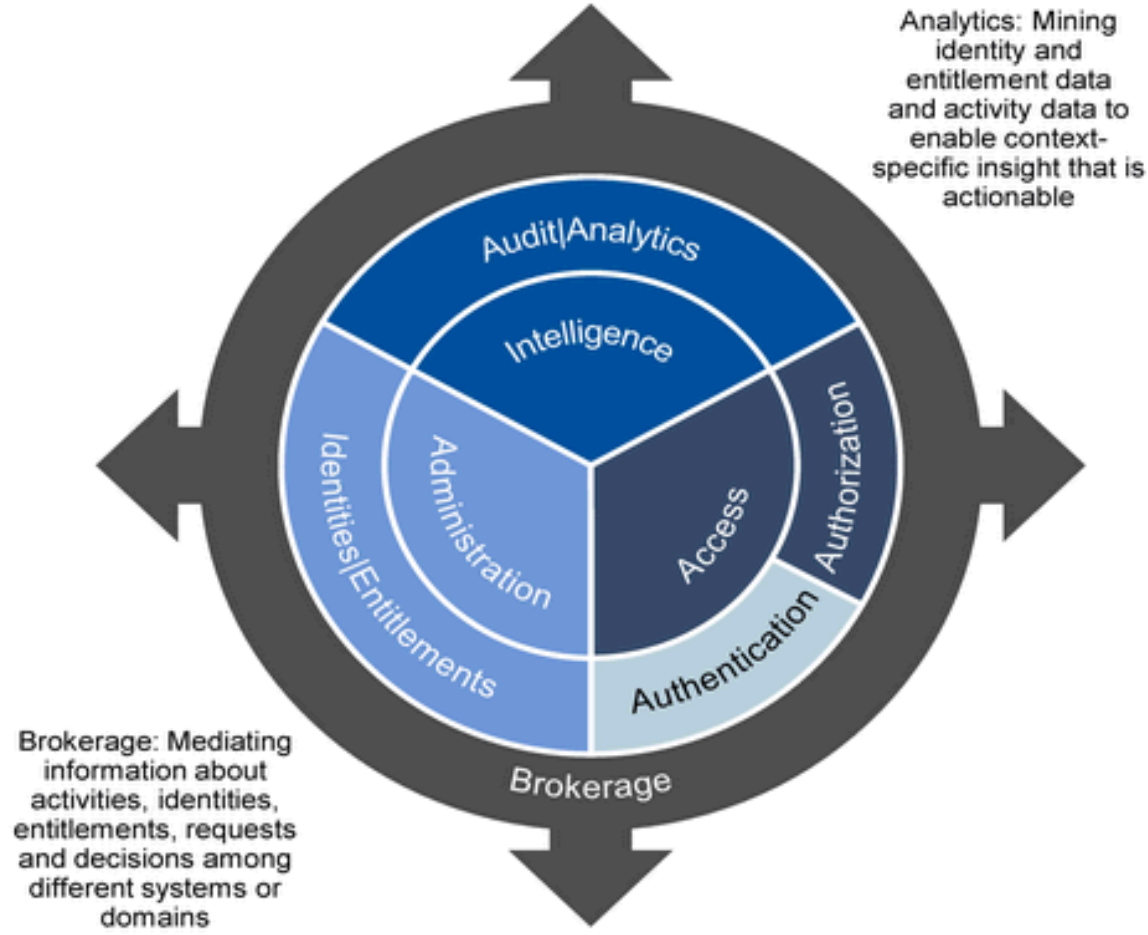
IAM är ett paraplybegrepp för produkter och teknologier som möjliggör hantering och styrning av användares digitala identitet och deras åtkomst till olika system. Gartner beskriver i korthet IAM på det här sättet:
Key issue: ”How will enterprise manage the complexity of authentication and access control in a highly distributed world?” (4 s. 6)
”Identity and access management is an information security, risk management and

business discipline with a broad range of benefits". (3 s. 2)
"IAM provides a viable, structured and coherent apporach to the management of users identities and access to applications, data and so on". (3 s. 2)
"IAM can be viewed as a set of complex functions that manipulate or consume three kinds od data: identity, entitlement and activity data". (3 s. 2)
"In short, IAM ensures the right people get access to the right resources at the right times for the right reasons" (3 s. 2)
Identitetsdata beskriver en fysisk persons digitala identitet i olika system såsom kontouppgifter eller profildata, användarnamn och lösenord. *Entitlement data* – behörighetsinformation beskriver vilka rättigheter en användare har gentemot ett system. Aktivitetsdata sparas i någon form av logg och skapas då användaren söker åtkomst till ett system och nekas eller beviljas samt då behörighetsinformation eller identitetsdata förändras. Funktioner och processer som ryms inom IAM kan grupperas in under antingen identitetshantering eller åtkomsthantering, det finns dock en viss överlappning (se Figur 3). Ett sätt att vidare gruppera in funktionalitet under dessa två är enligt (Figur 3) nedan – Administer, Audit, Authenticate och Authorize (4).



Figur 3 (4). Uppdelning av IAM

En senare gruppering av Gartner (3) grupperar in funktionaliteten under *administration*, *access and intelligence* (Figur 4). *Intelligence* inkluderar granskning (*audit)* men är ett vidare begrepp som även inkluderar analys - Business Intelligence med identitets-/accessdata. *Access* får agera paraply för både autentisering och auktorisering.



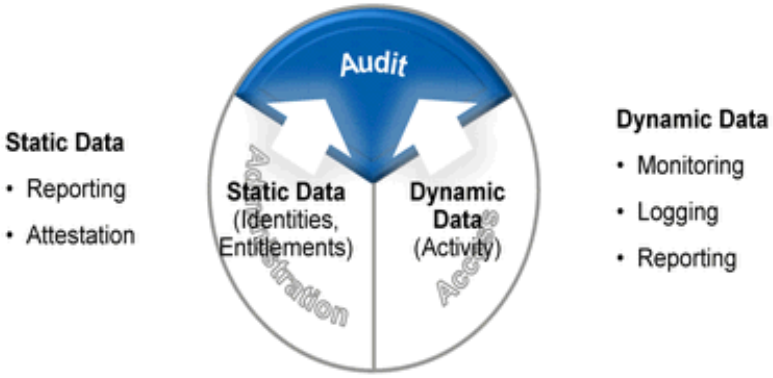
Figur 4. (5). Övergripande uppdelning av IAM

Under administration hanteras skapandet, ändrandet och inaktiveringen av identitets- och användardata som styr tillgången till och rättigheten i olika system (Figur 5). Även andra attribut kan vara knutna till en identitet beroende på vilken användardata, till exempel telefonnummer eller position, man väljer att hantera från IAM-systemet. Vilken information som skall hanteras var och hur och vilket system som äger så

Figur 5. (3). Administrationsdelen av IAM

kallad master-data om användaren bör vara definierat i någon form av styrdokument där ett företag som implementerar IAM beskriver sin strategi. Under *Credentials* bestäms den flora av lösenord som är kopplad till en identitet, i optimala fall bara en, och även de regler som bestämmer giltighetstid och komplexitets-krav på lösenord. Roller används som ett verktyg att gruppera ihop en uppsättning av olika rättigheter. Ett exempel på en roll skulle kunna vara s*tandard-användare* som definierar tillgång till 5 mappar, 2 servrar och 10 system som alla användare behöver tillgång till i sitt dagliga arbete.

Företag som implementerar *access management* får en motor som sköter all autentisering och auktorisering. Motorn svarar på anropande systems fråga om en given användare som försöker att ansluta eller nyttja vissa resurser skall beviljas detta. Autentiseringsdelen är den del som verifierar en användares identitet, att användaren är den som den utger sig för att vara - oftast genom kontroll av användarnamn och lösenord. Auktoriseringsdelen kontrollerar och svarar på om användaren har rätt behörighet (3).



Figur 6. (3) Intelligence / granskningsdelen av IAM

Intelligence-delen av en IAM-lösning ger möjlighet att ta rapporter och hitta olika typer av mönster från både statisk och dynamisk data (Figur 6). Syftet är att säkerställa att enbart behöriga har åtkomst till vissa resurser. Besvarar frågorna ”vem kan göra något”, ”vem gjorde något” och ”när och hur gjordes något”.

Utöver dessa tre finns även en fjärde kategori – katalogtjänster. Dessa fungerar som ett fundament som stödjer de andra tre. Katalogtjänsten agerar lagringstjänst för data kring identitet, olika regler och policys (5). Microsofts *active directory* är ett exempel på en väletablerad katalogtjänst ute hos företag.

3.3 IAM’s ingående delar

IAM är som tidigare nämnt ett paraplybegrepp för olika funktioner och teknologier. IAM-verktyg är de olika mjukvarulösningar genom vilka IAM implementeras, vissa av dessa kan fungera som mellanhänder som knyter ihop olika system eller olika delar av en IAM-lösning. VI kommer nu att lista och kort beskriva några av de verktyg som återfinns under de olika IAM-kategorierna. Det finns en viss överlappning i funktionalitet i vissa av verktygen.

3.3.1 Intelligence

Handlar i huvudsak om *business-intelligence* för IAM, att kunna få ut data som ger svar på frågor om verksamheten. I huvudsak ingår insamlande, analys, utvärdering, rapportering och stöd för regelbaserade beslut från identitetsdata. Dessa data skall hjälpa till att mäta, hantera och optimera informationssäkerhet och se till så att IAM-lösningen lever upp till och levererar affärsnytta. SIEM –"Security information and event management", SOD –"Segregation of duties"-controls och "Audit and compliance reporting tools" är några av verktygen. SIEM ger stöd för logghantering, loggarna innehåller data som ger svar på ifall krav från olika regler och lagar, till exempel från revisorer, uppfylls. Utöver detta skall SIEM även kunna hantera interna hot och övervakning av användandet av interna resurser i realtid. SOD controls är verktyg som upptäcker och sköter situationer där olika rättighetsinställningar påverkar och möjligen upphäver varandra. Den sista kategorin är olika former av rapportverktyg som använder loggdata som hämtats in av SIEM.

