Auktorisering i system för digitalt bevarande

Olivia Carlsson

C-uppsats
Huvudområde: Arkiv- och informationsvetenskap GR (C)
Högskolepoäng: 15 hp
Termin/år: VT 2019
Examinator: Erik Borglund
Kurskod/registreringsnummer: AK038G

Abstract

The purpose is to investigate, analyze and clarify the relationship between authorization and security policy for digital preservation system. Information security comes into focus when digital preservation systems are discussed. The handling of electronic documents in digital preservation systems is now widespread and a large part of many activities. This means that the business must ensure that it protects against the loss of information stored in the digital preservation system. Authorization and security policy are relevant to archive and information science because digital objects in digital preservation system are to be protected from unauthorized access. With a qualitative method the research will go through security policy, systems and models for access architecture. With open approach and open questions, the research will be summarized with a discussion on the most important conclusions for access management for digital preservation system, which are mainly built on roles. It is of great importance that the company uses roles and authorization levels to ensure that everyone knows with certainty what to do and what they cannot do.

Key words: Authorization, Security Policy, Access Control, Information system, Digital preservation system

Abstract (Swedish)

Syftet är att undersöka, analysera och klargöra relationen mellan auktorisering och säkerhetspolicy för system för digitalt bevarande. Informationssäkerhet kommer i fokus när system för digitalt bevarande diskuteras. Hanteringen av elektroniska dokument i system för digitalt bevarande är nu utbrett och en stor del av många aktiviteter. Det innebär att verksamheten måste se till att den skyddar mot förlust av information som lagras i system för digitalt bevarande. Auktorisering och säkerhetspolicy är relevant för arkiv- och informationsvetenskap eftersom digitala objekt i system för digitalt bevarande ska skyddas mot obehörig åtkomst. Med en kvalitativ metod kommer forskningen att gå igenom säkerhetspolicy, system och modeller för åtkomstarkitektur. Med öppet tillvägagångssätt och öppna frågor kommer forskningen slutligen att sammanfattas med en diskussion om de viktigaste slutsatserna för åtkomsthantering för system för digitalt bevarande, som huvudsakligen bygger på roller. Det är av stor vikt att företaget använder roller och auktoriseringsnivåer för att säkerställa att alla med säkerhet vet vad de ska göra och vad de inte får göra.

Ämnesord: Auktorisering, Säkerhetspolicy, Åtkomstkontroll, Informationssystem, System för digitalt bevarande

Innehållsförteckning

1 Inledning

Informationssäkerhet hamnar i fokus när informationsförvaltning och system för digitalt bevarande diskuteras. Hantering av elektroniska handlingar i system är nu utbrett och är en stor del av många verksamheter. Detta innebär för arkivvetenskapen att verksamheten måste se till att skydda mot förlust av information som lagras i system för digitalt bevarande, genom att åtkomst ska kunna skyddas, spåras i dåtid och nutid. Ett system för digitalt bevarande ska verka för långtidsbevarande, tillgänglighet och gynna verksamheten ekonomiskt därför är det av stor vikt att strategi för åtkomsthantering finns i verksamheten. Med system för digitalt bevarande kommer hanteringen av informationen innebära att många personer har tillgång till informationen och det ställer ökade krav på säker auktorisering till systemet för digitalt bevarande. [1] [2] Enligt Gustafsson och Paradis ska en långsiktig plan över auktorisering skapas, de menar att problem med säkerhetsrisker gällande åtkomsthantering hos företag och organisationer har ökat de senaste åren. Auktorisering och säkerhetspolicy måste alla företag och organisationer behandla. Problemen resulterar i att data kan stjälas, förstöras eller raderas, antingen på flit eller inte.[3] Det finns även en okunnighet inom organisationerna och de flesta företag samt organisationer använder inte medvetet någon modell för åtkomstkontroll. Det är just den här osäkerheten kring auktorisering och säkerhetspolicy som finns ute i organisationer som skapar brister gällande informationssäkerheten, det menar även Basic, Johnsson och Schuster.[4] Hur relationen ser ut mellan auktorisering och säkerhetspolicy för system för digitalt bevarande är den frågeställning som ska besvaras i den här studien, för att bidra med kunskap till denna problematik. Förstår verksamheten vikten av åtkomstsäkerhet och får kunskapen, kan informationen i system för digitalt bevarande vara i tryggt förvar.

Auktorisering i samband med IT-säkerhet betyder att det ger någon tillstånd, så kallad behörighet att få göra något.[5] Användarauktorisering innebär att säkerställa att varje företagsanvändare har auktoriserats för att ha tillgång (åtkomst) till funktioner och information, samt att funktioner och information som personen inte är behörig till är specifikt förhindrat.[6] Tillämpningen av säkerhetspolicy för informationssystem med mekanismer för

[1] Computer Sweden, IDG:s ordlista, *informationssäkerhet*
[2] Sveriges kommuner och landsting, *Informationsförsörjning och digital infrastruktur/E-arkiv*
[3] Gustafsson Staffan C., Paradis Mikael, *Rationalitet för identitet- och åtkomstlösningar i stora företag*, s. 36.
[4] Basic Amar, Johnsson Christoffer, Schuster Thomas, "*Rollbaserad åtkomstkontroll inom organisationer- Rätt åtkomst till rätt användare vid rätt tillfälle",* s. 50-51.
[5] Computer Sweden, IDG:s ordlista, auktorisation
[6] Sherwood, Clark, Lynas, *Enterprise Security Architecture*, s. 292.

åtkomstkontroll är ett omfattande och stort område inom informationssäkerhet. Det grundläggande målet med alla åtkomstkontrollmekanismer är att tillhandahålla ett verifierbart system för att garantera skyddet av information från obehörig och otillbörlig åtkomst, som anges i en eller flera säkerhetspolicyer. [7] [8] Doktor Hu talar för att organisationer som planerar att införa ett åtkomstkontrollsystem[9], så kallad Access Control System, ska beakta åtkomstkontrollpolicys, modeller och säkerhetsmekanismer. Han menar vidare att nästan alla system som har ekonomi, säkerhet och integritet inblandat har någon typ av åtkomstkontroll och att åtkomstkontrollen är en uppsättning procedurer och kontroller som begränsar eller upptäcker tillgång till informationsresurser, det vill säga; den definierar användare och behörigheter för åtkomst.[10] Sherwood, Clark och Lynas förespråkar *Sherwood Applied Business Security Architecture* som är baserad på en säkerhetsarkitekturmodell med 6 stycken lager: *Contextual (Business), Conceptual (Architeture), Logical (Design), Physical (Build), Component (Tools), Service Management*, och att organisationer ska använda sig av följande tillhörande nyckelfrågor som ska främja en analys och arbetet för att lösa säkerhetsarkitekturen kring auktorisering; *Vem, vad, varför, när, var* samt *hur*. Dessa nyckelfrågor ska besvaras genom att ha en plan kring användaridentiteter, rättigheter, funktioner, åtgärder och åtkomstkontroll.[11] Thinh, Shaun, Mehrzad menar även de att en säkerhetspolicy gällande auktorisering för system för digitalt bevarande ska besvara just dessa nyckelfrågor för att skapa en säkerhetsarkitekturmodell för verksamheten.[12] Kopplingen till arkivvetenskapen och den problematik som finns, är att de som arbetar med system för digitalt bevarande måste vara väl insatta i den säkerhetspolicy som gäller auktorisering, eftersom felhantering gällande åtkomst kan ge förödande konsekvenser om fel personer kommer åt skyddad information, som till exempel patientjournaler som kräver sekretessprövning av behörig användare som faktiskt har rollen arkivarie. System för digitalt bevarande ska säkerställa mot obehörig åtkomst med hjälp av auktorisering och säkerhetspolicy som har till syfte att skydda all information i systemet för digitalt bevarande.

[7] Ryan Ausanka-Crues, *Methods for Access Control: Advances and Limitations, Introduction, s. 1-4.*
[8] John Sherwood, Andrew Clark, David Lynas, *Enterprise sequrity architecture- a business-driven approach*, s. 39.

[9] Poniszewska-Maranda, s. 36.
[10] Dr. Vincent Hu, *Access Control Policy and Implementation Guides*, s. 43.
[11] Sherwood, *Enterprise Security Architecture*, s. 39, 41.
[12] Nguyen et al., *Identity And Access Management Framework* s. 3.

1.1 Syfte, mål och frågeställning

Uppsatsens syfte är att undersöka, klargöra samt analysera relationen mellan auktorisering och säkerhetspolicy för system för digitalt bevarande. Auktorisering och säkerhetspolicy är relevant för arkiv- och informationsvetenskap, eftersom digitala objekt i system för digitalt bevarande behöver skyddas från obehörig åtkomst.

Målet med uppsatsen är att den ska tydliggöra problemet, motivera till diskussion, och att forskning inom området auktorisering och säkerhetspolicy för system för digitalt bevarande ska öka.

Frågeställning
"Hur ser relationen ut mellan auktorisering och säkerhetspolicy för system för digitalt bevarande?"

2 Definitioner

Access Control – Se *åtkomstkontroll* på sidan 7.

Access Control Policy – Se *åtkomstkontrollpolicy* på sidan 7.

Användare- En användare definieras som en människa, men kan utvidgas till att omfatta maskiner, nätverk eller intelligenta autonoma medel.[13]

Auktorisation/Auktorisering/Auktoriserad - Begreppet Auktorisation / Auktorisering i samband med IT-säkerhet menas med att det ges något tillstånd, så kallad behörighet att göra något.[14] Användarauktorisering innebär att säkerställa att varje företagsanvändare har auktoriserats för att ha tillgång (åtkomst) till funktioner och information samt att funktioner och information som personen inte är behörig till är specifikt förhindrat.[15] En av de frågor företag bör ställa i säkerhetsarkitektur är *Vem*? Denna fråga ska besvaras gällande användaridentiteter, rättigheter, funktioner, åtgärder, åtkomstkontroll. [16]

[13] (SAIC), Role-Based Access Control (RBAC) Role Engineering Process, s. 1.
[14] Computer Sweden, IDG:s ordlista, auktorisation
[15] Sherwood, Clark, Lynas, *Enterprise Security Architecture*, s. 292.
[16] Sherwood, *Enterprise Security Architecture*, s. 39.

Archivematica - ”Archivematica är en webb- och standardbaserad öppen källkod som gör det möjligt för din institution att behålla långsiktig tillgång till pålitligt, autentiskt och pålitligt digitalt innehåll”.[17]

ABAC - ABAC står för Attribute-based access control (attributbaserad åtkomstkontroll). Den är baserad på användarens attribut. [18]

ACL – ACL står för Access Control List. ACL refereras till varje objekt som anger de ämnen eller grupper av ämnen som får göra åtkomst till det objektet.[19]

BAC - BAC står för Basic Access Control, som är en organisationsbaserad åtkomstkontroll.[20]

Big Data – Big Data står för mycket stora datamängder som kräver speciella metoder för analys. Oftast ostrukturerade data, som menas med data som inte kan ordnas i till exempel tabeller. Mängden av data är så stora att de inte kan bearbetas i vanliga program.[21]

DAC - DAC står för *Discretionary Access Control (*diskretionär åtkomstkontroll). Den ger tillgång till eller begränsar objektåtkomst via en åtkomstpolitik bestämd av ett objekts ägargrupp och / eller ämnen. [22]

E-arkiv - E-arkivet ska lagra informationen (elektroniska handlingar) i ett verksamhetssystem som ska verka för långtidsbevarande, tillgänglighet och gynna verksamheten ekonomiskt.

Elektroniska handlingar kan vara till exempel; texter, fotografier, video, ljud, kartor eller annan typ av data som kan komma från mätverktyg. E- arkiv är för långtidsbevarande och hanteringen av den digitala informationen sker på ett hållbart sätt, det menas med att användarnas behov, demokrati och ekonomi gynnas över tid.[23]

GAP- analys- Ett system som jämför hur ett företag arbetar nu med hur det skulle fungera och beräknar hur företaget kan använda tid, pengar etc. för att uppnå den eftersträvade framgången. [24] Det ska analyseras både på kort och lång sikt. Detta ska göras genom att identifiera hur tillgångar samt resurser används, och eventuellt inte utnyttjas. [25]

IAM- Identity and Access Management; ett system för att bestämma vilka användare som ska tillåtas att få tillgång till en organisations it-nätverk samt de resurser som varje användare ska tillåtas att få åtkomst till. Resurser i nätverket handlar om information, hårdvara och tjänster. IAM:s syfte är att det ska finnas funktioner för att administrera användare i nätverket. [26]

---

[17] Artefactual, Archivematica
[18] Fatima Sifou, Ali Kartit, Ahmed Hammouch *Different Access Control Mechanisms for Data Security in Cloud Computing*, s.42.
[19] Sherwood, s. 240.
[20] Sifou, s.42.
[21] IDG:s ordlista, *Big Data*
[22] Techopedia™, *Discretionary Access Control (DAC)*
[23] SKL, *Informationsförsörjning och digital infrastruktur/E-arkiv*
[24] Cambridge University Press, *Gap analysis*.
[25] 3M, *Så här gör man en GAP-analys: prestation, färdighet, marknad*
[26] Computer Sweden, *Identity and access management*

Informationssäkerhet- Begreppet informationssäkerhet betyder säker lagring och hantering av information i it-system. Det innebär att skydda mot förlust av information, åtkomst ska skyddas och kunna spåras.[27]

Information om åtkomsträttigheter (Access Rights Information)- Denna enhet identifierar åtkomstbegränsningar för informationen. Det är här den rättsliga biten kommer in, villkor för åtkomst som gäller för alla specifika objekt, åtkomst avtal samt de specifikationer som har angetts för att bekämpa brott som har begåtts i informationssystemet.[28]

LIS- Ledningssystem för informationssäkerhet. Består av policy, riktlinjer och rutiner med tillhörande resurser och aktiviteter för hantering av informationssäkerhet i organisationen.[29]

Logisk säkerhet - Logisk säkerhet innebär: autentisering, åtkomstkontroll och revision. Åtkomstkontroll tillhör begreppet logisk säkerhet. Åtkomstkontroll är den viktigaste tekniken på logisk säkerhetsnivå och används ofta det gör det möjligt att definiera användarens ansvar och möjligheter i ett system. Åtkomstkontroll ska innehålla åtkomstpolicyer samt säkerhetsmekanismer. [30]

Loggning/Revisionsspår (Audit Trails)- Så kallade loggar/revisionsspår handlar om att övervaka systemet. Det loggar ger oss är information om vad som hänt, och vad som händer precis nu. Loggar är ett starkt hjälpmedel för organisationen då det stärker informationssäkerhetsarbetet. Det varnar om problem som försiggår eller som redan har hänt, till exempel att fel användare är inne i systemet/informationen.[31] Systemet lagrar alla uppgifter om alla åtkomstförfrågningar och det är oavsett om personen har beviljats eller nekats åtkomst till objektet.[32]

MAC- MAC står för en obligatorisk åtkomstkontroll. Det innebär en uppsättning av säkerhetspolicyer som begränsas enligt systemklassificering, konfiguration samt autentisering. MAC- policyhantering/inställningar är begränsade till systemadministratörer.[33] [34]

Molntjänst (cloud computing)- Begreppet innebär leveransen av olika tjänster via Internet. Resurserna som också ingår är till exempel datalagring, databaser, nätverk och programvara. Användare kan lagra filer samt program på fjärrservrar och datatillgången sker via Internet. [35]

OAIS- OAIS står för *Open Archival Information System.* OAIS är ett arbete gällande en referensmodell för ett öppet arkivinformationssystem som CCSDS och Internationella organisationen för Standardisering (ISO) har arbetat fram. *[36]*

---

[27] Ibid., *Informationssäkerhet*
[28] (CCSDS), *Reference Model For An Open Archival Information System (Oais)*, s 1-8.
[29] Myndigheten för samhällsskydd och beredskap, informationssäkerhet - *Metodstödet.*
[30] Poniszewska-Maranda Aneta, *Management of access control in information system based on role concept*, s. 36
[31] Michael Cobb, *Best practices for audit, log review for IT security investigations*
[32] Sherwood, s. 239.
[33] Sifou, s. 41.
[34] Techopedia™, *Mandatory Access Control (MAC)*
[35] Investopedia, *Cloud Computing*
[36] (CCSDS), *(Oais)*, s 3.

