NORGES INTERNE REVISORERS FORENING

Revisjon av cybersecurity

Ledernettverket i NIRF

15. juni 2017 – Siv I. Aasen, partner IT-risikotjenester, BDO

Agenda

NORGES INTERNE REVISORERS FORENING

- Ulike rammeverk og kilder
- Revisjon av cybersecurity
- GTAG – Assessing Cybersecurity Risk
- Erfaringer fra revisjoner
- Oppsummerende «10 spørsmål å stille»

Trusselbildet

NORGES INTERNE REVISORERS FORENING

Petter Stordalens Choice Hotels er blant virksomhetene som er rammet av det internasjonale dataangrepet. Foto: Terje Pedersen/NTB Scanpix

Nyheter Teknologi

Choice Hotels ble rammet av WannaCry

Tre norske virksomheter er så langt rammet av det verdensomspennende dataviruset Wanna Decryptor. Choice Hotels ol rammede.

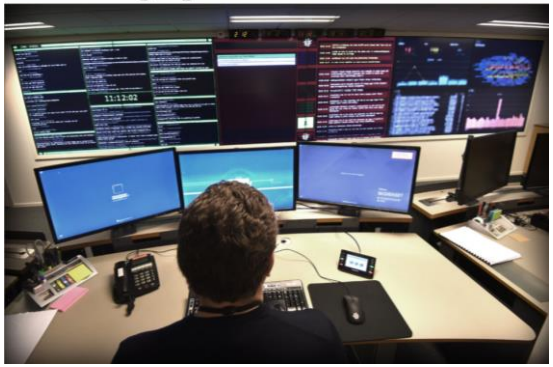
PST-sjef Benedicte Bjørnland la tidligere denne uken frem PSTs siste trusselvurdering. Foto: Roald, Berit,/NTB scanpix

Nyheter Utenriks

PST utsatt for russisk hackerangrep

Rammet av målrettet hackerangrep fra aktør knyttet til russiske myndigheter.

VG avslører: Politikere og toppbyråkrater rammet av hackerangrep



lettvalutaen Bitcoin stupte i verdi etter hackerangrep og tyveri. Illustrasjonsfoto: Jim Urquhart/Reuters/NTB canpix

Finans Bitcoin

Bitcoin-verdien stupte etter hackerangrep og tyveri

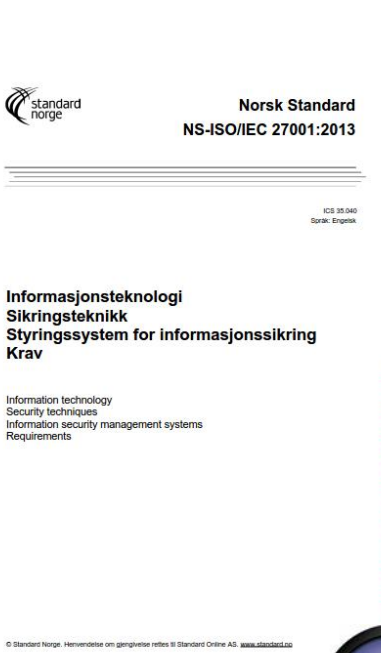
lettvalutaen falt med over 20 prosent etter at verdens tredje største bitcoin-plattform ble hacket.

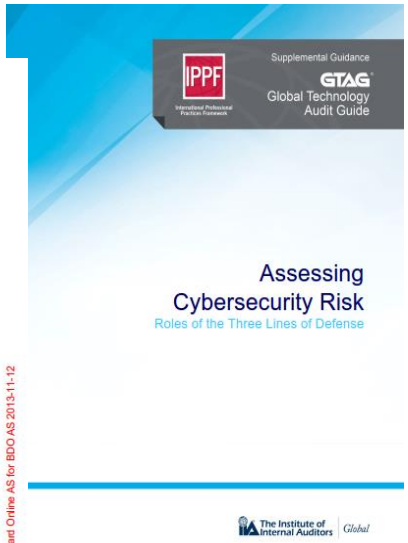
Ulike rammeverk og kilder

- GTAG – Assessing Cybersecurity Risk
  - Utstedt september 2016 fra IIA
- ISO 2700X- familien, spesielt:
  - ISO 27032:2012 – Information Technology – Guidelines for cybersecurity recommendations
  - ISO 27001:2013 – Styringssystem for informasjonssikkerhet
- NIST – National Institute of Standards & Technology
  - Framework for cybersecurity
  - Identify, protect, detect, respond & recover
- OWASP top 10 – Open Web Application Security Project
  - Kontinuerlig oppdatert

