

# Bacheloroppgave 38A

Grunnlaget for styringssystem for informasjonssikkerhet  
i norske IKT-bedrifter



Hege Myklebust og Knut Formo Buene

Veileder: Bjørn Klefstad

IT-støttet bedriftsutvikling, NTNU

2016

# Formålet med oppgaven

*Formålet med oppgaven er å kartlegge bruken av informasjonssikkerhetsstandardene ISO 27001 og ISO 27002 i norske IKT-bedrifter. Vi har innhentet informasjon gjennom kvantitative og kvalitative undersøkelser, samt fra relevant faglitteratur, rapporter og statistikk. Dette danner grunnlaget for oppgavens analyse, diskusjon og konklusjon.*

# Problemstilling

Problemstillingen er formulert som en hypotese:

Med stadig endring i bedrifiers trusselbilde, stilles det større krav til styring av sikkerhetsarbeidet. ISO-standardene 27001 og 27002 danner grunnlaget for arbeidet med informasjonssikkerhet i norske IKT-bedrifter.

- Det er stadig mer vanlig at norske IKT-bedrifter sertifiserer seg etter ISO 27001.
- Kunder krever oftere at IKT-bedrifter er sertifisert etter ISO 27001.
- Ikke-sertifiserte bedrifter benytter ISO 27001 som grunnlag for sikkerhetsarbeidet.
- IKT-bedrifter og sertifiseringsorganer i Norge har en felles forståelse av nytteverdien av å bli sertifisert.
- Sertifiseringsprosessen er for omfattende for små, norske IKT-bedrifter.

Oppgavens hypoteser vil enten bekreftes, avkreftes eller bli ansett som ikke mulig å trekke konklusjoner av.

# Teorigrunnlag

Oppgaven bygger på teori om:

- Informasjonssikkerhet
- ISO 27001 og ISO 27002
- Styringssystem for informasjonssikkerhet (ISMS)
- Kontinuerlig forbedring
- Kvalitetssystem
- Sertifiseringsorganer
- Andre standarder for styring av informasjonssikkerhet

# Kvantitativ forskningsmetode

Den kvantitative forskningsmetoden; spørreundersøkelse, inneholder kvalitative innslag. Dette er gjort ved å stille relativt få, men detaljerte spørsmål som legger opp til utdypende svar fra respondentene.

Spørreundersøkelser ble sendt til :

- 94 norske IKT-bedrifter og bransjeorganisasjoner
  - Svarprosent: 23,4 %
- 8 sikkerhetsekspertter
  - Svarprosent: 62 %

Total svarprosent for spørreundersøkelsene: 26,5 %

# Kvalitativ forskningsmetode

Fem intervjuer ble gjennomført:

- Ett personlig intervju, med:
  - En ansatt i IKT-bedrift
- Tre intervjuer over Skype, med:
  - To ansatte i ulike IKT-bedrifter
  - En sikkerhetseksper
- Ett telefonintervju, med:
  - En ansatt i et sertifiseringsorgan

# Statistikk og rapporter

I tillegg omfatter datagrunnlaget statistikk og rapporter fra eksterne aktører.

- Statistikk fra Statistisk sentralbyrå (SSB)
  - Tittel: “Bruk av IKT i staten”
  - Informasjon fra 2012-2015
- Rapporter:
  - Mørketallsundersøkelsen (NSR)
  - Risiko- og sårbarhetsanalyse (NorCERT)
  - Risiko 2015 (NSM)

# Funn

Våre funn vil danne grunnlaget for analyse, diskusjon og konklusjon.





2016