3.3.2 Administration

Verktyg för hantering av identiteter, listas nedan:

- Identities, Roles & Access policies (rules and entitlements)
- User provisioning
- Role life cycle management
- User self-service
- Active Directory – Unix bridge (5)

Identiteter, roller och åtkomstregler ger detaljerad styrning över skapandet, ändrandet och raderandet av rättigheterna till olika resurser. Verktygen här syftar till att definiera olika behörighetsdata.

User provisioning (Figur 7) ansvarar för att med automatik skapa, styra och hantera flöden av identitetsdata mellan olika system. När en användares identitet har skapats är de dessa verktyg som förser andra system med användradata. De ser även till att informationen är synkroniserad och hålls uppdaterad. De används i regel för att administrera interna användare. Stöd för olika typer av *workflows*, delegerad administration och lösenordshantering är ofta inkluderat. Dessa verktygs ansvar är således att administrera en användares identitet över dess så kallade livscykel vilken beskriver alla de faser som en identitet går igenom – skapande, förändrande och upphörande. Dessa faser motsvaras i IAM-domänspråket för dessa verktyg av orden

Figur 7. (12). User provisioning, de olika stadier en identitet kan befinna sig i.

provisioning, reprovisioning och *deprovisioning* vilket visas av bilden nedan.

Role life cycle management har funktioner för att automatiskt hitta roller genom att analysera de behörigheter som är definierade för diverse identiteter. Hela livscykeln av roller underhålls - bland annat ägare av en roll, förändringar av rollerna, roll och behörighetstilldelning, rapportering av rollanvändning etcetera. Rollhanteringen är ett mycket kraftfullt sätt att tilldela och hantera behörigheter på ett smidigt sätt.

Self-service syftar till att ge användarna olika sätt att få hjälp utan att det behöver belasta support- eller IT-avdelning. Vanliga tjänster är olika sätt för användaren att själv kunna återställa sitt lösenord samt att efterfråga åtkomst till olika system och resurser. Godkänns dessa förfrågningar ser *user-provisioning* till att automatiskt återställa lösenordet i alla påverkade system eller att ge utökad behörighet. Minskad kostnad för help-desk och minskade ledtider ger en ökad produktivitet och dessutom nöjda användare.

Active directory – unix bridge ger möjlighet för system i Unix, Linux och Mac att autentisera användare gentemot Microsofts Active Directory.

3.3.3 Access – Authentication

Verifierar i realtid äktheten hos en hävdad identitet. Kontroll av lösenord är fortfarande den vanligaste metoden för denna kontroll. Autentisering är en process som ofta körs via ett system som agerar mellanhand.

ESSO – enterprise single sign-on, möjliggör att användaren autentiserar sig en gång mot en autentiseringstjänst och blir sedan automatiskt autentiserad mot övriga system eller resurser när dessa nyttjas.

Password-propagation. Samma lösenord i alla system, ”ful-variant” till ESSO.

Federated Identity Management. Identitetsattribut kan delas mellan olika betrodda domäner vilket ger möjligheten att autentisera en identitet utanför den miljö och domän där den ligger lagrad. Ett exempel på detta är att autentisera mot ett företags interna katalogtjänst active directory från en molntjänst genom *Active Directory Federation Services* som då agerar mellanhand.

User-Centric Identity Frameworks. Ramverk som ger användare möjlighet att kontrollera hur deras identiet kan delas vid registrering av online-tjänster (5).

3.3.4 Access – Authorization

Entitlement management. Findetaljerad och precis behörighetsstyrning till tänkta målssytem med central hantering av övergripande policies. Ingår i *entitle life cycle management* som även inkluderar *role life cycle management*.

WAM – Web access management. Teknologin Web Access Management bistår med att hjälpa företaget att kontrollera vem som har tillgång till vilka webportaler och kan samtidigt erbjuda SSO till dessa. Arkitekturen bakom en WAM-teknik består oftast av en policy-server, policy-lagring och webagenter som kontrollerar åtkomst.
Åtkomst till portalerna sker via inloggning på till exempel ett AD och sedan genom att använda samma inloggningsuppgifter i WAM-agenten, som är en slags huvudportal för vidare åtkomst till de andra portalerna som användaren ska få tillgång till (5).

Enligt Gartner (5) är följande IAM-delar de vanligaste och mest använda:

- User provisioning
- ESSO
- WAM
- Identity Intelligence and SIEM
- Role life cycle management
- Directory services
- AD-Unix bridge

Ovan är alltså de vanligaste IAM-tekniker som införs på ett företag (5), men vilka motiv och orsaker ligger bakom ett IAM-projekt – det skall vi nu titta lite närmare på.

3.4 Drivkrafter som motiverar införande av IAM

Enligt IT Security Standard - IST (6) (6), en online-resurs specialiserad på säkerhetsstandarder inom IT, visar en refererad undersökning (7) att 93% av de tillfrågade företagen inte trodde att uppsagda före detta anställda medarbetare var en säkerhetsrisk. Cert visar i en undersökning att detta är en mycket farlig och potentiellt kostsam inställning. Vidare kände inte drygt hälften av företagen till vilka rättigheter dessa uppsagda anställda hade inom olika system. Fokus för säkerheten låg på de nuvarande anställda och man hade glömt eller ignorerat tidigare anställda (8). IST hävdar utifrån resultatet av annan studie att en orsak till detta är svårigheten att hantera tillgång till och rättigheter i informationssystemen. Det bör inflikas att studierna rör företag i ”enterprise”-storlek. Man menar fortsatt att datastöld av missnöjda eller giriga anställda är ett problem som måste hanteras.

En av forskarna resonerar att medvetenheten kring behovet av informationssäkerhet inte har hängt med i teknikutvecklingens explosiva takt samt att komplexiteten i moderna IT-miljöer ökar svårighetsgraden för ett lyckat informationssäkerhetsarbete.

“For the last two decades we have increasingly digitalized all sorts of information, from intellectual property to client details. Quick access and reproduction of information has increased productivity, but exposed companies to risks of noncompliance and IP theft. Accessibility to information has been fueled largely by technological innovation. This happened so fast that few have taken the time to think about the consequences in terms of IP and data security”. (6 s. 2)

“On top of this general trend we can recognize additional difficulties in protecting information. IT architectures have grown large, heterogeneous, and complex." (6 s. 2)

“Achieving a good level of information protection will require a combination of organizational and ethical initiatives, simplified IT architectures and management attention.” (6 s. 2)

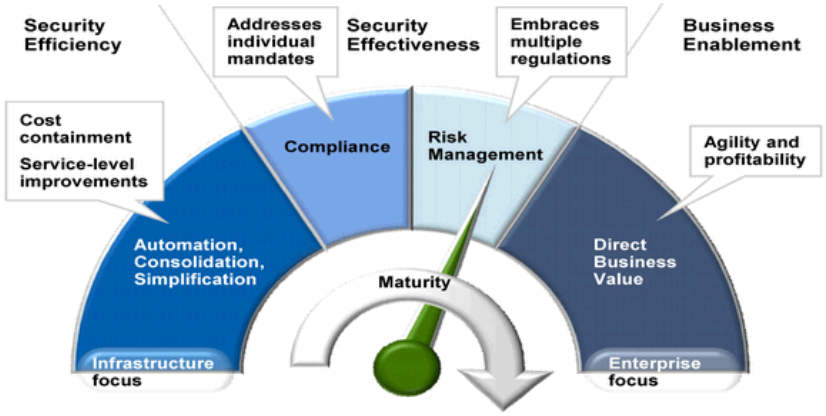
Den ökade informationssäkerhetsrisken påstås bero på resursbrist vad gäller budget och antalet anställda inom IT men även inkonsekvent hanterande av användares systemrättigheter. Studien ”2010 Access Governance Trends Survey” (9) kommer i huvudsak fram till att:

- Användares tillgång till olika informationssystem administreras fortfarande dåligt
- Organisationer klarar inte att hålla jämn takt med förändringarna av anställdas ansvar

- Regelverk och policys och deras uppfyllande följs inte upp regelbundet
- Organisationen har för liten budget, resurser och personal för kontroll och styrning av tillgång till informationssystem
- Molnet kommer i framtiden att ha stor inverkan på styrningen av tillgången till informationssystem (9)

Gartner nämner i sin forskningsartikel (10) några olika drivkrafter som kan motivera företag att införa IAM (Figur 8, Figur 9)

- Business facilitation
- Cost containment
- Operational efficiency
- IT risk management
- Regulatory compliance (10)



Figur 8. (12). Visar de drivkrafter som finns för IAM.

Vi kommer nu att kort gå igenom och beskriva några av drivkrafterna (Figur 9) övergripande med några exempel.

3.4.1 Business facilitation

Innebär att med bibehållen säkerhet möjliggöra att kunder, partners och anställda ges enkel och snabb tillgång till intern företagsinformation. Några behov och orsaker som kan ligga bakom den här drivande faktorn är till exempel att möjliggöra och förenkla affärsprocesser.

Den här drivkraftens fokus är på att möjliggöra affärer genom att företaget är förberett på nya affärsmöjligheter och snabbt kan reagera på och ta till vara på dessa.

*Möjlighet till självregistrering***.** Behovet uppstår när antalet kunder blir 100-tals eller 1000-tals, då blir det till slut en omöjlighet att hantera detta manuellt; självregistrering flyttar den administrativa kostnaden till brukaren.

Portaler och personanpassade tjänster. Personanpassade tjänster kräver att användaren har ett konto som används vid autentisering och auktorisering. Detta konto hanteras lämpligen av och i en IAM-lösning.

Outsourcing. Att lägga ut till exempel support på entreprenad kräver att dessa ges tillgång till interna resurser.

Dessa tre är exempel på situationer där företag, om de implementerar IAM, får möjlighet att ta till vara stora kundinströmningar eller snabbt byta och ansluta en ny leverantör till sina interna resurser (10).