OASIS - OASIS är en rollbaserad åtkomstkontrollarkitektur för att uppnå säker drift av tjänster i en öppen, distribuerad miljö. Användarna måste presentera de nödvändiga uppgifterna i det angivna sammanhanget för att aktivera en roll eller anlita en tjänst. Roller aktiveras endast under en session. [37]

Objekt (Object)- Begreppet objekt betyder att en enhet som innehåller eller tar emot information. Tillgång till ett objekt innebär potentiellt tillgång till den information som den innehåller. Exempel på objekt är poster, filer, kataloger, processer och program.[38]

PDI- Begreppet PDI står för *Preservation Description Information.* Den information som är nödvändig för tillräcklig bevarande av innehållsinformation och som kan kategoriseras som Proveniens, Referens, Fixitet, Kontext och Access Rights Information. [39]

Roll- En samling behörigheter i rollbaserad åtkomstkontroll, vanligtvis förknippad med en roll eller position inom en organisation. [40]

RBAC- RBAC står för role-based access control system. Det menas med en rollbaserad åtkomstkontroll som är en känd metod för åtkomstsäkerhet som bygger på en persons roll inom organisationen. [41] [42]

SABSA- Står för är Sherwood Applied Business Security Architecture. Baserat på en säkerhetsarkitekturmodell med 6 stycken lager. SABSA är en metod för att utveckla säkerhetsarkitekturen och strategin för företaget.[43]

SS-ISO/IEC 27000- serien- Är en svensk och internationell standardserie som talar för ett ledningssystem där säkerhetsnivån tar sin utgångspunkt i en verksamhetsanpassad riskanalys och tydlig process för informationssäkerhetsarbetet. *SS-ISO/IEC 27000* är en serie som hjälper informationssäkerhetsarbetet inom organisationer. Den förbättrar också möjligheterna att externt bedöma samt revidera säkerhet på ett bra sätt.[44]

Säkerhetspolicy- Uttalande om nödvändigt skydd för informationsobjekten.[45]

Tillstånd (privilegium)- Bemyndigande att utföra vissa åtgärder på ett system.[46]

Åtkomst Funktionsenhet (Access Functional Entity)- Funktionsenhet som gör information synligt för initiativtagaren.[47]

---

[37] Walt Yao, Ken Moody, Jean Bacon, *A Model of OASIS Role-Based Access Control and its Support for Active Security.*
[38] Vincent C. Hu David F. Ferraiolo D. Rick Kuhn, *Assessment of Access Control Systems*, s. 3.
[39] *(Oais)*, s. 1-14
[40] Vincent, s. 45.
[41] Sifou, s. 42.
[42] Techopedia™, *Role-Based Access Control (RBAC).*
[43] Sherwood, *foreword* and *preface*
[44] Myndigheten för samhällsskydd och beredskap, *Ledningssystem för informationssäkerhet – LIS*
[45] Vincent, s. 45.
[46] Ibid. s. 44.
[47] *(Oais)*, s. 1-8

Åtkomstkontroll policy (Access Control Policy)- Den uppsättning regler som definierar villkoren för åtkomst.[48]

Åtkomstkontroll (Access Control)- Åtkomstkontroll är en uppsättning procedurer och kontroller som begränsar eller upptäcker tillgång till informationsresurser. Den definierar användare och behörigheter för åtkomst.[49] Åtkomstkontroll tillhör begreppet logisk säkerhet. Logisk säkerhet innebär: autentisering, åtkomstkontroll och revision. Åtkomstkontroll är den viktigaste tekniken på logisk säkerhetsnivå och används ofta. Det gör det möjligt att definiera användarens ansvar och möjligheter i ett system. Åtkomstkontroll ska innehålla åtkomstpolicyer samt säkerhetsmekanismer.[50]

Ämne (Subject)- En aktiv enhet. Oftast en person, process eller enhet som orsakar information att flöda bland objekt eller ändrar systemstatus.[51]

3 Relaterad forskning

Den relaterad forskning som har funnits mest relevant till studien om relationen mellan auktorisering och säkerhetspolicy för system för digitalt bevarande, utgår främst från de formulerade problem som finns gällande området, samt de vanligast använda system och modeller inom området för att kunna lösa denna problematik om osäkerheten kring säkerhetspolicy för auktorisering i verksamheter. Dessa system och modeller har analyserats i relaterad forskning och kommer att vidare i den här studien få sin förklaring; *Sherwood Applied Business Security Architecture (SABSA- modellen), Identity and Access Management (IAM[52]), Cloud Service Security, (OASIS[53]), Role-Based Access Control (RBAC[54] [55]).*

I Staffan C. Gustafsson Mikael Paradis kandidatuppsats *"Rationalitet för identitet- och åtkomstlösningar i stora företag"* menar Gustafsson och Paris att säkerhet och användaradministration är två stora problem som alla företag måste behandla. Gustafsson och Paradis drar slutsatsen att för att lyckas med en Identity and Access Management (IAM[56])-lösning, som är ett system för att bestämma vilka användare som ska tillåtas att få tillgång till

[48] Vincent, s. 43.
[49] Ibid. s. 43.
[50] Poniszewska-Maranda, s. 36
[51] Vincent, s. 3.
[52] Figur 3, avsnitt Teori.
[53] Walt Yao, Ken Moody, Jean Bacon, *A Model of OASIS Role-Based Access Control and its Support for Active Security.*
[54] Sifou, s. 42.
[55] Techopedia™, *Role-Based Access Control (RBAC).*
[56] Figur 3, avsnitt Teori.

en organisations it-nätverk[57] så måste en långsiktig plan skapas för hur implementeringen ska gå till. Gustafsson och Paris menar vidare att företag måste också se till att få med sig alla delar av verksamheten för att lyckas med IAM. Gustafsson och Paradis talar för att problem med säkerhetsrisker gällande åtkomsthantering hos företag och organisationer har ökat de senaste åren, problemen resulterar i att data kan stjälas, förstöras eller raderas antingen på flit eller inte. Detta är just på grund av osäkerhet kring auktorisering och säkerhetspolicy som finns. Gustafsson och Paradis kommer fram till att huvudanledningen till att företag investerar i en IAM- lösning är att få en god och effektiviserad användaradministration. [58]

Hu, Ferraiolo, Kuhn menar i *Access Control Policy and Implementation Guides* att organisationer som planerar att införa ett åtkomstkontrollsystem ska beakta: åtkomstkontrollpolicys, modeller och säkerhetsmekanismer. Avvägningar och begränsningar är inblandade i alla säkerhetsmekanismer och åtkomstkontrolldesigns. Det är användarens ansvar för att bestämma de bästa säkerhetsmekanismerna som fungerar för deras verksamhet funktioner och krav.[59]

Enligt John Sherwood, Andrew Clark och David Lynas i *Enterprise Security Architecture - A Business-Driven Approach* talar de utifrån *Sherwood Applied Business Security Architecture* (SABSA[60]) som är en metod för att utveckla säkerhetsarkitekturen och strategin för verksamheten. Den är baserad på en säkerhetsarkitekturmodell med 6 stycken lager; Contextual (Business), Conceptual (Architeture), Logical (Design), Physical (Build), Component (Tools), Service Management. [61] Vidare utgår författarna från SABSA matrixens 6 stycken nyckelfrågor som ska ställas under varje lager i modellen, som ska främja en analys och arbetet med informationssäkerheten i verksamheten; *Vad, Varför, Hur, Vem, Var* samt *När*? Enligt författarna ska dessa nyckelfrågor besvaras enligt följande:

- *Vad?* Frågan ska besvaras med vad verksamheten försöker göra på det specifika lagret, det innebär de tillgångar som skyddas av säkerhetsarkitekturen.
- *Varför?* Ska besvaras gällande varför verksamheten ska göra det? Det menas med motivationen för att vilja tillämpa säkerhet, uttryckt i villkoren för detta lager.

[57] Computer Sweden, IDG:s ordlista, *Identity and access management*
[58] Gustafsson Staffan C., Paradis Mikael, *Rationalitet för identitet- och åtkomstlösningar i stora företag*, s. 36.
[59] Vincent, s. 42.
[60] Figur 2, avsnitt Teori.
[61] Sherwood, *foreword* and *preface*

- *Hur?* Hur ska verksamheten göra det? Det innebär funktioner som behövs för att uppnå säkerhet gällande lagret.
- *Vem?* Vem som är involverad – vilka människor samt organisationella aspekter av säkerhet.
- *Var?* Menas med platser där verksamheten ska utöva säkerhet.
- *När?* Innebär när verksamheten ska göra det, de tidsrelaterade aspekterna av säkerhet. [62]

Nguyen, Cuttill, Timothy, Mehrzad i *Identity And Access Management Framework*, utgår även dem från frågorna; *Vem, Vad, När, Var* och *Hur*. De menar att *Vem* representerar identiteten av användaren, *Vad* menas med typ av data plattform som användaren använder resursen ifrån, *När* handlar om åldern av autentiserings-/auktoriserings sessionen, *Var* handlar om var användaren befinner sig, men också i vissa fall handlar det även om vilken typ av nätverk. *Hur* innebär mekanismen eller metoden som auktorisering och autentisering blir uppfylld. [63] En säkerhetspolicy gällande auktorisering för system för digitalt bevarande ska besvara just dessa frågor. Dessa nyckelfrågor kommer att besvara min frågeställning om relationen mellan auktorisering och säkerhetspolicy[64].

Aneta Poniszewska-Maranda som författat; *Management of access control in information system based on role concept*, menar att åtkomsthantering i informationssystem som är baserade på roller speglar på bättre sätt företagets organisation på åtkomstnivå. Poniszewska-Maranda menar att modellen med roller för åtkomsthantering kan användas av systemutvecklare och säkerhetsadministratörer för att vara stöd i jobbet med att säkerställa säkerheten för den data som lagras och hanteras i informationssystemet, samt är den ett verktyg till den globala samverkan med regler för åtkomstkontroll i hela systemet. Poniszewska-Maranda menar även att den rollbaserade modellen för åtkomsthantering tillhör logisk säkerhet som Sherwood, Clark och Lynas menar.[65]

Vidare har författarna Amar Basic, Christoffer Johnsson, Thomas Schuster i sin kandidatuppsats "*Rollbaserad åtkomstkontroll inom organisationer- Rätt åtkomst till rätt användare vid rätt tillfälle"* kommit fram till att samtliga organisationer som ingick i deras

[62] Sherwood, s. 41.
[63] Nguyen et al., *Identity And Access Management Framework* s. 3.
[64] Se avsnitt: Resultat.
[65] Poniszewska-Maranda, *Management of access control in information system based on role concept*, s. 35.

undersökning använder en rollbaserad åtkomstkontroll, förkortat RBAC.[66] Basic, Johnsson, Schuster kom även fram till att de flesta organisationerna inte har en fullständig rollbaserad lösning på grund av okunnighet. Det vill säga att det saknas en användarroll för varje yrkesroll. De menar att det finns en okunnighet inom organisationerna och att de flesta företagen och organisationer inte medvetet använde någon modell för åtkomstkontroll.[67] Det är just den här osäkerheten som finns ute i organisationer och i verksamheter skapar brister gällande informationssäkerheten och därav resulterar i åtkomstrisker.

Författarna Walt Yao, Ken Moody, Jean Bacon till *A Model of OASIS Role-Based Access Control and its Support for Active Security* förespråkar och formaliserar OASIS [68] modellen som är rollbaserad som menas med att tjänster namnger sina klientroller och verkställer policy för aktivering av roller samt service.[69]

Den rollbaserade åtkomstkontrollen (RBAC) och logisk säkerhet förespråkas starkt av författarna, detta kommer uppsatsen att vidare behandla. Men eftersom användningen av molnlagring i digital bevarande används allt mer, utvecklas snabbt [70] samt att åtkomstkontroll betraktas som en nyckelkomponent i molnsäkerhet.[71] Är det relevant att för arkivvetenskapens framtid att åtkomstkontroll och informationssäkerheten för molnhantering tas i beakt.[72] Därför är det viktigt att även ställa auktorisering och säkerhetspolicy gentemot molnlagring.

Enligt författarna I.Indu, Rubesh Anand och Vidhyacharan Bhaskar i *Identity and access management in cloud environment: Mechanisms and challenges* är identitets- och åtkomsthantering en av de bästa metoderna för att mäta molntjänster. I.Indu, Rubesh Anand och Vidhyacharan Bhaskar menar att IAM ger effektiv säkerhet för molnsystem. Modellen säkerställer med hjälp av säkerhetsmekanismer som autentisering, auktorisering och tillhandahållande av lagring och verifiering. I.Indu, Rubesh Anand och Vidhyacharan Bhaskar talar för att IAM-systemet garanterar säkerheten för identiteter och attribut hos molnanvändare genom att se till att rätt personer är tillåtna i molnsystemen. IAM-system

[66] Se avsnitt: Definitioner och i Resultatdelen; Access Control typer.
[67] Basic Amar, Johnsson Christoffer, Schuster Thomas, "*Rollbaserad åtkomstkontroll inom organisationer*, s. 50-51.
[68] Se avsnitt: Definitioner och i Resultatdelen.
[69] Yao, Moody, Bacons, s. 180.
[70] Neil Beagrie, Andrew Charlesworth, and Paul Miller, *How Cloud Storage can address the needs of public archives in the UK, Abstract.*
[71] Sifou, s. 41.
[72] Artefactual, Archivematica

hjälper också till att hantera åtkomsträttigheter genom att kontrollera om rätt person med rätt behörighet får tillgång till information som lagras i molnsystem. För närvarande använder många organisationer IAM-system för att ge mer säkerhet för känslig information som lagras i molnmiljön. [73]

Sifou, Kartit, Hammouch har i *Different Access Control Mechanisms for Data Security in Cloud Computing,* förespråkat attributbaserad åtkomstkontroll (ABAC[74]) som den mest lämpliga åtkomstkontrollen. Attributbaserad åtkomstkontroll tar utgångspunkt i egenskaper som beskriver användare, informationsobjekt och miljön där dessa verkar. Det kontrollerade systemet kan använda en policy för att bestämma om rätt attribut är tillgängliga. Modellen stödjer distribuerat system och ger skalbar och flexibel säkerhet verktyg. Följaktligen väljer vi ABAC-modellen för att säkerställa datasäkerhet i molnet. Denna mekanism är mer säker, flexibel och skalbar än andra modeller. Dessutom det ger en hierarkisk struktur för att underlätta åtkomstkontrollen. [75] [76]

4 Metod

För att ringa in mitt ämne har jag valt att i undersökningen fördjupa mig i auktorisering inriktat på system för digitalt bevarande. Den vetenskapliga metod jag har valt att använda mig av är *kvalitativ* metod. Vad *kvalitativ* forskning innebär är forskning som ger resultat som inte uppnåtts genom kvantifieringsmetoder, som till exempel statistisk. En kvalitativ analys innebär att en hypotes skapas utifrån samlade data som därefter tolkas. Jag har valt att använda den tillhörande metoden *konstant jämförande analys*, som innebär att den data som samlas in jämförs med andra liknande eller annorlunda data för att visa på dess relationer mellan varandra.[77]

Målet med jämförelse i den här studien är att finna likheter mellan begreppen och att mönster ska kunna upptäckas bland kategorierna. Konstant jämförelse går hand i hand med teoretisk provtagning som sker genom att data väljs ut med omsorg efter hand som de teoretiska idéer

[73] I.Indu P.M. Rubesh Anand Vidhyacharan Bhaskarb, *Identity and access management in cloud environment: Mechanisms and challenges, Introduction.*
[74] Se avsnitt: Definitioner och Resultatdelen; Access Control typer
[75] Lars Westerdah, Amund Gudmundson Hunstad, Fredrik Mörnestedt, *Sammanfattning av Projektet - Objektbaserad Säkerhet*, Totalförsvarets forskningsinstitut (FOI)
[76] Sifou, s. 44.
[77] Pickard Alison Jane, *Research Methods in Information*, s. 267, 269

som preliminärt uppkommer. Detta ger chans att svara på frågor som uppstått från analys över tidigare data.[78] Eftersom det inte finns så mycket tidigare forskning om auktorisering och säkerhetspolicy i system för digitalt bevarande, så känns det naturligt att söka data om åtkomsthantering i informationssystem som ändå tillhör samma område som system för digitalt bevarande. Insamlingen av data har därefter tolkats och jämförts med varandra och är den mest lämpade metoden för denna undersökning[79] för att kunna få svar på hur relationen ser ut mellan auktorisering och säkerhetspolicy för system för digitalt bevarande.

