# FFI-RAPPORT

17/01169

# Sikkerhetsarkitektur for Forsvarets informasjonsinfrastruktur

## en innledende studie av rammeverk og begreper

Federico Mancini,
Bodil Farsund,
Frode Lillevold

# Sikkerhetsarkitektur for Forsvarets informasjonsinfrastruktur

## en innledende studie av rammeverk og begreper

Federico Mancini,
Bodil Farsund,
Frode Lillevold

Forsvarets forskningsinstitutt (FFI) 14. juli 2017

## Emneord

Sikkerhetsarkitektur
Virksomhetsarkitektur
Informasjonssikkerhet
Risikovurdering

**FFI-rapport:**
FFI-RAPPORT 17/01169

**Prosjektnummer**
1294

**ISBN**
P: 978-82-464-2928-1
E: 978-82-464-2929-8

**Godkjent av**
Nils A. Nordbotten, *forskningsleder*
Anders Eggen, a*vdelingssjef*

# Sammendrag

Mange nye kapabiliteter som ønskes realisert i Forsvaret, forutsetter ny funksjonalitet i informasjonsinfrastrukturen. Men for å oppnå ønsket operativ evne, må tilstrekkelig sikkerhet være på plass for å beskytte mot aktuelle trusler. Dette har en økonomisk kostnad og kan sette begrensinger på hva som kan realiseres i praksis av ønsket funksjonalitet. Det er også vanskelig å vurdere hva som er tilstrekkelig sikkerhet for en gitt funksjonalitet og for informasjonsinfrastrukturen som helhet.

En helhetlig sikkerhetsarkitektur har lenge blitt nevnt som en mulig tilnærming for å håndtere kompleksiteten rundt informasjonssikkerhet i Forsvaret. Med arkitektur menes en strukturert tilnærming til planlegging og utvikling av komplekse systemer over tid, samt en formell beskrivelse eller detaljert plan på komponentnivå. Man kan da tenke på en sikkerhetsarkitektur som en beskrivelse av tekniske sikkerhetsløsninger og de prinsippene og retningslinjene som styrer deres utvikling. Disse løsningene skal både være konsistente på tvers av Forsvaret og samtidig sørge for at informasjonsinfrastrukturen som helhet kan operere innenfor et akseptabelt risikonivå. For å sikre dette er det nødvendig å se sikkerhet i et bredere perspektiv. En helhetlig sikkerhetsarkitektur skal sørge for at sikkerhetsarbeidet forankres i virksomhetens strategiske mål og behov og at også ikke-tekniske aspekter blir identifisert og integrert i planlegging og utvikling av sikkerhetsløsninger. Slike aspekter kan for eksempel være forretningsprosesser, kontekster som virksomheten opererer i, lover og regelverk, økonomiske rammer, eller nye teknologiske muligheter.

Til tross for at det finnes flere rammeverk som definerer verktøy, metoder og modeller for å bygge en slik arkitektur, er det likevel utfordrende å realisere den i praksis. Generelt er det vanskelig å vurdere og måle risiko, noe som er sentralt i alt sikkerhetsarbeid. I tillegg er det uklart hvordan sikkerhetsarkitektur og virksomhetsarkitektur skal integreres. Vi diskuterer derfor relevante utfordringer knyttet til risikovurdering, og på bakgrunn av dette diskuterer vi eksisterende rammeverk for virksomhetsarkitektur og sikkerhetsarkitektur. Rapporten gir også en kort beskrivelse av de viktigste dokumentene som gir føringer for informasjonssikkerhet i Forsvaret, siden de er med på å definere rammene for en sikkerhetsarkitektur.

Vi konkluderer med at et arkitekturrammeverk kan gi oss metoder og verktøy, men Forsvaret må selv avgjøre riktig omfang og utforming av arkitekturarbeidet for å dra nytte av det. Erfaringsmessig er rammeverkene for omfattende og generiske til å brukes slik de er, og tilpasningsbehovet er derfor stort. Det er viktig at det er målene en virksomhet vil oppnå med sikkerhetsarbeidet, og ikke selve rammeverkene, som danner grunnlaget for en arkitektur. Faren er ellers at man fokuserer for mye på arkitekturmetoden og glemmer de underliggende problemene den skal hjelpe med å løse.

# Summary

Many new capabilities that the Armed Forces intend to implement require new functionality in the information infrastructure, but in order to achieve the desired operative effect, adequate security must be in place to protect against relevant threats. This has an economical cost and can limit the functionality that can be implemented in practice. It is especially challenging to determine the adequate level of security both for capabilities and for the infrastructure as a whole.

A comprehensive security architecture is an approach that has long been mentioned as a possible way to address the complexity of information security in the Armed Forces. Architecture is a structured approach to planning and developing complex systems over time, as well as a formal description or detailed plan at the component level. One can then think of a security architecture as a description of technical security solutions, as well as the principles and guidelines that govern their development. However, in order to ensure that these solutions are consistent across the Armed Forces, and that the information infrastructure as a whole operates within an acceptable risk level, one needs to see security in a broader perspective. A comprehensive security architecture should ensure that security supports the enterprise's strategic goals and needs. It should also ensure that relevant aspects apart from the technical ones are identified and integrated in the planning and developing of security solutions. Such aspects can for example be business processes, laws and external regulations, the contexts the enterprise operates in, or new technological possibilities.

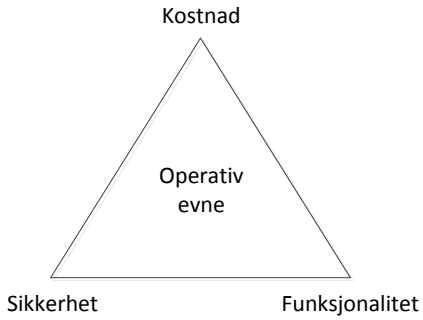
Despite the fact that there are various frameworks that define tools, methods and models to build such a security architecture, it is still challenging to implement one in practice. One reason is that it is difficult to assess and measure risk in general, something that is central to all security work. Another is that it is unclear how security architecture and enterprise architecture should be integrated. Therefore, we discuss relevant challenges associated with risk assessment, and based on this we present existing frameworks for enterprise and security architecture. The report also briefly describes the most important documents concerning information security in the Armed Forces, as they may help define the scope of a security architecture.

We conclude that while the frameworks can provide the methods and tools to build an architecture, the Armed Forces must themselves decide the correct scope and form of the architecture work in order to benefit from it. From experience, these frameworks are too comprehensive and generic to be used as they are, and require significant adaptations. It is therefore important that an enterprise's information security goals form the basis for an architecture – not the frameworks. Otherwise, the danger is to focus too much on the architecture method instead of the problems it should help solving.

# Innhold

# 1 Innledning

Forsvarets informasjonsinfrastruktur (INI)[1] «understøtter hele bredden av Forsvarets virksomhet, legger til rette for samhandling i nettverk, og er en forutsetning for et nettverks-basert Forsvar (NbF)» [1], men for å oppnå ønsket operativ evne må tilstrekkelig sikkerhet være på plass for å beskytte mot aktuelle trusler. For eksempel er det ønskelig at informasjon kan flyte mellom sikkerhetsdomener, også på tvers av graderingsnivå, for å muliggjøre mer effektivt samarbeid [2]. Mekanismer må da være på plass for å hindre datalekkasje og spredning av skadevare. Slike mekanismer er imidlertid kostbare, bare tilgjengelig for enkelte typer dataflyt, og effekten er vanskelig å fastslå. Høyest mulig operativ evne oppnås ved å balansere tilstrekkelig sikkerhet med ønsket funksjonalitet og økonomisk kostnad (Figur 1.1), noe som ofte er vanskelig i praksis.




*Figur 1.1 En kapabilitet har funksjonalitet som må beskyttes mot potensielle trusler for å gi ønsket operativ evne. Både sikkerhet og funksjonalitet har en økonomisk kostnad. Alle tre faktorene må derfor balanseres.*

En mulig tilnærming for å håndtere kompleksiteten rundt informasjonssikkerhet i Forsvaret er en *helhetlig sikkerhetsarkitektur*. Med arkitektur menes en strukturert tilnærming til planlegging og utvikling av komplekse systemer over tid, samt en formell beskrivelse eller detaljert plan av systemet på komponentnivå [3]. Man kan da tenke på en sikkerhetsarkitektur som en beskrivelse av tekniske sikkerhetsløsninger og de prinsippene og retningslinjene som styrer deres utvikling. For å sikre at disse løsningene både skal være konsistente på tvers av Forsvaret, og sammen sørge for at INI som helhet kan operere innenfor et akseptabelt risikonivå, trenger man å se sikkerhet i et bredere perspektiv. Da tenker man gjerne på en *virksomhetsinformasjonssikkerhetsarkitektur* (Enterprise Information Security Architecture), som skal sørge for at sikkerhet forankres i virksomhetens strategiske mål og behov og at også andre relevante aspekter enn de tekniske blir identifisert og integrert i planlegging og utvikling av sikkerhetsløsninger. Slike aspekter kan være kontekstene virksomheten opererer i, eksterne lover og regler, økonomiske rammer, forretningsprosesser, strategiske mål, og kritiske

[1] Begrepet INI defineres i Forsvarets IKT-strategi som kjernen i militært tilpasset og anvendt Informasjons- og kommunikasjonsteknologi (IKT). Den eksakte avgrensingen vil måtte defineres for en arkitektur, men det er ikke vesentlig for denne rapporten.

avhengigheter av informasjonssystemer. I denne rapporten er det en slik helhetlig sikkerhetsarkitektur vi diskuterer.

Forsvaret bruker en tilsvarende tilnærming for å sørge for at informasjonssystemene utvikles i takt med virksomhetsmål og -behov, nemlig *virksomhetsarkitektur*. En sikkerhetsarkitektur bør integreres og harmoniseres med denne, fordi sikkerhet ikke har noe mening utenfor konteksten den skal realiseres i. Likevel er det fortsatt mye usikkerhet rundt hva en slik sikkerhetsarkitektur egentlig er og hvordan den kan integreres med en virksomhetsarkitektur. Det finnes noen rammeverk som kan hjelpe med dette, og vi vil se nærmere på dem i rapporten. Det finnes også noen styrende dokumenter om sikkerhet i Forsvaret, og det er viktig å forstå hvordan disse kan legge føringer på, eller bli en del av, en sikkerhetsarkitektur. Siden sikkerhet dreier seg hovedsakelig om å håndtere risiko, og noen sentrale utfordringer med å realisere en sikkerhetsarkitektur er knyttet til dette, gir vi i denne rapporten også en oversikt over risikorelaterte konsepter og begreper.

Rapporten starter med å se på relevante dokumenter i kapittel 2. Deretter blir eksisterende metoder og begreper knyttet til risikovurdering presentert i kapittel 3. I kapittel 4 introduserer vi mer i detalj virksomhetsarkitektur og eksisterende metoder og rammeverk. Dette etablerer grunnlaget for å diskutere sikkerhetsarkitektur og en mulig integrasjon mellom de to i kapittel 5. Til slutt oppsummerer vi med noen tanker rundt bruk av sikkerhetsarkitektur i Forsvaret, og eventuelt hva vi mangler for å kunne realisere den.

# 2 Styrende dokumenter for sikkerhet

Det finnes en del styrende dokumenter om informasjonssikkerhet i Forsvaret. Disse kan legge føringer på eller bli en del av en sikkerhetsarkitektur. Vi gir her en kort beskrivelse av de som vi mener er de viktigste.

Sikkerhetsloven [4] og Forskrift for informasjonssikkerhet (FoI) [5] er de styrende dokumentene for håndtering og beskyttelse av gradert informasjon. De gir overordnende krav for hvordan sikkerhet skal håndteres i Forsvarets informasjonsinfrastruktur. Veiledningene fra NSM utdyper forskriftene, og blir i praksis brukt for å utarbeide sikkerhetskonsepter for nye systemer. Ugraderte systemer blir sikret etter sivile standarder og faller inn under Riksrevisjonens ansvar.

Det er få styrende dokumenter med en tilnærming til sikkerhet som er tilpasset Forsvarets operative bruk, og som kan brukes for å utvikle en langsiktig sikkerhetsstrategi. «Sikkerhetskonsept for et nettverkbasert forsvar» [6] diskuterer hvordan man skal tenke sikkerhet for å kunne støtte en nettverksbasert tilnærming i Forsvaret, og «Informasjonssikkerhetsstrategi for forsvarsektoren» [7] setter overordnede mål for informasjonssikkerhet for hele forsvarssektoren. Begge dokumentene er viktige fordi de gir en

felles innretning til sikkerhetsarbeidet i Forsvarets INI, men de er ikke tilstrekkelige til å dekke Forsvarets behov for å utvikle en sikker INI.