3.4.2 Cost containment

Drivkraften att få mindre kostnader för hanteringen kring säkerhet och användarkonton.

Minska behovet av personal. Behovet av personal inom support, systemadministration och säkerhetsadministration, som hanterar förfrågningar från

användare om tillgång till system och lösenordsfrågor, minskar.

Gemensam IAM arkitektur. En standardiserad infrastruktur för autentisering och auktorisering förenklar integrationen av och säkerheten i internutvecklade applikationer (10)**.**

3.4.3 Operational efficiency

Är detta den drivande faktorn, är företaget ute efter minskade ledtider för åtkomstbaserade frågor från användare och att mindre tid skall behöva spenderas för att administrera olika rättigheter. Företaget önskar nå en ökad effektivitet i den operationella nivån av organisationen.

Förbättrade SLA – Service Level Agreement. Det tar mindre tid att svara på en förfrågan om systemtillgång, det är möjligt att nå ned till en ledtid på max ett dygn. Detta är näst intill omöjligt utan de verktyg som finns i en IAM-lösning. För en nyanställd som behöver tillgång till många system minskas ledtiden radikalt då kontoskapande i olika system automatiseras.

Förbättrad produktivitet. En anställd eller en partner som behöver tillgång kan börja jobba snabbare – mindre dötid. Ledtiden för godkännande av systemtillgång, vilket kan kräva beslut eller godkännande av chef eller informationsägare, kan minskas genom användandet av speciella attesteringsfunktioner i IAM-lösningar. Möjligheten för användare att själv byta och återställa lösenord utan att kontakta support minskar användarens nertid - den tid som den anställde inte kan arbeta.

Användarnöjdhet. Lösenordshantering, möjlighet till självbetjäning samt single sign-on skapar nöjdare användare.

Rapportering. Förenklas och snabbas upp då identitetsdata hanteras centralt (10).

3.4.4 IT risk management

Kraven att hantera risker inom IT genom att kunna påvisa uppnådda säkerhetskrav, både interna och externa kan också vara orsak till att IAM-lösningar undersöks. Alla lösningar inom IAM förutom SSO bidrar till en ökad säkerhetsnivå.

Granskning (eng.- audit). Att snabbt och korrekt kunna granska systemtillgång sparar pengar för revisorer, chefer och systemadministratörer.

Uppsägningar. Att omedelbart genom automatik kunna spärra en uppsagd medarbetares tillgång till system minskar risken för informationsstöld eller sabotage. Utan ett livscykelflöde för användares rättighet – där inaktiveringen av rättigheter sker manuellt - är risken överhängande att något system fortfarande har kvar användarkonto för den uppsagde.

Uppfyllande av regelverk. IAM-lösningar ser till att upprätthålla regler för lösenord, roller, åtkomster et cetera.

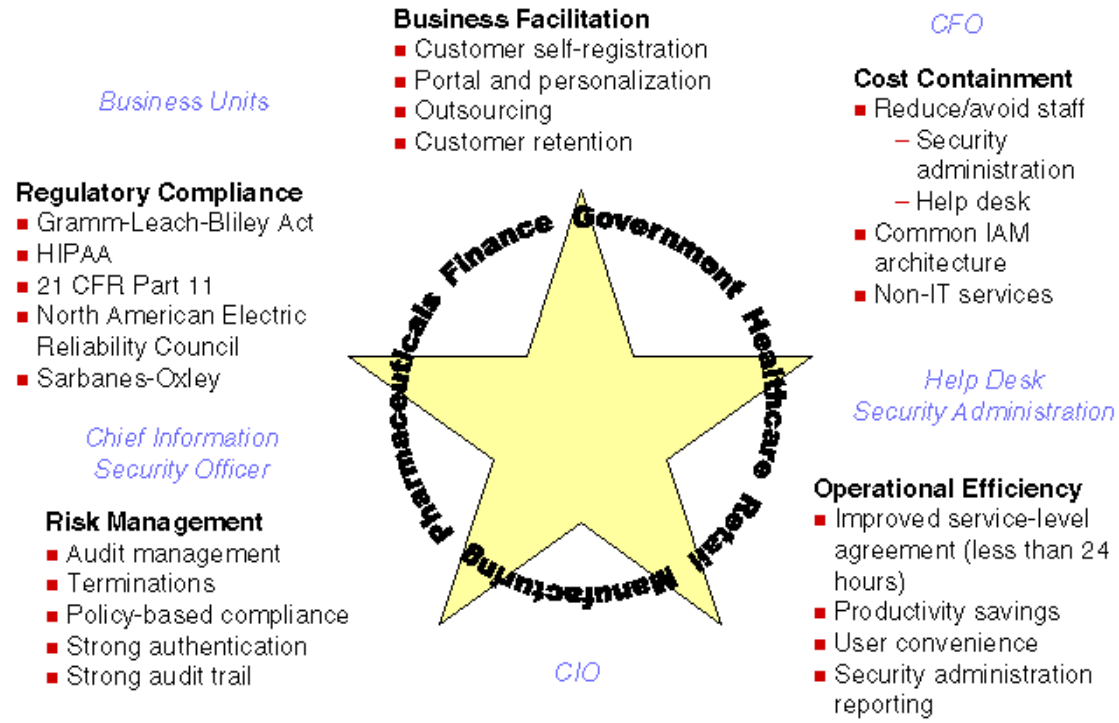
Kraftfull spårning (eng- strong audit trail) och *starka autentiseringsmetoder* är IAM-funktioner som minskar IT-relaterade risker (10).

3.4.5 Regulatory compliance

Regelverk och lagar från utomstående kravställare, till exempel myndigheter och revisorer, kan kräva säkerhet i form av infrastruktur som reglerar information och systemåtkomst. Drivkraften är att det föreligger krav för uppfyllande av dessa regler. SOX är mycket vanligt då handel sker med amerikanska bolag.

PUL – personuppgiftslagen, en lag som reglerar hanteringen av personuppgifter – är ett exempel på en svensk lag, granskande myndighet eller revisor kan av företag kräva bevis för uppfyllande. Detta förenklas av de starka rapporteringsmöjligheter som

IAM inrymmer.



Figur 9 (10). Bilden visar drivkrafterna för IAM och vilka intressenter dessa har.

3.5 Koppling mellan drivkrafter och IAM-funktioner

Det finns en korrelation mellan vilka drivkrafter som agerar som motorer i en upphandling av IAM och de IAM-funktioner som utväljs för implementering (Tabell 1). Drivkrafterna kan likställas med organisatoriska mål som uppnås med hjälp av funktionerna i IAM-lösningar. Valet av funktioner som införs beror på vilka drivkrafter eller organisatoriska mål som väger tungt i ett företags IAM-projekt.

Tabell 1. Visar för vilka drivkrafter respektive IAM-verktyg är relevant (10).

IAM Business Drivers and Components					
	Business Facilitation	Cost Containment	Operational Efficiency	IT Risk Management	Regulatory Compliance
Authentication Services	X	X		X	X
Enterprise Single Sign-On	X	X	X		
Password Management	X	X	X	X	X
User Provisioning, Metadirectory, Identity Administration	X	X	X	X	X
Operating-System Security				X	X
Database Security				X	X
Extranet Access Management, Identity Administration	X	X	X	X	X

3.6 Förutsättningar för en lyckad IAM-satsning

IAM-system har en stor kostnad förknippad med sig, mjukvarulicenserna är relativt dyra och implementationen är en komplicerad och tidskrävande process. Komplexiteten beror på mängden system och integrationen dessa kräver samt de organisationsförändringar som ofta krävs då system, bland annat genom automatisering, skall effektivisera delar av verksamheten. För att lyckas med IAM-programmet – att få ut affärsnyttan av IAM- och förhindra att kostnaden blir för hög måste vissa kriterier uppfyllas.

Forskningen (11) hävdar att den största anledningen till varför IAM-program misslyckas är att organisationen planerar otillräckligt och inte förstår vad de vill eller behöver åstadkomma. I planeringsstadiet måste IAM-programmets mål, strategi, intressenter och övergripande planering definieras. Att sätta upp ett mål – en vision för

vad som skall åstadkommas – är nödvändigt innan organisationen försöker nå ett mål. Föregående beskriver alltså devisen – *vet man inte vart man vill, vet man inte var man hamnar.*
”Having a vision is what begins the process of IAM program planning. And, without planning, one can only reasonably expect failure” (11 s. 4)
Visionen måste utvecklas med koppling till IAM-teknologi och verksamhetens behov. En metodiskt utförd undersökning och utvärdering av verksamhetens behov måste alltså finnas till hands. Visionen behöver vidare förankras och kommuniceras inom organisationen.
Några frågor som kan stödja utvecklandet av en vision:

- Vad är fel med sättet vi idag hanterar identiteter och rättigheter?
- Vilka är de huvudsakliga målen och drivkrafterna?
- Vilka IAM-koncept eller teknologier kan förändra det sätt vi arbetar
- Vad är vårt framtida önskvärda tillstånd, hur skiljer det sig från dagens och varför är det bättre?
- Vilka delar av organisationen kan vara intresserade?
  (11)

3.7 Gartners slutsatser för IAM-satsningar

- Develop long-term (that is, three-year) goals related to how IAM can meet organizational technical and business needs. (12 s. 3)
- Research and be able to articulate the drivers and benefits of an IAM program across multiple divisions of your organization. (12 s. 1)
- Formulate a compelling vision for your IAM program. (12 s. 1)
- Your IAM plan should be less about specific technologies and more about business objectives. (11 s. 1)
- Your IAM plans and goals should seek to address needs/wants expressed by multiple departments within the organization (not just IT or security). (11 s. 1)
- Treating IAM as a process unifies the main functional categories of IAM: access, administration and intelligence for planning, deployment and operations. (13 s. 1)
- Most enterprises approach IAM the wrong way — by working with production requirements first. IAM process requirements should always precede organization and technology decisions. (13 s. 1)
- Create an IAM steering committee. (12 s. 4)
- Formulate a communications and cross-division relationship creation/management strategy. (12 s. 4)