Ulike rammeverk og kilder

- GTAG – Assessing Cybersecurity Risk
  - Utstedt september 2016 fra IIA
- ISO 270XX- familien, spesielt:
  - ISO 27032:2012 – Information Technology – Guidelines for cybersecurity
  - ISO 27001:2013 – Styringssystem for informasjonssikkerhet
- NIST – National Institute of Standards & Technology
  - Framework for cybersecurity
  - Identify, protect, detect, respond & recover
- OWASP top 10 – Open Web Application Security Project
  - Kontinuerlig oppdatert



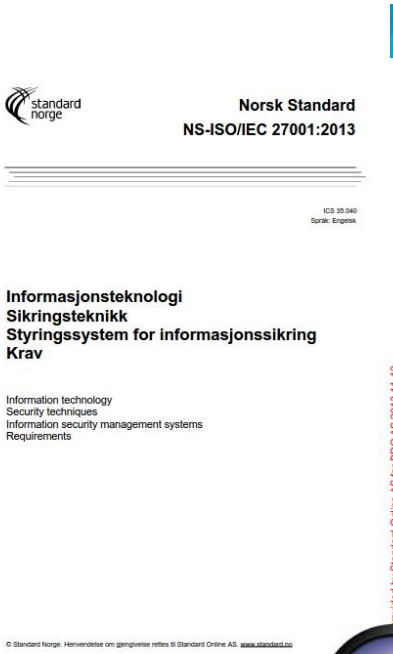


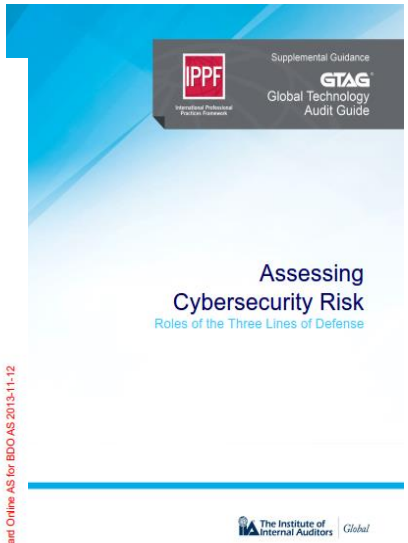
Ulike rammeverk og kilder

- GTAG – Assessing Cybersecurity Risk
  - Utstedt september 2016 fra IIA
- ISO 2700X- familien, spesielt:
  - ISO 27032:2012 – Information Technology – Guidelines for cybersecurity recommendations
  - ISO 27001:2013 – Styringssystem for informasjonssikkerhet
- NIST – National Institute of Standards & Technology
  - Framework for cybersecurity
  - Identify, protect, detect, respond & recover
- OWASP top 10 – Open Web Application Security Project
  - Kontinuerlig oppdatert

Ulike rammeverk og kilder

- GTAG – Assessing Cybersecurity Risk
  - Utstedt september 2016 fra IIA
- ISO 2700X- familien, spesielt:
  - ISO 27032:2012 – Information Technology – Guidelines for cybersecurity recommendations
  - ISO 27001:2013 – Styringssystem for informasjonssikkerhet
- NIST – National Institute of Standards & Technology
  - Framework for cybersecurity
  - Identify, protect, detect, respond & recover
- OWASP top 10 – Open Web Application Security Project
  - Kontinuerlig oppdatert