## 2.1 Sikkerhetsloven

Lov om forebyggende sikkerhetstjeneste blir ofte omtalt som sikkerhetsloven. Dens formål er i følge NSM «å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste. Loven med forskrifter angir minimumskravene for beskyttelse av informasjon og objekter av betydning for rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Regelverket fastsetter forebyggende tiltak mot forberedelser til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger.»

Loven gjelder for alle forvaltningsorganer, samt leverandører til forvaltningsorganer når disse kan få tilgang til skjermingsverdig informasjon eller objekt. Den gjelder også for virksomheter med kritiske samfunnsfunksjoner, som for eksempel Telenor, NSB og Avinor.

Kapittel 4 i Sikkerhetsloven er om informasjonssikkerhet. Det omhandler sikkerhetsgradering, plikt til å beskytte sikkerhetsgradert informasjon, sikkerhetsmessig godkjenning av informasjonssystemer, sikkerhetsmessig overvåking av godkjente informasjonssystemer, kryptosikkerhet, monitorering av og inntrengning i informasjonssystemer, og tekniske sikkerhetsundersøkelser.

Ny sikkerhetslov er under utarbeidelse, noe som kan medføre enkelte endringer.

## 2.2 Forskrift om informasjonssikkerhet

Forskrift om informasjonssikkerhet (FoI) har samme formål og virkeområde som sikkerhetsloven, og gjelder også for informasjon sikkerhetsgradert i samsvar med NATOs bestemmelser. Kapittel 5 omhandler informasjonssystemsikkerhet, med underkapitler om grunnleggende sikkerhetskrav, systemtekniske sikkerhetskrav, administrative sikkerhetskrav, sikkerhetsgodkjenning av informasjonssystemer og sikkerhetsdokumentasjon.

Under «grunnleggende sikkerhetskrav» omtales grunnleggende egenskaper for sikkerhet, hovedmål for informasjonssystemsikkerhet, samt grunnleggende sikkerhetstiltak og sikkerhetsprinsipper. Vi opplever disse begrepene og sammenhengen mellom dem som noe uklar. Videre står det at det skal gjennomføres kontinuerlig risikostyring, uten at det sies hvordan dette skal gjøres.

Overordnet ansvar for informasjonssikkerhet plasseres gjennom «Virksomheter som har informasjonssystemer som behandler sikkerhetsgradert informasjon skal etablere en datasikkerhetsorganisasjon. Organisasjonen skal ha tilstrekkelig myndighet, kompetanse og

ressurser til å ivareta sikkerheten i systemene, og skal minimum bestå av datasikkerhetsleder med stedfortreder.»

## 2.3 NSMs veiledninger

NSM gir jevnlig ut veiledninger som utdyper og utfyller krav som blir stilt i sikkerhetsloven[2]. De fleste veiledningene, men ikke alle, er ugraderte.

En rekke veiledninger beskriver krav til systemteknisk sikkerhet, hovedsakelig beregnet for teknologer. De tar for seg krav til sikring av ulike IKT-komponenter i graderte systemer, og kan også benyttes for ugraderte systemer. I tillegg er det veiledninger med sikkerhetsråd for ugraderte systemer.

Det fins veiledninger innenfor mange av områdene som omfattes av sikkerhetsloven. Noen overskrifter er: objektsikkerhet, informasjonssystemsikkerhet, sikkerhetsgraderte anskaffelser, sikkerhetsadministrasjon, personellsikkerhet, informasjonssikkerhet og administrativ kryptosikkerhet. Under sikkerhetsadministrasjon ligger veiledninger for verdivurdering og for sikkerhetsstyring.

## 2.4 Sikkerhetskonsept for et nettverkbasert forsvar

Gjennom samhandling i nettverk ønsker Forsvaret å kunne utnytte sine ressurser bedre. Dette omtales som nettverksbasert forsvar (NbF), og tanken er at man skal få mer kampkraft ut av hver enhet. Forsvaret ønsker å øke sin NbF-modenhet, men det er en del utfordringer spesielt knyttet til informasjonsinfrastrukturen og sikkerhet [8].

«Sikkerhetskonsept for et nettverksbasert forsvar» ble utgitt i 2011 [6]. Dette dokumentet presenterer en annen måte å tenke sikkerhet på enn det Sikkerhetsloven og Forskrift om informasjonssikkerhet gjør.

«Økt effekt oppnås gjennom en sterkt forbedret evne til allokering og synkronisering av innsatskomponenter og økt tempo i operasjonene. Evne til innsamling, bearbeiding og distribusjon av informasjon, kunnskap, intensjoner og kontekstuell forståelse står sentralt i en slik ambisjon. Forutsetningen for effektøkningen er derfor hovedsakelig å finne i etablering av en informasjonsinfrastruktur som bidrar til radikalt forbedret evne til informasjonsdeling, informasjonskvalitet, samhandling og felles situasjonsbevissthet.»

Konseptet peker spesielt på økt informasjonsdeling som en viktig faktor for å oppnå NbF. Det ønskes å kunne utveksle gradert informasjon også med enheter utenfor NATO og å sammenkoble systemer som er godkjent for og inneholder informasjon med ulik gradering.

[2] https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/

Dokumentet sier at dette er så viktig at Sikkerhetsloven og Forskrift om informasjonssikkerhet må endres for å få dette til, og at det utfordrer eksisterende regelverk på i alle fall tre punkter:

- Krav til sikkerhetsklarering (Sikkerhetsloven §§19-22)
- Tilgang til sikkerhetsgradert informasjon (FoI §§3-1 og 3-2)
- Sammenkobling av informasjonssystemer (FoI §5-4)

I følge konseptet bør det satses på å etablere forsvarbare fysiske, logiske og organisatoriske strukturer. Forsvarbarhet beskrives her som «tiltak som begrenser en motstanders offensive handlingsrom og samtidig forsterker vår evne til å avsløre og bekjempe fiendtlige informasjonsoperasjoner». På samme måte sier konseptet at risikohåndtering bør ha som målsetning «å balansere egne sikkerhetstiltak i forhold til motstanderens offensive informasjonsoperasjoner», men det sier lite om hvordan dette skal gjøres i praksis.

Videre sier konseptet at følgende prinsipper bør legges til grunn for en sikkerhetsarkitektur for informasjonsinfrastrukturen:

- Kontrollert: Tilstedeværelse av kontrollmekanismer som reduserer muligheten for bruk som er i strid med sikkerhetspolicy, herunder f eks aksesskontroll, etablering av enklaver, perimetersikring med videre. Kontrollmekanismene skal også kunne anvendes i CND operasjoner.
- Minimert: Tilgjengelige tjenester avgrenses til de som gir eller underbygger militær evne. Tekniske sårbarheter og angrepsvektorer reduseres derigjennom til et minimum.
- Oppdatert: Komponenter, operativsystemer og applikasjoner skal fortløpende sikkerhetsoppdateres.
- Sikkerhetsmessig overvåket: Sikkerhetsmessig overvåking er en integrert del av CND og har til hensikt å avdekke sikkerhetstruende hendelser i Forsvarets informasjonsinfrastruktur som tiltak.
- Sporbarhet: Aktiviteter i INI skal kunne lokaliseres til enklave, utstyr og bruker.

## 2.5 Informasjonssikkerhetsstrategien for forsvarssektoren

Forsvarsdepartementets strategi for informasjonssikkerhet i forsvarssektoren er fastsatt for bruk i Forsvarsdepartementet og underlagte etater. En overordnet målsetting er: «Informasjonssikkerhetsarbeidet skal bidra til at forsvarssektoren kan løse sine oppgaver i fred, sikkerhetspolitisk krise og væpnet konflikt.» I strategien handler informasjonssikkerhet om å sikre informasjonens konfidensialitet, integritet, tilgjengelighet og sporbarhet.

Kort fortalt definerer strategien fem ulike mål med tilhørende strategiske prioriteringer:

- God sikkerhetsstyring gjennom etablering av et helhetlig styringssystem og tydelig ledelsesforankring og styrking av sikkerhetskulturen.

- Styrket informasjonskontroll gjennom styrket bevissthet om skjermingsbehov og økt bruk av krypto.

- Resiliente informasjonssystemer gjennom robuste og dynamiske systemer, kontinuerlig forbedring, og redusert antall ugraderte systemer som ikke er underlagt sentral forvaltning.

- Effektiv håndtering av digitale angrep gjennom økt sporbarhet og øving på hendelseshåndtering og bortfall av kommunikasjon.

- Godt tverrsektorielt samarbeid innenfor informasjonssikkerhet som bidrar til å kartlegge avhengigheter av sivil infrastruktur, økt sikkerhetsforståelse i leverandørkjeden og å styrke samarbeidet med relevante samarbeidspartnere

## 2.6 Diskusjon

I dag kan det se ut som om Forsvaret har utfordringer med å utvikle INI for NbF fordi det er stor tvil knyttet til hva som er mulig å få til av funksjonalitet samtidig som informasjonssikkerheten skal ivaretas. Det er vanskelig å løse sikkerhetsutfordringene fordi det ikke eksisterer en slik INI å vurdere sikkerheten ut i fra. Generelt er det vanskelig å si noe konkret om sikkerhetstiltak uten et system og konteksten det skal brukes i.

Forskrift om informasjonssikkerhet sier lite om hvordan mål, tiltak og prinsipper skal gjennomføres. Noe av dette avklares i NSM sine veiledninger på et mer teknisk nivå, men de tar ikke i betraktning alle nødvendige aspekter for sikkerhetsarbeid i Forsvarets fremtidige INI. Disse dokumenter handler nemlig om minimumskravene til sikkerhet og er ikke spisset mot operative behov i Forsvaret. Tilleggskrav for å gjøre en fremtidig INI tilstrekkelig sikker kunne vært avklart i sikkerhetskonsept for NbF, men de løsningene som skisseres der forutsetter en del endringer i dagens sikkerhetslov og forskrift om informasjonssikkerhet. Vi mener at Forsvaret må forholde seg til lovverket, og vi tror ikke det vil være hensiktsmessig å basere sikkerhetsløsningene på at dette kan endres. Konseptet mangler også en beskrivelse av hvordan de foreslåtte kapabilitetene kan realiseres på et overordnet nivå.

Informasjonssikkerhetsstrategien for forsvarssektoren er ganske ny, og gir en oversikt over hovedmålene innen informasjonssikkerhet. Denne sier heller ikke noe konkret om hvordan målene skal gjennomføres, men det skal heller ikke en strategi gjøre.

Dokumentene vi har sett på inneholder et godt utgangspunkt for videre arbeid med sikkerhet i INI, men de må harmoniseres og integreres i en arkitektur slik at de kan brukes som grunnlag og sees i sammenheng med eventuelt nye konsepter som Forsvaret vil utvikle.

# 3 Risiko

Risikovurderinger danner grunnlag for sikkerhetstiltak, og det er ønskelig å måle risiko for å kunne vurdere ulike sikkerhetstiltak opp mot hverandre. Systemer kan utsettes for risiko fra både utilsiktede og tilsiktede hendelser. Mens det er mulig å modellere systemsvikt som skyldes tilfeldige hendelser som ulykker og værfenomen basert på historikk og statistikk, er det vanskeligere å gjennomføre risikovurderinger som omhandler tilsiktede uønskede hendelser.

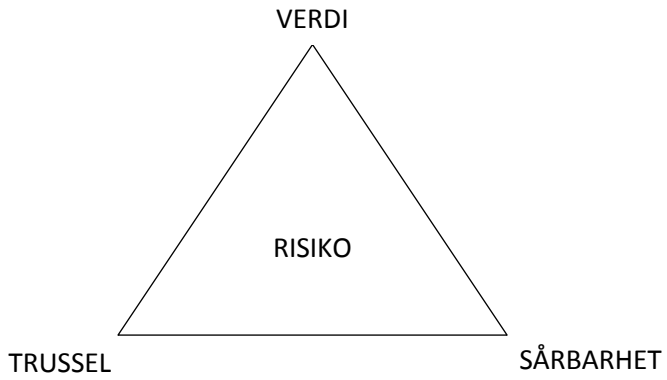
Forsvarets INI består av mange ulike systemer som skal fungere under svært ulike forhold. For eksempel vil infrastrukturen og kritikaliteten til infrastrukturen være annerledes for et forvaltningssystem i fredstid enn for et kommando- og kontrollsystem i en væpnet konflikt. Både verdi- og trusselvurderingene vil være forskjellige, og denne diversiteten skiller Forsvarets systemer fra de fleste sivile systemer.