Informationsinhämtningen har gjorts via sökningar på internet och litteratur. All den data som har inhämtats har valts ut med omsorg, både inom Sverige och internationellt. Gällande föreskrifter och standarder har de hämtats från Riksarkivet, Myndigheten för samhällsskydd och beredskap, Sveriges kommuner och landsting (SKL), Datainspektionen och National Institute of Standards and Technology. De uppslagsverk och sökportaler som jag har kunnat söka fram relevanta vetenskapliga dokument på är hemsidor som Cambridge University, Springer, Research Gate, ACM Digital Library, Computer Security Resource Center (CSRC), Nationalarchives. Jag har använt mig av artiklar från internationella tidskrifter som Securitymagazine, International Journal of Computer Science & Engineering Survey, Weekly Digital Magazine, American Journal of Software Engineering and Applications, SC Magazine UK. Projektrapport från Totalförsvarets forskningsinstitut, uppsatser från Lund och Göteborgs universitets institutioner för informationsteknologi har kunnat förse mig med information till ämnet. Hemsidor av verksamma företagare inom digitalisering som Artefactual, som är ledande utvecklare av mjukvarorna Archivematica och AtoM för långtidsbevarande sågs som högst relevant till min insamling av data. Inhämtning har även gjorts från litteratur som Sherwood, Clark, Lynas, *Enterprise Security Architecture - A Business-Driven Approach.*

De sökord jag använt mest under insamlingen av all data; “Authorization”, “Security Policy”, “Access Control”, “Information system”, “Digital preservation system”.

Under undersökningen var det viktigaste att jag höll ett öppet förhållningssätt och vidareutbildat mig under undersökningens gång, vartefter nya data har tillkommit för att kunna dra slutsatser. Detta öppna förhållningssätt har även låtit tillhörande frågeställningar till

[78] *A Purposeful Approach to the Constant Comparative Method in the Analysis of Qualitative Interviews*, s. 392-393
[79] Bibik Magdalena, Milton Filippa, Månsson Caroline, Svensson Linda, *Kvalitet i kvalitativa undersökningar*. s. 22.

min huvudsakliga frågeställning vara öppna och har fått utvecklats under arbetets gång. [80] Den första tillhörande frågeställningen jag valde att utgå från först var; ”Vilka huvudsakliga delar ska finnas med i en säkerhetspolicy för auktorisering i ett system för digitalt bevarande enligt myndigheters föreskrifter och standarder?” Jag valde att fördjupa mig i *Metodstödet- Ledningssystem för informationssäkerhet (LIS), Sherwood Applied Business Security Architecture (SABSA Modell), Identity and Access Management (IAM), Cloud Service Security* och främst delen *”Authorization”.* Jag började att undersöka vad Myndigheten för samhällsskydd och beredskap (MSB) ser på informationshantering och säkerhet samt Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar *RAFS: 2009:1, 6 kap Informationssäkerhet* - ska en plan för informationssäkerhet upprättas i ett arkiv och rutiner ska skapas för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld med utgångspunkt i standarden *SS-ISO/IEC 27002:2005.* Vidare samlade jag information om *SS-ISO/IEC 27001:2006 Ledningssystem för informationssäkerhet (LIS).* Under arbetets gång förstod jag att de två ISO-standarderna; *SS-ISO/IEC 27002:2005 och SS-ISO/IEC 27001:2006* båda var upphävda. Jag valde då att vidare undersöka och samla information om två gällande ISO- standarder inom samma område: *SS-EN ISO/IEC 27001:2017 – Informationsteknik- Säkerhetstekniker- Ledningssystem för informationssäkerhet- Krav* och *SS-EN ISO/IEC 27002:2017 – Informationsteknik- Säkerhetstekniker- Riktlinjer för informationssäkerhetsåtgärder.* Vidare valde jag att gå igenom *GAP- analys* som MSB har tagit fram, som ska fungera som en checklista för informationssäkerhet i verksamheten. Efter att noggrant studerat och samlat in information om relevanta föreskrifter och standarder inom området växte därefter en till tillhörande frågeställning fram; ”Vilka system, modeller och mekanismer är lämpliga för åtkomstarkitektur?”. Jag samlade då in information från internet om åtkomstsystemen*: Identity and access management (IAM), Open Archival Information System (OAIS).* Vidare insamling av data om säkerhetsmodell *Sherwood Applied Business Security Architecture (SABSA)* och åtkomstkontrollmodeller. Genom alla den insamling av data förstod jag allt mer att den mest använda åtkomstkontrollmodellen är rollbaserad, därefter valde jag att vidare studera tillhörande frågeställning; ”Hur ser roller och behörighetsnivåerna ut i ett system för digitalt bevarande?”. Jag samlade information om roller i system för digitalt bevarande. För att få större inblick i hur dessa behörighetsnivåer kollas upp, valde jag att samla in information om revisionsspår så kallade loggar för att få en större förståelse för hur behörigheter och uttag av elektroniska handlingar kan spåras. Big data

[80] Bibik Magdalena, Milton Filippa, Månsson Caroline, Svensson Linda, *Kvalitet i kvalitativa undersökningar*. s. 22.

och Artificiell intelligens (AI) gentemot åtkomstkontroll för framtiden kom naturligt in i slutet av insamlingen, då jag förstod att de kommer allt mer ha en del i system för digitalt bevarande. Uppsatsen avslutas med en diskussion, slutsats och förslag till framtida forskning.

5 Teoretiskt ramverk

Jag har valt att utgå från fyra system och modeller för att söka svaret på min forskningsfråga. De system och modeller jag funnit relevanta för min frågeställning är följande; *Metodstödet- Ledningssystem för informationssäkerhet (LIS), Sherwood Applied Business Security Architecture (SABSA modellen), Identity and Access Management (IAM) och Cloud Service Security.* Valet av dessa fyra system och modeller har jag genom kvalitativ metod - med mängd av insamlade data, därefter tolkats vara de mest aktuella för att besvara min frågeställning. Genom att undersöka, klargöra och analysera dessa, visade det mig vägen genom arbetet, gav mig svar på frågeställningen samt har skapat nya kunskaper om hur relationen ser ut mellan auktorisering och säkerhetspolicy för system för digitalt bevarande.

Figur 1: Metodstödet – *Ledningssystem för informationssäkerhet (LIS)* är uppdelad i fyra områden som skapar tillsammans ett systematiskt informationssäkerhetsarbete; *Identifiera och analysera*, *Använda*, *Följa upp och förbättra* samt *Utforma*. *Utforma* som är det mest aktuella området för uppsatsen. [81]

Figur 2: *Sherwood Applied Business Security Architecture* (*SABSA Modell*) – Arkitektur komponenter [82] Det är främst det logiska lagret som uppsatsen kommer behandla.

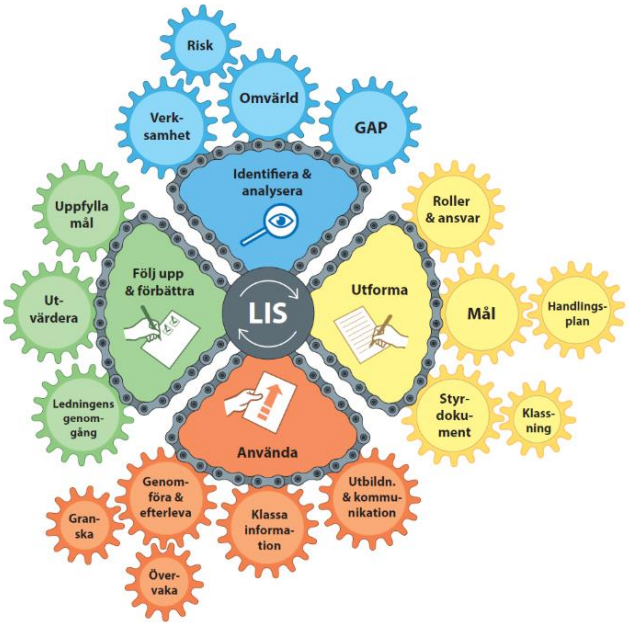
Figur 3: *Identity and Access Management (IAM)* [83] IAM är en organisatorisk och teknisk skyddsåtgärd, som har kontroll och utövar uppföljning av åtkomst.

Figur 4: *Cloud Service Security*.[84] Uppsatsen utgår från delen ”*Authorization*” med de två delarna åtkomstkontrollmekanismer och åtkomstkontrollstyrning. Modellen är aktuell då

[81] MSB, *Metodstödet*
[82] Wood Andy, *SABSA Model – Architectural Components*
[83] Jetabroad, *IAM - Identity and Access Management*
[84] I.Indu, Rubesh Anand, Vidhyacharan Bhaskar, *Identity and access management in cloud environment: Mechanisms and challenges*, Engineering Science and Technology

användningen av molnlagring i digital bevarande används allt mer och utvecklas snabbt.[85] Access Control (åtkomstkontroll) betraktas som en nyckelkomponent i molnsäkerhet.[86] Archivematica och AtoM[87] kan integreras med arkivmolnlagring samt lagringstjänst därav viktigt att molnsäkerhet tas med i undersökningen. [88]

Figur 1.



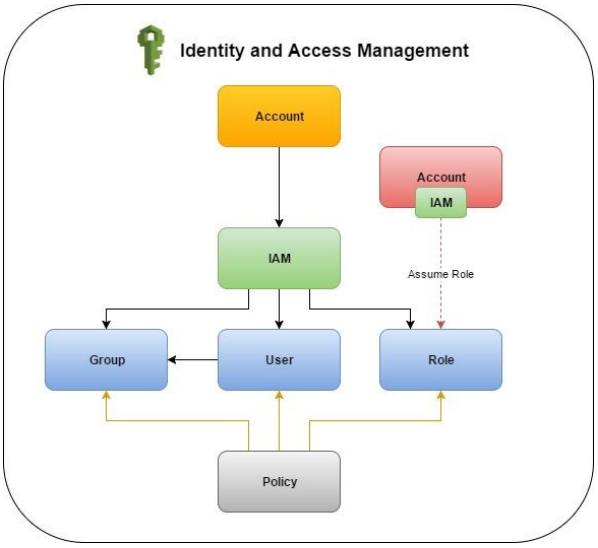
Figur 2.

SABSA Model – Architecture Split

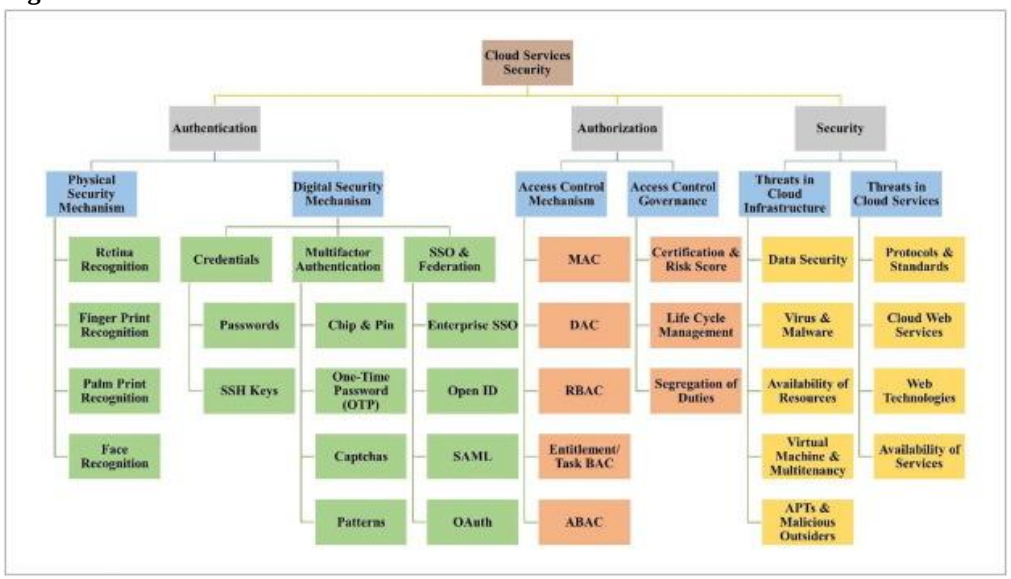
	WHAT (Assets)	WHY (Motivation)	HOW (Process)	WHO (People)	WHERE (Location)	WHEN (Time)
CONTEXTUAL (Business)	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
CONCEPTUAL (Architecture)	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
LOGICAL (Design)	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
PHYSICAL (Build)	Business Data Model	Security Rules, Practices & Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastucture	Control Structure Execution
COMPONENT (Tools)	Detailed Data Structures	Security Standards	Security Products & Tools	Identities, Functions, Action and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
SERVICE MANAGEMENT	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule
	Business Architecture	Security Architecture	Information Architecture	Application Architecture	Technology Architecture	Risk Management Architecture	Service Architecture

[85] Neil Beagrie, Andrew Charlesworth, and Paul Miller, *How Cloud Storage can address the needs of public archives in the UK, Abstract.*
[86] Sifou, s. 41.
[87] Se avsnitt: Resultat.
[88] Artefactual, Archivematica

Figur 3.



Figur 4.



6 Resultat

”Vilka huvudsakliga delar ska finnas med i en säkerhetspolicy för auktorisering i ett system för digitalt bevarande enligt myndigheters föreskrifter och standarder?”

6.1 Föreskrifter och standarder

Enligt Myndigheten för samhällsskydd och beredskap (MSB) ska rutiner för informationshantering resultera i att medborgare och företag känner sig trygga**.** Det är viktigt att offentlig förvaltning, medborgare och företag kan lita på varandra. Myndigheter måste

känna tillit till varandra vid utbyte av information och åtkomst. Regeringen vill att teknik för information och kommunikation ska verka för service, demokrati och effektivitet. Myndighetens beslut om ansvar och tjänstemannens arbetsbehov ska styra åtkomsten till systemet för digitalt bevarande. Lagstiftningar ska också beaktas, som till exempel handlingar som är offentliga (Offentlighets- och sekretesslagen). Riktlinjer ska också tas fram för åtkomst och behörighet som uppfyller de krav som finns gällande informationssäkerhet. Riktlinjerna ska också omfatta loggningskrav samt uppföljning, både internt och externt som till exempel samarbete med andra myndigheter. Rutiner för åtkomst- och behörighet ska finnas som beskriver behörighetsfördelning, upphörande, förändringar och uppföljning. Tilldelning av behörighet ska systemägare eller tjänsteman med liknande ansvar för information ansvar för.[89]

Eftersom uppsatsen behandlar området system för digitalt bevarande är det högst relevant att utgå från Riksarkivets föreskrifter. *Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling) RA-FS 2009:1, 6 kap* ska en plan för informationssäkerhet upprättas i ett arkiv. Det som är planens syfte är att myndigheter ska skapa rutiner för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld med utgångspunkt i standarden SS-ISO/IEC 27001:2006 (LIS- Ledningssystem för informationssäkerhet). Detta kan ske genom bl.a. behörighetssystem, loggsystem, skydd mot skadlig kod, säkerhetskopior etc. Riksarkivet beskriver även att myndigheten ska ta stöd av riktlinjerna i SS-ISO/IEC 27002:2005.[90] Följande står skrivet i Riksarkivet RA-FS 2009:1: 6 kap. Informationssäkerhet 1 §: *"Myndigheten ska för att säkerställa ett bevarande av de elektroniska handlingarna skapa och upprätthålla rutiner för samt vidta åtgärder för att skydda handlingarna från skada, manipulation, obehörig åtkomst och stöld. Det ska ske med utgångspunkt ur SS-ISO/IEC 27001:2006, Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet (LIS), och med stöd av riktlinjerna i SS-ISO/IEC 27002:2005, Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet."*

Plan för informationssäkerhet 2 §: *"Myndigheten ska upprätta en plan för hur de elektroniska handlingarna ska skyddas och dokumentera de åtgärder och rutiner som ska vidtas. Myndigheten ska regelbundet kontrollera och dokumentera hur planen efterlevs."*

[89] Allmänna råd MSBFS Remissutgåva, *Förslag till Myndigheten för samhällsskydd och beredskaps allmänna råd och kommentarer om krav på informationssäkerhet*, s. 2, 6.
[90] Riksarkivet, *Informationssäkerhet*

