

ATEA

informasjonssikkerhetstjenester

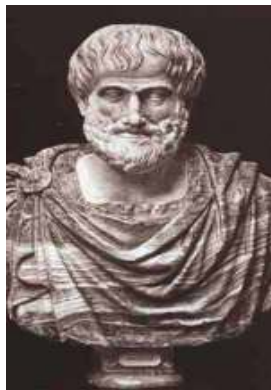
Versjon: 1.0 Dato: Mai 2009 Utarbeidet av: Sjefkonsulent Bjørn A. Tveøy – BBA, CISSP, CISM mm

ROS-vurderinger

Revisjon av informasjonssikkerhet

Sikkerhetspolicy og regelverk

Sikkerhetskultur



”Det er sannsynlig at noe usannsynlig vil skje!”
Aristoteles (384-322 f.Kr.)

1. Oppdrag, kunder og erfaring

Ateas konsulenter har lang og omfattende erfaring (fra 10 til 30+ år) fra leveranse av informasjonssikkerhetstjenester til våre kunder i offentlig og privat virksomhet. Tjenestene omfatter områdene

- ROS-vurderinger
- Revisjon av informasjonssikkerhet
- Sikkerhetspolicy og regelverk
- Sikkerhetskultur

Tjenestene er kort beskrevet nedenfor og utføres basert på nasjonale og internasjonale standarder og på beste praksis av våre sertifiserte konsulenter.

Blant kundene av tjenestene kan nevnes Bufetat (det landsdekkende, statlige barne- og familievernet), Arcus, Helse Midt-Norge, Finansdepartementet, Color Line, Gilde, Post- og teletilsynet, Kripos, Departementenes Service Senter (DSS, tidligere Statens forvaltningstjeneste), et 50-talls kommuner og kommunale foretak (noen ferske eksempler er Oslo kommune, Kollektivtransporten i Oslo, Melhus kommune), Norges Bank, Helse Øst, Kreftforeningen, Arbeidstilsynet, Konkurransetilsynet, Forsvaret, Post- og teletilsynet, Storebrand Kapitalforvaltning samt Nærings- og handelsdepartementet. Oppdragene har belyst problemstillinger som:

1. "Hvor lenge kan produksjon og distribusjon være uten IKT-støtte?"
2. "Kan sykehusene gå over til papirløs journal?"
3. "Krever arbeidsoppgavene i Tilsynet IKT-støtte 24/7?"
4. "Hvordan sikre informasjonsbehandling og formidling på et akuttssenter, et ungdomssenter, et familiesenter i barnevernet?"
5. "Kan elektroniske beslag være tilgjengelig i det interne nettverket som har Internettforbindelse?"
6. "Tilfredsstill den fysiske sikringen av IKT akseptabelt risikonivå?"
7. "Hvor robust er IKT-støtten til kollektivtransporten?"
8. "Hvordan sikre informasjonsbehandlingen i et nettforum for kreftframmede og deres pårørende?"
9. "Hvordan sikre varsel og varslere i og utenfor kommunen av kritikkverdige forhold i en elektronisk løsning?"
10. "Hvordan etablere tilstrekkelig informasjonssikkerhet i kommunens informasjonsbehandling og – formidling slik at behovet og kravet fra borgerne, de ansatte og lov- og regelverket oppfylles?"
11. "Hvordan overholder departementene sikkerhetsbestemmelsene i sin ordinære saks- og informasjonsbehandling og -formidling?"
12. "Er bruk av det nye fødselssystemet i tråd med informasjonssikkerhetsbestemmelsene?"
13. "Kan epikrise formidles elektronisk til pasient slik at sikkerhetsbestemmelsene oppfylles?"
14. "Hvor robust er IKT-støtten til våre aksjemeglere og finansforvaltere?"

2. Sertifiseringer

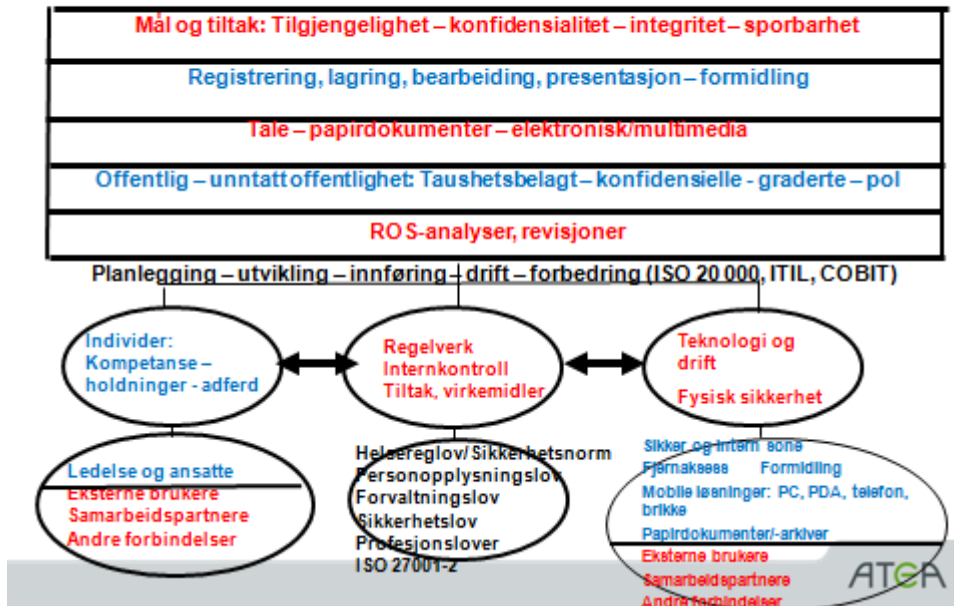
Ateas konsulenter er ledende i Norden når det gjelder produkttekniske sertifiseringer. Våre konsulenter er også sertifisert på områdene

- CISA
- CISM
- CISSP
- COBIT Foundation
- ISO 20 000
- ISO 27001/2
- ITIL Foundation
- ITIL Manager

3. Tjenester

Tjenestene tar utgangspunkt i følgende modell hvor informasjonsbehandlingen i virksomhetsprosessene og deres krav til sikkerhet, er det grunnleggende.