## 3.1 Ulike tilnærminger til risiko

Det er ulike måter å vurdere risiko på. Den vanligste er antakelig å definere risiko som en kombinasjon av sannsynligheten for og konsekvensen av en uønsket hendelse. Denne tilnærmingen er også brukt i Norsk Standard 5814:2008 [9]. For å kunne si noe om sannsynlighet må man kjenne systemet og dets sårbarheter.

NS 5832:2014 [10] definerer risiko som forholdet mellom verdier, trusler og sårbarheter. Denne blir omtalt som «trekantmodellen» (se Figur 3.1). Fordelen er at den omgår begrepet sannsynlighet, selv om man må gjøre sannsynlighetsvurderinger indirekte i analysen, for eksempel når man vurderer hvilke trusler som er aktuelle [11].

Som tidligere nevnt er det spesielt vanskelig å si noe om sannsynligheten for tilsiktede uønskede handlinger, noe som er utførlig beskrevet i [11]. En tilnærming for tilsiktede uønskede hendelser som i enkelte sammenhenger kan gi mening for Forsvaret, kan være å anta at en sårbarhet vil bli utnyttet av en motpart dersom han har ressurser til det og anser det som fordelaktig. Dette er imidlertid kunnskap vi ofte ikke har. Det er heller ikke enkelt å si noe om konsekvenser av uønskede hendelser. For å kunne si noe om hvilke konsekvenser ulike trusler og sårbarheter i INI vil kunne gi, bør man ha et operativt scenario der man kan gjøre operative vurderinger.




*Figur 3.1 Trekantmodell for risiko.*

## 3.2 Risikohåndtering

Risiko kan unngås, reduseres, deles/overføres eller aksepteres. Hvilken strategi som vurderes som best er først og fremst avhengig av kostnader og konsekvenser ved de ulike strategiene. Konsekvensene er igjen scenarioavhengig, og i mange tilfeller kostnadene også. Typisk vil man unngå en risiko med høy sannsynlighet og høy konsekvens, redusere en risiko med høy sannsynlighet og lav konsekvens, spre en risiko med lav sannsynlighet men høy konsekvens, og akseptere risikoer med lav sannsynlighet og lav konsekvens.

I informasjonssikkerhet finnes det mange kjente sikkerhetstiltak det er ønskelig å ha på plass fordi de forebygger eller reduserer noen kjente typer risiko. Et eksempel er CIS-Capability Breakdown [12] som forsøker å liste alle sikkerhetskapabilitetene som kan være aktuelle for NATO. Forsvaret bør også realisere lignende kapabiliteter, men utfordringen er å få til dette på en helhetlig og balansert måte som fungerer tilfredsstillende med tanke på blant annet lover og forskrifter og under ulike forhold.

## 3.3 Verdivurdering

En verdi er en ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen [13]. Verdien kan være både materiell og immateriell, og eksempler kan være informasjon, infrastruktur, omdømme, kapital og liv og helse.

Dagens sikkerhetsregime vektlegger verdivurdering av informasjon. Konsekvensen ved tap av konfidensialitet, integritet og tilgjengelighet skal vurderes med tanke på rikets sikkerhet, noe som angir hvilken sikkerhetsgradering informasjonen skal merkes med. Konfidensialitet kan også beskyttes med bakgrunn i andre lover, eller ut fra informasjonens verdi for oppdraget.

Selv om sikkerhetsloven åpner for at informasjon kan ha kortvarig beskyttelsesbehov, kreves det i praksis at graderte informasjonssystemer må godkjennes med tanke på lang tids beskyttelse mot en teknisk avansert motstander. Blant annet for informasjon som er gradert ut fra et

operasjonssikkerhetsperspektiv kan kravene virke strenge, spesielt i operasjoner der motparten har lav teknologisk kompetanse.

Integritet og tilgjengelighet er også viktig. Tilgjengelighet kan kvantifiseres med oppetid eller redundanskrav, og man kan definere tjenester og informasjon Forsvaret er mest avhengig av. Integritet er noe Forsvaret vanligvis alltid ønsker seg. Upålitelig informasjon er ofte lite brukbar i praksis. Manipulert informasjon kan i mange tilfeller få store konsekvenser, som for eksempel at målkoordinater er endret slik at man begynner å skyte på egne styrker.

## 3.4 Sårbarhetsvurdering

I NS 5830:2012 [13] defineres sårbarhet som manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.

Et informasjonssystem er en kompleks sammensetning av teknologi, programvare og mennesker. En sårbarhet i denne konteksten kan kort beskrives som en svakhet ved systemet som muliggjør uønskede endringer eller hendelser og som dermed gir systemet annerledes oppførsel enn tiltenkt ved systemets design [14]. Det finnes flere ulike sårbarheter [14]:

- *Fysiske sårbarheter* omfatter i første rekke sårbarheter grunnet materiellfeil, materiellsabotasje og manglende fysisk beskyttelse og redundans. Virkemidler som fysisk maktbruk og elektronisk krigføring retter seg direkte mot denne type sårbarheter

- *Logiske sårbarheter* omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrep i dette domenet kan være alt fra utnyttelse og bruk av allmenn tilgjengelig kode publisert som nettverksverktøy på Internett, til angrepskode og mer spesialskrevne verktøy. Alle komponenter som kjører programvare, og alle systemer som helt eller delvis er realisert eller styres via programvare, kan være sårbare i det logiske domenet.

- *Sosiale sårbarheter* omfatter den menneskelige kontakten og innflytelsen på et datasystems utvikling, drift og vedlikehold, styring og bruk. Herunder faller krav til menneskelig kompetanse, håndtering av konfigurasjonsendringer, oppdateringer, uvøren bruk og organisatoriske aspekter. «Social engineering» er en type angrep som utnytter det menneskelige element direkte.

- *Avhengigheter* dekker sårbarheter som oppstår grunnet avhengigheter mellom systemet og andre systemer, eller avhengigheter innad i systemet. Dette kan være avhengigheter til helt andre infrastrukturer (for eksempel strøm og vann), en tjenestes avhengighet av en annen tjeneste eller indre avhengigheter av spesielle noder i systemet grunnet arkitektur og design. Avhengigheter vil kunne omfatte både fysiske, logiske og sosiale sårbarheter.

Et angrep vil som oftest både kunne utnytte og ha effekter i flere av disse kategoriene. For eksempel vil svake driftsrutiner grunnet menneskelig svikt kunne føre til åpne angrepsvektorer som kan utnyttes i det logiske domenet.

## 3.5 Trusselvurdering

I Norsk Standard 5830:2012 defineres en trussel som en mulig uønsket handling eller hendelse som kan gi negative konsekvenser for en entitets sikkerhet. Sikkerhet defineres som en reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare. Trusler i vår kontekst kan være både utilsiktede og tilsiktede uønskede hendelser. De tilsiktede hendelsene kan være spesielt vanskelig å beskytte seg mot siden en motstander vil kunne innrette angrepet slik at effekten blir størst mulig.

En trusselvurdering beskriver det gjeldende trusselbildet for det som ønskes beskyttet, og gir en vurdering av hvordan trusselbildet kan utvikle seg [15]. Hovedfokus bør være på reelle og potensielle trusselaktørers intensjon om, og kapasitet til, å ramme virksomheten. Det er viktig at den dekker et lengre tidsperspektiv.

Relevante faktorer ved en trusselvurdering kan være:

- Historikk – har egen eller lignende virksomhet vært truet tidligere?
- Tilstedeværelse – Finnes det trusselaktører i området hvor virksomheten er etablert?
- Intensjon – Har trusselaktøren et uttalt eller antatt ønske om å ramme virksomheten?
- Kapasitet – Har trusselaktøren evne til å ramme virksomheten?

Det er vanskelig å gjøre en trusselvurdering uten et scenario hvor man har en definert motpart.

## 3.6 Diskusjon

Risikovurderinger utgjør en vesentlig del av prosessen en sikkerhetsarkitektur skal støtte og bygge på. Hensikten med sikkerhetstiltak er som tidligere nevnt å redusere risiko. Som vist i dette kapittelet er det vanskelig å gjøre risikovurderinger for tilsiktede uønskede handlinger, og det er viktig å beskytte INI mot nettopp dette.

For å gjøre risikovurderinger trengs scenarioer for å kunne si noe om hvordan INI vil se ut og hvilke sårbarheter som ligger her. De er viktige for å kunne si noe om motparten og hvilke trusler som er aktuelle, og på samme måte vurdere de kritiske verdiene og de operative konsekvensene av ulike trusler og sårbarheter. En metode for å gjøre slike risikovurderinger er tidligere utviklet ved FFI [14]. For å kunne gjøre risikovurderinger og vurderinger av sikkerhetstiltak må man derfor ned på et teknisk nivå. Spørsmålet er om det er mulig å gjøre tilsvarende vurderinger på et logisk nivå, og i så tilfelle hvordan.

Generelt er det ingen omforent beste fremgangsmåte internasjonalt eller nasjonalt for risikovurdering for tilsiktede uønskede handlinger. Likevel er det noen kjennetegn som går igjen i en god tilnærming til risikovurdering for slike hendelser [11]:

- Å sette ned en arbeidsgruppe med bred kompetanse
- Å kartlegge kunnskapsstyrken – viktig å ha med den rette kompetansen
- Å benytte en metode som er strukturert og som:
    - er konkret og basert på systemforståelse
    - har et helhetlig perspektiv
    - tydelig kommuniserer usikkerhet og risiko
    - er gjennomsiktig, sporbar og etterprøvbar

Det pekes også på at kunnskap og metodeforståelse synes å være viktigere enn valg av metode og tilnærming. Det er spesielt viktig med en tverrfaglig ekspertgruppe der folk har ulike perspektiver, kompetanse og bakgrunn, og når resultatene skal presenteres er det viktig å kommunisere usikkerhetene i vurderingene som er gjort.

# 4 Virksomhetsarkitektur

En virksomhet har mange domener, avdelinger, forretningsområder eller funksjoner som må koordineres for å oppnå et felles mål. En virksomhetsarkitektur vil være en «beskrivelse av organisasjonens forretningsdrift og den underliggende IT-støtten for driften. [Den] er vanligvis knyttet til løpende kommunikasjon og styring av endring, og vil typisk omfatte organisasjonsstruktur, IT-landskapet, identifikasjon av strategiske forbedringsmuligheter og identifikasjon av omfattende omstillingsaktiviteter» [3]. Den modellerer altså sammenhengen mellom virksomhetens overordnende mål og IKT-behovene man må dekke for å oppnå disse målene. Virksomhetsarkitekturen kan deretter være grunnlag for å formulere en overordnet strategi for hvordan behovene skal dekkes, og være utgangspunktet for mer detaljerte planer om hvordan ulike deler av virksomheten kan bidra til å realisere strategien. Dette kan gjerne gjøres ved å utforme domenespesifikke arkitekturer som har forankring i virksomhetsarkitekturen. Målet er å bidra til konsistens på tvers av virksomheten og å sørge for at løsningene som tas fram bidrar til at virksomheten som helhet oppnår sine mål.

Å modellere en stor organisasjon og skape en felles visjon om hvordan virksomheten kan oppnå sine mål på tvers av både avdelinger og interessentgrupper er både tids- og resurskrevende. En arkitekt(gruppe) må prøve å avklare forventninger, behov, krav og mål til de ulike interessentene, samt skape en ramme for arkitekturen som alle er enige om. I tillegg må arkitekturen vedlikeholdes fortløpende for å tilpasse seg nye behov og erfaringer. Å velge riktige verktøy er derfor både avgjørende og utfordrende.

Det å realisere en arkitektur forutsetter at man gir en ramme for hva arkitekturen skal dekke som en taksonomi eller en inndeling i arkitekturdomener, og en metode for å planlegge, implementere og vedlikeholde arkitekturen. Et modelleringsspråk kan også være nyttig for å definere modellene som arkitekturen beskriver på en konsistent og klar måte. I praksis er det ingen veletablert og omforent måte å utarbeide en fungerende virksomhetsarkitektur på. Det er utviklet mange rammeverk som bare dekker ett eller to av disse elementene, gjerne ved å bygge på tidligere ideer, skreddersy og utdype dem for mer spesifikke sektorer, eller rett og slett å kalle de samme tingene for noe annet. Det fins dermed mange tilsynelatende forskjellige prosesser, metoder, modelleringsspråk, taksonomier og retningslinjer for hvordan man skal bygge en virksomhetsarkitektur.