OWASP
Open Web Application Security Project

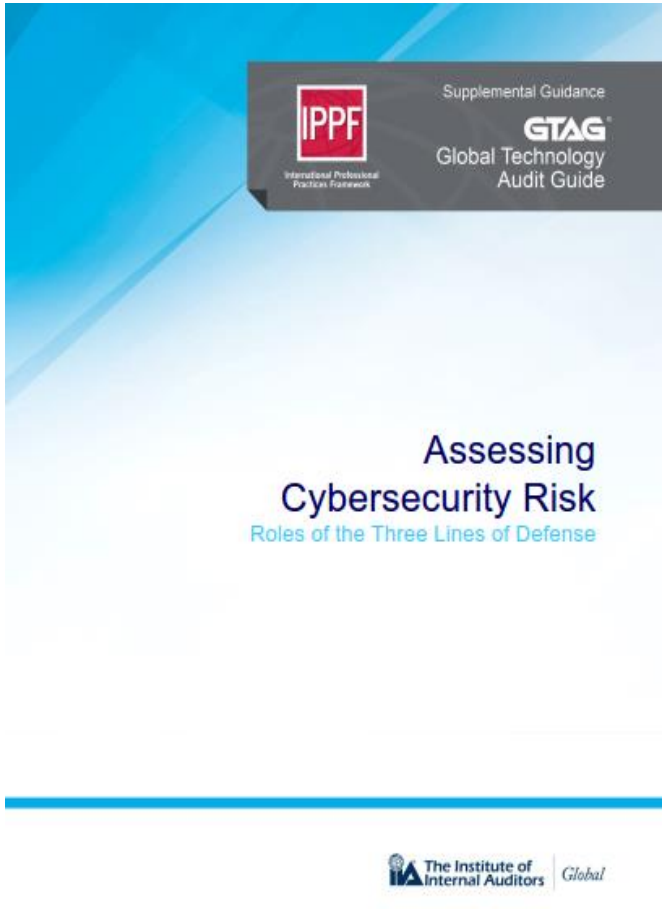
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NSMs 4 råd

- Utsagn: *«9 av 10 dataangrep kunne vært unngått hvis fire enkle råd ble fulgt»*
  - Oppgradere program- og maskinvare
  - Installere sikkerhetsoppgraderinger så fort som mulig
  - Ikke tildele sluttbrukere administratorrettigheter
  - Blokkere kjøring av ikke-autoriserte programmer

GTAG – Assessing Cybersecurity Risk

- God veiledning for å forstå:
  - Rollene til de 3 forsvarslinjene:
    - Management, Risk, Control & Compliance, Internal Audit
  - Kjente Cyber Threats
  - Klassifisering av informasjonsverdier
    - Kritiske tjenester, prosesser og IT-systemer
  - Fremgangsmåte for å identifisere og vurdere risiko og kontroller



Revisjon av cybersecurity

NORGES INTERNE REVISORERS FORENING

Planlegging

- Hvilke risikoer er aktuelle innen cybersecurity?
- Hvilke lovverk, rammeverk og standarder er relevante?
- Hvordan forankre og avgrense gjennomføringen?
- Hvilke områder bør kartlegges og vurderes i gjennomføringen?

Gjennomføring

- Avtale møter med relevante objekter
- Forberede intervjumaler og dokumentasjonslister
- Gjennomføre intervjuer, samle inn dokumentasjon, gjennomføre tester
- Evaluere innsamlede revisjonsbevis
- Verifisere resultater og konkludere

Rapportering

- Hvordan rapportere?
- Faktaverifikasjon
- Utkast og endelig rapportering

Forstå risiko

- Hva er kritiske scenarier?
  - Tap av kunder eller samarbeidspartnere
  - Tap av renomme
  - Økonomiske tap
- Teknologiske utfordringer
  - Stans eller opphør av tjenester
  - Manglende tilgang til informasjon
- Bransjen betyr noe ift. risiko
  - Handel/ kundeinformasjon
  - Intellektuell eiendom
  - Effektivitet og kvalitet i produksjon
  - Sensitiv person- eller forretningsinformasjon

Forstå risiko

- Hvilken informasjon/tjenester er det attraktivt for andre å:
  - Stjele
  - Korrumpere/ ødelegge
  - Forstyrre / stanse
- Hvem er de typiske trusselaktørene?
  - Konkurrenter, interne medarbeidere
  - Nasjonale stater, kriminelle nettverk, hacktivister