Akseptabel informasjonssikkerhet i virksomhetsprosessene - kvalitet



Atea legger til grunn at arbeid med informasjonssikkerhet er en kontinuerlig forbedringsprosess (P-D-C-A).

3.1 ROS-VURDERINGER

Ateas konsulenter har bred erfaring med bruk av de ROS-metodikkene og ROS-veiledninger som anvendes pt i Norge fra

1. NSM
2. Datatilsynet
3. Helsedirektoratet
4. Kredittilsynet
5. SSØ

Disse er alle basert på NS 5814 og er tatt opp i den nye ISO 27005. I tillegg har vi erfaringene og publikasjonene fra BAS5-prosjektet. Gjennomføring av ROS kan illustreres med følgende trinn, ref Kredittilsynets veiledning

Ramme inn: Kartlegge IKT-løsningen: Befaring, dokumentasjon, intervjuer, hendelser, driftsopplegg, endringsregime, fysisk sikring, sårbarheter, barrierer/tiltak, underleverandører etc, krav til informasjonssikkerhet og akseptabel risiko

Idégenerering: Hva kan gå galt? Hvilke uønskede hendelser (interne/eksterne, tilfeldige/tilsiktete) kan utnytte sårbarhetene? Årsaker? Hvilken skade/konsekvenser kan dette medføre?

Skalere: Rangere sannsynlighet eller mulighet for uønskede hendelser og for skader/konsekvenser.

Innkapsle: Utarbeide forslag til tiltak for å redusere de uønskede hendelsenes sannsynlighet/mulighet og redusere skade/konsekvens til akseptabelt risikonivå. Tiltak kan også omfatte å fjerne eller overføre risiko. Gjenværende risiko (restrisiko) synliggjøres.

Kontrollere: Innføre og kontrollere at tiltakene virker som forutsatt.

Oppsummere og informere alle interesseparter om resultatene av risikovurderinger og tiltak.

SSØs metode er opprinnelig utviklet for å vurdere operasjonell risiko, men er også tatt i bruk for å ROS-vurdere informasjonssikkerhet. Dermed holder virksomheten seg til en metode som også egner seg godt for ROS-vurderinger i grupper. Framgangsmåten er punktvis som følger:

1. Mål for informasjonssikkerhet for det aktuelle området formuleres.
2. Risikotabeller utarbeides – sannsynlighet/mulighet/letthet og konsekvens, gradere (fargelegge) risikomatrise.
3. Formulere suksesskriterier for å nå målene, gruppen prioriterer et antall av disse.

4. Formulere risikofaktorer (uønskede hendelser) som kan hindre den enkelte suksessfaktor, gruppen prioriterer et antall risikofaktorer.
5. Gruppen vurderer sannsynlighet/letthet/mulighet og konsekvens for den enkelte prioriterte risikofaktor.
6. Risikomatrix produseres, risikofaktorer over akseptabelt risikonivå bearbeides videre.
7. For hver av disse risikofaktorene, formuleres et antall tiltak som kan redusere risiko.
8. Mottiltakene prioriteres av gruppen.
9. Hvert prioritert tiltak vurderes av gruppen med hensyn på verdi for virksomheten og realiserbarhet samt risikoreduksjon.
10. Resultatene vurderes og oppsummeres i en ROS-rapport som inneholder prioriterte forslag til tiltak.

3.2 REVISJON AV INFORMASJONSSIKKERHET

Ateas konsulenter har en enestående bredde i kompetanse og erfaring på revisjon av informasjonssikkerhet: Fra brannmur og servere, nettverk og datakommunikasjon via datarom og fysisk sikring til applikasjoner, drift, katastrofeplaner, regelverk og sikkerhetskultur. Vi baserer oss på metodikk fra ISACA, ISO 27001/2, ISO 20000, ITIL, Cobit, Kredittilsynet og har delt opptjenesteområdene i tråd med ISACA:

- Governance
- Applikasjoner og infrastruktur
- Fysisk/datarom/tilførsler/overvåking og varsling
- Leveransetjenester
- Informasjonsaktiva
- Kontinuitet- og katastrofe

3.3 SIKKERHETSPOLICY OG REGELVERK

Atea har utviklet maler for sikkerhetspolicy og regelverk som er basert på ISO 27001/2, Datatilsynet og HelseDirektoratets sikkerhetsnorm samt ISACA. Vi deler innholdet i følgende grupper:

- Styrende, overordnede
- Organisering, oppgaver og ansvar
- Policy og standarder
- Veiledninger
- Rutiner og prosedyrer
- Sjekklistor
- Lederansvar
- Metaregler, publisering

3.4 SIKKERHETSKULTUR

Atea er av den oppfatning at tilstrekkelig god sikkerhetskultur, dvs holdninger, kompetanse og adferd er helt avgjørende for å nå de sikkerhetsmål en har satt seg.

Vi bruker SjekkIT fra NTNU som hjelpemiddel i kartlegging av sikkerhetskulturen og som grunnlag for gapanalyse og for å utarbeide forslag til tiltak. Vår erfaring har gitt oss et bredt spekter av virkemidler som kan tas i bruk

1. Kampanjer
2. IS-dag
3. Video
4. Intranett
5. Misjonering
6. eLæring
7. Plakater
8. Skjermbeskyttere
9. Aktiv revisjon
10. Konkurranser