## 4.1 Zachmans rammeverk

J.A. Zachman betraktes som den første som prøvde å formalisere alle aspekter en arkitektur skal dekke [16]. Han analyserte veletablerte produksjonsprosesser for komplekse systemer som fly, informasjonssystemer og byggverk, og systematiserte fellestrekkene i en matrise som ble kontinuerlig videreutviklet til den vist i Figur 4.1. Den er ment å beskrive alle aspekter av en idé, produkt, system eller virksomhet for alle interessenter og involverte i produksjonsprosessen.

De seks radene er *perspektiver* som skal formidle relevant informasjonen om systemet til en spesifikk målgruppe på et språk gruppen forstår. Kjøpere, potensielle investorer, aksjonister, klienter, osv. er opptatt av konteksten til virksomheten eller systemet, og hva de vil få igjen for pengene sine. Ledelse, eiere eller styret er opptatt av forretningskonseptene og -prosessene. Arkitekter skal oversette forretningskonseptene til logiske krav, prosesser, dataelementer og funksjoner på systemnivå. Ingeniører skal gjøre systemkonsepter om til teknologispesifikke planer. Teknikere skal implementere eller anskaffe og konfigurere systemet. Til slutt er det et perspektiv som tar for seg hele virksomheten eller systemet og hvordan den skal opereres. Kolonnene består av seks spørsmål som skal bryte ned aspekter av systemet på en konsistent måte i hvert perspektiv: Hva (Verdier); Hvordan (Prosesser); Hvor (Distribusjon); Hvem (Ansvar); Når (Tid); Hvorfor (Motivasjon).

Zachmans rammeverk er hovedsakelig en taksonomi over aspektene man trenger for å utarbeide en komplett og systematisk beskrivelse av produksjonsprosessen til komplekse systemer. Det er nyttig for å etablere et felles språk og en felles forståelse av systemet, men det definerer ingen klar metode for hvordan man bør jobbe seg gjennom cellene i matrisen eller hvordan overgangen mellom perspektiver best kan realiseres. Zachman er grunnlaget for de fleste andre arkitekturrammeverk, selv om noen bare bruker et utvalg av cellene mens andre også prøver å

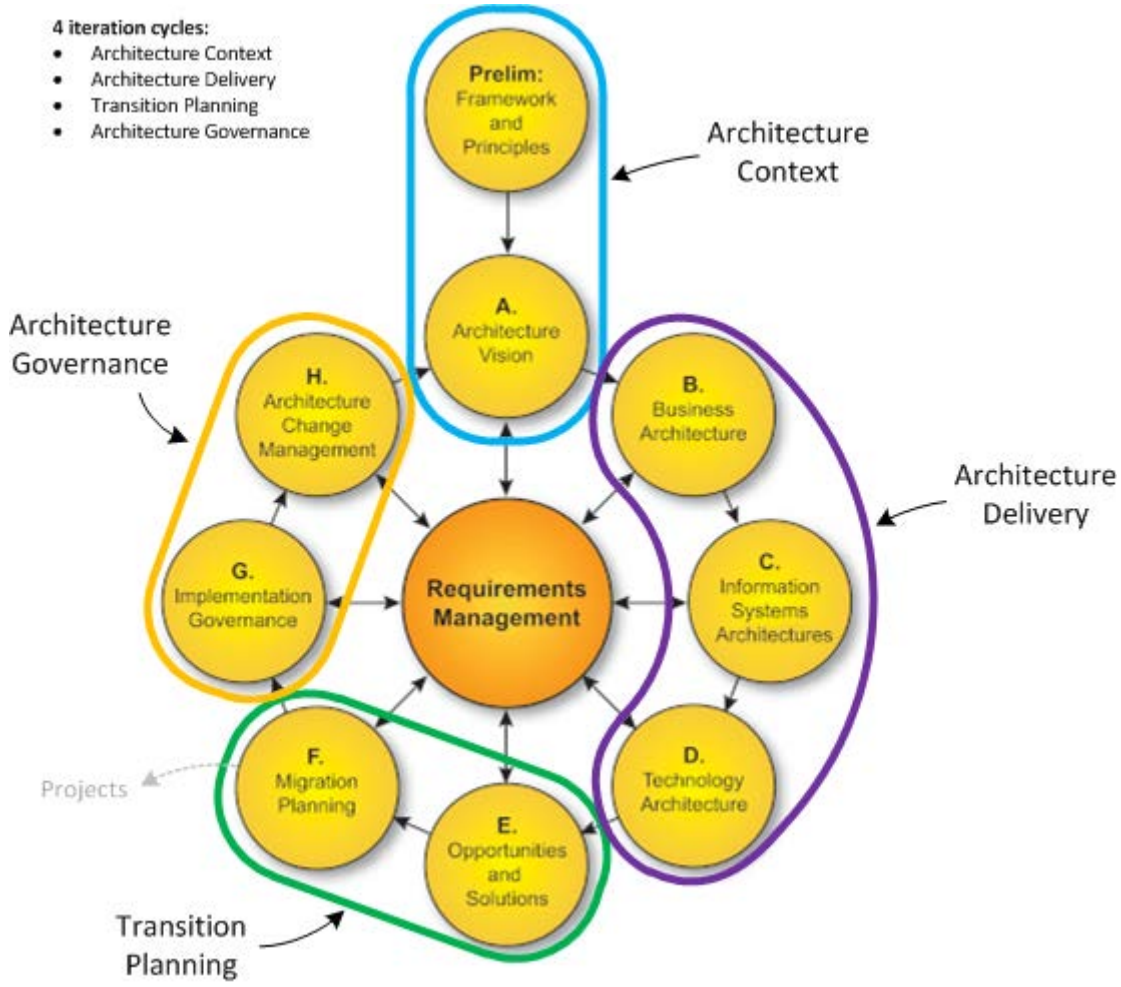
definere den metodologiske biten. Ideen om systematisk å beskrive et system fra forskjellige perspektiver og synliggjøre sammenhengene mellom ulike parter er med på å gjøre arkitektur attraktivt.

| | WHAT (Asset) | HOW (Function) | WHERE (Location) | WHO (People) | WHEN (Time) | WHY (Motivation) |
|---|---|---|---|---|---|---|
| CONTEXTUAL {Executive Perspective} | | | IDENTIFY | | | |
| CONCEPTUAL {Business Perspective} | | | DEFINE | | | |
| LOGICAL {Architect Perspective} | | | REPRESENT | | | |
| PHYSICAL {Engineer Perspective} | | | SPECIFY | | | |
| TECHNICAL {Technician Perspective} | | | CONFIGURE | | | |
| OPERATIONAL {Enterprise Perspective} | | | INSTANTIATE | | | |

*Figur 4.1 Zachmans matrise. Cellene er ikke vist i detalj.*

## 4.2 TOGAF

TOGAF (The Open Group Architecture Framework) [17] er et virksomhetsarkitekturrammeverk som også gir en metode for å definere, planlegge, implementere og vedlikeholde en virksomhetsarkitektur. TOGAF ADM (Architecture Development Methodology) er illustrert i Figur 4.2.



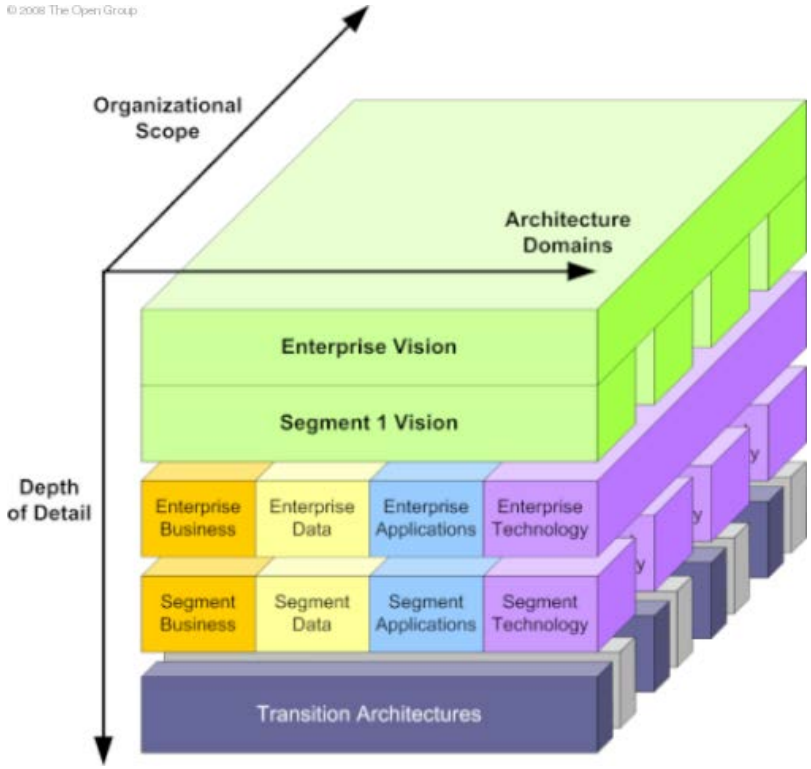

*Figur 4.2 TOGAF ADM*[3]

Prosessen består av en forberedende fase der prinsippene for arkitekturarbeidet defineres og arkitekturrammeverket tilpasses til virksomheten, fulgt av åtte andre faser. Den første skal skissere målarkitekturen. De neste tre skal definere domenearkitekturer definert i TOGAF: forretning, informasjonssystemer som består av data og applikasjon, og teknologi. Så skal man undersøke om det finnes løsninger som kan dekke behovene identifisert i domenearkitekturene, og eventuelt sette i gang prosjekter. Til slutt skal man sørge for at arkitekturen blir oppdatert eller endret basert på lærdom fra de andre fasene. For å sikre konsistens skal alle fasene styres etter virksomhetens krav, men disse er dynamiske og skal endres ved behov.

TOGAF bruker en annen inndeling enn Zachman for sine arkitekturdomener eller perspektiver, men det er mulig å få disse domenene til å korrespondere med grupper av celler i Zachmans matrise[4]. Det som er nytt i TOGAF er at man bruker en iterativ prosess til å bygge arkitekturen og at man gradvis realiserer en *målarkitektur* fra den eksisterende *baseline-arkitekturen*

[3] Fra https://www.linkedin.com/pulse/togaf-adm-big-bang-theory-andrew-brownlie
[4] http://www.opengroup.org/architecture/0210can/togaf8/doc-review/togaf8cr/c/p4/zf/zf_mapping.htm

gjennom en del *transisjonsarkitekturer*. I tillegg kan prosessen anvendes på ulike nivåer i virksomheten (se Figur 4.3).




*Figur 4.3 Alle arkitekturdomenene kan beskrives i mer detalj i hvert virksomhetssegment (og muligens ned til kapabilitetsnivå som ikke vises i bildet), samtidig som man definerer en plan for å realisere målarkitekturen på forskjellige nivå gjennom flere transisjonsarkitekturer*[5].

Arkitekturarbeidet skal også dokumenteres gjennom *artefakter*. TOGAF definerer tre typer artefakter: kataloger, diagrammer og lister. For å sørge for at alle artefaktene og andre relevante ressurser blir tatt vare på og gjort tilgjengelig for alle, og danner grunnlag for videre arbeid, definerer TOGAF «Architecture Repository». Dette er et viktig element for å sikre konsistens og fremgang i arkitekturarbeidet.

TOGAF definerer altså både en inndeling av arkitekturen og en utviklingsmetode. Forsvaret har adoptert TOGAF som offisiell arkitekturutviklingsmetode [1].

## 4.3 NAF

NAF (Nato Architecture Framework) [18] er et rammeverk som er utformet med tanke på hvordan en militær virksomhet vanligvis opererer og er organisert. Målsetningen er å gjøre

[5] Bildet fra https://mikethearchitectblog.wordpress.com/2011/02/24/navigating-through-the-complexities-of-architectures/

beslutningstakere og andre interessenter i stand til å fokusere på informasjonen de har behov for gjennom å strukturere kompleksitet og balansere ulike brukerbehov.

NAF består av fire arkitekturer. En overordnet arkitektur som ser flere år framover og beskriver hva og hvorfor virksomheten gjør det den gjør. En referansearkitektur som dekker noen få år og beskriver hvordan virksomheten fungerer. Målarkitekturer som dekker tekniske aspekter ved løsningene identifisert i referansearkitekturen. En baselinearkitektur som beskriver de tekniske aspektene ved virksomheten slik den er nå. Dette korresponderer med de tilsvarende TOGAF arkitekturtyper.