Riskanalys innan driftsättning eller uppdrag 3 §: *"Myndigheten ska genomföra en riskanalys innan driftsättning eller innan uppdrag ges till annan myndighet eller enskild för att bedöma behovet av säkerhetsrutiner*. "Skydd 4 §: "*Elektroniska handlingar ska förses med behörighetssystem¸ loggsystem och skydd mot skadlig kod om det inte är uppenbart obehövligt."* [91]

SS-ISO/IEC 27001:2006 - Ledningssystem för informationssäkerhet (LIS)

Ett Ledningssystem för informationssäkerhet, förkortat LIS består av policy, riktlinjer och rutiner med tillhörande resurser och aktiviteter för hantering av informationssäkerhet i organisationen. I ett ledningssystem är ledningens stöd centralt. Ledningen bör se till att organisationen antar en policy för informationssäkerhetsarbetet. I också riktlinjer och styrdokument kan ledningen ge vägledning till mellanchefer och annan personal. I riktlinjer är det vanligt med bestämmelser om till exempel: incidenthantering, behörighetsadministration och loggning. Det är viktigt att policy och riktlinjer går att förstås och att alla i organisationen vet om att det finns. Detta skapar trygghet i vardagliga arbetet. Att hålla i ett ledningssystem innebär därför också att informera personal om de regler som finns. [92] LIS är uppdelad i fyra områden. Dessa fyra områden i LIS skapar tillsammans ett systematiskt informationssäkerhetsarbete; *Identifiera och analysera*, *Använda*, *Följa upp och förbättra* samt *Utforma*. *Identifiera och analysera* innebär: Verksamhet, Omvärld, Risk och Gap. *Använda* innebär: Genomföra och efterleva, Utbildning och kommunikation och Informationsklassning. *Följa upp och förbättra* innebär: Utvärdera övervakning/ mätning och Ledningens genomgång. *Utforma* som är det mest aktuella området för uppsatsen innebär: *Organisation* - roller och ansvar, som betyder att en tydlig organisation för informationssäkerhet ska skapas. Det innefattar; roller, ansvar och arbetsuppgifter. Det ska bli dokumenterat om ansvar, mandat, organisation och roller. Råd och forum för informationssäkerhet ska också behandlas i denna del. *Informationssäkerhets mål* - I denna del ska verksamhetens strategiska samt kortsiktiga mål med informationssäkerhet, utifrån verksamhetens interna och externa förutsättningar. Mål i organisationen, risk-analysen och gap-analysen ska stödja detta. *Styrdokument*- Ett beslutande dokument. Den reglerar aktiviteter i organisationen som är informationssäkerhets relaterade. Innefattar informationssäkerhetspolicyn, underliggande styrdokument som exempelvis riktlinjer och rutiner. *Handlingsplan* - en årlig och beslutad plan som syftar till att eliminera och/eller reducera valda information säkerhetsrelaterade brister. Handlingsplanens syfte är att behov

[91] Riksarkivet, *RA-FS 2009:1*
[92] MSB, *Ledningssystem för informationssäkerhet – LIS.*

genomförs och följs upp. Resultatet av Gap-analysen och informationssäkerhetspolicyn används som hjälp till handlingsplanen. Handlingsplanen ska behandla dessa punkter; mål, aktiviteter, kostnader, ansvar och tidsplan. *Klassningsmodell* - Skapa en modell för att klassa informationstillgångar, det vill säga information och resurser för att hantera information. Konfidentialitet, riktighet, tillgänglighet och säkerhetsåtgärder är i fokus. Klassning modellen ska följas upp, övervakas, mätas samt göras intern/extern revision.[93]

De två ISO-standarderna *SS-ISO/IEC 27001:2006 och* SS-ISO/IEC 27002:2005 är båda upphävda. Vidare undersöker jag två gällande ISO-standarder inom samma område.

SS-EN ISO/IEC 27001:2017-Informationsteknik-Säkerhetstekniker- Ledningssystem för informationssäkerhet- Krav

Enligt standarden ska *styrning av åtkomst* innebära verksamhetskrav för styrning av åtkomst. Målet ska vara att begränsa åtkomst till information och informationsbehandlingsresurser. De verksamhetskrav som ska dokumenteras ska bygga på de regler som skrivits för styrning av åtkomst. Reglerna ska upprättas, dokumenteras och vara till hjälp vid uppföljning. *Hantering av användaråtkomst* är en viktig del, med målet att säkerställa att behörig användaråtkomst uppfylls och att inte obehörig åtkomst sker. Hanteringen innebär åtgärder som *användarregistrering* och *avregistrering*. För att få åtkomst krävs att beslut har gjorts om det är en behörighet som innebär att endast kunna läsa informationen, eller om åtkomsten ska innebära att personen både ska kunna läsa och ändra informationen. Myndigheten ska ta fram en process för *tilldelning och återkallande av åtkomsträttigheter*, det samma gäller även för åtkomsträttigheter som är privilegierade. Åtkomsträttigheterna ska ständigt kontrolleras av tillgångens ägare, det innebär *justering* och *borttagning*. *Loggning* är också en viktig del som menas med att händelser loggas för att övervakas och för att kunna skapa bevis. Enligt standarden innebär loggning att aktiviteter som användaren gör, även avvikelser, felaktigheter, andra händelser gällande informationssäkerhet ska komma fram. Händelseloggar ska regelbundet framställas, bevaras och undersökas. De verktyg som ska användas till loggning samt informationen som skrivs utifrån det ska skyddas mot obehörig åtkomst. Loggning gäller även för administratörer samt operatörer för systemet/systemen. *Tid* är också en viktig del för att skydda mot obehörig åtkomst, det betyder att systemklockor ska synkroniseras till samma källa för tid.[94]

[93] MSB, *Metodstödet*
[94] SS-EN ISO/IEC 27001:2017-*Ledningssystem för informationssäkerhet- Krav*

SS-EN ISO/IEC 27002:2017-Informationsteknik-Säkerhetstekniker-Riktlinjer för informationssäkerhetsåtgärder

Standarden SS-EN ISO/IEC 27002:2017 tar upp liknande som SS-EN ISO/IEC 27001:2017 men går in djupare i införandet, som menas med de åtgärder verksamheten ska ta sig an. Enligt standarden ska ett ramverk över organisationen tas fram. Målet med detta är att ramverket ska styra organisationens införande och drift av informationssäkerhetsarbetet.

Användarkonton som är unika och som är kopplade till rätt handlingar, delade konton är tillåtet endast vid behov och ska vara dokumenterat och godkända. *Roller och ansvar* inom informationssäkerhet ska tas fram, benämnas och tilldelas. Ansvarsfördelning ska tas enligt policyn för informationssäkerhet. Detta innebär även att specifika processer inom informationssäkerhet/behandling ska skrivas ned detaljerat. Ägaren av tillgången ska fastställa regler för roller angående styrning av åtkomst, rättigheter och begränsningar för vissa. *Säkerhetsrisker* gällande informationen ska styra hur skarpa dessa regler ska vara. Tilldelat informationssäkerhetsansvarig kan överlåtas till andra men de dokumenterat ansvariga ska dock följa upp att det blev gjort rätt. Det är enligt standarden viktigt att behörighetsnivåer ska dokumenteras och benämnas. Medarbetare med ansvarsområden ska även skrivas ned. Uppdelning av arbetsuppgifter är viktigt då det inte ska ske någon möjlighet till obehörig åtkomst, oavsiktlig ändring eller missbruk mellan ansvarsområden som står emot varandra. Ingen enskild person ska få tillgång utan tillstånd. Möjligheter till samverkan ska tänkas över gällande åtgärder av säkerhet. Utsedda personer bör ha *områdeskompetens* och vara ständigt med i utvecklingen. Styrning av åtkomst vanligaste principer är att personen beviljas tillgång endast till informationen som behövs för att utföra arbetsuppgifterna. Även att personen beviljas tillgång till de resurser som behövs, kan handla om IT-utrustning, program, rutiner etc. *Åtkomsträttigheter* samt reglerna för *klassning av information* ska stämma i överens (för samtliga nätverk och system verksamheten/erna har). *Åtkomstkontroller* ska både vara logiska och fysiska. Vilka verksamhetsmässiga krav som bör uppfyllas genom åtkomstkontroller ska informeras till användare och tjänsteleverantörer. Rollbaserad åtkomstkontroll är lyckat hos många verksamheter enligt standarden. Gällande *Tilldelning, borttagning eller justering av användaråtkomst* är detta citat högst aktuellt, taget från standarden *"Allt är generellt förbjudet om det inte uttryckligen tillåts."* Hantering av användaråtkomst ska ske regelbundet. Det innebär koll gällande identifiering, ta bort, inaktivera användare identifikationer. Det ska säkerställas att överflödiga användarkonton ska inte utfärdas. En process för tilldelning av användaråtkomst ska tas fram, då det beskriver process för tilldelning och återkallande av

åtkomst för alla typer av användare till informationstillgångar/system/tjänster. Processen innebär att ägaren ska ge tillstånd och då kan även ett godkännande från ledning vara aktuellt. Processen ska även se till så att inte åtkomsträttigheter aktiveras innan tillstånd är klart, handha ett centralt *register över godkända åtkomsträttigheter*, anpassning av åtkomst för de användare som slutat eller bytt roll eller tjänst. *Privilegierade rättigheter* ska beskrivas, innebär information om begränsning och styrning utifrån deras behov samt rättigheter/regler i enlighet med de regler som finns för styrning av åtkomst. Dokumentationen om tilldelning ska också omfatta ett formellt godkännande för varje system eller process och giltighetstid för behörighet. Det är viktigt att arbetstagarens kompetens ses över regelbundet för att se om kompetensen stämmer i enlighet med informationstillgångar. Denna granskning av rättigheter ska ske regelbundet av ägaren av tillgångarna. Det står skrivet i standarden att användarkonton med åtkomsträttigheter som inte används, som har lämnat verksamheten ska omedelbart tas bort eller rent av avaktiveras. Det innebär även fysisk och logisk åtkomst. Borttagning/justering kan ske genom borttagning, ta tillbaka eller byta ut nycklar, ID-kort, resurser för informationsbehandling, prenumerationer. Den dokumenterade informationen om behörigheten ska följas och tas bort. Om ett delat användarkonto med en person som slutat ska personen tas bort från grupp åtkomstlistor och informera övriga gruppen. Kraven på begränsning av åtkomst innebär att det ska vara möjligt att i systemet kunna styra åtkomsten och styra vilken data som kan nås av en viss användare. Det innebär att åtkomsträttigheterna ska kunna styras, det innefattar funktioner som läsa, skriva, radera, exekvera, begränsa etc. [95] Informationssäkerhet vid *leverantörsrelationer* är också viktigt att benämna och dokumentera.

Att *inrätta* roller är en politisk fråga för den säkerhetsmyndighet som ansvarar för policyn på det området. Processen kräver en noggrann analys av företagens behov för att identifiera de roller som ska användas. Målet bör vara att skapa endast få roller för att minimera rollåtkomst administration. I vissa applikationer kan det vara acceptabelt att ha endast en roll - du tillhör eller du tillhör inte. [96]

[95] SS-EN ISO/IEC 27002:2017- *Informationsteknik- Säkerhetstekniker- Riktlinjer för informationssäkerhetsåtgärder*
[96] Sherwood, s. 309.

6.1.1 GAP-analys

Myndigheten för samhällsskydd och beredskap har tagit fram en GAP-analys. GAP-analysen är en del av metodstödet från ”informationssäkerhet.se” som tidigare har beskrivits i uppsatsen. Den GAP-analys som Myndigheten för samhällsskydd och beredskap talar för fungerar som en checklista för informationssäkerheten i verksamheten. De huvudsakliga rubrikerna i GAP-analysen beskriver utifrån nivåläget; “Nivå: 0=Oacceptabel Risk (Ingen Efterlevnad), 1=Risk (Bristfällig Efterlevnad), 2=Liten Risk (Acceptabel Efterlevnad), 3=Mycket Liten Risk (Stor Efterlevnad)”. Djupare under varje rubrik i GAP-analysen är det så kallade nivåstyrande frågor och då ska något av dessa alternativ besvaras. JA, NEJ, VET EJ.

6.1.2 Verksamhetskrav på styrning av åtkomst

Under kapitel 11. *Styrning av åtkomst*, 11.1 *Verksamhetskrav på styrning av åtkomst.* Står detta målet beskrivet: *“Mål: Att styra åtkomst till information. Åtkomst till information, informationsbehandlingsresurser och verksamhetsprocesser bör styras på grundval av verksamhets- och säkerhetskrav. Regler för styrning av åtkomst bör ta hänsyn till policyer för spridning och behörighet till information”.* Vidare står det att en

åtkomstpolicy ska arbetas fram (11.1.1 Åtkomstpolicy) och den borde fastläggas, dokumenteras och granskas. Detta ska vara baserat på de verksamhets- och säkerhetskrav som är aktuella gällande åtkomst. Åtkomstpolicy tillhör säkerhetsåtgärd då utan åtkomstkontrollpolicy ökar risken att användare kan få, eller har kvar en högre rättighet än vad de egentligen behöver. Detta leder till obehörig åtkomst och risken för attack ökar.

De nivåstyrande frågor som tillhör Åtkomstpolicy är följande: regler för styrning av åtkomst och rättigheter för varje användare eller grupp av användare. Säkerhetsåtgärder för åtkomst kan vara både logiska och fysiska. Användare av tjänster bör få veta tydligt de verksamhetskrav åtkomststyrningen skall uppfylla. Det policyn bör ta hänsyn till är: de säkerhetskrav på varje enskild verksamhetstillämpning, identifiering/riskanalys av all information som rör verksamhetstillämpningarna, policyer för informationsspridning och rättigheter, t.ex. informationsklassificering. Konsekvenser som finns mellan system och nätverk åtkomststyrningsriktlinjer och policyer för informationsklassificering. Regler som är rättsliga och avtalsrättsliga skyldigheter gällande åtkomstskydd av data eller tjänster. Åtkomstprofiler för användare med vanliga befattningar. Åtkomsträttigheters hantering i

distribuerade miljöer och i nätverksmiljöer (uppkoppling ska tas hänsyn till). Åtskillnad av roller vid styrning av åtkomst, t.ex. åtkomstbegäran, åtkomsttillstånd, åtkomstadministration;

Krav på formellt godkännande av begäran om åtkomst. Krav på periodisk granskning av styrningen av åtkomst. Borttagning av åtkomsträtt.

Under kapitel 11. *Styrning av åtkomst*, 11.2 *Styrning av användares åtkomst*

står detta målet beskrivet: *"Mål: Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem. Formella rutiner bör finnas för att styra tilldelningen av åtkomsträttigheter till informationssystem och tjänster. Rutinerna bör täcka alla stadier i användaråtkomstens livscykel, från den första registreringen av nya användare till slutlig avregistrering av användare som inte längre behöver åtkomst till informationssystem och tjänster. Särskild försiktighet bör iakttas, där det är lämpligt, i fråga om behovet av att styra tilldelning av privilegierade åtkomsträttigheter som tillåter användare att förbigå normala systemspärrar."*

Under 11.2 *Styrning av användares åtkomst* beskrivs 11.2.1 *Användarregistrering* som innebär registrering, avregistrering (medge, återkalla åtkomst) samt att det ska finnas en formell rutin för de gällande informationssystem samt tjänster som används. Detta tillhör kritisk säkerhetsåtgärd därför om det saknas formella rutiner för registrering samt avregistrering av användare ökar risken för att felaktiga rättigheter ges. Användarkonton som finns kvar i systemet som inte används ökar risken för angripare. De nivåstyrande frågorna tillhörande detta område är följande:

Rutin för registrering och avregistrering av användare borde innehålla; användning av unik användar-id, användning av grupp-id (när det är nödvändigt av verksamhets- eller driftskäl), kontroll av att användaren har systemägarens tillstånd att utnyttja informationssystemet eller tjänsten (ledningens godkännande kan vara nödvändigt), kontroll av åtkomstnivån är rättad efter verksamhetens ändamål samt överensstämmer med säkerhetspolicy. Skriftligt besked till användarna om tilldelade rättigheter till åtkomst ska ges. Krav på att användare undertecknar förbindelse som visar att de förstår reglerna för åtkomst. Säkerställa att tjänsteuppdragstagare inte tillåter åtkomst förrän tillståndsrutinen fullgjorts. Skapa ett formellt register över alla personer med åtkomsttillstånd, omgående ta bort eller blockera åtkomsträtten för användare som har bytt roller eller arbetsuppgifter eller lämnat organisationen. Periodiskt kontrollera och avlägsna eller blockera redundanta användar-id och konton. Säkerställa att inaktuella användaridentiteter inte tilldelas andra användare.