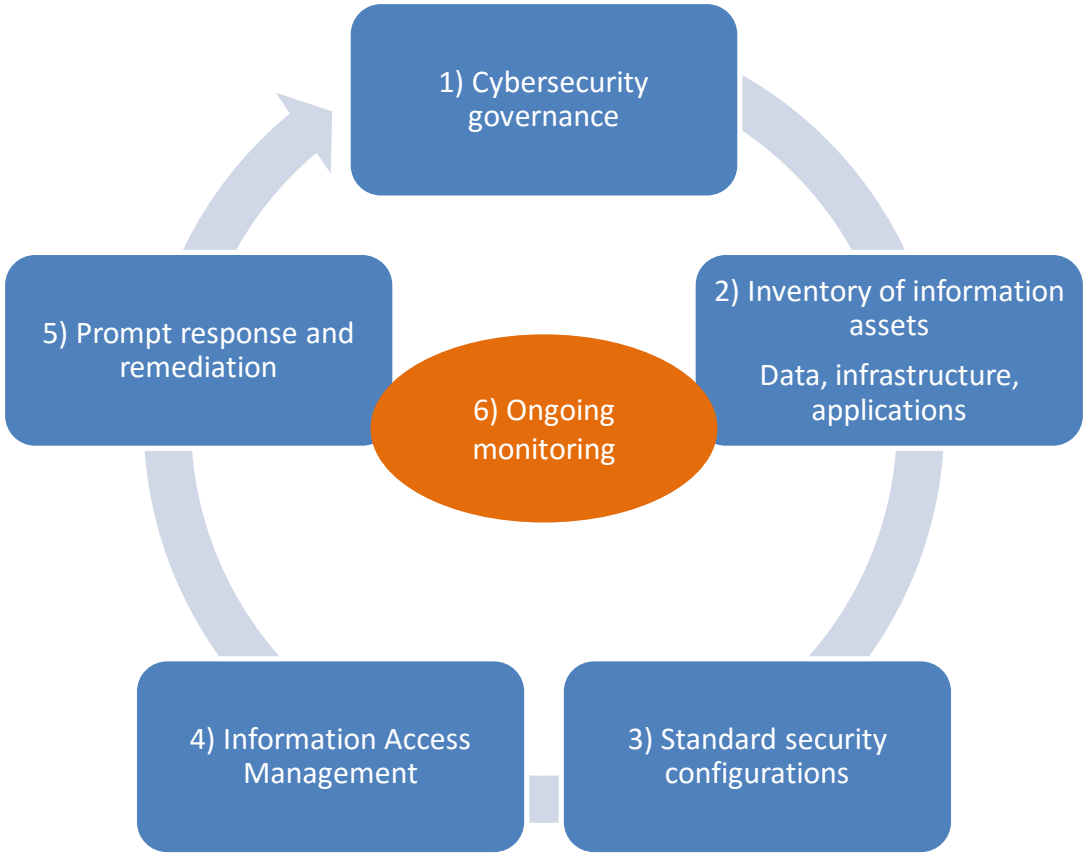
Forstå rammer og formål

- Lovverk, rammeverk etc.:
  - GTAG
  - ISO 27001
  - NIST, OWASP el annet
  - PCI DSS
  - GDPR/personvern
  - Sikkerhetsloven
- Hva er formålet og scopingen?
  - Bekrefte at cybersecurity er styrt og kontrollert på en forsvarlig måte
  - Få trygghet for at cyber-security er forsvarlig ivaretatt

GTAG – Cybersecurity

NORGES INTERNE REVISORERS FORENING

Rammeverk for risikovurdering av cybersecurity



1. Cybersecurity Governance

NORGES INTERNE REVISORERS FORENING

Hovedelementer i Cybersecurity Governance:

- Governance, risikohåndtering og internkontroll
- Organisasjon, roller og ansvar
- Strategisk planlegging og forankring i organisasjonen
  - Toppledelse, avdelingsledere, prosess- og systemeiere, risk & compliance, internrevisjon, 3djeparter, kunder & leverandører
- Prosess for oppdatering og vurdering av risikoer
- Fastsette risikoappetitt og toleranse
- Planlegge for kontinuitet og gjenoppretting
- Rask respons på sikkerhetsbrudd
- Holdning og kultur knyttet til cybersecurity
- Opplæring

1. Cybersecurity Governance

- Erfaringer fra revisjoner:
  - Manglende forankring hos toppledelsen
  - Risikoappetitt og risikovurderinger ikke dokumentert
  - Raske omstillinger i organisasjon og systemportefølje krever kontinuerlig fokus på cybersecurity
  - Økt kompleksitet og mange parter involvert krever høy kompetanse for alle, inkl. tredjepart
  - Massive matriser med områder som skal tas omfattes av et cybersecurity program – kommer aldri i mål…
- ***Internrevisjonen kan bidra med verdi:***
  - Bringe fokus til toppledelsen
  - Metodikk/tilnærming til definisjon av risikoappetitt og risikovurderinger
  - Bistå organisasjonen med innspill på prioritering av tiltak
  - Opprettholde kontinuerlig fokus ved regelmessige revisjoner