Det NAF fokuserer på er hva arkitekturbeskrivelsen skal inneholde, og hvordan den skal struktureres. NAF versjon 3 definerer følgende syv «views»:

- *All View:* Tilsvarer virksomhetsarkitekturen.
- *Capability View:* En taksonomi av eksisterende og ønskede kapabiliteter.
- *Operational View:* Aktiviteter, elementer og informasjonsutvekslingsbehov for å realisere kapabilitetene.
- *Service-Oriented View:* Tjenestene som realiserer operasjonene beskrevet i operational view.
- *Systems View:* Teknologien nødvendig for å realisere operational view.
- *Technical View:* Spesifikasjoner, standarder og retningslinjer for å implementere systemer.
- *Programme View:* Knytter sammen kapabilitetskravene og pågående prosjekter.

I likhet med Zachman har NAF ikke definert en egen utviklingsmetode. TOGAF med sine ADM-faser vil derfor utfylle NAF. I den kommende versjonen av NAF (v4.0) er viewene foreslått omorganisert etter Zachmans matrise.

## 4.4 Diskusjon

Forsvaret har valgt å bruke en integrasjon av TOGAF og NAF som arkitekturrammeverk [19].

De fleste arkitekturrammeverkene baserer seg på de samme ideene og prosessene, gjerne omorganisert og presentert med mer eller mindre detaljer, eller tilpasset spesifikke typer virksomheter. Det er gjort mye arbeid med å finne korrespondanser mellom rammeverk, og til og med kritikken av dem er nokså lik. Den grunnleggende ideen virker tiltalende i teorien, men det finnes nesten ingen konkrete eksempler på vellykket bruk av disse rammeverkene slik som de er. De er for omfattende eller teoretiske til å kunne brukes uten store forenklinger og tilpasninger [20] [21] [22] [23]. Det kan virke som erfaringene fra Forsvaret også støtter denne

konklusjonen.  Mye arbeid har blitt gjort for å tilpasse og forenkle TOGAF og NAF for Forsvaret [19] [24] og integrere dem med andre standarder [25], uten at det dermed fins enda en veletablert og fungerende virksomhetsarkitekturfunksjon som konsistent støtter Forsvarets aktiviteter. Det ble påpekt i en tidligere rapport at arkitektur i enkelte sammenhenger har blitt synonymt med teknisk systemarkitektur i Forsvaret [24], men det kan se ut som dette er i ferd med å endre.

Hovedkonseptet innenfor virksomhetsarkitekturdisiplinen er en top-down tilnærming som modellerer virksomheten på kontekstuelt- og forretningsnivå først og deretter identifiserer og utvikler den riktige teknologien som støtter de strategiske virksomhetsbehovene. Arkitekturen skal sørge for at teknologien er både *relevant* og *konsistent* på tvers av virksomheten. Arkitekturrammeverkene vi har sett her foreslår mulige måter å beskrive virksomheten på og generiske metoder for å jobbe strukturert med planlegging og utvikling av informasjonssystemer, men de må tilpasses den enkelte virksomheten. Forsvaret har allerede gjort en del av jobben, men å integrere sikkerhetsaspektet kan være enda mer utfordrende.

# 5 Sikkerhetsarkitektur

Forretnings-, data-, applikasjon- og teknologiarkitektur er godt integrert i de fleste virksomhetsarkitekturrammeverkene, men dette gjelder ikke sikkerhet. Det finnes mange standarder, modeller, retningslinjer og anbefalinger innen informasjonssikkerhet, men ingen dekker alle behovene til hver virksomhet. For en helhetlig sikkerhetstilnærming er det naturlig å forsøke å anvende samme metoder og prinsipper som for virksomhetsarkitektur. Utfordringen er at sikkerhet ikke er et system i seg selv, men snarere et aspekt av et system. Begrepet virksomhetsinformasjonssikkerhetsarkitektur (Enterprise Information Security Architecture eller EISA [26]) brukes ofte for å skille dette fra tekniske sikkerhetsarkitekturer. I denne rapporten er det EISA vi referer til når vi snakker om sikkerhetsarkitektur.

Informasjonssystemer har blitt mer komplekse, sammenkoblet og tettere integrert med forretningsprosesser og organisasjon, samtidig som trusselbildet er komplekst og dynamisk, og avhengig av faktorer som ikke bare er teknologiske. Informasjon og systemer kan kompromitteres ved å utnytte sosiale og logiske sårbarheter. Konsekvensene av et sikkerhetsbrudd på systemnivå kan påvirke andre prosesser i virksomheten som ikke direkte bruker den kompromitterte informasjonen. Sikkerhet må derfor sees i sammenheng med alle aspektene av en virksomhet og kontekstene den opererer i, ikke bare teknologi [27].

Det fins ingen entydig definisjon av sikkerhetsarkitektur [27] [28], men den knyttes vanligvis til begreper som sikkerhetskrav, risiko og policyer, i tillegg til en måte å beskrive alt dette på.

Det ser også ut til å være enighet om sikkerhetsarkitekturens rolle

- Den skal være en referanse for sikkerhetsevaluering
- Den skal være en referanse for å planlegge og implementere sikkerhet
- Den skal integrere sikkerhet innenfor og på tvers av virksomhetslagene
- Den skal standardisere prosessene rundt informasjonssikkerhet
- Den skal bidra til rask og god håndtering av sikkerhetsproblemer

I tillegg kan den bidra til økonomisk besparing, og hjelpe til med å prioritere sikkerhetsrelaterte prosjekter og aktiviteter [27].

Det er identifisert hovedsakelig tre ulike måter å integrere en helhetlig sikkerhetstilnærming med virksomhetsarkitekturen på [28] [26]: Sikkerhetsarkitektur som eget arkitekturdomene under virksomhetsarkitekturen, sikkerhetsaspektet integrert i alle lag og domener i virksomhetsarkitekturen, eller sikkerhetsarkitektur som eget domene i teknologiarkitekturen. Det er vanskelig å se for seg en sikkerhetsarkitektur helt isolert fra de andre domenene, og det forutsetter i så fall god forankring i virksomhetsarkitekturen. Integrasjonen av sikkerhet i hele arkitekturen virker kanskje mest fornuftig, men det kan bli utfordrende å sikre helhet og konsistens. Det å begrense sikkerhetsarkitektur til teknisk arkitektur er neppe akseptabelt hvis målet er å oppnå en helhetlig tilnærming til sikkerhet. Overgangen til en mer helhetlig sikkerhetstilnærming ser altså ut til å være en lang prosess som fortsatt er i en tidlig fase.

Det finnes noen rammeverk for sikkerhetsarkitektur, men de er mindre modne og brukt enn de for virksomhetsarkitektur. Her skal vi gi en oversikt med spesiell vekt på SABSA, som kanskje er det eneste som kan kategoriseres som et komplett virksomhetsarkitekturrammeverk for sikkerhet.

## 5.1 SABSA

SABSA (Sherwood Applied Business Security Architecture) [29] er et virksomhetsdrevet sikkerhetsarkitekturrammeverk som utrykker virksomhetsbehov ved standardiserte og gjenbrukbare attributter, og deretter modellerer sikkerhetskrav og måler hvor effektivt de støtter virksomhetens mål. I praksis brukes SABSA til å modellere og styre risikoen i virksomheten slik at den kan opererer innenfor et akseptabelt nivå. SABSA definerer også en overordnet utviklingsmetode, hovedsakelig med tanke på integrasjon.

Som vist i Figur 5.1 bygger SABSA tungt på Zachmans rammeverk og består også av seks lag:

- Et *kontekstuelt* lag der man definerer virksomhetens krav, mål og behov utfra et forretningsperspektiv.
- Et *konseptuelt* lag der man identifiserer hvordan sikkerhet kan støtte, beskytte og høyne virksomhetens mål, og hvordan dette kan måles i forskjellige virksomhetsdomener.
- Et *logisk* lag der sikkerhetstjenester og tillitsrelasjoner mellom domener blir utledet.
- Et *fysisk* lag som inkluderer systemer, plattformer og sikkerhetsmekanismer.
- Et *komponent*-lag med verktøy, nettverk og konkrete produkter.
- Et *management*-lag som har blitt til en egen matrise. Den sier noe om de aktivitetene som skal utføres for hver celle i de andre lagene av SABSA-matrisen.

På samme måte som Zachmans rammeverk, er det på hvert lag fokus på seks faktorer eller spørsmål som skal bidra til en helhetlig tilnærming til sikkerhetsutfordringer. Verdier gir «hva?», risikovillighet gir «hvorfor?», arbeidsprosesser gir «hvordan?», personell gir «hvem?», beliggenhet gir «hvor?», og tidsaspekter gir «når?».

SABSA er bygget rundt risiko. Sikkerhetsarkitekturen skal identifisere, måle og håndtere risiko slik at virksomheten kan operere trygt innenfor sin risikovillighet, og dermed øke sannsynligheten for å oppnå sine mål fordi de kritiske verdiene er beskyttet. Sporbarhet er et sentralt konsept i SABSA; det er viktig at alle sikkerhetsløsninger er forankret i konkrete virksomhetsbehov som understøtter virksomhetens strategiske mål.

SABSA bruker attributter for å knytte sikkerhetskrav sammen med verdiene og kapabilitetene som er kritiske for å oppnå de strategiske målene. Et attributt skal abstrahere et konkret virksomhetsbehov og skal knyttes til ett eller flere sikkerhetskrav. Et eksempel kan være en virksomhet som har godt omdømme som en kritisk verdi. Attributter knyttet til omdømme kan være kosteffektiv, tilgjengelig, åpen og etterprøvbar. Disse attributtene vil oversettes til mer konkrete sikkerhetskrav i forskjellige domener for å beskytte de verdiene virksomhetens omdømme støtter seg på. Det vil da kunne stilles krav til oppetid og tilgjengelighet av web-tjenester, overvåking og logging av aktiviteter for å forhindre og etterforske uønskede hendelser, signering og kildeautentisering for å sikre dataintegritet og troverdighet, osv.

SABSA tar altså for seg alle aspekter av sikkerhet i en virksomhet, fra forretningsrisiko til teknisk IKT-sikkerhet, og prøver og koble det hele sammen gjennom attributtmodellering. Dette kan klassifiseres som en komplett sikkerhetsarkitektur som også integrerer virksomhetsarkitekturaspektene. Det defineres likevel ingen klare metoder for risikovurdering eller andre sentrale aktiviteter; bare hvor i matrisen og livssyklusen disse aktivitetene skal

gjennomføres og hva de skal føre til. Brukerne må bruke sine foretrukne rammeverk eller verktøy til å gjøre det i praksis.

SABSA MATRIX

| | ASSETS (What) | MOTIVATION (Why) | PROCESS (How) | PEOPLE (Who) | LOCATION (Where) | TIME (When) |
|---|---|---|---|---|---|---|
| CONTEXTUAL ARCHITECURE | Business Decisions | Business Risk | Business Processes | Business Governance | Business Geography | Business Time Dependence |
| | Taxonomy of Business Assets, including Goals & Objectives | Opportunities & Threats Inventory | Inventory of Operational Processes | Organisational Structure & the Extended Enterprise | Inventory of Buildings, Sites, Territories, Jurisdictions, etc. | Time dependencies of business objectives |
| CONCEPTUAL ARCHITECTURE | Business Knowledge & Risk Strategy | Risk Management Objectives | Strategies for Process Assurance | Roles & Responsibilities | Domain Framework | Time Management Framework |
| | Business Attributes Profile | Enablement & Control Objectives; Policy Architecture | Process Mapping Framework; Architectural Strategies for ICT | Owners, Custodians and Users; Service Providers & Customers | Security Domain Concepts & Framework | Through-Life Risk Management Framework |
| LOGICAL ARCHITECTURE | Information Assets | Risk Management Policies | Process Maps & Services | Entity & Trust Framework | Domain Maps | Calendar & Timetable |
| | Inventory of Information Assets | Domain Policies | Information Flows; Functional Transformations; Service Oriented Architecture | Entity Schema; Trust Models; Privilege Profiles | Domain Definitions; Inter-domain associations & interactions | Start Times, Lifetimes & Deadlines |
| PHYSICAL ARCHITECTURE | Data Assets | Risk Management Practices | Process Mechanisms | Human Interface | ICT Infrastructure | Processing Schedule |
| | Data Dictionary & Data Inventory | Risk Management Rules & Procedures | Applications; Middleware; Systems; Security Mechanisms | User Interface to ICT Systems; Access Control Systems | Host Platforms, Layout & Networks | Timing & Sequencing of Processes and Sessions |
| COMPONENT ARCHITECTURE | ICT Components | Risk Management Tools & Standards | Process Tools & Standards | Personnel Man'ment Tools & Standards | Locator Tools & Standards | Step Timing & Sequencing Tools |
| | ICT Products, including Data Repositories and Processors | Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools | Tools and Protocols for Process Delivery | Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists | Nodes, Addresses and other Locators | Time Schedules; Clocks, Timers & Interrupts |
| SERVICE MANAGEMENT ARCHITECTURE | Service Delivery Management | Operational Risk Management | Process Delivery Management | Personnel Management | Management of Environment | Time & Performance Management |
| | Assurance of Operational Continuity & Excellence | Risk Assessment; Risk Monitoring & Reporting; Risk Treatment | Management & Support of Systems, Applications & Services | Account Provisioning; User Support Management | Management of Buildings, Sites, Platforms & Networks | Management of Calendar and Timetable |