Nästa tillhörande område är 11.2.2 *Hantering av särskilda rättigheter*

Tilldelning och användning av privilegierad åtkomsträtt bör begränsas och styras. Denna del tillhör kritisk säkerhetsåtgärd för utan rutiner för att hantera åtkomsträttigheter ökar risken för att användare får högre rättigheter än de behöver. Tilldelade privilegier bör styras med formell process, det inkluderar dessa delar: åtkomstprivilegier som avser enskilda system, en rutin och register för tilldelning av behörighet, särskilda rättigheter bör inte beviljas förrän tillståndsrutinen är färdig, utveckling och användning av systemrutiner bör föredras för att undvika behov av att medge särskilda rättigheter till användare; utveckling och användning av program som undviker behovet att utnyttja privilegier bör främjas, privilegier bör tilldelas med användning av annan användaridentitet än den som utnyttjas i den normala verksamheten.[97]

6.2 Åtkomstsystem

”Vilka system, modeller och mekanismer är lämpliga för åtkomstarkitektur?”

6.2.1 Identity and access management

Identity and access management (IAM) är ett system för att bestämma vilka användare som ska tillåtas att få tillgång till en organisations it-nätverk samt de resurser som varje användare ska tillåtas att få åtkomst till. Resurser i nätverket handlar om information, hårdvara och tjänster. IAM:s syfte är att det ska finnas funktioner för att administrera användare i nätverket. [98] IAM-systemet ska ske med verktyg och teknik till administratörer. Det innebär att administratörerna ska kunna ändra en användares roll, spåra aktiviteter som användaren gör/gjort, skapa rapporter om aktiviteter som gjorts, policyer ska genomföras. IAM- system ska vara utformade att dessa ska möjliggöra att användaråtkomst ska kunna administreras över hela företaget. Policyer samt bestämmelser ska överensstämma och ta hjälp av IAM-systemet. Arkitekturen för IAM syftar till att kunna vara som stöd till de olika regelverk som gäller för respektive sektor/verksamhetsområde. [99] Identitets- och åtkomsthantering är en viktig del i alla säkerhetsplaner i företaget. Många organisationer har användarna ibland fler åtkomstbehörigheter än vad som egentligen är nödvändigt. Ett IAM- system som är utförligt gjord med tillämpning av regler för åtkomst samt policy över hela organisationen. Fördelar

[97] MSB, *Gapanalys - checklista, 11. Styrning av åtkomst,* s. 152-162.
[98] Computer Sweden, *Identity and access management*
[99] Inera, s. 11-12.

med ett fungerande IAM-system är att företagets produktivitet ökas och kostnader hålls nere för att ingen information läcks ut till fel användare. Oavsett vilken miljö som arbetas ifrån säkras, det gör att produktiviteten i företaget stärks. [100] För närvarande använder många organisationer Identity and Access Management system för att förse med mer säkerhet till känslig information som är bevarad i molnmiljön (Cloud Environment). [101] Tidigare var IAM ett system uppbyggt av fyra stycken element. Elementen omfattade en katalog över personuppgifter som systemet använder för att definiera enskilda användare. Det andra elementet var en verktygsuppsättning som hade funktioner som att lägga till, ändra, ta bort data. Det tredje elementet var ett system som reglerade användaråtkomst och det innefattade säkerhetspolicyer samt åtkomstbehörigheter. Det fjärde och sista elementet var ett revisions- och rapporteringssystem som beskrev vad som händer i systemet. Idag är det mer komplexare. Nu när säkerheten oftare är hotad innehåller identifieringssystem idag även verktyg som biometri som innebär autentiseringstekniker som bygger på mätbara fysiska egenskaper som kan kontrolleras automatiskt som exempelvis ansiktsigenkänning, röst och fingeravtryck. Samt kan identifieringsverktyg innehålla maskininlärning, artificiell intelligens samt autentisering som är riskbaserad.[102] [103]

6.2.1.1 IAM och GDPR

Det är främst två krav The General Data Protection Regulation (GDPR[104]) ställer på hanteringen av personuppgifter som gör IAM relevant. De är principer: “Personuppgifter får bara behandlas i enlighet med angivet ändamål för behandlingen och så länge detta ändamål är giltigt, därefter ska de raderas.”, “Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet, inklusive skydd mot obehörig eller otillåten behandling.”. Varför GDPR och IAM hänger ihop är för att identiteter, konton och behörigheter är personuppgifter. IAM är en organisatorisk och teknisk skyddsåtgärd, som har kontroll och utövar uppföljning av åtkomst till personuppgifter inom en organisation.[105]

[100] James Martin, John K. Waters, *What is IAM? Identity and access management explained*
[101] Indu, s. 575-576.
[102] James Martin, *What is IAM? Identity and access management explained*
[103] Beal Vangie, Webopedia, *biometrics*
[104] Datainspektionen, Dataskyddsförordningen (GDPR)
[105] Acando, *Så ökar ni ert digitala förtroende*

6.2.2 Open Archival Information System

Open Archival Information System (OAIS). OAIS är ett arbete gällande en referensmodell för ett öppet arkivinformationssystem som CCSDS och Internationella organisationen för Standardisering (ISO) har arbetat fram.[106] Begreppet PDI som nämns i OAIS står för *Preservation Description Information.* Den information som är nödvändig för tillräcklig bevarande av innehållsinformation och som kan kategoriseras som *Proveniens, Referens, Fixitet, Kontext* och *Access Rights Information*. Gällande *Access Rights Information* anger villkoren för tillträde, inklusive bevarande, distribution och användning av innehållsinformation. I OAIS modellen beskrivs ett exempel av PDI. Gällande informationstypen *Rymdvetenskapsdata* innehåller kolumnen "Access Rights" följande: identifiering av den behöriga gemenskapen (Åtkomstkontroll), behörighets beviljande för bevarande och för distribution samt Pointers to Fixity och provenance information (t.ex. digitala signaturer och rättigheter innehavare). Gällande informationstyp: *Digitala biblioteks kollektioner,* är dessa Access Rights kopplade till den typ av information: rättsliga ramverk, licens erbjudanden, specifikationer för rättigheter tillämpning åtgärder tillämpas vid spridningstid, behörighets beviljande för bevarande och för distribution. Information om vattenmärkning tillämpas vid inlämning och bevarande tid, pointers to Fixity och Provenance Information (t.ex. digitala signaturer och rättigheter innehavare). Gällande informationstyp *Mjukvarupaket* är följande aktuellt: utpekad gemenskap, rättsliga ramverk

licens erbjudanden, Information om vattenmärkning tillämpas vid inlämning och bevarande tid, pointers to Fixity och Provenance Information (t.ex. digitala signaturer och rättigheter innehavare).[107]

6.3 Modeller

6.3.1 Sherwood Applied Business Security Architecture

Sherwood Applied Business Security Architecture (SABSA). Startpunkten för denna modell var *ISO 7498-2 1989 "Information processing systems- Open Systems Interconnection - Basic Reference Model - part 2: Security Architecture.* [108] Modellen är baserad på en

[106] *(OAIS),* s. 3.
[107] Ibid. s. 4-31/32.
[108] Sherwood, *Preface.*

säkerhetsarkitekturmodell med 6 stycken lager; Contextual (Business), Conceptual (Architeture), Logical (Design), Physical (Build), Component (Tools), Service Management, och 6 stycken nyckelfrågor, som tidigare i uppsatsen har beskrivits i relaterad forskning avsnittet. Access Control System arkitekturens huvudsakliga delar enligt SABSA modellen besvarar frågorna; *Vem? Vad? Varför? När? Hur?*. Det just auktorisering tillhör är logisk säkerhet[109], som innebär fysiska säkerhetsmekanismer, i det här fallet gällande auktorisering är det Access Control List (ACL[110]) som finns i SABSA lager; ”Tools” under nyckelfrågan ”*Vem*”[111]. ACL refereras till varje objekt som anger de ämnen eller grupper av ämnen som får göra åtkomst till det objektet. Auktorisering tillhör applikations och systems säkerhetstjänster. Tjänsterna skyddar applikationer och system från missbruk och hackerattacker. Oftast ska de avslöja eller förhindra obehörig åtkomst av de som har beviljats åtkomst. Att skapa roller för en resursgemenskap är en policyfråga för den säkerhetspolicy ansvarige för systemet. Processen kräver noggrann analys av verksamhetens behov för att identifiera de roller som ska användas. Syftet ska vara att göra så fåtal roller som möjligt. Bara en roll kan vara aktuellt, då handlar det om att du tillhör eller inte. *Subject* - Ämnet är en part som begär tillgång. Det kan vara en mänsklig användare eller ett externt system som agerar efter användaren. *Object* - Objektet är resursen som ämnet begär tillgång till. Objektet kan vara en datastruktur som till exempel en fil eller datorsystem. *Access Control Enforcement Function* - Funktionen för kontroll av tillträdesstyrning. Funktionen genomför besluten om ämnesförfrågningarna ska få tillgång till objektet eller inte. *Access Control Decision Function* -Funktionen tar beslutet om huruvida åtkomstförfrågan kommer att beviljas eller nekas. *Subject registry* - Ämnesregistret innehåller all information om alla registrerade subject, inklusive dess namn, autentiseringsinformation och deras åtkomstbehörigheter. *Access Control List (ACL)* - ACL refereras till varje objekt som anger de ämnen eller grupper av ämnen som får göra åtkomst till det objektet. *Audit Logging sub-system* -Systemet lagrar alla uppgifter om alla åtkomstförfrågningar oavsett om användaren har beviljats eller nekats åtkomst till objektet. Åtkomstkontroll innebär att beslutet avgörs av följande frågor; *Är* subjektet registrerat? *Har* autentiseringen gått rätt till? *Innehåller* subjektets åtkomstbehörighets profil ett tillstånd till detta objektet? *Tillåter* åtkomstkontrolllistan som tillhör objektet att åtkomst ges? Ett strategiskt rollbaserat åtkomstkontrollsystem säkerställer från problem som till exempel säkerhetsrisker som kan uppkomma om företaget bara skulle

[109] Se avsnitt: Definitioner, *Logisk säkerhet*, s. 4.
[110] Se avsnitt: Teori, Figur 2
[111] Ibid.

använda sig utav ovanstående arkitekturs huvuddelar. Autentiserings service är en del, men också så kallad role-based access control system (RBAC).
I SABSA beskrivs strategin för autentisering, auktorisering och granskning enligt följande: Först gör så kallade ämnet, initiativtagaren (subject) en åtkomstförfrågan till åtkomstkontroll funktionen (Access Control Enforcement Function, Reference Monitor). Denna funktion samarbetar med Access Control Decision Function som avgör förfrågan och ger respons. Access Control Decision Function refererar till ACLs (Acess Control List) som i sin tur är kopplat till Object (målet). Är du godkänd i Access Control Decision Function ger Access Control Enforcement Function dig tillgång till objektet (målet). Varje objekt är refererade av en ACE i en ACL. Access Control Desicion Function skriver en registrering av en begäran och beslut genom revisionsloggar. Access Control Decision Function refererar till ämnesregistret och profiler (regler). [112]

6.3.2 OASIS

OASIS är en rollbaserad åtkomstkontrollmodell för att uppnå säker drift av tjänster i en öppen, distribuerad miljö. Användarna måste presentera de nödvändiga uppgifterna i det angivna sammanhanget för att aktivera en roll eller anlita en tjänst. Roller aktiveras endast under en session. En roll avaktiveras omedelbart om någon av villkoren för medlemskapsregeln blir falsk. OASIS använder inte rolldelegation men istället utnämning, varigenom en användare i viss roll kan utfärda ett avtal med certifikat till en annan användare. De tjänstgöringsvillkoren för tjänster kan innefatta utnämningscertifikat, förutsättningsroller och miljöhinder. OASIS modellen som är rollbaserad menas med att tjänster namnger sina klientroller och verkställer policy för aktivering av roller samt service. Tjänsterna kan utvecklas självständigt, som en del av en lös federation av administrativa domäner, men servicenivåavtal (SLA) tillåta deras säkra samverkan. En stor fördel med en formell modell som OASIS är att det blir möjligt att resonera om förhållandet mellan en specifik policy och dess genomförande. Om rollaktiverings- och auktoriseringsbestämmelserna genomförs korrekt, kommer den angivna politiken att genomföras. [113]

[112] Sherwood, s. 239-240.

[113] Walt Yao, Ken Moody, Jean Bacon, s. 492, 536–538.

6.4 Access Control (åtkomstkontroll)

Verksamheter till system för digitalt bevarande måste se till att skydda mot förlust av information som lagras i system för digitalt bevarande, samt att säkerställa mot obehörig åtkomst och att åtkomst ska kunna spåras. Företaget utgår från frågan: *Vem?* En del av svaret till den frågan är så kallad Access Control (åtkomstkontroll). Det grundläggande målet med alla åtkomstkontrollmekanismer är att tillhandahålla ett verifierbart system för att garantera skyddet av information från obehörig och otillbörlig åtkomst, som anges i en eller flera säkerhetspolicyer.

Vad åtkomstkontroll innebär är att huvudfunktionen hos denna metod är att kunna styra en användares åtkomst till ett system och dess egna resurser. Det betyder att en systemadministratör använder den här mekanismen för att bestämma varje kunds rättigheter för åtkomsträttigheter. Systemadministratören bestämmer rättigheterna utifrån de fördefinierade kriterier som finns inom företaget eller organisationen. Gällande system för digitalt bevarande i molnmiljö så är åtkomstkontroll att betraktas som en stor nyckelkomponent i molnsäkerhet. De vanligaste och olika access control modeller (åtkomstkontroll modeller) diskuteras närmare nedan.[114] Organisationer som planerar att införa ett åtkomstkontrollsystem ska beakta: åtkomstkontrollpolicys, modeller och mekanismer. Nästan alla system som har ekonomi, säkerhet, integritet inblandat har någon typ av åtkomstkontroll. Det är ledningen som ansvarar för grundläggande säkerhet för informationen och dess informationssystem. De flesta system kräver komplex kontroll för åtkomst. Åtkomstkontroll policy är krav på hög nivå som anger hur åtkomst hanteras och vem som får tillgång till information samt under vilka omständigheter. På hög nivå verkställs policyerna för åtkomstkontroll genom en mekanism som översätter en användares begäran om åtkomst. Det är ofta i form av en struktur som ett system tillhandahåller, oftast Access Control List. [115] Digitala bevarandestrategier fokuserar på de strategier som varje system erbjuder för att säkerställa långsiktig tillgång, integritet och äkthet av lagrade data. Auktorisering och autentiserings funktioner bedömer förekomsten av åtkomstkontrollmekanismer och möjligheten att spåra användarnas åtgärd över data.[116]

[114] Sifou, s. 41.
[115] Dr. Vincent Hu, *Access Control Policy and Implementation Guides*.
[116] Carlos André Rosa, Olga Craveiro and Patricio Domingues, *Open Source Software For Digital Preservation Repositories: A Survey*, s. 27.

6.4.1 Access Control typer

6.4.1.1 Basic Access Control

Basic Access Control (BAC) är en organisationsbaserad åtkomstkontroll. I denna modell beror tillgången till molnresurser oftast på användarens roller inom en organisation. Olika parametrar har inverkan på beslutsfattande som ämne, handling, objekt, vy och sammanhang. Denna lösning syftar till att säkerställa finjusterad åtkomstkontroll. I ett nödfall kan en särskild roll tilldelas en läkare för att hantera den särskilda situationen. [117]

6.4.1.2 Discretionary Access Control

Discretionary Access Control (DAC) står för diskretionär åtkomstkontroll som är en typ av säkerhetsåtkomstkontroll. Den ger tillgång till eller begränsar objektåtkomst via en åtkomstpolitik bestämd av ett objekts ägargrupp och / eller ämnen. DAC är diskret, eftersom personen (ägaren) kan överföra autentiserade objekt eller informationstillträde till andra användare. Det menas med att ägaren bestämmer objektbehörighet. Enligt DAC har varje fil/dataobjekt en ägare och det är den som bestämmer åtkomsten. Användaren kan överföra objektägande till en annan användare och bestämma andra användares åtkomsttyp, efter flera försök begränsar behörighetsfel användaråtkomsten. Obehöriga användare kan inte se objektets egenskaper, som till exempel filstorlek och namn. Objektåtkomst bestäms under behörighetskontrolllistan (ACL) och baseras på användaridentifiering och / eller gruppmedlemskap. [118] Ägaren av objekt styr åtkomsten till dessa objekt baserat på användarentitet. Dessutom kan användarna skapa behörigheter konfigurationer för dataåtkomst och dela dem med andra ämnen. Detta är den vanligaste modellen för kommersiella operativsystem på grund av dess flexibilitet jämfört med andra modeller. [119]

Fördelarna med DAC är att den gör åtkomstkontrollen mer flexibel samt att den används i miljö som inte kräver en hög skyddsnivå. Huvudsaklig fördel med att använda DAC, är för den gör möjligheten att kontrollera systemobjektet detaljerat. DAC kan då enkelt användas för att genomföra åtminstone privilegierad åtkomst. DAC är också intuitivt i implementering och

[117] Ibid. s. 42.
[118] Techopedia™, *Discretionary Access Control (DAC).*
[119] Sifou, s. 42.