Ett lyckat IAM-program kan medföra många positiva effekter, tyvärr kan få av dessa enkelt kvantifieras ekonomiskt, vilket försvårar skapandet av investeringsunderlag och ROI-kalkyl.
“Deriving direct monetized benefits from IAM programs remains a heated topic. Although there are published examples on how to save money and time with core IAM functions (such as password reset/management), clear financial returns for broader, more complex solutions in administration and intelligence remain elusive.” (14 s. 4)

3.8 Sammanfattning av litteraturstudie

- IAM är system för administration och styrning, granskning och uppföljning av användares identitet och systemåtkomst.
- IAM ger en ökad säkerhetsnivå, där riskerna för ekonomisk skada genom felaktig informationstillgång minimeras.
- IAM sänker - genom automatisering, flexibel styrning, central hantering och övergripande regler - kostnaden och ledtiden för hantering av användares tillgång till system
- IAM sänker kostnaden för och möjliggör kontroll och uppfyllande av interna och externa regelverk genom utförlig loggning och flexibel rapportering
- IAM ökar nöjdhet och produktivitet för användare genom olika självbetjäningstjänster
- Vanliga drivkrafter för att införa IAM är att få minskade kostnader, ökad effektivitet, förbättrad säkerhet och riskhantering samt uppfyllande av regelverk
- Ett lyckat IAM-program kräver en ordentlig utredning av verksamhetsbehov och drivkrafter i berörda delar av organisationen samt en tydlig vision som är väl förankrad och kommunicerad.
- IAM-programmets styrgrupp måste definiera mål, strategi, intressenter samt skapa en plan för förverkligande.

4 Empirisk undersökning

Frågorna till de olika nyckelpersonerna på företagen föregicks av en slags förstudie/frågefokusering som Säljaren hjälpte oss med. Vi baserade våra frågor på litteratur och studier och intervjuade leverantören i syfte att utforska intressanta frågor och tankeställningar. Leverantören arbetar med att skapa bakgrunden till deras IAM-lösningar och har gjort detta i 10 år.

4.1 Leverantör

Drivkrafter
Säljaren framhåller att det i första hand handlar om att företag lägger stora summor pengar på att administrera användarkonton. Företagen känner att de inte har någon kontroll på kostnaden och användarna uttrycker sitt missnöje med att inte få tillgång till resurser och applikationer inom en rimlig tid. Andelen *orphan accounts* ett företag har kan också motivera införandet av IAM.
”…vilket innebär att det är ju inte helt ovanligt att man i ett företag med tusen anställda har femhundra orphan accounts…”
Det kan även vara en nyanställd med erfarenhet från andra ställen där en IAM-lösning har löst processproblem som kommit med idéer. Det kan även bero på att företagen har krav på sig från en revisionsmyndighet. Ett sådant krav kan vara att företaget ska kunna visa på vem som har access till vilka resurser. Vidare berättar han att mer sällan ligger en tekniktanke bakom, till exempel att företaget vill ha SSO till sina användare. Han tar ett exempel med Företag X som vill undvika SOX-kraven som finns i USA och därför har bojkottat den marknaden helt. Däremot så har de krav från svensk bolagskod att kunna visa vem som har tillgång till olika resurser. Han berättar om ett annat exempel med Lunds Universitet (LU) där de valt att implementera en Open Source-lösning för att hantera användarkonton. I den tillväxttakten de har så kan inte Open Source-lösningen bistå med lösning på med de krav LU har fått från nya lagar och regler. Att byta en IAM-lösning menar respondenten är väldigt svårt.

För att en IAM-lösning ska löna sig så behöver företaget ha minst 1000 användare, riktig lönsamhet uppnår man vid 3-4000 användare.Ett företag med ordning och reda på sina användarkonton uppnår direkt en säkrare miljö då mängden användarkonton utan ägare kan minskas.

Implementation
Leverantören berättar att det som alla kunder vill ha med är Active Directory(AD) koppling. HR-systemkoppling är också en vanlig förfrågan. Kunder vill ha processen med att skapa en ny användare automatiserad. Att kunna skriva in användarens uppgifter i ett gränssnitt och så skapas inlogg, mail, partitioner på nätverkshårddiskar, tillgång och ibland även automatisk installation av applikationer. Vidare efterfrågas även koppling till något av deras egna system. Detta kan till exempel vara ett affärssystem eller ekonomisystem.

Angående de funktioner som implementeras, så sätter sig leverantören med kunden och gör en road map. I denna finns projektledare från det aktuella företaget med och där bestäms hur arbetet kommer att fortgå. Ofta vill kunden vara med, med egen teknisk expertis, men det slutar ofta med att leverantören får en supportroll.
SSO är mindre vanligt att man inför även om det för företaget är en dröm. Han berättar

ett exempel där en organisation för krishantering hade 9 olika system där tiden för att logga in på de systemen som behövdes, i en sådan situation, var helt orimlig. Där infördes SSO och ett växlingssystem för användarsessioner.

Han nämner vidare att en användare som inte innehar en kritisk roll ofta inte har något emot att logga in på 2-3 olika system. Ibland så övertygas företaget att implementera SSO på vissa delar, då det ger ett handfast bevis på att Säljaren har gjort något. Oftast är det som implementeras osynligt för vanliga användare.

Ofta implementeras en web-SSO så att kunder med olika login till olika portaler slipper logga in flera gånger. Fördelen är att man med en SSO ofta får med en password-reset-funktion.

4.2 Företag 1

Bakgrund
Inom produktionsdelarna av koncernen används IDM (identity management) av runt 11000 idag men beräknas inom en snar framtid nå 15000. Företaget har cirka 30000 anställda inom produktion. Inom Sales&Service bolag (filialer eller helägda) finns 30000 till.

Företag 1 har cirka 800 IT-system, många har circa 5-15 användare, 400 lite större applikationer har cirka 50 användare. Företaget har ett helägt dotterbolag som levererar deras IT, dotterbolaget tar emot och effektuerar beställningar på IT, till exempel ny användare.

Respondenten är förvaltningsansvarig för IDM-lösningen på Företag 1. När diskussioner om IAM började föras ansåg Företag 1 det lämpligt att försöka ta ett holistiskt grepp om IAM, de startade därför upp ett IAM-program. Dess syfte och uppgift var att skapa en strategi för IAM - hur företaget skulle gå till väga, definiera långsiktiga mål, bestämma vilka delar av koncernen som skulle inkluderas med mera. Inom det här programmet skapades ett ramverk som definierade vad IAM var för Företag 1 och vilka funktioner och komponenter inom IAM som var relevant.

De tankar och idéer som så småningom mynnade ut i ett IAM-program kom från avdelningen ansvarig för access control, deras huvudsakliga uppgift är att hantera anställdas tillgång till olika IT-resurser. Vår respondent var teamleader för den här avdelningen, han berättar *”Jag hade sett ett behov där för vi mäktade inte med mer manuell hantering”*. Både vår respondent och andra inom företagets IT-avdelning hade börjat nysta i problematiken kring den manuella hanteringen. Frågan landade tillslut hos IT-staben på koncernnivå och de tog på sig ägarskap och finansieringsansvar för det projekt som skapades för att lösa problematiken. Initiativtagare och sponsor för projekten återfanns alltså på koncernnivå.

Respondenten blev övergripande projektledare för hela satsningen med uppgiften att uppnå de mål som sattes upp i och med IAM-programmet. Den mängd aktiviteter och projekt som då sattes igång inkluderade bland annat en förstudie och en jämförelse av de olika produkter för IAM som fanns på marknaden. I förstudien gjordes en kartläggning av processerna kring användaridentiteter, förbättringspotentialen för dessa undersöktes, mappning av dessa mot IAM-området gjordes samt en undersökning om hur processerna kunde förbättras med hjälp av IAM-verktyg. Den påföljande upphandlingen inkluderade aktiviteter som kravställning mot leverantör, offertutvärdering och val av leverantör.

Drivkrafter
Vår respondent berättar att ”*Inom Företag 1 pratar vi mycket om ordning och reda”*. Kontrasten var stor mellan det som eftersträvades i form av ordning och reda och hur det faktiskt låg till med hanteringen kring anställdas digitala identiteter. Några brister nämndes kort:

- Det fanns många inaktiva användare.
- Rättigheter togs inte bort när en anställd bytte avdelning.
- Användare togs inte bort när en anställd slutade på företaget.
- Dålig kvalitet på användarinformation (felaktig).
- Långa ledtider.

Vidare fanns ingen central kontroll över anställdas IT-identiteter vilket försvårade överblicken av problemets omfattning.
”För att ge nån övergripande bild så kan vi säga som så att vi hade en process när det gällde att beställa och administrera användare som var totalt manuell egentligen.”

För att skapa en användare krävdes användning av många olika system. Utöver detta skedde den nödvändiga kontrollen mot informationsägare, av anställdas behörighet, vid ansökan om systemrättigheter, helt manuellt.

Ett exempel ges för att illustrera vilka effekter detta hade: *”Skulle man ha åtkomst tex till någon delad folder på en windows server eller liknande eh…så kunde det ta ..det tog faktiskt minst 5 dagar”.*

Exemplet ovan avser redan anställd användare vid efterfrågan av åtkomst till en resurs. Den totala tid som förflyter innan fullständiga rättigheter erhållits är linjär i förhållande till antalet resurser som efterfrågas; för nyanställda får detta stora konsekvenser. På frågan om hur lång tid det tar för en nyanställd att få tillgång till alla de system denne behöver för att arbeta svarar han:
”Ja cirka 5 dagar tills man hade ett användarkonto över huvudtaget. Eh… och det fanns inga egentliga mallar eller roller så att man fick någorlunda hyfsad uppsättning rättigheter heller utan det följdes nog i snitt av ytterligare en 3-5 beställningar där man tillslut hade kompletterat upp sin skörd av rättigheter i olika system då.”