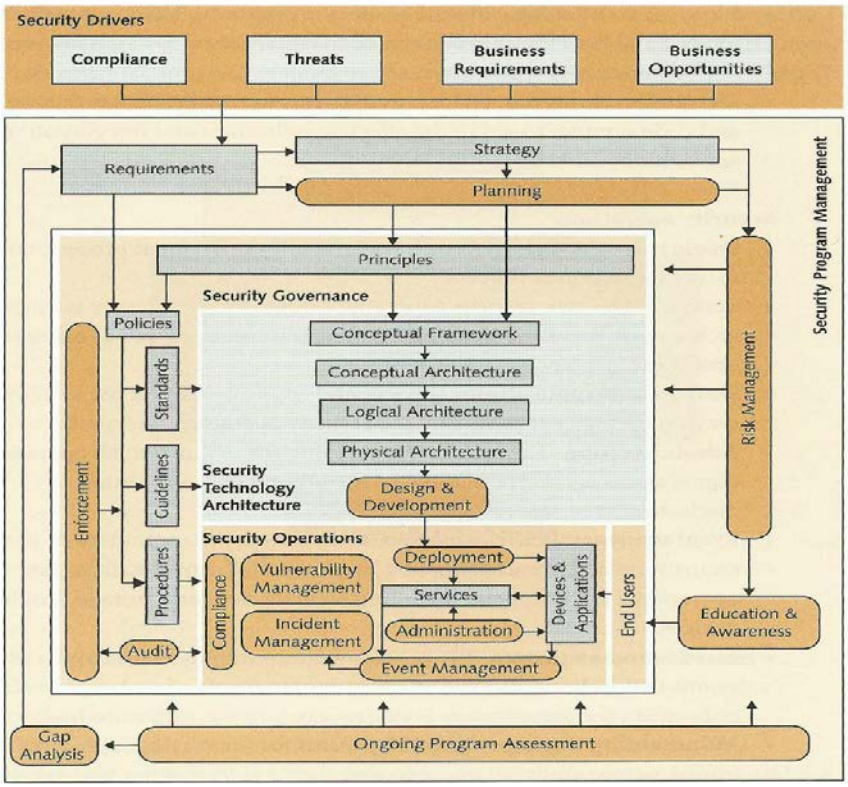


*Figur 5.1 SABSA- matrisen besto opprinnelig av 36 celler, men den nederste raden har blitt utvidet til en egen matrise med en celle for hver celle i de andre fem radene.*

## 5.2 The Open Enterprise Security Architecture (O-ESA)

O-ESA kommer fra samme gruppe som de som har utviklet TOGAF og er beskrevet som et rammeverk og mal for policy-drevet sikkerhet [30]. Det fokuserer mest på teknisk sikkerhet. Virksomhetsbiten er skissert som «Security Drivers» øverst i Figur 5.2, og kan sammenlignes med kontekstlaget i SABSA. Sikkerhetskravene skal utledes fra disse driverne og en gap-analyse av den eksisterende arkitekturen, men hvordan prosessen gjennomføres er ikke beskrevet. Dette tilsvarer attributtmodelleringsprosessen i SABSA. Man kan utlede fra figuren at sikkerhetskravene hovedsakelig danner grunnlag for en sikkerhetsstrategi, planen som skal implementere strategien, samt selve policyene som arkitekturen skal håndheve. I praksis fokuserer rammeverket på implementasjon av mekanismene for å håndheve policy på både konseptuelt, logisk og fysisk nivå.

Bruken av rammeverket er begrenset til virksomheter som har det kontekstuelle laget på plass og som ønsker en policy-drevet sikkerhetsstrategi. Sammenhengene mellom komponentene i arkitekturen er nyttig, siden en veldefinert avhengighetsoversikt mangler i SABSA.

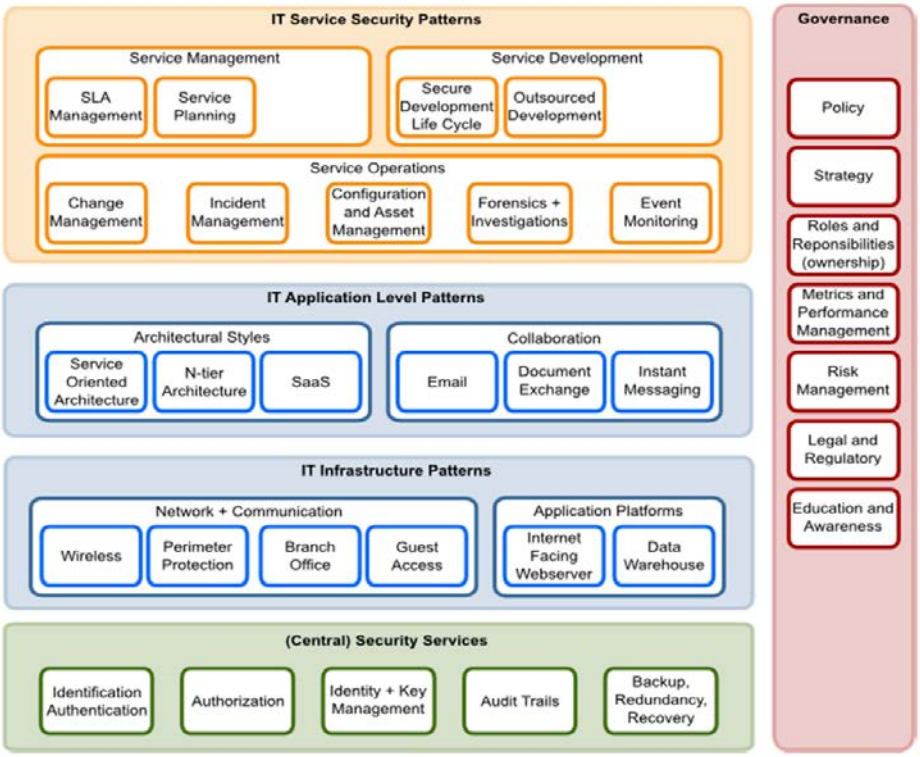



*Figur 5.2 E-OSA standarden dekker bare den innerste boksen som inkluderer «Security Governance», «Security Technology Architecture» og «Security Operations», men forutsetter at de andre komponentene er på plass for å kunne være en helhetlig virksomhetssikkerhetsarkitektur [30] [28].*

## 5.3 Open Security Architecture (OSA)

OSA[6] er et åpent arkitekturrammeverk ment som en katalog av byggeklosser det kan bygges en egen arkitektur fra. Byggeklossene er en katalog med kjente trusler, en katalog med sikkerhetsmekanismer tatt fra NIST [31], en katalog med «patterns» som kan brukes til å utforme sikkerhetsløsninger, samt generisk informasjon om OSA og prinsippene bak. «Patterns» er organisert etter en egen taksonomi (Figur 5.3). Dessverre ser det ikke ut som prosjektet har kommet veldig langt, og det er lite aktivitet og materiale på web-siden. Den beskriver ikke heller kriteriene man bør bruke til å velge de riktige komponentene. Noe som vanligvis bygger på en risikovurdering.

[6] http://www.opensecurityarchitecture.org/cms/index.php




*Figur 5.3 OSA-arkitekturlandskap*[7].

## 5.4 Sikkerhet i TOGAF

TOGAF [17] har et kort kapittel om sikkerhetsarkitektur. Sikkerhet beskrives som en del av alle ADM-fasene, og input og output til sikkerhetsarbeidet blir definert for hver fase. Denne tilnærmingen oppfattes imidlertid som implisitt, begrenset og for knyttet til forretningsarkitekturdomenet. Det er derfor foreslått å integrere SABSA med TOGAF for å forbedre sikkerhetsaspektet og dermed oppnå et bedre og mer komplett virksomhetsarkitektur-rammeverk [32]. For de fleste SABSA-konseptene er integrasjonen naturlig, og TOGAF gir en bedre og mer strukturert metode for å jobbe seg gjennom SABSA matrisen enn den SABSA selv definerer. Denne integrasjonsprosessen er fortsatt i gang [33], men siden TOGAF er den standarden Forsvaret følger vil en mulig sammenslåing kunne være relevant for sikkerhetsarkitekturaktiviteten i Forsvaret.

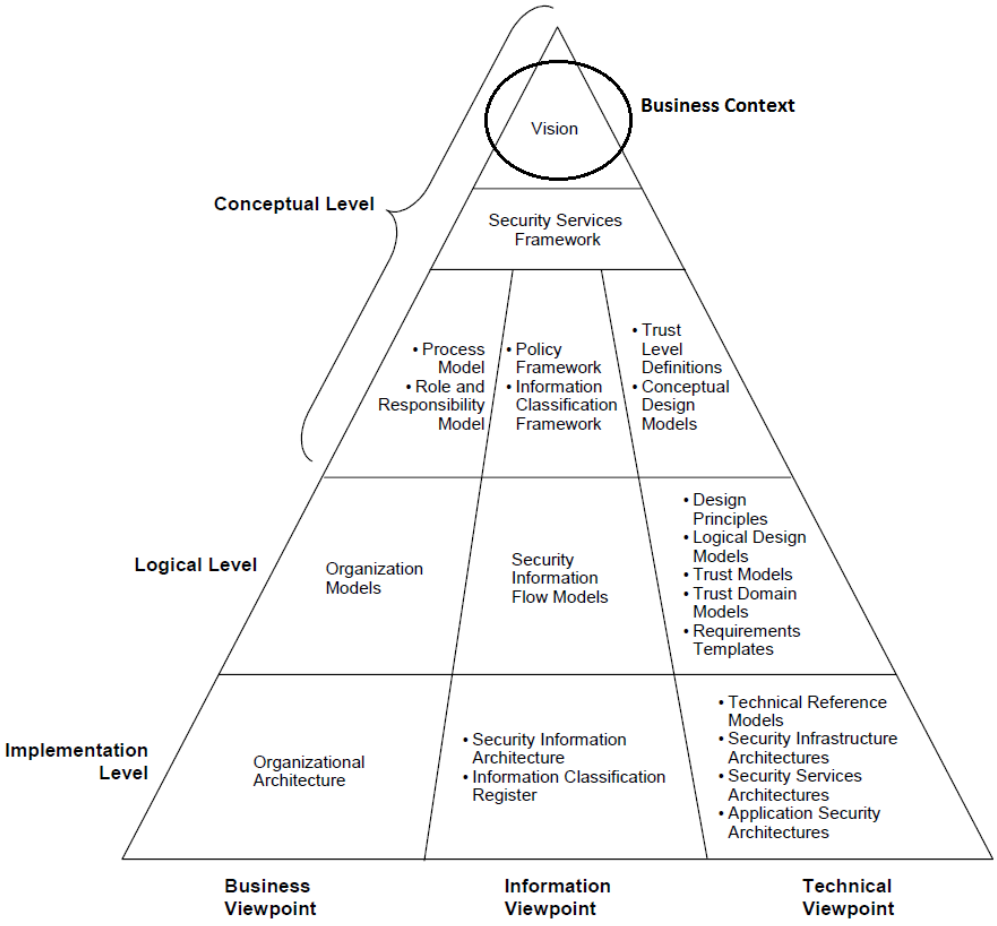
## 5.5 Gartner EISA

Gartner var blant de første som foreslo integrasjon av sikkerhetsarkitektur og virksomhetsarkitektur [26]. Sikkerhetsaspektet blir håndtert i de lag og domener som er vist i Figur 5.4. De fleste lagene er som i SABSA: kontekstuelt, konseptuelt, logisk og

[7] http://www.opensecurityarchitecture.org/cms/foundations/osa-landscape

implementasjon. Komponentlaget mangler. Videre brukes arkitekturdomenene forretning, informasjon og teknisk istedenfor de seks spørsmålene som SABSA bruker. Det er likevel en klar korrespondanse mellom cellene i de to rammeverkene, slik at forskjellen hovedsakelig er hvordan aspektene blir gruppert. Det virker imidlertid som om fokuset på risiko er mindre enn i SABSA.