2. Informasjonsverdier

Oppdatert register over informasjonsverdier:

- Klassifisering iht. kritikalitet
- Definere og implementere sikkerhetstiltak for å sikre:
  - Kontinuerlig beskyttelse ift. hvor kritiske de er for virksomheten
  - Kontinuerlig overvåkning av at tiltakene fungerer
- Informasjonsverdier
  - Data: typer, klassifisering, miljøer
  - Infrastruktur: servere, nettverkskomponenter, lagring, utstyr hos sluttbruker (laptop, mobiltelefon etc.)
  - Applikasjoner
- Eksterne forhold: 3djepart, deling av data med eksterne

2. Informasjonsverdier

- Erfaringer fra revisjoner:
  - Informasjonsverdier er ikke dokumentert, eller er ufullstendig
  - Omfatter interne forhold, men «glemmer» tredjepart
  - Sikkerhetskrav er ikke tydeliggjort overfor tredjepart
- ***Internrevisjonen kan bidra med verdi:***
  - Metodikk for identifisering og klassifisering av informasjonsverdier
  - Vurdere fullstendighet ift. informasjonsverdier – er alle relevante områder med?
  - Vurdere om sikkerhetskrav er stilt til tredjepart

3. Sikkerhetsinnstillinger

NORGES INTERNE REVISORERS FORENING

Sikkerhetsinnstillinger:

- Sentraliserte og automatiserte systemer for å sikre baseline for oppsett av utstyr, servere, operativsystemer, databaser, applikasjoner, laptoper etc.
  - Preventive vs. oppdagende innstillinger
- Ekstra sikkerhet for webapplikasjoner (OWASP top 10)
- Løpende patching og sikkerhetsoppdateringer

3. Sikkerhetsinnstillinger

- Erfaringer fra revisjoner:
  - Manglende helhetlig oversikt over implementerte tiltak
  - Mye preventive tiltak, lite oppdagende
- ***Internrevisjonen kan bidra med verdi:***
  - Vurdere helhetlig tilnærming til implementering av tiltak
  - Innspill til oppdagende kontroller som kan bidra til kontinuerlig overvåkning, rask respons ved hendelser og løpende læring/forebygging basert på trender

4. Tilgangsstyring

Styre tilgang til informasjonsverdier:

- Preventive kontroller for tildeling av rettigheter
- Endring når noen bytter stilling internt og deaktivering når noen slutter
- Kontroll og overvåkning av privilegerte rettigheter
  - Applikasjoner og data
  - Infrastruktur: Nettverk, operativsystemer og databaser
  - Logging, holdninger/opplæring, bruk vs. behov
- Tilegne seg passord eller installere malware
- Tiltak for å begrense tilgang til sensitiv eller kritisk informasjon

4. Tilgangsstyring

- Erfaringer fra revisjoner:
  - Gode prosesser rundt tildeling av rettigheter, men ofte svakheter på avslutning når brukere forlater
  - Stort sett gode på rettigheter i applikasjonslaget
  - Manglende fokus på innskrenking av rettigheter i infrastruktur hos IT-personale / tredjepart – spesielt viktig ift. sensitiv informasjon
  - Lite oppfølging av logger/aktiviteter
- ***Internrevisjonen kan bidra med verdi:***
  - Innspill til forbedringer vedr avslutningsprosedyrer/ kompenserende kontroller
  - Innspill til oppdagende kontroller som kan bidra til overvåkning av brukeres aktiviteter

5. Respons og omstilling

Evne til rask respons og implementering av tiltak:

- Effektivitet og modenhet ift. respons og omstilling
- Kommunisere risikoer av betydning
- Bidra til omstilling og tiltak
- Registrere og følge opp hendelser frem til løsning
- Rapportering på trender og løsninger i organisasjonen

5. Respons og omstilling

- Erfaringer fra revisjoner:
  - Interaksjon mellom Security Incidents og Incident Management Process
  - Informasjon om sikkerhetshendelser hos tredjepart
  - Utfordrende med rotårsaksanalyser og læring av hendelser – ser ofte at de samme hendelsene inntrer på nytt
  - Kan bli en «brannslokker» i stedet for å implementere effektive tiltak
  - Katastrofeplan/beredskapsplan blir «sovepute» - blir ikke tilstrekkelig testet og oppdatert
- ***Internrevisjonen kan bidra med verdi:***
  - Innspill til forbedringer vedr kommunikasjon mellom Incident Management prosessen og security incidents – hvem oppdaterer hvem, hvordan bør denne prosessen dokumenteres, hvordan sikre læring
  - Etablere arena for å få informasjon om sikkerhetshendelser hos tredjepart som ikke eksplisitt rammet virksomheten
  - Innspill til prosesser for å sikre kontinuerlig læring, implmentering av tiltak og informasjon til virksomheten

6. Kontinuerlig overvåkning

NORGES INTERNE REVISORERS FORENING

Overvåkning:

- Monitorering av hver av de 5 komponentene ovenfor
- Hvordan håndteres risikoer og hvordan implementeres korrigerende tiltak?
- Har 2. linje etablert kontinuerlig overvåkning?
  - Overvåkning av privilegerte brukere av sensitiv eller kritisk informasjon/ funksjonalitet for å vurdere sårbarheter
  - Sårbarhetsvurderinger – periodisk skanning eller evaluering
  - Eksterne websider eller applikasjoner
  - 3djepartsleverandører
  - Penetrasjonstester eller etablering av CERT-funksjon
  - Ondsinnet kode/ programvare
  - Hendelsesrapportering

6. Kontinuerlig overvåkning

- Erfaringer fra revisjoner:
  - Sjeldent definert klare KPIer på cybersecurity
  - Lite formalisme rundt rapportering på cybersecurity til ledelsen bortsett fra ved sikkerhetshendelser
  - Ikke definert krav til 1. linje om hva som skal rapporteres
  - Ikke definert krav til 2. linje hva som skal overvåkes
- ***Internrevisjonen kan bidra med verdi:***
  - Innspill til definisjon av rapporteringskrav, KPIer og løpende aktiviteter innen området
  - Innspill til hva som bør overvåkes og hvordan dette kan gjøres

Test ved revisjon av cybersecurity

- Eksempler på områder:
  - Hvordan er kritiske informasjonsverdier er beskyttet?
    - Infrastruktur og applikasjoner
    - Lagring
    - Sikkerhetsinnstillinger, kryptering eller annet
    - CERT tilknyttet nettverk, tjenester eller data
    - Kontinuitet/beredskap
  - Forståelse av ansvar og roller
  - Opplæring, kontinuerlig læring og holdningsskapende arbeid
  - Oppfølging av risikovurdering og prioriterte tiltak
  - Resultat av monitorering og implementering av tiltak

Cybersecurity for internrevisjon

NORGES INTERNE REVISORERS FORENING

Oppsummerende spørsmål vedrørende Cybersecurity:

1) Er toppledelsen oppmerksom på risikoer knyttet til cybersecurity, og har det høy nok prioritet?
2) Har ledelsen gjennomført risikovurdering og identifisert verdier som er utsatt for angrep/ sikkerhetsbrudd ift cybersecurity?
3) Samarbeider 1. og 2. linje med andre i bransjen for å holde seg oppdatert om cybersecurity?
4) Er det utarbeidet policyer og prosedyrer for cybersecurity?
5) Er det implementert IT-prosesser og sikkerhetstiltak som vil bidra til å forebygge og oppdage angrep eller trusler?
6) Er det etablert regelmessig rapportering som viser status på cybersecurity programmer som er etablert?
7) Er det etablert nødprosedyrer for å håndtere angrep eller trusler?
8) Er internrevisjonen i stand til å vurdere kvaliteten på prosesser og kontroller som er etablert for cybersecurity?
9) Har virksomheten en oversikt over 3djepartleverandører og tjenester, og systemer og data som forvaltes hos disse?
10) Har internrevisjonen vurdert vanlige trusler ift. cyber og tatt hensyn til disse i planleggingen av internrevisjonsoppdrag?

NORGES INTERNE REVISORERS FORENING

- Spørsmål?