Ledtiden för att leverera en nyanställds flora av rättigheter landar alltså totalt på runt en månad. Kvaliteten på användarinformation nämner vår respondent som en annan utmaning. ”*När IT-avdelningen i sitt helpdesk system tog upp en användare var det ofta felaktig information där, till exempel fel avdelningstillhörighet eller telefonnummer”.* Problematik fanns kring att hålla användares information uppdaterad och korrekt. Orsaken finner vi i de många system som innehöll information om användare, det var inte heller tydligt vilket system som ägde informationen. Vidare så uppdaterades inte alla system med ny information då ändring gjordes i ett system, att hålla information uppdaterad och därmed uppnå hög datakvalitet krävde således en tidsödande manuell hantering.

Ett krav från revisorerna var en regelbunden så kallad *access-review* process där användares rättigheter till system och resurser granskades - vem har tillgång till vilka system. Uppföljningen gjordes varje år och processen var även här till största delen manuell.
”Nån går in i ett system och tar någon print-screen eller gör nån export av information och klistrar in i excel och så skickas det runt till informationsägare, chefer och allt vad det kan vara för nåt. En helt vansinning och framförallt tidskrävande process.”

Den affärsprocess Företag 1 såg mest vinst i att implementera var livscykelhantering av användare, att kunna skapa, uppdatera och ta bort användare på ett kontrollerat sätt. Någon formaliserad livscykelhanteringsprocess fanns inte, Företag 1 hade enbart en process för att efterfråga rättigheter kallad ”*access ordering process*”.

Under undersökningsfasen utvärderade Företag 1 rollhantering i stor skala, livscykelhantering av roller samt hur de skulle få verksamheten att nyttja IAM och därmed realisera lösningens affärsnytta. Utöver dessa funktioner utforskades även säkerhetsrelaterade bitar som ”*auditing*” (granskning) och loggning och hur dessa skulle kunna hanteras centralt, med syfte att öka spårbarhet och säkerhet och smidigare kunna tillmötesgå revisorskrav.

Resultaten av den utförda förstudien gav insikten att som fundament för en IAM-lösning på Företag 1 krävs en produkt i botten som skötte *”identity management”* - IDM.

IDM var en förutsättning för ”*access management*”, ”*role management*”, ”*auditing*” och logghantering.
Krav på lösningen var utöver livscykelhantering av användare möjlighet till verktyg för loggningshantering, granskning och rapporter – *SIEM.*

Implementation
Företag 1 valde att implementera följande funktioner:

- User roles
- User provisioning
- User self-service
- Password propagation
- AD-Unix brigde

Dessa funktioner grupperas under IAM i huvudsak in under *Identity management*, Microsofts *Active Directory* används som katalogtjänst.
Varken *SIEM (Security Information and Event Management)* eller *ESSO* (Enterprise Single Sign-On) är implementerat men båda finns med i en road-map för framtiden.
”…vi har skapat förutsättningar, i och med att vi har ordning och reda på användaren, för att kunna ha både SIEM-lösning och SSO”.

Det finns alltså ingen implementerad helhetslösning för säkerhetsrapportering men – *”…viss loggning och auditing [finns] i vår IDM-implementation, vi kan se vem som tilldelade vissa rättigheter och när….”*.
I nuläget så är inte *WAM (Web Access Management)* implementerat, däremot har de genom en annan lösning fått liknande funktionalitet. En separat IDM-produkt används för att ge externa användare, till exempel personal ute på service-bolag, leverantörer och kunder tillgång till vissa applikationer som är publicerade ut mot internet. Åtkomsten sker genom speciella web-portaler. Vår respondent berättar att ”*fler funktioner och projekt är på gång– den gångna finanskrisen medförde att IAM-projekten tillfälligt pausades.”*
”Det finns även en rolltilldelning, där användaren får en uppsättning rättigheter enligt en mall som tillhör rollen.”

Företag 1 jobbar både med något de kallar för business-roller, som är formade efter funktion eller verksamhet, och så kallade IT-roller där kraven specificeras hårdare.
”IT-roll här kan vara tex konton i en speciell miljö, eller en specifik uppsättning rättigheter för en administratör eller kanske bara medarbetare på en speciell avdelning”.

Några citat från vår respondent om IDM.
”Idag agerar IDM-lösningen spindeln i nätet vad gäller användarinformation, IDM ser till att rätt attribut är påklistrade på användaren”.
”IDM garanterar att informationen är uppdaterad och korrekt.”.
”…när användaren skapas så används IDM-verktyget och informationen tilldelas användaren med automatik till stor del”.
”…vi automatiserar hela livscykeln och då hämtar info från HR-system när det gäller anställda användare”.
”I och med att dom skapar användaren så kompletteras med automatik de mesta av informationen om användaren från HR-system”.
Spindeln i nätet och den automatisering som nämns löses av ”*user provisioning”*-verktyg, dessa ser till att information hämtas och skickas till rätt system. Hela livscykeln – skapande, uppdaterande och borttagning av användare sköts av dessa verktyg.

Den implementerade self-service-funktionen innebär för Företag 1 att användare kan själv återställa sina lösenord men även att via ett formaliserat och automatiserat flöde beställa tillgång till en IT-resurs till exempel mapp, intranät eller system. Företagets implementation av password propagation har genomförts genom att ca 10 av de största applikationerna är ombyggda så att de autentiserar med hjälp av information som de föds med från AD.

Implementationen har påverkat processer i hela företaget, däremot har inga nya tillkommit som en följd av IAM. Implementationen löpte över ett halvår men lösningen var inte färdig förrän efter 1.5 år. Respondenten återger att en mängd barnsjukdomar behövde åtgärdas innan miljön var mogen.

”Detta berodde bland annat på fintrimning av processen, icke identifierade fällor i processen – främst från HR. Det berodde också på organisationsförändringar som inte skedde som angivits i förstudien. Räkna alltså med en lång inkörningsperiod.”

En del utmaningar fanns, bland annat, som tidigare nämnda, från HR-avdelningen. Då mycket användarinformation ägs och styrs från HR krävdes vissa förändringar för att IAM-systemen skulle få rätt information med hög kvalitet i rätt tid. Anpassningsbehov uppkom, både från IAM mot HR och HR mot IAM; vissa rutiner har HR tvingats ändra och vissa IAM-funktioner har behövt specialanpassas.

”Eftersom vi automatiserar hela livscykeln och då hämtar info från HR-system när det gäller anställda användare…största utmaningen var … ta del av en HR-process…som innehöll en mängd olika….hur skall jag göra det här politiskt korrekt….många märkligheter.”

”… det var en hel del i HR-processen som krävde lite okonventionella lösningar från oss och lite work-arounds.”

Verksamhetseffekter

Effekter som IAM-lösningen gett är kortare ledtider och bättre datakvalitet. Ledtiden har kapats från 5 dagar till en timme vid beställning av åtkomst till IT-resurser. Vid beställning av en ny IT-användare finns merparten av de rättigheter som krävs för att kunna arbeta inom en timme. Möjlighet till självbetjäning, till exempel glömt lösenord eller åtkomst till en viss resurs. ”*Det är den största effekten för användaren – att de slipper efterfråga informationen eller rättigheten utan kan efterfråga det i ett system. Beställningsfunktionen för ny användare har inte påverkats nämnvärt; det skickas fortfarande ett mail men sedan så sköts mycket automatiskt när processen väl är igångsatt i vårt IDM-verktyg.”*

IDM-lösningen har även skapat förutsättningar för både SIEM och SSO.

”Säkerheten överlag har ökat (pga ordning och reda, systemstöd samt formaliserade processer).”

”Lösenordshanteringen för att återställa lösenord är visserligen challenge-response frågor, dessa är möjligen lätta att ta reda på svaren för. Men det är högre säkerhet än innan för då gick det att ringa help-desk, säga vem man var och få nytt lösenord över telefon.”

”Ur ett säkerhetsperspektiv så har vi idag enormt mycket bättre datakvalitet på vår användardata. Det är som dag och natt.”

En bieffekt som inte räknats med var att andra system började prenumerera på data från IDM. På grund av den höga datakvaliteten som fanns i IDM ledde detta till högre datakvalitet även i dessa system. IDM levererar alltså användarinformation som tjänst genom en utgående kö till andra system bland annat faktureringssystem, help

desk system, etcetera. Många system har inte en riktig integration mot IDM men använder sig av användaruppgifterna som IDM levererar.

Som en följd av implementationen har ägarskap kring information stramats upp. Ett exempel som gavs var att någon kunde ringa till help-desk och meddela att det är fel på informationen i någon applikation. ”*Tidigare så ändrade helpdesk i just det systemet, men idag är det källsystemet som har ansvar för att ha ordning och reda på sin datakvalitet.”* Idag är vissa system eller avdelningar ägare av attribut, HR äger till exempel namn, avdelningstillhörighet och kostnadsställe. ”*Vi kan ha ordning och reda genom hela processen och har ett tydligt ägandeskap av datat.”*

Utvärdering

”Vi har inte gjort en formell utvärdering av projektet utöver uppföljning av business-case. Det finns en referensgrupp som fångar in åsikter från slutanvändare, vi tror vi förstår bristerna och nyttan.”

I upphandlingen skapades ett business-case (investeringsunderlag) som inkluderade diverse mätpunkter. Dessa mätpunkter gav svar på till exempel ledtid för en viss process eller kostnad för en viss uppgift. Mätpunkterna mäts på innan implementering för att få en baseline och sen efter för att kunna jämföra och se vilka effekter som implementationen har fått. Företag 1 fick hjälp med att skapa detta business-case av Säljaren.

”Vi satte ju upp ett business-case egentligen där vi räknade på vilken payback vi skulle kunna få. Vi har ju även en self-service del i den här lösningen också. Hur mycket vi skulle kunna effektivisera och så satte vi en prislapp på det både när det gäller användningen av self-service, styra bort samtal från våra help-desk. Även automatiseringarna. Vi har uppnått målen till 75%. Vad gäller effekten av funktionaliteten så är den 100%.”

Varför Företag 1 inte uppnått målen till 100 % förklarar respondenten med att de inte har mäktat med samma utrullningstakt globalt som i Sverige.

Vår respondent berättar att det är svårt att sätta upp de här mätvärdena, att hitta rätt och relevanta mätvärden. I efterhand visade det sig att de mätvärdena de satt upp inte var så relevanta och att det inte var dessa de egentligen var ute efter. Andra positiva effekter var värda desto mer, som till exempel kundnöjdhet (alltså bolagets användare) som uppstår av self-service. ”*Väldigt svårt att sätta en prislapp på.* ”

”Det vi mätte på – hur mycket tjänar vi på att en användare byter lösenord själv istället för att ringa vår help-desk. Visst, det går ju att sätta en prislapp på det men byter lösenord gör man inte så hemskt mycket ändå. Man glömmer inte bort det så många gånger heller. Men visst används det och visst sparar vi in tid på det men saker som datakvaliteten det ser vi, och det är inte direkt mätbart och det ger betydligt bättre effekt för oss på Företag 1 och i ett längre perspektiv också.”

Företag 1 har räknat på ROI och har bedömt den till 3,5 år. Precisionen och relevansen som ligger till grund för kalkylen var däremot svårt att bedöma då ROI-beräkningen i huvudsak baseras på de mätvärden som formades när business-case dokumentet skapades; de var inte nöjda med sitt business-case. ”*Hade vi gjort business-case’et idag så hade det sett annorlunda ut. Svårt att hitta performance-indicators när vi byggde upp business-case’et.”*

En funktion som överraskade var möjligheten att tilldela roller.*”Rollhanteringen visade sig vara en oväntat användbar funktion – den har använts mycket mer än vad vi trodde vi skulle göra.”*

Användandet av lösenordsåterställning via challenge-response var även det något som överraskade. Det visade sig att bara 30 % hade registrerat frågorna som krävs för återställning, en låg siffra visserligen men stämde överens med den som kalkylerades med i business-case, men av dessa var det 30 % var 70 % som använde funktionen – en hög siffra. Lösenordsåterställningen används frekvent efter semestrar och julledighet.

Vår respondent berättar att en stor utmaning som de har är hur de skall kunna öka användningen av systemen i organisationen. Med så många system var IT-avdelningen rädd att det här skulle bli ytterligare ett system i mängden. "*Det fanns en rädsla för att IDM skulle bli ytterligare en grej i soppan, och så var det lite i början också*." IT-avdelningen har fört en massiv marknadsföringskampanj för att öka nyttjandegraden av IAM-lösningen men trots detta är det många som använder gamla arbetssätt och rutiner. *"Men vi har jobbat hårt på att kampanja, informera och kommunicera om den funktionaliteten – och det märker vi att det kommer vi behöva göra i all oändlighet."* Flyers, informationsträffar, gruppchefer som pushar på och försöker sälja in till användarna är några av de aktiviteterna som i slutändan inte gett så mycket resultat. Ett resonemang som förs låter oss förstå att det finns många faktorer som påverkar, bland annat att det finns olika kulturer inom företaget och att IT-användningen / mognaden är som natt och dag mellan olika delar av bolaget.
"De enda som har fått upp användningsgraden är när vi gör riktade utskick till slutanvändare själva. Och vi har bett varje gruppchef att ta upp det på informationsmöten och förklara vad det här är och pusha för det och sälja in det hos användarna. Och det är det enda som har gett resultat. Artikeln i interntidningen har gett ingenting."

Respondenten svarar jakande på påståendet att detta med den låga nyttjandegraden i huvudsak är ett decentraliseringsproblem; det finns för många självständiga affärsenheter som man inte kan påverka så hårt som man skulle vilja. *"Marknadsföringsbiten har faktiskt var tuff och tuffare än jag förväntat mig."*

4.3 Företag 2

Bakgrund
Företaget är en byggnadsentreprenör och finns i många olika länder. De är ca 55000 anställda. De har ca 300 system och ca 6000 användare av systemen. IAM-lösningen ligger på 11 servrar, administrerade av företaget själv.

I företaget så är IT fragmenterat ut från företaget och är en egen autonom enhet, dit även IT-staben flyttats. Projektet kom från affärssidan av företaget. Om IT hade startat projektet så hade det varit mer naturligt. IT-avdelningen fick en beställning från affärssidan att ordna med infrastruktur. Inget business-case gjordes men man tog fram lite mättal, bland annat på lösenordsåterställning, från support-avdelningen för att sedan kunna följa upp en framtida mätning gjord efter implementation. Respondenten jobbar som Informationssäkerhetschef och innehar rollen som ägare av deras IAM-lösning och har varit med sen starten av IAM-implementeringen 2006. Respondenten arbetar halvtid i Sverige och halvtid på den autonoma IT-enheten, som är ett dotterbolag till Företaget. För mig är IAM att varje person skall ha rätt åtkomst utifrån vad den ska nå för information berättar vår respondent.

På frågan om varför man inte försökte lyfta projektet så att det kördes och styrdes från en högre nivå i organisationen svarar respondenten att det handlar om företagets struktur. Dem är väldigt projektdriven och alla projekt konsolideras i olika affärsområden

som är autonoma. Varje affärsområde rapporterar bara resultatpengar upp till koncernledningen och koncernledningen ställer aldrig krav ner mot regionen eller projekten inom de olika affärsområdena, vare sig IT, HR eller ekonomi.

Drivkrafter

IAM-lösningen är implementerad enbart för användare i Sverige. Respondenten kan inte svara på hur många system som är anslutna, mer än ”100-tals” svara han.

Respondenten säger att huvudanledningen till att de implementerade IAM-lösningen var för att de ville ha ordning och reda. Dem ville få struktur på användare och roller och har nu en katalog med alla användarna. SSO var en drivande faktor till införandet. Kostnaderna för administration var höga och de ville de få ner. Någon processkartläggning gjordes aldrig.

Implementation

”*Respondent: vi utvärderade dem ur ett tekniskt perspektiv, och sen marknadsperspektiv. och sen så pratade vi lite med Gartner, och så tittade vi lite på mogenhet och förståelse. och då fanns det inte så många att välja på när man lyfte på huven. Microsoft hade ju inte kommit nån stans.*”

Implementationen gjordes främst för att helpdesk skulle få ett enklare jobb. Användarna av systemen märker av implementationen i det att de bara behöver logga in i AD för att få tillgång till alla system som de har behörighet att nå. De har samma inloggningsuppgifter på alla system som inte har tillgång till AD-inloggning, kallas password sync. Funktioner för identity intelligence finns, men används inte.

Rollivscykelhantering finns, men används inte. Däremot används rollhantering. Han berättar att det de gått ner till minsta gemensamma roller och har tre stycken. Ingen AD-unix-bridge då de inte har unixsystem. Lösenordsåterställning via user-selfservice finns på ett ställe, en webportal. User-provisioning ligger i botten.

Utvärdering

De har gjort en utvärdering av projektet över vad som kan göras framöver och vilka delar som fattas. De ska införa en automatisk process med hire/fire. Respondenten säger att målen med projektet har nåtts men att det tagit mycket längre tid än förväntat. En lätt besvikelse finns över att de inte kommit längre i sitt IAM-program, det finns stora framtidsplaner och en hög ambitionsnivå men trots det har färre än önskade funktioner implementerats. Hade de vetat att projektet hade tagit så lång tid så hade de aldrig upphandlat det. De har inte räknat på om ledtider, antal inblandade parter och kostnad.
*” Respondent: ...gud... *suck* det är svårt att mäta på det. teoretiskt sätt så borde det ju blivit så inom vissa delar, men vi har inte räknat...”*

De har inte räknat på ROI men han tror att det är svårt att räkna hem det. De är över lag nöjda med lösningen men de hade önskat att de hade kommit längre. De hade en stor ambitionsnivå från början men har mötts av motgångar i form av tekniker som inte gjorde det de skulle och annat. De stötte på problem genom att inte hela koncernen var med på projektet. Användarna vet knappt om att de har implementerat IAM-lösningen. Det enda som de märker är att det är samma lösenord till alla system.

4.4 Sammanfattning av empiri

Tabell 2. Sammanfattning, i kategorier, över respondenters svar.

Leverantör	Företag 1	Företag 2
Bakgrund		
• VD • Säljare av IAM-lösningar • Antal amvändare: 1000-4000	• Förvaltningsansvarig • Projektledare • Antal anställda: 35000 • Antal användare: 15000 • Antal system: 800 • Ansvarig för att målen med systemen uppnåddes • Företagsstruktur: hierarkisk, central ledning • Idén kom från IT – access control gruppen som inte mäktade med den manuella hanteringen • Business case gjordes med flera mätpunkter	• Informationssäkerhetschef • Ägare av IAM-lösningen • Antal anställda: 55000 • Antal användare: 6000 • Antal system: 300 • Företagsstruktur: Projektdriven, autonoma affärsgrupper, central ledning med liten styrning av affärsgruppernas förehavanden • Idén till IAM kom från en affärsgrupp, ej från koncernledningsnivå. • Inga krav på vare sig IT, HR eller ekonomi från koncernledningsnivå • Business case gjordes ej men räknade på kostnad för lösenordsåterställning för supportavdelning
Drivkrafter		
• Ordning och reda • Minska kostnader för administration • Kostnadskontroll för administration • Användare vill ha enkel tillgång till resurser • Revision/bolagskod-krav • Sällan tekniktanke bakom	• Ordning och reda • Minska manuell hantering • Säkerställa att användare hade korrekta rättigheter • Högre kvalitet på användarinformation • Säkerhet: auditing och loggning, central hantering, spårbarhet • Lagkrav/revisionskrav • Automatisera kontroll mot informationsägare vid beställning av rättigheter • Minska ledtid för skapande av nytt konto och leverans av beställda rättigheter	• Ordning och reda • Minska kostnader för administration • Få struktur på användare och roller • Katalog över användarkonton • SSO (Single Sign-on)