Det er noen interessante punkter om denne sikkerhetsarkitekturen som er verdt å nevne her siden de er ganske grunnleggende uansett hvilke rammeverk man velger [34] [35]. Et av hovedmålene med sikkerhetsarkitektur er å etablere et felles språk for sikkerhet. Arkitekturen er en kontinuerlig iterativ prosess som defineres gjennom abstraksjonslagene: konsept, logisk og implementasjon. Arkitekturen består av et hierarki av dokumenter. Høyt oppe er fokus på langsiktige konsepter. Lengre ned i hierarkiet blir dokumentene mer dynamiske og tekniske.

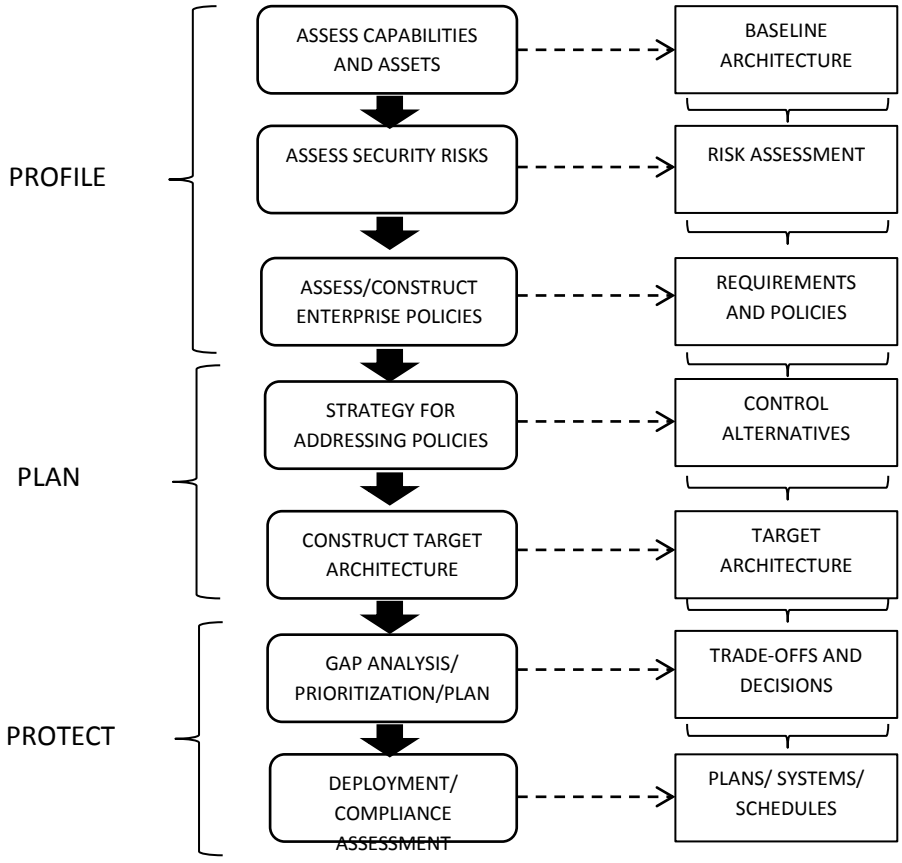



*Figur 5.4 Gartner sitt forslag til å integrere sikkerhet i virksomhetsarkitekturen [34] [35].*

## 5.6 RISE

RISE (Roadmap for Information Security across the Enterprise) [36] er en metodikk for å introdusere risikodrevet sikkerhet i virksomheten. Den integrerer trusselbasert risikostyring på virksomhetsnivå og definerer en iterativ livssyklus for trusselvurdering og respons som er integrert i virksomhetens planleggings- og investeringsprosess. RISE beskriver bare en metode og er ikke et selvstendig arkitekturrammeverk [37].

Risikokonseptene er gitt i Figur 5.5. I motsetning til arkitekturer med en top-down tilnærming, ser vi at behovsanalysen her forankres i en risikovurdering av eksisterende kapabiliteter, og ikke i langsiktige og strategiske virksomhetsbehov. Livssyklusen er også mer detaljert siden den beskrives i et risikoperspektiv. Andre rammeverk gir inntrykk av at risikovurdering bare gjennomføres før planleggingsfasen, mens her er den tett integrert også med planlegging og kontrollfasen.




*Figur 5.5 Overordnet metodikk og livssyklus i RISE.*

## 5.7 Diskusjon

Virksomheter er avhengig av at informasjonssystemene fungerer som forventet og garanterer informasjonens tilgjengelighet, integritet og konfidensialitet. Systemteknisk sikkerhet utvikles ofte for å løse spesifikke problemer som følge av angrep eller feil. Dette resulterer ofte i sammensatte løsninger som skalerer og samvirker dårlig og som raskt blir utdatert. Derfor et det behov for en mer helhetlig tilnærming til sikkerhet som tar i betraktning sammenhengen mellom komplekse, sammenkoblet systemer og forretningsbehov. Dessverre er det for tidlig å avgjøre om anvendelsen av virksomhetsarkitekturtilnærmingen til sikkerhet har vært vellykket. Imidlertid er det mange gjennomgangskonsepter i de eksisterende rammeverkene som kan være et godt utgangspunkt for en foreløpig vurdering og videre arbeid. Prinsippene for hensiktsmessig arkitekturarbeid i Forsvaret som ble utarbeidet i en tidligere FFI rapport [24], kan også brukes til vurdering av sikkerhetsarkitektur.

Et viktig poeng er at sikkerhet ikke kan eksistere i isolasjon fra det som skal sikres, og det samme gjelder for en sikkerhetsarkitektur: "… an Enterprise Security Architecture does not exist in isolation. As part of the enterprise, it builds on enterprise information that is already available in the Enterprise Architecture, and it produces information that influences the Enterprise Architecture" [33]. SABSA, for eksempel, markedsføres som en komplett, virksomhetsdrevet sikkerhetsarkitektur, men krever i praksis at man bygger en underliggende virksomhetsarkitektur for å kunne definere sikkerhet. Så, hvis Forsvaret skulle ha adoptert et sikkerhetsarkitekturrammeverk, ville det uansett stått ovenfor en ganske tungvint integrasjonsprosess mellom det utvalgte rammeverket og de virksomhetsarkitekturrammeverkene som allerede er i bruk, nemlig TOGAF og NAF. Mens TOGAF ser ut til å ha startet en integrasjon mot SABSA, har ikke NAF noe dedikert grensesnitt mot et sikkerhetsperspektiv.

Det finnes heller ikke noe etablert og utbredt modelleringsspråk for sikkerhet som kunne ha gjort integrasjonen enklere [38]. Tidligere arbeid har vist at NAF kan brukes til risikovurdering av eksisterende systemer og prosesser [14], men dette brukte en egenutviklet og forenklet metode som ikke var basert på noe sikkerhetsarkitekturrammeverk. Dette peker i retning av at egenutviklete metoder kan etter de prinsippene definert i [24] være mer hensiktsmessig enn store og etablerte rammeverk som likevel krever tilpasning. Faren er at slike metoder blir for spesialiserte og brukes i isolasjon. En forankring i en virksomhetsarkitektur virker derfor nødvendig for et konsistent og helhetlig sikkerhetsarbeid. Hvordan dette skal gjøres er det ikke enighet om. Uten en klar og etablert virksomhetsarkitektur i Forsvaret er det vanskelig å vurdere hvilken tilnærming som kunne passet best.

Alle rammeverkene sier at sikkerhet skal være risikodrevet, men vi så hvor vanskelig risikovurderingsprosessen kan være i Seksjon 3. Vi har ikke fått inntrykk at rammeverkene gir noen bedre metode for å vurdere og håndtere risiko enn de som allerede brukes. Bottom-up tilnærmingen til RISE-metodikken virker for eksempel ganske standard. Den baserer seg på en vurdering av eksisterende systemer som en input til en gap-analyse som igjen brukes til å skissere en målarkitektur. Denne arkitekturen kan ikke være langt fram i tid, og den skal ha

konkrete mål som gjerne baserer seg på anskaffelse eller integrasjon av eksisterende løsninger. Forsvaret, som skal operere i mange forskjellige kontekster og må tenke langsiktig, kan bruke denne metoden for kortsiktige mål, men trenger også en tilnærming for å skissere sikkerhetsarbeid lenger fram i tid. Top-down tilnærmingen foreslått i andre rammeverk som SABSA og Gartner virker mer hensiktsmessig for dette, men vår erfaring er at det er vanskelig å komme ned til et nivå som er konkret nok til å kunne brukes i praksis. Slike rammeverk definerer altså ikke metoder som dekker Forsvarets behov slik som de er. Et naturlig alternativ er å bruke både en top-down og en bottom-up prosess som O-ESA skisserer i Figur 5.2, men det finnes ingen klare eksempler på hvordan dette kan gjøres på en effektiv måte.

Et aspekt som er felles til alle rammeverkene, og som vi mener kan hjelpe Forsvaret, er arkitekturens laginndeling. Som påpekt i Seksjon 0, representerer arkitekturlagene forskjellige abstraksjonsnivå som beskriver et hierarki av konsepter som er mindre detaljerte og langsiktige på toppen, og mer konkrete og dynamiske på bunnen. At man sier «mindre detaljerte» er egentlig misvisende, siden en langsiktig strategi gjerne kan ha mange detaljer, men helst ikke tekniske. Med andre ord er overordnete konsepter mer teknologiuavhengige, mens på implementasjonsnivå er konseptene sterkt knyttet til eksisterende teknologier. Fra et sikkerhetsperspektiv kan dette bety at det finnes forskjellige typer sikkerhetskonsepter, med varierende grad av tekniske detaljer, som henger sammen i et hierarki og sørger for den sporbarheten man ønsker mellom forretningsnivå og teknologi. Dette kan hjelpe Forsvaret med å identifisere hvilke konsepter som mangler i dag.

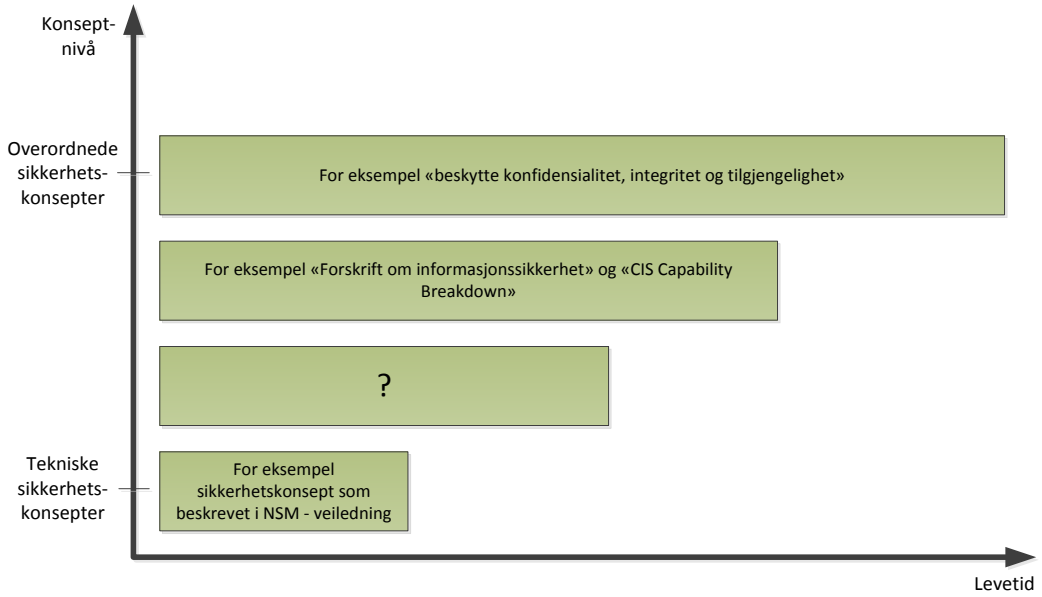
Sikkerhetsarkitekturtilnærmingen virker altså fornuftig i teorien, men det er fortsatt mange kritiske områder innenfor sikkerhet som ikke har en klar løsning. Det hjelper ikke å bruke resurser på å velge og å integrere et rammeverk hvis de underliggende utfordringer ikke blir løst. Mye av problemet består i at det mangler etablerte metoder for å samle, diskutere og bruke erfaringer og ekspertise som trengs for risikovurderinger og utvikling av konsistent og relevant sikkerhet.