är mestadels osynligt för användarna så det anses vara mest kostnadseffektiva för hem- och småföretagare. Nackdelarna är att DAC passerar privilegier mellan användare, attackeras enkelt av trojaner samt att säkerhetspolitiken kan förändras med skadligt program som införs. Underhåll av systemet och verifiering av säkerhetsprinciper är extremt svårt för DAC-system eftersom användare kontrollerar åtkomsträttigheter till ägda objekt. [120] [121]

6.4.1.3 Mandatory Access Control

Mandatory Access Control (MAC) står för en obligatorisk åtkomstkontroll. Det innebär en uppsättning av säkerhetspolicyer som begränsas enligt systemklassificering, konfiguration samt autentisering. MAC- policyhantering/inställningar är begränsade till systemadministratörer. Systemadministratören ansvarar endast för hantering och definiera en policy för åtkomstkontroll som inte kan ändras av ämnen. För bästa praxis är MAC-policybeslut baserade på nätverkskonfiguration. MAC fördelar och nackdelar beror på organisatoriska krav. MAC ger strängare säkerhet eftersom endast en systemadministratör kan komma åt eller ändra kontroller. MAC-policyer minskar säkerhetsfel. MAC-hanterade operativsystem (OS) avgränsar och märker inkommande applikationsdata, vilket skapar en specialiserad extern program för åtkomstkontroll.[122] [123] Den obligatoriska åtkomstkontrollen är utbredd i datorsystem. MAC är mer tillförlitlig än diskretionär åtkomstkontroll, eftersom den gör det möjligt att blockera kanalerna för informationsläckage "enligt minnet". [124] MAC används mest i system där konfidentialitet är den centrala frågan. [125]

Fördelarna med MAC är att den ger stark säkerhet och har en centraliserad säkerhetspolitik. MAC är den modell som används av militär- och underrättelsebyråer för att den kan behålla begränsningar för klassificering åtkomstpolicy restriktioner. Trots detta är MAC jämförelsevis enkel och är en modell som är bra för system som är i fientliga miljöer (med hög risk för attacker) som till exempel webbservrar och finansinstitut där objekten som ska skyddas är värdefulla. Nackdelarna är att den behöver en hög systemhantering. Tilldelningen och säkerställandet av säkerhetsnivåer av systemet enligt MAC-modellen ställer begränsningar för

[120] Ibid. s. 40-44.
[121] Ausanka-Crues Ryan, Methods for Access Control: Advances and Limitations, s. 1-4.
[122] Techopedia™, *Mandatory Access Control (MAC).*
[123] Sifou, s. 41.
[124] S. V. Belim, S. Yu. Belim, *Implementation of Mandatory Access Control in Distributed Systems,* s. 1124
[125] Sifou, s. 41.

användaråtgärder som, samtidigt som de följer säkerhetsprinciperna, förhindrar dynamisk förändring av den underliggande policyn och kräver stora delar av operativsystemet och tillhörande verktyg till vara "betrodda" och placerade utanför ramen för åtkomstkontroll. MAC är också kostsamma och kan vara svåra att genomföra. [126] [127]

6.4.1.4 Attribute-based Access Control

Attributbaserad åtkomstkontroll (ABAC) tar utgångspunkt i egenskaper. Det finns olika varianter av attributbaserad åtkomstkontroll [128] men främst handlar det om egenskaper som beskriver användare, informationsobjekt och miljön där dessa verkar. Exempel på attribut: *Användare*: namn, identitet, roll, formella behörigheter, mm. *Informationsobjekt*: titel, format, ägare, kategori, mm. *Miljö*: IP-adress, nätverksadress, geografisk position, tid, mm. Det kontrollerade systemet kan använda en policy för att bestämma om rätt attribut är tillgängliga. Det samma gäller att relationen mellan attributen stämmer med policyn. [129] E-tjänsten får resursbegäran från användare och avgör om åtkomst ska godkännas eller inte. Med hjälp av förmågan Policy Decision Point (PDP) ska e-tjänsten se till att regelverket följs för ett åtkomstbeslut. Policy Enforcement Point (PEP) är en extern komponent (regelmotor) som e-tjänsten kan välja för att ge åtkomst eller inte, men denna komponent är inget krav. [130]

ABAC är baserad på användarens attribut, det betyder att innan du tillåter åtkomst till objekt, är det nödvändigt att jämföra attributen med de regler som är associerade med varje objekt för att bevilja eller neka åtkomst. ABAC löser problemet med att tilldela privilegier. ABAC bygger på en klient, en så kallad servermodell. Detta betyder att den kräver åtkomst till resurser av server/servrar för att realisera åtkomstkontroll.[131] ABAC är en nästa generations auktoriseringsmodell. Modellen ger en dynamisk, kontextmedveten och risk-intelligent åtkomstkontroll. ABAC använder attribut som byggstenar i ett strukturerat språk som definierar regler för åtkomstkontroll och beskriver åtkomstförfrågningar. Attribut är uppsättningar av etiketter eller egenskaper som kan användas för att beskriva alla enheter som måste övervägas för tillstånds ändamål. Varje attribut består av en nyckelvärdespar som "Roll

[126] Ibid. s. 40-44.
[127] Ausanka-Crues Ryan, Methods for Access Control: Advances and Limitations, s. 1-4.
[128] Lars Westerdah, Amund Gudmundson Hunstad, Fredrik Mörnestedt, *Sammanfattning av Projektet - Objektbaserad Säkerhet*, Totalförsvarets forskningsinstitut (FOI)
[129] Ibid.
[130] Inera, s. 25.
[131] Sifou, s. 42.

= Manager". Attributen hämtas ofta från olika informationssystem inom infrastrukturen. En policy kan således kombinera tillståndet för data i många system för att lösa en tillståndsförfrågan. Modellen möjliggör integration för att stödja arbetsflöden som innehåller IT-stöd från flera IT-system. Detta är praktiskt omöjligt att hantera med traditionella åtkomstkontrollmodeller.[132]

ABAC-modellen använder attribut för att definiera privilegier och tre typer av attribut är relaterade till åtkomstkontroll. Dessa är: ämne, resurs- och miljöattribut. Ett ämnesattribut, så kallad subjekt är ett ämne som är en enhet som kan driva resursen, det kan vara en användare, en ansökan eller en process. Varje ämne (subjekt) har många attribut som identifierar och beskriver ett ämne. Dessa attribut kan vara till exempel ID, namn, adress och titel. Resursattribut är en enhet som drivs av ämnena (subjekten) Det kan handla om webbserver, dokument etcetera. Varje resurs har många attribut att identifiera och beskriva en resurs som kan användas som en åtkomstkontrollpolitisk utvärdering. Gällande miljöattribut ska de användas till att beskriva olika miljöer när ett ämne får tillgång till en resurs, såsom teknisk, operativ, situationer och kontextmiljö. [133]Fördelarna med ABAC är att det ger mer flexibel i en dynamisk och distribuerad miljö. Är enklare att genomföra och den stöder det globala avtalet. Nackdelarna är att det kräver en lång körtid. ABAC är också svårt att hantera. [134] [135]

6.4.1.5 Role-Based Access Control

Rollbaserad åtkomstkontroll (RBAC) är en känd metod för åtkomstsäkerhet som bygger på en persons roll inom organisationen. Rollbaserad åtkomstkontroll är ett sätt att tillhandahålla säkerhet eftersom det endast tillåter anställda att få tillgång till information som de behöver för att göra sina jobb. I denna modell ges åtkomsträttigheter till roller som tilldelats användare. Varje användare kan ha mer än en roll. Det kan vara en uppsättning objekt och handlingar som är förknippade med användaren.

RBAC hindrar även personer att komma åt ytterligare information som inte är relevant för dem. En arbetstagares roll bestämmer de behörigheter som han eller hon beviljats och säkerställer att anställda på lägre nivå inte har tillgång till känslig information eller utför

[132] *Axiomatics, Attribute Based Access Control (ABAC), USA.*
[133] *Zhijie Fan, Ya Xiao1, Chunmei Wang2, Bing Liu, Research on Access Control in Cloud Storage System: From Single to Multi-Clouds,* s. 4.
[134] Ausanka-Crues, *Methods for Access Control: Advances and Limitations, Introduction, s. 1-4.*
[135] Sifou, s. 40-44.

uppgifter på hög nivå. RBAC har flera administrativa strategier centraliserade, hierarkiska, kooperativa, äganderätt eller decentraliserade.[136] [137]

En företagsanalys av all ämnesaktivitet utförs för att definiera ett antal ämnesroller. Dessa kan lätt kartläggas i arbetsfunktioner och arbetsbeskrivningar. Roller är väsentligen affärsbaserade. Detta ger ett mycket praktiskt sätt att se till att användarna beviljas (och begränsas till) de tillträdespersoner som behövs för att uppfylla sina jobb. Varje ämne tilldelas en eller flera roller och dessa lagras i det kalandraliserade ämnesregistret. Även i ämnesregistret lagras de målsystem som varje användare har blivit behörig för tillträde. Varje målsystem är nu inrättat för att registrera roller i stället för enskilt ämnesnamn i åtkomstkontroll listorna (Access Control lists= ACL) som är associerade med objekten i systemet. Dessa roller förändras sällan och kartläggs inuti målet åtkomstkontrollsubsystem på lokala objekt. Ännu viktigare är att varje målsystem nu bara har en handfull rollregistrering snarare än tusentals enskilda ämnesregistreringar. administratorn för dessa målsystemprofiler är nu sällsynt och lätt uppgift. Den exakta kartläggningen av en roll på en uppsättning systemobjekt beror på resultatet av analysen av affärsverksamheter för att bestämma att funktioner och data behövs för att uppfylla de arbetsuppgifter som är förenade med en särskild roll. [138]

RBAC är flexibel och stödjer administrativt genom att det kan ta på sig organisatoriska egenskaper när det gäller politik och struktur. Den administrativa uppgiften består av bevilja och återkalla medlemskap till uppsättningen av angivna namngivna roller inom systemet. När en ny person går in i organisationen, ger administratören helt enkelt medlemskap till en befintlig roll. När en persons funktion förändras inom organisationen kan användarens behörighet, enkelt raderas och nya kan beviljas. När en person lämnar organisationen raderas alla medlemmar till alla roller. En rollbaserad säkerhetspolitik är det enda logiska valet för en organisation som upplever en stor omsättning av personal.[139]

Fördelarna med RBAC är att säkerhetspolitiken är väldigt enkel att hantera, tilldelningen av roller baserad på minst privilegium minimerar skadan av information av inkräktare. I stora organisationer, konsolidering av åtkomstkontroll för många användare till en enda rollingång möjliggör mycket enklare hantering. RBAC är vanlig åtkomstkontroll för hälsovården.

[136] Sifou, s. 42.
[137] Techopedia™, *Role-Based Access Control (RBAC).*
[138] Sherwood, s. 241.
[139] David F. Ferraiolo and D. Richard Kuhn, *Role-Based Access Controls*

Genomförande inom hälsovårdssystemen, har dock varit en utmaning med ett brett utbud av vårdpersonal roller och uppgifter. RBAC är avgörande för säkerhetsaspekterna inom vårdorganisationerna. Nackdelarna är att det är svårt att implementera det i en dynamisk och distribuerad miljö. Omöjligt att ändra rättigheterna till åtkomst till användare utan att ändra användarens roller. [140] [141] [142]

6.5 Audit Trails (Revisionsspår)

Revisionsspår som också kallas för loggar handlar om att övervaka systemet. Loggar ger oss information om vad som hänt, och vad som händer nu. Det ger oss säkerhet för att det varnar om problem som till exempel att fel användare är inne i systemet/informationen. Försvarsåtgärder kan möjliggöras om loggar används i systemet. Alla misstänkta beteenden eller händelser av kritisk karaktär ska generera en varning som sedan ska ageras efter. En logg ska bland annat innehålla användar id, datum och tid för inloggning, framgångsrika och misslyckade åtkomst försök, terminal identitet.[143] Loggar ger historiskt bevis på aktivitet för övervakningsändamål eller rättsmedicinska undersökningsändamål. De behöver ett robust revisionsspår service inte bara mekanismer för att fånga och lagra händelsesinformationen utan även mekanismer för att skydda integriteten hos den lagrade informationen. [144] Den händelselogging som används för att spela in några systemhändelser kan ha betydelse för förvaltningen av tjänsterna. Händelseloggen skapar som sagt ett revisionsspår av vad som hänt, detta spår måste lagras under en överenskommen tidsperiod för att underlätta historisk analys och undersökning. Följande händelser anses som viktiga rörande säkerhetshanteringen i systemet; undantag - händelser som är ovanliga och bortom det mönster som normalt förväntas, misslyckade inloggningsförsök, framgångsrika inloggningar och efterföljande logoffs tillgång till några särskilt känsliga informationsresurser som har flaggats för åtkomst händelseloggning. Användning av privilegierade resurser som administratör eller rootidentifierare, fel i några logiska eller fysiska systemkomponenter, säkerhetsvarningar från antivirusprogram, brandväggar och intrångsdetekteringssystem, upphörande av säkerhetsuppgifter och auktorisationer.[145] En loggpost måste innehålla data som är tillräcklig

[140] Sifou. s. 40-44.
[141] (SAIC), The Healthcare RBAC Task Force, s. 1.
[142] Ausanka-Crues Ryan, Methods for Access Control: Advances and Limitations, s. 1-4.
[143] Cobb, *Best practices for audit, log review for IT security investigations.*
[144] Sherwood, s. 310.
[145] Ibid. s. 533-534.

för att kunna se posten som användbar. Dessa fält är vanliga i en händelselog; data och tid för händelsen, användare som är associerade med händelsen, logisk eller fysisk plats eller båda, evenemangstyp, alla andra kontextuppgifter som behövs för att förklara händelsen. [146] Vissa revisionsspår hålls under korta tidsperioder och lagras ofta i ett ändamålsenligt lagringsområde. Under andra omständigheter kan det vara lämpligare att hålla revisionsspår i flera år, i vilket fall de senaste händelseloggarna hålls online och det äldre materialet arkiveras varje månad eller så. Vilken typ av revisionsspår som helst är det normalt att lagras i kronologisk ordning och du måste ha lämpliga verktyg för att hantera och söka händelsesinformation. Dessa verktyg innehåller ett antal kapabiliteter: sökande efter vissa händelsetyper eller vissa identifierare, sökande efter vissa kombinationer och mönster av händelser, med hjälp av normal databas eller sökmotorfrågor definitioner (AND, OR, NOT, XOR) för att kombinera villkorliga sökningar efter kombinationer av fält i poster, statistisk analys av händelsemönster, frekvens och svårighetsgrad, arkivering, indexering, hämtning av händelseloggar. [147]

6.6 Rollteknik och role mining

”Hur ser roller och behörighetsnivåerna ut i ett system för digitalt bevarande?”

Rollteknik är den process genom vilken en organisation utvecklar, definierar, verkställer och upprätthåller rollbaserad åtkomstkontroll.[148] Rollteknik ska fungera som ett ramverk. Det ska kunna svara på fråga om vad? Varje rollteknisk insats kan svara på sina egna frågor om *När? Varför? Hur? Vem? Var?* För att använda RBAC ska organisationen först identifiera en uppsättning roller som ska vara fullständiga, effektiva samt korrekta. Dessa roller tilldelas till användare som får behörigheter. För att använda rollteknik finns det två tillvägagångssätt: top-down och bottom-up. Top-down innebär att göra en analys som är detaljerad över de processer som finns i verksamhet. Processerna innefattar de organisatoriska affärsprocesser, arbetsfunktioner som är speciella, ska delas till mindre enheter. Top-down har också använts i samband med role mining. Bottom-up-tillvägagångssättet så kallade role mining använder data mining tekniker för att upptäcka roller från befintliga systemkonfigurationsdata, särskilt

[146] Ibid. s. 533-534.
[147] Ibid. s. 533-534.
[148] Shawn McKinney, CON 2324 A Practical Guide to Role Engineering.

behörighetssuppgifter i till exempel åtkomstkontrollistor (ACL). Det finns allmän förståelse för vad role mining innebär men inga bestämda regler vad som är en bra role mining lösning. Men det finns tre stycken olika aspekter av role mining och det är; den formella problemdefinitionen, mining algoritmen för roll och kvalitetsåtgärder för bedömning av rollresultatet. Den första aspekten definierar formellt målet om role mining av att specificera vad som ges, vad som antas och vad som måste hittas. Den andra aspekten handlar om formaliseringen av tillvägagångssätt som tagits för att lösa problemet genom att ge en algoritm. Den tredje aspekten beskriver hur resultaten utvärderas. Allmänt är alla tre av dessa aspekter inbördes relaterade och i idealfallet är de överens. Det vill säga algoritmen borde lösa det formulerade problemet genom att det ger det bästa möjliga resultatet som definieras av kvalitetsmålet. En annan rollteknik metod är Hybrid, det innebär att dra nytta av resultaten från både top-down och bottom-up-tillvägagångssätten. Det menas med att data samlas in med hjälp av bottom-up-metoder och resultaten används av små samt medelstora företag. Samtidigt som man utför toppnära aktiviteter. Detta kan eventuellt spara tid och ansträngning på för de små och medelstora företag som fortfarande producerar giltiga resultat.

De grundläggande entiteterna i RBAC är användare, tillstånd, roller. Användarna ska ha relation till rollerna, rollerna ska ha relation till tillstånd, användarna ska ha relation till tillstånd. [149] [150] [151] En roll är en arbetsfunktion inom ramen för en organisation med några associerade semantik avseende myndighet och ansvaret som tilldelats användaren till rollen. En roll kan benämnas med namn och innebär skillnader i åtkomst; *Basic Role, Functional Role, Organizational Role, Role Group, Junior Role, Senior Role.* Funktionella roller speglar den väsentliga verksamheten funktioner som behöver utföras. Funktionsroller definieras av en uppsättning av standardhälsovårdsuppgifter (t.ex. neurolog). Funktionsroller består av alla behörigheter för system för hälsoinformationssystem, som behövs för att utföra en uppgift. Funktionella rollnamn associerar grupper av behörigheter för att göra det lättare att tilldela användare. En användare kan tilldelas en eller flera funktionella roller. Rollen kan innebära data/program funktioner som skapa, läsa, uppdatera, radera, exekvera etc.).

Rollgrupper placerar personer i organisationshierarkin som tillhör kategorier av vårdpersonal som garanterar olika nivåer av åtkomstkontroll. Liknande organisatoriska roller, rollgrupper tillåter användare att delta i organisationens arbetsflöde (t.ex. uppgifter) efter jobb, titel eller

[149] Mario Frank Joachim M. Buhmann David Basin, *On the Definition of Role Mining*, s.1.
[150] *StateMiner: An efficient similarity-based approach for optimal mining of role hierarchy*, s. 55.
[151] Edward J. Coyne, Timothy R. Weil, D. Richard Kuhn, *Role Engineering: Methods and Standards*

position men inte specificera detaljerad behörighet för specifika informationsobjekt. Rollgrupper tillåter en användare att "ansluta" till en resurs men inte bevilja godkännanden. Exempel på rollgrupp kan vara läkare eller apotekare. *Basic Role* - grundroller, även kallade statiska roller, kan ses som en föregångareroll som ger en persontillgång till en "session" eller "anslutning". *Organizational role*- Organisatoriska roller motsvarar hierarkisk organisation i ett företag i termer av interna strukturer. *Junior Role* - En yngre roll i en rollhierarki, Roll A är junior till roll B, om roll B ärver alla behörigheter som är associerade med roll A. *Senior Role* - En viktig roll i en rollhierarki, Roll A är senior till roll B om roll A ärver alla behörigheter som är associerade med roll B.[152]

6.7 E-arkivets roller

Det finns ett antal generella roller som du behöver i ett e-arkiv. Den första benämns *Ingester* som hanterar individuella “accession” och “ingest” processer från början till slut, inklusive eventuella nödvändiga kontakter med användaren som för in informationen. Denna roll utförs vanligtvis av bibliotekarier eller arkivarier med lämplig utbildning. *Cataloger* säkerställer att beskrivande metadata skapas och fångas till lämpliga standarder antingen under eller efter intag. Denna roll utförs vanligtvis av befintlig katalogiseringspersonal. I vissa fall kan det kombineras med ingester rollen. *Repository manager* hanterar repository funktion, inklusive ingest, bevarande och åtkomst. Detta är den mest specialiserade repository rollen, och kan fyllas av lämplig utbildad personal eller en specialiserad digital arkivarie. *System support* stöder användare av e-arkivet som normalt kallas som förstahandsstöd (first-line support). Komplexa problem kan hänvisas till systemadministratörer eller leverantörer. Därför bör detta integreras med alla befintliga IT-helpdesk support, men i en liten organisation kan den kombineras med e-arkiv chefsrollen. *System administrator* hanterar det system och infrastruktur som förvaret som beror på repository. Det kan handla om uppgifter som understödsstöd (second line support), databasadministration och hantering av lagrings- och användarkonton. Denna roll utförs normalt av IT-personal.[153]

[152] *(SAIC), s. 4.*
[153] Brown Adrian, *Practical Digital Preservation - A how-to guide for organizations of any size,* s. 79-80.

6.8 AtoM, ett åtkomstsystem

AtoM är ett innehållshanteringsverktyg som är det åtkomstsystem som Archivematica använder. Archivematica är ett system för digitalt långtidsbevarande och med det tillhörande åtkomstsystemet AtoM som styr auktoriseringen. *”Archivematica är en webb- och standardbaserad öppen källkod som gör det möjligt för din institution att behålla långsiktig tillgång till pålitligt, autentiskt och pålitligt digitalt innehåll.”* [154] AtoM står för åtkomst till minne (Access to Memory) och det är en applikation som är open-source webbaserad för standardbaserad arkivbeskrivning samt åtkomst. Ett användarkonto i AtoM är knutet till en av fem roller som representerar nivå av åtkomst till systemet, i det här fallet funktionerna i AtoM. Det är bara en administratör som kan lägga till, redigera och ta bort en användare eller grupp i AtoM. De fem rollerna som AtoM har definierat är följande; *Forskare (Researcher)* som är en användare som är offentlig och inte inloggad. Endast tillgång till programmet och kan söka samt bläddra beskrivningar som arkivbeskrivningar, register från myndigheter och arkivinstitutioner. *Medarbetare (Contributor)* kan skapa, redigera, uppdatera, söka, bläddra, se utkast samt exportera beskrivningar. Publiceringsstatus för ett informationsobjekt kan inte en medarbetare ändra, men kan dock komma åt referens- och master digitala objekt. *Redaktör (Editor)* kan kan skapa, redigera, uppdatera, söka, bläddra, se utkast, exportera beskrivningar samt redigera kontrollerade vokabulärtermer. Redaktören kan ändra publiceringsstatus för informationsobjektet samt komma åt referens- och master digitala objekt. *Översättare (Translator)* kan söka och bläddra i beskrivningar som är publicerade och användargränssnitt och databasinnehåll kan Översättaren översätta. Översättaren kan se men inte redigera utkastbeskrivningar. *Administratör (Administrator)* kan importera, exportera, skapa, läsa, uppdatera, publicera och radera post i systemet. Rollen innebär även att kunna anpassa program till institutionsspecifika krav. Administratören kan hantera användarkonton och profiler. Administratören kan också skapa nya användarroller, ställa in finkorniga behörigheter för den rollen och sedan tilldela eller avregistrera användare från den nya rollen.

[154] Artefactual, Archivematica

6.9 Big Data och åtkomstkontroll

De viktigaste kraven bakom definitionen av en åtkomstkontrollmekanism för Big Data[155]-plattformar är en Fine- Grained Access Control (finkornig åtkomstkontroll), förkortat FGAC. Eftersom data bearbetas av Big Data analytiska plattformar refererar de ofta till användarens personliga egenskaper. Det är viktigt att reglerna för åtkomstkontroll kan vara bunden till data vid de finaste granularitetsnivåerna. De relaterade tillsynsmekanismerna måste uppfinnas från början, som de föreslagna för traditionella system lita på data som hänför sig till känt schema, i samband med Stora data, data är heterogena och schemaless. Context Management (kontexthantering) är viktigt som ska stödja kontextbaserade åtkomstbegränsningar det resulterar i väldigt anpassad åtkomstkontroll. Kontexthanteringen kan begränsa tillgången till exempel tidsperioder eller geografiska platser. Åtkomstkontroll för Big Data kräver effektivitet då Big Data är komplext, detta kommer att kräva verkställighetsstrategier och policyöverrensstämmelsemekanismer. FGAC har verkställts enligt två huvudmetoder. Den första är den visningsbaserade, där användarna är får bara få tillgång till en vy av måldatasetet som uppfyller de angivna begränsningarna för åtkomstkontroll, medan den andra är baserad på omskrivning av frågan. En av de största svårigheterna med att utveckla en åtkomstkontroll lösning för Big Dataplattformar, är bristen på en standardmodell och relaterad manipulation språk som åtkomstkontrollreglerna och de relaterade övervakningsövervakning kan vara bunden. Åtkomstkontrolllösningar under kategori *Plattformsspecifika metoder* är endast avsedda för ett system. Det kan handla om inbyggd åtkomstkontrollfunktioner på den skyddade plattformen. Den största fördelen av detta tillvägagångssätt är att den utformade åtkomstkontrollen lösningen kan optimeras för målsystemet, men dess användbarhet och driftskompatibilitet är mycket begränsad. *Plattformsoberoende metoder* är avsedda inte bara mot en specifik plattform. Plattformsoberoende metoder är mer generell än plattformsspecifika lösningar och är tillämplig till skyddet av datakällor som förvaltas av heterogena plattformar.[156]

---

[155] IDG:s ordlista, *Big Data*
[156] Pietro Colombo, Elena Ferrari, *Access Control in the Era of Big Data: State of the Art and Research Directions,* s. 3.

6.10 Artificiell intelligens och åtkomstkontroll

Med hjälp av artificiell intelligens (AI) och maskininlärningsteknik (ML) kommer det resultera i en effektiv IAM och mycket frustration kan övervinnas. Teknikerna kan den alltför tekniska åtkomsthanteringen utvecklas till att hantering blir förståelig på alla nivåer inom organisationen. Analys som är kombinerat med artificiell intelligens kan göra att fokus och kontextuell insikt stärks. Detta resulterar i att både tekniska och anställda som inte är tekniskt insatta kan arbeta mer tidseffektivt. Automation av processer möjliggörs av modern teknik och kommer att påskynda de befintliga IAM- kontroller drastiskt. Modern teknik kommer att ha koll på systemet på ett annat effektivare sätt, avvikelser och potentiella hot kommer snabbt upptäckas utan att ett stort team av säkerhetsexperter kommer behövas. De anställda, oavsett om de är kunniga inom teknik eller inte, kommer att kunna ta beslut som är korrekta. Detta kommer att stärka säkerheten avsevärt då processen kommer att bli snabbare. Organisationen kommer med hjälp av AI och maskininlärningsteknik att kontinuerligt vara i kontroll, oavbrutet säkra och kompatibla. Artificiell intelligens och maskininlärning kan inte automatisera hela processen i IAM, i alla fall inte idag. Dessa moderna tekniker visar sig vara mest användbara när de implementeras för att göra en uppgift i stället för många. Så medan full automatisering ännu inte är möjlig kan AI och maskininlärning definitivt hjälpa till och förbättra identitets- och åtkomsthantering.[157]

6.11 Problemområden inom åtkomsthantering

Utan åtkomsthantering av information bland organisationer skulle ge förödande konsekvenser i samhället. Tänk om alla skulle komma åt informationen som rörde rikets säkerhet, som försvar och ekonomi? Det skulle bli ett samhälle i kaos med dataöverträdelser. Identitets- och åtkomsthantering står i centrum av företagets säkerhet. Tim Farrell, VD och medgrundare av FutureSoft anser att: *‘‘Nyckeln är att identifiera 20 procent av data som är affärskritisk och skydda det, istället för att försöka skydda allt."* Simon Godfrey, chef för säkerhetslösningar, CA, anser att: *"Det är utan tvekan ett av de mest utmanande projekt som ett företag kan åta sig, och människor är verkligen nyckeln till den här. Tekniken är väldigt mycket på andra plats. Det handlar om att du har stark metodik och har bästa praxis policy på plats, samt att*

[157] Elimity, *The Impact of Artificial Intelligence on Identity & Access Management.*

hålla den komplexa processen på rätt håll med en hög nivå av projektstyrning. IAM är i slutändan mindre av ett projekt, mer av ett program.''[158]

Ett vanligt problem inom Identity and Access Management är att användarna oftast ges åtkomsträttigheter som baseras på dennes roll i organisationen. Problemet är att de inte ofta passar in i enskilda roller. Till exempel kan det handla om att användaren behöver komma åt objektet en gång eller om personen har samma roll men behöver olika typer av åtkomst. Detta skapar invecklade situationer i organisationen och orsakar mycket tidsåtgång eftersom många avdelningar kan bli inblandade. Att inaktivera ett konto som användaren inte använder längre då den till exempel inte är anställd i organisationen längre är ett vanligt återkommande problem. Det är lika viktigt att ta bort som att lägga till en behörighet. [159]

7 Diskussion

Genom att undersöka, klargöra samt analysera genom den kvalitativa metoden och mängden insamling av data med öppet synsätt, kunde jag besvara min huvudsakliga frågeställning. Relationen mellan auktorisering och säkerhetspolicy är högst relevant för arkiv- och informationsvetenskapen eftersom digitala objekt i system för digitalt bevarande ska skyddas från obehörig åtkomst. Fungerar inte åtkomsthanteringen i system för digitalt bevarande kommer det skapa kaos i samhället, till exempel kan det handla om användare som inte ska ha tillgång till information får åtkomst. Till exempel hemlig information för rikets säkerhet kommer i fel händer. För att detta inte ska hända i en verksamhet med ett system för digitalt bevarande så måste ett ledningssystem med säkerhetspolicy för auktorisering finnas. Insamlingen av data som jag har gjorts från myndigheters föreskrifter och standarder från Myndigheten för samhällsskydd och beredskap (MSB), Riksarkivet, och standarden SS-ISO/IEC 2700-serien med Ledningssystem för informationssäkerhet har jag kommit fram till att de huvudsakliga delarna i en säkerhetspolicy för auktorisering för system för digitalt bevarande innefattar främst krav och riktlinjer gällande; användarregistrering, avregistrering av åtkomst, roller, ansvarsfördelning, behörighetsnivåer, register över godkända åtkomsträttigheter, dokumentation av priviligierade rättigheter och loggning. Myndigheter

[158] Mayne Mark, *The problems and benefits of identity and access management.*
[159] Wiech Dean, *The Consequences of Neglecting Access Management.*

måste känna tillit till varandra vid utbyte av information och åtkomst.[160] Därför är det viktigt att säkerhetspolicy och riktlinjer går att förstås och att alla i organisationen vet om att det finns samt informeras, detta skapar den trygghet som behövs i det vardagliga arkiv- och informationsarbetet. [161] Genom all den insamling av data jag har gjort har jag kommit fram till att det är viktigt att säkerhetspolicy ska anpassas efter verksamhet och alltid ställa sig frågorna; *Vem, Vad, När, Var, Hur* och *Varför* och inte gå vidare förrän alla har ett säkert och förståeligt svar. Alla måste ha en relation till varandra, annars står kugghjulet still när det brister på något av svaren till frågorna *Vem, Vad, När, Var, Hur* och *Varför*. Efter min undersökning och insamling av mängd av data, har det framkommit att vilket informationssystem verksamheten än har, så måste man tillhandahålla någon form av åtkomstkontrollmekanism. Den vanligaste i Sverige och internationellt som informationssystem använder är en rollbaserad åtkomstkontrollmekanism. Enligt LIS är rollbaserad åtkomstkontroll (RBAC) lyckat hos många verksamheter, som handlar om att kartlägga verksamheten och dess anställda i olika roller. Det resulterar i att rätt användare kommer åt rätt information. Även i den relaterad forskning jag funnit har de flesta författarna också kommit fram till att rollbaserad åtkomstkontroll är det vanligaste och bästa sättet att hantera åtkomst i informationssystem. System för digitalt bevarande för långtidsbevarande som Archivematica och tillhörande åtkomstsystemet AtoM är även de baserade på rollbaserad åtkomstkontroll. Varför denna åtkomstkontrollmekanism är populär har med att det är av stor vikt att verksamheten använder sig av roller och behörighetsnivåer för, att alla ska veta med säkerhet vad de ska göra och vad de inte får göra. Vad gäller framtidsutsikten för åtkomsthantering i system för digitalt bevarande verkar det se ljust ut. Med hjälp av artificiell intelligens och maskininlärningsteknik kommer åtkomsthantering bli allt mer effektivare och säkrare. Hanteringen kommer underlättas med hjälp av AI då automation av processer kommer att påskynda åtkomstkontroller, men samtidigt ha styrkan att snabbt märka av hot. Artificiell intelligens innebär att anställda inte behöver vara tekniskt kunniga för att ett korrekt beslut ska kunna tas, detta kommer att stärka åtkomsthanteringens säkerhet avsevärt i framtiden. Men verksamheter måste ändå koncentrera sig på att utarbeta säkerhetspolicy med dess roller och ansvarsbeskrivningar noggrannare, som ska uppdateras regelbundet, eftersom arbetsuppgifter och kompetens förändras ofta i verksamheter. Där ska det stå exakt vilka arbetsuppgifter man har och utifrån det göra en rollbeskrivning som även den måste

[160] Allmänna råd MSBFS Remissutgåva, *Förslag till Myndigheten för samhällsskydd och beredskaps allmänna råd och kommentarer om krav på informationssäkerhet*, s. 2, 6.
[161] MSB, *Ledningssystem för informationssäkerhet – LIS.*

uppdateras kontinuerligt. Denna rutin skulle göra alla medvetna över sitt ansvar och att auktorisering inte skulle glömmas bort.

8 Slutsats

Min uppsats och frågeställning om hur relationen ser ut mellan auktorisering och säkerhetspolicy för system för digitalt bevarande hade som syfte att undersöka, klargöra, analysera området och motivera till diskussion, samt öka trycket på att fler ska vilja forska vidare inom området. Jag vill avsluta och understryka att min uppsats har varit lärorik, och att auktorisering och säkerhetspolicy måste ha en stark relation till varandra i system för digitalt bevarande, för att digitala objekt i system för digitalt bevarande ska kunna skyddas från obehörig åtkomst. Auktorisering och säkerhetspolicy går hand i hand eftersom myndigheternas rutiner för informationshantering ska resultera i att medborgare och företag känner sig trygga och kan lita på varandra**.** Har verksamheten ingen säkerhetspolicy som alla anställda kan förstå och följa, kan inte auktorisering gå till på rätt sätt i system för digitalt bevarande. En säkerhetspolicy för auktorisering för system för digitalt bevarande ska innefatta krav och riktlinjer gällande; användarregistrering, avregistrering av åtkomst, roller, ansvarsfördelning, behörighetsnivåer, register över godkända åtkomsträttigheter, dokumentation av priviligierade rättigheter och loggning. Det är av stor vikt att säkerhetspolicyn anpassas efter verksamhet och att verksamheten använder roller och auktoriseringsnivåer för att säkerställa att alla med säkerhet vet vad de ska göra och vad de inte får göra. Det följande avsnittet är mitt förslag till framtida forskning om området som jag tror kommer att ha stor inverkan på det fortsatta arbetet med åtkomsthantering för de digitala objekten i system för digitalt bevarande som ska skyddas från obehörig åtkomst.

9 Förslag till framtida forskning

I framtida forskning skulle man kunna intervjua företag med den frågeställning jag utgått från med tillhörande frågor. De personer som ska intervjuas skulle kunna väljas utifrån deras kunskap om system för digitalt bevarande, auktorisering, informationssäkerhet, men också artificiell intelligens (AI) och maskininlärningsteknik som nu är i tiden. Svaren skulle kunna komma att analyseras i sin helhet och vara som stöd i undersökningen. I fortsatt forskning om

auktorisering och säkerhetspolicy för system för digitalt bevarande är det högst relevant att fördjupa sig mer om artificiell intelligens (AI) och maskininlärningsteknik, om hur dessa processer kommer att kunna inverka säkerhetsmässigt och effektiviteten för auktorisering i system för digitalt bevarande i framtiden. Detta är något som skulle kunna utvecklas vidare i framtida forskning.

10 Referenser

[Hämtat vårterminen år 2019]

Acando, Så ökar ni ert digitala förtroende, Stockholm, https://www.acando.se/vad-vi-kan/teman/cio-insights/sa-okar-ni-ert-digitala-fortroende-och-vander-gdpr-till-er-fordel/

Artefactual, *Archivematica*, https://www.archivematica.org/en/

Axiomatics, Attribute Based Access Control (ABAC), USA, https://www.axiomatics.com/attribute-based-access-control/

Ausanka-Crues Ryan, Methods for Access Control: Advances and Limitations, Harvey Mudd College, Claremont, California, https://pdfs.semanticscholar.org/6192/f0308dc8d7782b55a0557dfb66f323638853.pdf

Basic Amar, Johnsson Christoffer, Schuster Thomas, "*Rollbaserad åtkomstkontroll inom organisationer- Rätt åtkomst till rätt användare vid rätt tillfälle, 2014,* http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=4498836&fileOId=4498850

Beal Vangie, Webopedia, *biometrics*, https://www.webopedia.com/TERM/B/biometrics.html

Beagrie Neil, Charlesworth Andrew, Miller Paul, *How Cloud Storage can address the needs of public archives in the UK*, nationalarchives.gov.uk, http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf

Belim S. V., Belim S. Yu., *Implementation of Mandatory Access Control in Distributed Systems,* Automatic Control and Computer Sciences, 2018, Volume 52, Issue 8, pp 1124–1126, https://www.researchgate.net/publication/331603364_Implementation_of_Mandatory_Access_Control_in_Distributed_Systems

Boeije Hennie, *A Purposeful Approach to the Constant Comparative Method in the Analysis of Qualitative Interviews*, Utrecht University, Faculty of Social Sciences, Department of Methodology & Statistics, https://www.researchgate.net/publication/226282093_A_Purposeful_Approach_to_the_Constant_Comparative_Method_in_the_Analysis_of_Qualitative_Interviews

Brown Adrian, *Practical Digital Preservation - A how-to guide for organizations of any size, 2013, facet publishing, London.*

Cambridge Dictonary, *gap analysis*, Cambridge University Press, https://dictionary.cambridge.org/dictionary/english/gap-analysis

Cobb Michael, *Best practices for audit, log review for IT security investigations*, Computer Weekly, https://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations

Colombo Pietro, Ferrari Elena, *Access Control in the Era of Big Data: State of the Art and Research Directions*, Varese, Italy, 2018, https://www.researchgate.net/publication/325638965_Access_Control_in_the_Era_of_Big_Data_State_of_the_Art_and_Research_Directions

Computer Sweden, IDG:s ordlista, auktorisation, https://it-ord.idg.se/ord/auktorisation/

Computer Sweden, IDG:s ordlista, big data, https://it-ord.idg.se/ord/big-data/

Computer Sweden, IDG:s ordlista, informationssäkerhet, https://it-ord.idg.se/ord/informationssakerhet/

Computer Sweden, IDG:s ordlista, identity and access management, https://it-ord.idg.se/ord/identity-and-access-management/

Coyne Edward, Weil Timothy, Kuhn Richard, *Role Engineering: Methods and Standards, National Institute of Standards and Technology, 2011*, https://www.researchgate.net/publication/260305908_Role_Engineering_Methods_and_Standards

Datainspektionen, Dataskyddsförordningen (GDPR), https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/

Elimity, *The Impact of Artificial Intelligence on Identity & Access Management,* Belgium, 2018, https://www.elimity.com/blog/the-impact-of-artificial-intelligence-on-iam

Fan Zhijie, Xiao Ya, Wang Chunmei, Liu Bing, Research on Access Control in Cloud Storage System: From Single to Multi-Clouds, American Journal of Software Engineering and Applications, Volume 7, Issue 1, March 2018, Pages: 1-14, Science publishing group, http://article.sciencepublishinggroup.com/pdf/10.11648.j.ajsea.20180701.11.pdf

Ferraiolo David, Kuhn Richard, *Role-Based Access Controls*, 15th National Computer Security Conference (1992) Baltimore, pp. 554 – 563, National Institute of Standards and Technology, Gaithersburg, U.S. https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf

Frank Mario, Buhmann Joachim, Basin David, Department of Computer Science ETH Zurich, Switzerland, On the Definition of Role Mining http://inf.ethz.ch/personal/basin/pubs/sacmat10-drm.pdf

Frankenfield Jake, Investopedia, *Cloud Computing*, https://www.investopedia.com/terms/c/cloud-computing.asp

Gustafsson C Staffan, Paradis Mikael, *Rationalitet för identitet- och åtkomstlösningar i stora företag*, https://gupea.ub.gu.se/bitstream/2077/26691/1/gupea_2077_26691_1.pdf

Hu Vincent, Ferraiolo D. David, Kuhn Rick, Interagency Report 7316, *Assessment of Access Control Systems*, National Institute of Standards and Technology, 2006, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

Hu Vincent, *Access Control Policy and Implementation Guides*, National Institute of Standards and Technology, 2016, updated 2018, https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides

I.Indu, Rubesh Anand, Vidhyacharan Bhaskar, *Identity and access management in cloud environment: Mechanisms and challenges*, Engineering Science and Technology, an International Journal, 2018. https://www.sciencedirect.com/science/article/pii/S2215098617316750#s0065

Inera AB, Per Mützell, 2017, http://rivta.se/documents/ARK_0046/Referensarkitektur-Identitetochatkomst-RevA.pdf

Jetabroad, *IAM - Identity and Access Management*, 2017, http://techblog.jetabroad.com/2017/06/iam-identity-and-access-management.html

Management Council of the Consultative Committee for Space Data Systems (CCSDS), *Reference Model For An Open Archival Information System (Oais)*, https://public.ccsds.org/pubs/650x0m2.pdf

Martin James, Waters John, *What is IAM? Identity and access management explained*, CSO, IDG Communications, Inc, 2018, https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

Mayne Mark, The problems and benefits of identity and access management, 2009, https://www.scmagazineuk.com/problems-benefits-identity-access-management/article/1469381

McKinney Shawn, CON 2324 A Practical Guide to Role Engineering, Symas, JavaOne San Francisco, 2015, https://iamfortress.files.wordpress.com/2016/07/con2324-mckinney.pdf

Myndigheten för samhällsskydd och beredskap (MSB):

Terminologi och begrepp inom informationssäkerhet- Hur man skapar en språkgemenskap, 2016, https://www.msb.se/RibData/Filer/pdf/28002.pdf

Förslag till Myndigheten för samhällsskydd och beredskaps allmänna råd och kommentarer om krav på informationssäkerhet, https://www.msb.se/upload/kunskapsbank/foreskrifter/remisser/allmanna_rad_krav_informationssakerhet.pdf

Metodstödet, https://www.informationssakerhet.se/metodstodet/metodstodet/

Ledningssystem för informationssäkerhet – LIS,
https://www.msb.se/sv/Produkter--tjanster/Informationssakerhet---stod--verktyg/Standardisering/LIS-ISO-27000/
Gapanalys - checklista, 11. Styrning av åtkomst, https://www.informationssakerhet.se/siteassets/gamla-metodstodet-for-lis/2.-analysera/gapanalys-checklista.pdf
Nguyen Thinh, Cuttill Shaun, Nguyen Timothy T., Mahdavi Mehrzad, *Identity And Access Management Framework*, Patent Application Publication, Pub. No: US 2008/0028453 A1, OSHA. LIANG. L.L.P. f. SLB, United States, 2008,
https://patentimages.storage.googleapis.com/2e/03/42/adcca4ad74dcd8/US20080028453A1.pdf

Pickard Alison Jane, *Research Methods in Information*, Chapter 23, Qualitative analysis, Facet Publishing, 2012.

Poniszewska-Maranda Aneta, *Management of access control in information system based on role concept*, Lodz University of Technology, 2011, Scalable Computing: Practice and Experience, Volume 12, Number 1, pp. 35–49,
https://www.researchgate.net/publication/220101285_Management_of_access_control_in_information_system_based_on_role_concept

Riksarkivet
Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling), RA-FS 2009:1, https://riksarkivet.se/rafs?pdf=rafs/RA-FS%202009-01.pdf
Riksarkivet, *Informationssäkerhet*, https://riksarkivet.se/informationssakerhet

Rosa Carlos André, Craveiro Olga, Domingues Patricio, *Open Source Software For Digital Preservation Repositories: A Survey*, Portugal, 2017, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.8, No.3, https://arxiv.org/ftp/arxiv/papers/1707/1707.06336.pdf

(SAIC), The Healthcare RBAC Task Force, Developed by: Science Applications International Corporation, *Role-Based Access Control (RBAC) Role Engineering Process*, https://csrc.nist.gov/csrc/media/projects/role-based-access-control/documents/healthcarerbactfroleengineeringprocessv3_0.pdf

Sherwood, Clark, Lynas, *Enterprise Security Architecture - A Business-Driven Approach*, CMP Books, år 2005.

Sifou Fatima, Kartit Ali, Hammouch Ahmed, *Different Access Control Mechanisms for Data Security in Cloud Computing*, United Kingdom, 2017. https://dl.acm.org/citation.cfm?id=3141128.3141133

Svensk Standard https://www.sis.se/standarder/
SS-EN ISO/IEC 27001:2017- *Informationsteknik-Säkerhetstekniker- Ledningssystem för informationssäkerhet-Krav, Swedish Standards Institute, 2017.*
SS-EN ISO/IEC 27002:2017- *Informationsteknik- Säkerhetstekniker- Riktlinjer för informationssäkerhetsåtgärder, Swedish Standards Institute, 2017.*

Sveriges kommuner och landsting (SKL), Informationsförsörjning och digital infrastruktur / E-arkiv
https://skl.se/naringslivarbetedigitalisering/digitalisering/earkiv.350.html

Takabi Hassan, Joshi James, StateMiner*: An Efficient Similarity-Based Approach for Optimal Mining of Role Hierarchy*, Pittsburgh, USA,
https://www.researchgate.net/publication/221366991_StateMiner_An_efficient_similarity-based_approach_for_optimal_mining_of_role_hierarchy

Techopedia™:
Discretionary Access Control (DAC),
https://www.techopedia.com/definition/229/discretionary-access-control-dac
Mandatory Access Control (MAC),
https://www.techopedia.com/definition/4017/mandatory-access-control-mac
Role-Based Access Control (RBAC),
https://www.techopedia.com/definition/23933/role-based-access-control-rbac

Yao Walt, Moody Ken, Bacon Jean, *A Model of OASIS Role-Based Access Control and its Support for Active Security*, University of Cambridge,
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.146.1437&rep=rep1&type=pdf

Westerdah Lars, Gudmundson Hunstad Amund, Fredrik Mörnestedt, *Sammanfattning av Projektet - Objektbaserad Säkerhet*, Totalförsvarets forskningsinstitut (FOI), 2014. https://www.foi.se/rest-api/report/FOI-R--4011--SE

Wiech Dean, The Consequences of Neglecting Access Management, 2015, BNP Media, https://www.securitymagazine.com/articles/86566-the-consequences-of-neglecting-access-management

Wood Andy, Security Professional Security Architecture, Design & Engineering, https://andywood.info/2014/04/08/sabsa-model-architectural-components/

3M, *Så här gör man en GAP-analys: prestation, färdighet, marknad*, https://www.3msverige.se/3M/sv_SE/post-it-notes/ideas/articles/gap-analysis/