Implementering		
Vanligast: • Koppling mot AD • User provisioning • Automatisera processen att skapa ny användare • Koppling till befintliga system • Webb-SSO • Ibland implementeras SSO för att det är ett bevis på att VDs företag har gjort något	• Koppling mot befintligt AD - Active Directory • User self-service, lösenords-återställning och resursbeställning • Roll/kontohantering • User provisioning • SIEM / identity intelligence kommer att implementeras • AD/unix-bride • 6 månader för teknisk implementation, 18 månader för mogenhet • Under projektet - utmaning med HR rutiner	• Koppling mot befintligt AD - Active Directory • User self-service med lösenordsåterställning • Roll/kontohantering • User provisioning • SSO – Single sign-on • Password propagation (ful-SSO) på resterande system • Fokus på helpdesk • Många problem med ägandeskap och mogenhet.
Verksamhetseffekter		
	• HR-avdelningen har fått ändrade rutiner • Rolltilldelning sker automatiskt • Ledtiden är kapad från 5 dagar till en timme • IDM delar information om roller, användare, tillgångar till resterande system. • Password reset kan ske på användarsidan • Förhöjd datakvalitet • Användare kan själva begära resurstillhörighet • Loggning på vem som tilldelade en viss rättighet	• Användarna är knappt medvetna om implementationen, endast märkbar effekt av password propagation och SSO • Helpdesk har fått lättare att utföra sina uppgifter då det är struktur på konton och roller
Utvärdering		
Säljaren är sällan med och utvärderar	• Ingen formell utvärdering av projektet utöver utvärdering av business case. ROI = 3.5 år • Många barnsjukdomar • 100% funktionalitet är uppnådd, 75% av implementationsmålen är uppnådda • Missnöjda med sitt business case, hade idag gjort annorlunda bla mätpunkter • Andra effekter än de i business case var mycket värda, hög datakvalitet • God respons från användarna på införandet av att kunna efterfråga rättigheter (self-service) • Svårt med marknadsföring-internt. Lägre nyttjandegrad av IAM än önskat.	• Osäker på om investeringen går att räkna hem • Projektet tog mycket längre tid än beräknat • Målen är nådda • ROI = ”svårt att räkna hem” • Nöjda med lösningen, men önskar de kommit längre • Hade de vetat att projektet skulle ta så lång tid att implementera så hade de aldrig kört det • Antalet implementerade funktioner är lägre än önskat, beror på organisationen själv.

5 Analys

Bakgrund
I Företag 1 uppstod idén ute i verksamheten hos de som skötte användarnas kontoadministration, de klarade inte av mer manuell hantering. Projektet lyftes sedan upp och drevs högt upp i organisationen med syfte att ta ett helhetsgrepp om IAM. De började med att skapa en strategi som inkluderade långsiktiga mål, lösningens omfattning och vilka delar av organisationen som skulle inkluderas. En processkartläggning och en mappning av dessa mot IAM gjordes. Den forskning vi har tittat på rekommenderar denna ansats – ett starkt visionsarbete och processfokus – för införande av IAM. Företag 2 verkar i motsats till detta haft en otillräcklig vision, beställningen på IAM kom från affärssidan, projektet drevs på en icke koncern-gemensam nivå och fokus låg på att leverera beställda funktioner. Båda företagen uttrycker svårigheten att skapa ett investeringsunderlag och att hitta bra mätpunkter som sedan efter implementering av IAM kan följas upp. Företag 1 skapade ett business-case och flera mätpunkter, flera på olika ledtider, medan Företag 2 nöjde sig med att mäta på funktionen lösenordsåterställning och vilken tidsmässig vinst den i framtiden skulle ge.

Drivkrafter
Empirin visar att en drivkraft för båda företagen var ordning och reda i sin hantering av användares identiteter och systemrättigheter, att gå från en dålig struktur i hanteringen av användarkonton och användaråtkomst till en bättre. Detta beskrivs även i artikeln ”2010 Access Governance Trends Survey” (9). Företag 1 hade en lång rad verksamhetsbehov vilka sammantaget starkt motiverade en IAM-lösning. Företag 2 hade en specifik teknisk funktion som drivkraft med en svagare förankring i verksamhetsbehov.

Leverantören hävdade att det är mycket ovanligt att en teknik ligger till grund för en upphandling och rapporten ”IAM Foundations Part 1” säger att företag ska försöka undvika att fokusera på en teknik utan ska istället se på företagets förehavanden som processer som kan automatiseras eller förenklas
Den svagare förankringen menar vi kan påvisas genom att IAMs varande uppkom från ett specifikt krav i ett affärsområde och inte utökades för att tillräckligt omfatta behov i andra delar av organisationen. Detta går tvärt emot den rekommendation vi hittat i forskningen. *“Your IAM plans and goals should seek to address needs/wants expressed by multiple departments within the organization.”* (11 s. 1)

Vidare har vi hittat rekommendation att inte närma sig IAM med fokus på verksamhetskrav – det här vill vi ha - utan att förstå behovet av IAM genom kopplingen till processer inom företaget. Här skiljer sig företagen sig åt, Företag 1 hade formaliserat sina behov genom ett visionsarbete som tagit hänsyn till perspektivet - koppling IAM och process.

I huvudsak var den tyngsta drivkraften för båda företagen det som i teorin refereras operationell effektivitet. Den beskriver effekter som minskad ledtid, förbättrad produktivitet, ökad användarnöjdhet och förbättrade rapportmöjligheter. Just ledtiden och den dåliga kvaliteten och ordningen på användardata var för Företag 1 en stor orsak till IAM-programmets uppkomst. Minskade kostnader kan argumenteras vara en drivkraft för Företag 1 då deras problem med den resurskrävande manuella hanteringen av användares rättigheter i förlängningen hade lett till ökade personalbehov.

Rapporteringsmöjligheterna förenklade för Företag 1 att vid revision styrka korrekt hantering av användarrättigheter i olika system. Teorin i kapitlet om drivkrafter för IAM

(under ”IT risk-management”) kopplar samman detta med viljan att minska IT-risker genom att kunna uppfylla granskningskrav.
Enligt leverantören är de vanligaste drivkrafterna att minska kostnaderna, nå en ökad operationell effektivitet samt implementera och visa på uppfyllande av regelkrav, vilket mycket väl stämmer överens med de drivkrafter som företagen haft för IAM.

Implementering
Enligt Gartner (5) var följande IAM-delar vanligast implementerade.

- User provisioning
- ESSO
- WAM
- Identity Intelligence and SIEM
- Role life cycle management
- Directory services
- AD-Unix bridge

Leverantören styrker att olika katalogtjänster, rollivscykelhantering och user-provisioning av de Garner-nämda (5) funktionerna är vanliga, SSO menar de är mer sällsynt efterfrågat och övriga nämns inte . Företag 1 och 2 inkluderade identity management & user provisioning, rollhantering samt lösenordsåterställning i sina IAM-program. Företag 1 implementerade även åtkomstbesällning i sina självbetjäningstjänster, Företag 2 valde istället IAM-funktionen SSO.

Effekter på verksamheten
Båda företag nämner minskade ledtider, Företag 1 har här uppnått en dramatisk skillnad på vissa flöden – tiden för skapandet av ny användare är minskad från fem dagar till en timme. Förbättrad produktivitet till var en effekt båda erfor. Företag 2 är osäker på om användarna märker någon skillnad överhuvudtaget, utöver att de är samma lösenord överallt men help-desk har fått mindre arbete på grund av IAM-projektet. Som en följd av user-provisioning sker nu mycket automatiskt vad gäller användarinformation i båda företagen. Företag 1 har varit tvungna till en stor översyn av rutiner på HR-avdelningen för att få en fungerande IAM-miljö. Användarnöjdheten nämns ha ökat, Företag 1 åtnjöt stor och positiv respons på möjligheten att själv via portal kunna beställa systemtillgång. Dessa effekter är väntade då drivkraften ”operational efficiency” (10) ligger till grund för IAM. Rapporten ”Insider threat study: computer system sabotage in critical infrastructure sectors” (8) menar säkerhetsriskerna minimeras eftersom felaktig användarinformation minskar till följd av en IAM-implementation. Sambandet mellan de implementerade funktionerna, drivkrafterna som föregick dessa samt de verksamhetseffekter som resulterade för båda företagen visas sammanställda i tabell 3.

Utvärdering
Inget av företagen gjorden någon formell utvärdering av projektet, Företag 1 gjorde uppföljning av sitt business-case och kalkylerade ROI till 3.5 år. Båda nämner svårigheten med mätpunkter och utvärdering av dessa. Företag 2 var inte säker på om invsteringen gick att räkna hem. Målen nåddes för båda företagen men tiden för implementeringen sågs som för lång, Företag 1 hade barnsjukdomar och ansåg lösningen färdig först efter 1.5 år. Företag 2 skulle inte gått vidare om det på förhand vetat om den långa implementeringstiden. Företag 1 upptäckte positiva effekter som de inte förutsett och som inte var strikt ekonomiska. Användarnöjdheten nämns och även

att förutsättningar finns för att i framtiden uppfylla SOX som i nuläget inte är ett krav. Både leverantören och företagen nämner att det är svårt att räkna ekonomiskt på ett IAM-projekt vilket även Gartner visar (14).

Koppling implementerade funktioner – drivkrafter – effekter
Sammanfattar de olika IAM-funktioner som införts, vilka drivkrafter (eller organisatoriska mål) som fanns för dessa funktioner och vilka effekter som funktionerna gav.

Tabell 3. Tabellen visar kopplingen mellan vilka funktioner som är implementerade av vilket företag, drivkrafterna som motiverade en IAM-upphandling för respektive funktion samt vilka effekter på verksamhet respektive funktion gav. ”Password management” och ”User selfservice: password reset” implementerades men var inte faktorer som för företagen motiverade upphandling av IAM.

Koppling mellan implementerade funktioner, drivkrafter och verksamhetseffekter			
IAM funktioner	Implementerat av	Drivkrafter	Verksamhetseffekter
Enterprise Single Sign-On	Företag 2	• Operationell effektivitet • Kostnads-reducering	• Nöjdare användare • Minskad kostnad för lösenords-återställning
Password Management	Företag 2	*Inte en drivkraft*	• Förbättrade ledtider
Identity Administration, User Provisioning	Företag 1	• Operationell effektivitet • Kostnads-reducering • Hantering av it-risker	• Förbättrade ledtider • Nöjdare användare • Minskade administrativa kostnader • Förenklad granskning (*audit)*
	Företag 2	• Operationell effektivitet	• Förbättrade ledtider • Nöjdare användare • Minskade adminsitrativa kostnader
User self-service: password reset	Företag 1 Företag 2	*Inte en drivkraft*	• Förbättrade ledtider • Nöjdare användare
User self-service: access ordering	Företag 1	• Operationell effektivitet • Kostnads-reducering	• Förbättrade ledtider • Nöjdare användare • Minskade administrativa kostnader
User role management	Företag 1 Företag 2	• Operationell effektivitet	• Förbättrade ledtider • Nöjdare användare

6 Diskussion

Huvudorsaken till att företag implementerar en IAM-lösning är för att få ordning och reda på sina användarkonton samt att se till att rollhanteringen fungerar och att policys om resurstilldelning är uppdaterade. Detta är en säkerhetsåtgärd som ser till att användarkonton inaktiveras när en anställd slutar och att dennes roller tas bort eller ändras om den anställde byter befattning. Företag 2 hade en annan inställning till IAM och ville främst implementera SSO. Detta var den huvudsakliga drivande faktorn till upphandlingen av IAM. All litteratur vi sökt om ämnet varnar för att motivera uppköp med en teknik och säger att företag ska försöka tänka i processer. Om ett arbetsflöde kan automatiseras eller förenklas med IAM är det ett stort steg på vägen till att införa till exempel SSO. Varför Företag 2 valde att fokusera på SSO kan bero på att idén till införandet av lösningen kom från en autonom affärsgrupp och inte från koncernledningsnivå. Teorin vi har presenterat säger att för att lyckas med en IAM-implementation så måste alla delar av koncernen finnas representerade i den långsiktiga implementeringsplanen. Koncernledningen i Företag 1 är enbart intresserade av resultatpengar från de underliggande affärsgrupperna. Företag 1 är nöjd med lösningen trots att den har tagit mycket längre tid att implementera än beräknat. Mognadsgraden för ett IAM-projekt är något som Företag 1 hade räknat med skulle ta lång tid, vilket den också gjorde. De har svårt att få ut lösenordsåterställningen till de anställda (endast 30 % av de anställda har registrerat challenge response-frågorna) och de märkte att det enda sättet att få användarna att börja använda teknikerna var genom riktade utskick.

Företag 1 fick mycket god respons för implementerandet av självbetjäningstjänsten. Den innebar att användare själva kunde begära tillgång till resurser, utan att gå via help desk. Ledtiderna för skapandet av konton har blivit kapade från 5 dagar till 1 timme på Företag 1 till följd av en delvis automatiserad process för nyanställningar. På Företag 2 har helpdesk, som sköter användarkontona, fått sina arbetsuppgifter förenklade. Detta är en av de stora delarna av en IAM-lösning och teorin vi presenterar visar att detta är, förutom en av anledningarna till att införskaffa IAM, även en effekt som är efterfrågad bland företag.

Då säkerhetsriskerna med att ha roller och resurstilldelningar kvar på konton som inte längre används är ett allvarligt problem för företag, så är det bara knappt hälften av företagen som vet vad dessa risker innebär. Resultatet av vår undersökning visar att Företag 1 upplevde en högre grad av säkerhet eftersom datakvaliteten på användarkontona hade blivit högre. Företag 2 kunde inte svara på om säkerheten hade förändrats.

Vår förutfattade mening om att lagar och regler ligger till grund för införandet av en IAM-lösning visade sig stämma då både Säljaren och Företag 1 nämnde detta. Företag 2 fokuserade, som tidigare nämnt, enbart på SSO och ordning och reda.

7 Slutsats

Vår studie visar att den tyngsta drivkraften för de undersöka företagen är det som i teorin refereras operationell effektivitet. Den beskriver effekter som minskad ledtid, förbättrad produktivitet, ökad användarnöjdhet och förbättrade rapportmöjligheter. Företag, i storleken 2000+ användare, som saknar en IAM-lösning upplever att de saknar kontroll över användarkonton och kostnaden för administration av dessa och att de vill ha ordning och reda på sina användare. Vidare kan vi dra slutsatsen att för att lyckas med en IAM-lösning så måste en långsiktig plan skapas för hur implementeringen ska gå till. Företag måste också se till att få med sig alla delar av verksamheten för att lyckas med IAM. De effekter ett företag kan räkna med när en IAM-lösning införs är till exempel minskade ledtider för skapande av användarkonton, förhöjd datakvalitet och mindre arbete för helpdesk. Båda företagen valde att implementera *identity management & user provisioning, rollhantering* och lösenordsåterställning. En bidragande faktor till att företagen inte gjorde en formell utvärdering av projektet var svårigheten att finna mätpunkter och att utvärdera dessa, samt att de mätpunkterna de använde i business case inte värderades lika högt efter implementeringen. Ingen utvärdering behövdes dock för de båda bolagens konstanterande att implementering tog lång tid – mycket längre än räknat med. Vi finner även att en verksamhets struktur påverkar både förarbete och implementering. Företag som har en stark och centraliserad styrning av IT kan få en effektivare implementation med bredare effekt på verksamheten, förutsatt att implementeringsprojektet styrs från en hög nivå, helst koncernledningsnivå. Uppfyllande av regelverk och lagar i form av bolagskod och bestämmelser, till exempel Basel II och Sarbanes-Oxley är en annan drivande faktor till att ett företag börjar undersöka IAM-lösningar. Revisorskrav, i form av krav att vet vem som har tillgång till vilka system, spårbarhet med mera, kan också ligga till grund för införandet av en IAM-lösning.

8 Vidare forskning

Företagen som vi har intervjuat personal på är alla av betydande storlek. Företag 1 har 15000 användare och Företag 2 har 6000 användare (IAM implementerades enbart för svenska användare). Säljaren vi pratade med sa att man kan uppnå lönsamhet vid 1000 användare, men att riktig lönsamhet först uppnås när företaget är uppe i 2000+ användare. Detta är något som kan komma att ändras när IAM-lösningar i molnet blir mer vanligt då en molbaserad lösning skulle innebära att flera företag skulle kunna dela på samma tekniska infrastruktur. Kostnaderna för en IAM-lösning skulle kunna kapas drastiskt, och då skulle även mindre företag kunna ta del av teknikerna. Detta är ett ämne som blir mer och mer aktuellt, då molnbaserade IAM-lösningar, IDaaS (Identity as a service), är en teknik som är på frammarsch.

Ur ett företagsorganisatoriskt perspektiv så skiljer sig företagen åt i det avseendet att Företag 1 är centralt styrt med en stark hierarkisk struktur medan Företag 2 är projektstyrt och är fragmenterat i flera autonoma affärsgrupper. Detta kan ha haft en inverkan på vad som implementerades och bör undersökas mer. Exempel på områden som kan undersökas är: hur påverkar ett företags organisation graden av IAM-implementering, samt hur kan ett företag med en stark projektdriven företagsstruktur implementera IAM.

9 Källförteckning

1. **Ball, Tony.** Challenging corporate thinking on implementing IAM solutions. *The Free Library.* [Online] 2010. [Cited: 5 10, 2011.] http://www.thefreelibrary.com/Challenging+corporate+thinking+on+implementing+IAM+solutions.-a0219556356.
2. **Peter Esaiasson, Mikael Gilljam, Henrik Oscarsson, Lena Wägnerud.** *Metodpraktikan: Konsten att studera samhälle, individ och marknad.* Stockholm : Norsted Juridik, 2007. 9789139108658.
3. **Allan, Ant.** *Identity and Access Management Defined in 100 tweets.* s.l. : gartner, 2010.
4. **Roberta J. Witty, Ant Allan, John Enck, Ray Wagner.** *Identity and Access Management Defined.* s.l. : Gartner, 2003.
5. **Carpenter, Perry.** *IAM Foundations Part 2: Tools and Technologies.* s.l. : Gartner, 2010.
6. Sloppiness in access and authorization management can cost enterprises dearly. *IT security standard.* [Online] 04 26, 2010. [Cited: 05 23, 2011.] http://www.itsecuritystandard.com/blog/?p=1516.
7. **Dolan, Pamela Lewis.** amednews.com. [Online] 2010. http://www.ama-assn.org/amednews/2010/04/19/bica0419.htm.
8. **Michelle Keeny, Dawn Cappelli.** *Insider threat study: computer system sabotage in critical infrastructure sectors.* s.l. : Carnegie mellon, 2005.
9. **Institute, Ponemon.** *2010 Access Governance Trends Survey.* s.l. : Aveksa, 2010.
10. **Witty, Roberta J.** *Five business drivers of identity and access management.* s.l. : Gartner, 2003.
11. **Carpenter, Perry.** *IAM Foundations, Part 3: Developing Your IAM Plan .* s.l. : Gartner, 2010.
12. —. *IAM Foundations, Part 1: So You've Been Handed an IAM Program ... Now What? .* s.l. : Gartner, 2010.
13. **Perkins, Earl.** *A Process View of Identity and Access Management Is Essential.* s.l. : Gartner, 2011.
14. **Earl Perkins, Perry Carpenter, Ant Allan.** *Cutting IT Costs Within IAM and With IAM .* s.l. : Gartner, 2008.
15. *Network authentication using Single Sign-On: The challenge of aligning mental models.* **Rosa Heckle, Wayne G. Lutters, David Gurzick.** Baltimore : University of Maryland, 2008, Vol. 14.
16. *Ponemon Study Reveals Enterprises Not Keeping Pace with User Access Changes; Face Significant Business and Compliance Risks.* s.l. : pr-inside.com, 2010.
17. **Huggins, Ronni Dale.** *Web access management and Single Sign-On.* 2010.