# 6 Oppsummering og diskusjon

Forsvarets INI skal understøtte effektiv informasjonsdeling og legge til rette for bruk av ny teknologi som kan dekke fremtidige behov. Samtidig må INI bestå av kosteffektive løsninger og kunne fungere under avanserte cyberangrep. Risikoen INI står overfor til enhver tid varierer basert på mange ulike faktorer som politisk situasjon, ny teknologi som ønskes innført, nye måter å operere på, og nye allierte. En virksomhetsarkitektur kan synliggjøre sammenhengen mellom INI, andre deler av virksomheten og konteksten den opererer i, og danne grunnlaget for å vurdere risiko og nødvendig sikkerhetstiltak. Det trengs imidlertid en felles strukturert tilnærming for å bruke denne informasjonen i en kontinuerlig risikovurdering som skal resultere

i konsistente og hensiktsmessige sikkerhetstiltak innenfor virksomhetens rammebetingelser. Dette er målet for en sikkerhetsarkitektur.

Det har blitt foreslått ulike rammeverk for å realisere en sikkerhetsarkitektur. Erfaringer med bruk av disse rammeverkene er imidlertid ikke veldig positive. De er umodne sammenlignet med rammeverkene for virksomhetsarkitektur, og oppfattes ofte som for store og generiske til å kunne anvendes direkte. Likevel er det noe fra rammeverkene det vil være hensiktsmessig å benytte. For eksempel kan en lagdelt arkitektur danne grunnlaget for et hierarki av sikkerhetskonsepter. Her vil overordnede konsepter ha lang levetid og få tekniske detaljer, og være grunnlaget for å utforme mer tekniske og kortsiktige konsepter. På denne måten vil konkrete sikkerhetstiltak kunne spores til overordnede sikkerhetsbehov, og dermed bidra til konsistens av sikkerhetsløsninger på tvers av Forsvaret.




*Figur 6.1 Et hierarki av konsepter følger naturlig fra arkitekturinndeling, og kan brukes til å knytte sammen en top-down med en bottom-up tilnærming til sikkerhet.*

I Figur 6.1 forsøker vi denne tilnærmingen på eksisterende dokumenter. Det ser ut til å mangle konsepter som kan koble sammen og utfylle de styrende dokumentene og de tekniske sikkerhetsveiledningene. Dette er de konseptene som bør beskrive sikkerhetskapabilitetene på logisk nivå. Sikkerhetskonsept for NbF ligger egentlig på dette nivået, men det beskriver ikke hvordan prinsippene som skisseres kan gjennomføres i INI. Generelt er det krevende å si noe om sikkerhet på dette nivået fordi man ikke har konkrete systemer å forholde seg til.

Risikovurderinger står sentralt i alt sikkerhetsarbeid, noe som er utfordrende siden Forsvarets INI skal fungere i så ulike kontekster. Mange vurderinger er vanskelig å gjennomføre uten et konkret scenario, blant annet trussel- og sårbarhetsvurderinger. Det er spesielt vanskelig å vurdere risiko for tilsiktede uønskede hendelser som cyberangrep. Rammeverkene påpeker

gjerne at dette må gjøres, men sier ikke hvordan. Bruk av scenarioer med høy detaljeringsgrad er ressurskrevende, men kan være en mulig løsning. Det er imidlertid utfordrende både å lage representative scenarioer, og å sikre konsistens på tvers av dem.

Det er et klart behov for å etablere en helhetlig og konsistent måte å jobbe med informasjonssikkerhet i Forsvaret på. Det er kritisk at det finnes gode prosesser for å gjennomføre risikovurderinger basert på all relevant input som erfaringsrapporter, operasjonskonsepter, beskrivelser av INI, lovverk, scenariobaserte spill, samt ekspertdiskusjoner. Dette forutsetter at informasjonen man trenger lett kan samles inn, organiseres og gjøres tilgjengelig, og at det finnes felles retningslinjer for hvordan risikovurderinger legges til grunn for utvikling av sikkerhetstiltak. En sikkerhetsarkitektur kan legge til rette for dette og hjelpe med å gjøre sikkerhetsarbeidet mer strukturert og effektivt, men Forsvaret må selv avgjøre riktig omfang og utforming av arkitekturarbeidet for å dra nytte av det. Faren er ellers at man kan ende med å fokusere for mye på å velge og implementere en arkitekturmetode, og glemme de underliggende problemene den skal løse.

# Referanser


[1] Forsvarets departement, «Forsvarets ikt-strategi,» 2013.

[2] Forsvaret, «Framtidige anskaffelser til forsvarssektoren (FAF) 2017–2025,» 2017.

[3] The Open Group, «Open Group Standard - TOGAF® 9.1 Translation Glossary: English - Norwegian,» The Open Group, 2015.

[4] *Sikkerhetsloven, aksessert januar 2017.*

[5] Forsvarsdepartementet, *Forskrift om informasjonssikkerhet,* 2012.

[6] Forsvarets informasjonsinfrastruktur (INI), *Sikkerhetskonsept for et nettverksbasert forsvar,* 2011.

[7] Forsvarsdepartementet, *Informasjonssikkerhetsstrategi for forsvarsektoren,* 2017.

[8] E. Gjørven, B. H. Farsund, B. J. Hansen og P. Kristiansen, «Forsvarets informasjonsinfrastruktur – videreutvikling mot understøttelse av et nettverksbasert forsvar på modenhetsnivå 3,» FFI-rapport 2015/01221, Begrenset, FFI, Kjeller, NO, 2015.

[9] «Krav til risikovurderinger,» Norsk Standard 5814:2008, 2008.

[10] «Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse,» Norsk Standard 5832:2014, 2014.

[11] O. Busmundrud, M. Maal, J. H. Kiran og M. Endregard, «Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger,» FFI-rapport 2015/00923, FFI, Kjeller, NO, 2015.

[12] G. Hallingstad, S. Gay, J.-F. Suret og N. Virvilis-Kollitiris, «CIS Security Capability Breakdown - Comprehensive Approach Version 2.0,» NCI Agency, The Hauge, NL, 2015.

[13] «Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi,» Norsk Standard 5830:2012, 2012.

[14] K. O. Nystuen og B. H. Farsund, «Operative evne og behvet for sikkerhetsegenskaper i INI - Metode og resultater,» FFI rapport 2009/00646, Begrenset, FFI, Kjeller, NO, 2009.

[15] Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste, «TERRORSIKRING - En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede

handlinger,» NSM, POD, PST, Oslo, NO, 2015.

[16] J. Zachman, «A framework for information systems architecture,» *IBM Systems Journal,* vol. 26, nr. 3, 1987.

[17] The Open Group, «Open Group Standard - TOGAF® Version 9.1,» The Open Group, 2011.

[18] NATO Consultation, Command and Control Board, «NATO Architecture Framework v4.0 Documentation (Draft),» 2016. [Internett]. Available: http://nafdocs.org/. [Funnet mars 2017].

[19] H. D. Jørgensen, T. Liland og S. Skogvold, «Aligning TOGAF and NAF - Experiences from the Norwegian Armed Forces,» i *The Practice of Enterprise Modeling: 4th IFIP WG 8.1 Working Conference, PoEM 2011*, Oslo, NO, 2011.

[20] F. Ahlemann, E. Stettiner, M. Messerschmidt og C. Legner, Strategic Enterprise Architecture Management - Challenges, Best Practices, and Future Developments, Springer-Verlag Berlin Heidelberg, 2012.

[21] D. L. Goodhue, L. J. Kirsch, J. A. Quillard og M. D. Wybo, «Strategic Data Planning: Lessons from the Field,» *MIS Quarterly,* vol. 16, nr. 1, pp. 11-34, 1992.

[22] S. Kotusev, «The critical scrutiny of TOGAF,» April 2016. [Internett]. Available: http://www.bcs.org/content/conWebDoc/55892. [Funnet Mars 2017].

[23] T. Ylimaki og V. Halttunen, «Method engineering in practice: A case of applying the Zachman framework in the context of small enterprise architecture oriented projects,» *Information Knowledge Systems Management,* vol. 5, pp. 189-209, 2005.

[24] M. Hansbø, H. D. Jørgensen og R. Rasmussen, «Arkitekturarbeid i Forsvaret med forenklet bruk av NATO Architecture Framework (NAF),» FFI, 2013.

[25] T. H. Bloebaum, J. E. Hannay, O.-E. Hedenstad, S. Haavik og F. Lillevold, «Architecture for the Norwegian defence information infrastructure (INI) – remarks on the C3 Classification Taxonomy,» FFI, 2013.

[26] G. Kreizman og B. Robertson, «Integrating Security Into the Enterprise Architecture Framework,» Gartner, 2006.

[27] S. Jalaliniya og F. Fakhredin, «Enterprise Architecture & Security Architecture Development,» Department of Informatics, Lund University, Lund, SE, 2011.

[28] R. v. Os, «Comparing Security Architectures - Defining and Testing a Model for Evaluating and categorising security architecture frameworks,» Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, Luleå, SE, 2014.

[29] J. Sherwood, A. Clark og D. Lynas, Enterprise Security Architecture - A business Driven Approach, CRC Press, 2005.

[30] The Open Group, «Open Enterprise Security Architecture (O-ESA) - A framework and template for policy-driven security,» Van Haren Publishing, 2011.

[31] NIST, «NIST Special Publication 800-53 Rev. 2 - Infromation Security,» National Institute of Standards and Technology , 2007.

[32] The Open Group TOGAF-SABSA Integration Working Group, «TOGAF® and SABSA® Integration - How SABSA and TOGAF complement each other to create better architectures,» The Open Group, 2011.

[33] Security Forum and The SABSA Institute, «Integrating Risk and Security within a TOGAF® Enterprise Architecture,» The Open Group, 2016.

[34] G. Kreizman, «An Introduction to Information Security,» i *Gartner The Future of IT Conference*, Mexico City, MX, 2011.

[35] T. Scholtz, «Structure and Content of an Enterprise Information,» Gartner, 2006.

[36] J. A. Anderson og V. Rachamadugu, «Managing Security and Privacy Integration across Enterprise Business Process and Infrastructure,» i *SCC'08 - IEEE International Conference on Services Computing*, Honolulu, HI, USA, 2008.

[37] NIST; OMB; CIO Council, «Federal Enterprise Architecture Security and Privacy Profile v3.0 - Final,» 2010.

[38] S. v. d. Bosch, «Designing Secure Enterprise Architectures - A comprehensive approach: framework, method, and modelling language,» University of Twente, Twente, NL, 2014.

[39] Forsvardepartement, «Kampkraft og bærekraft - Langtidsplan for forsvarssektoren,» 2016.

## About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

### FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

### FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

### FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

## Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

### FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

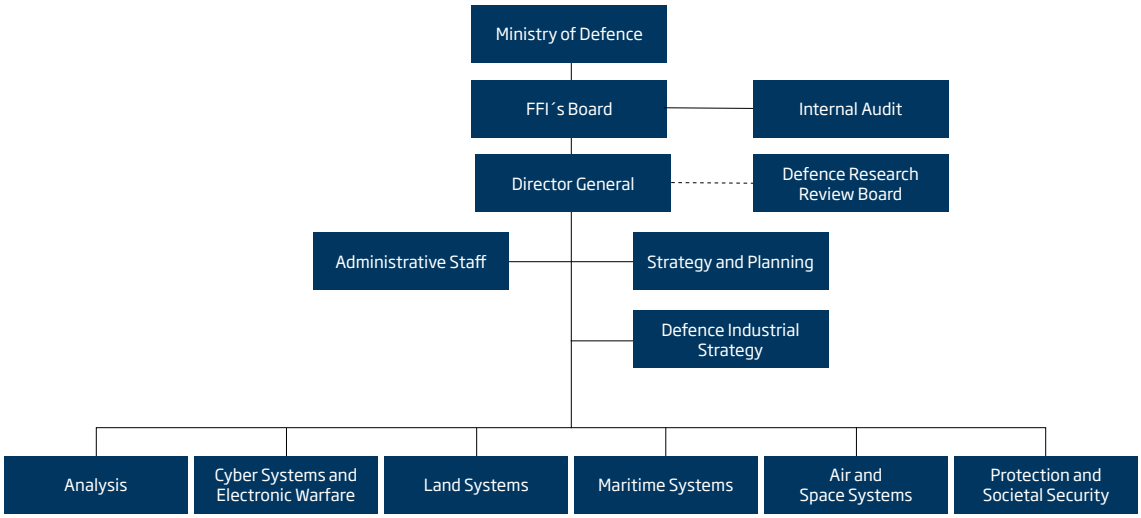
### FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

### FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

## FFI's organisation



**Forsvarets forskningsinstitutt**
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

**Norwegian Defence Research Establishment (FFI)**
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment