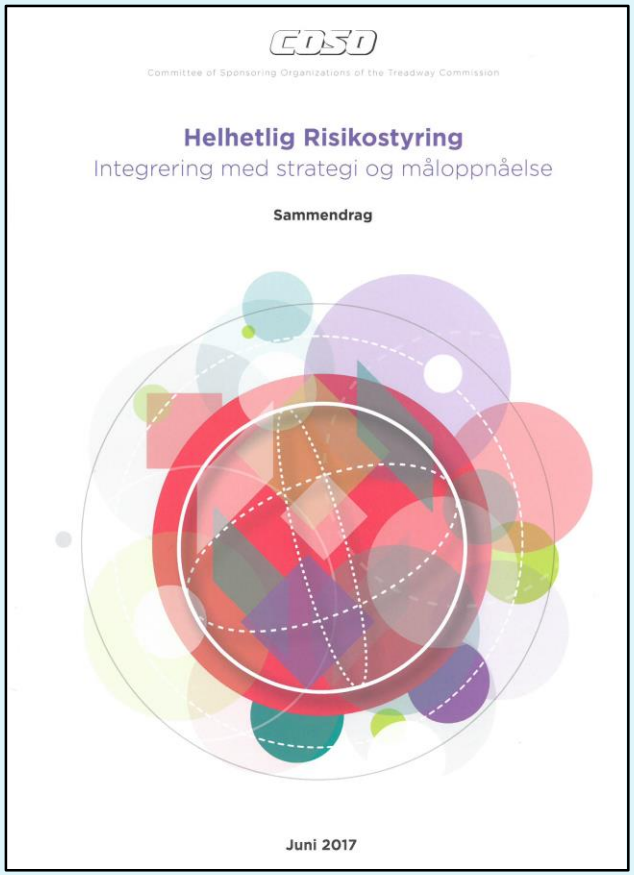
COSO ERM – Integrering med strategi og måloppnåelse



Tor Solbjørg
Helse Nord RHF

Trygve Sørlie
Trygve Sørlie Services EPF

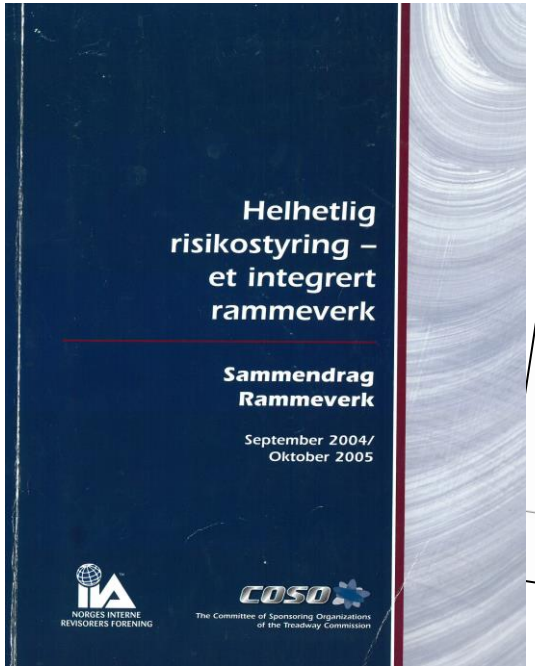
Frokostmøte IIA Norge
06.06.18

En presentasjon av «nye» COSO ERM i løpet av en tidlig morgentime:

1. Innledning: Historien bak rammeverket – og hva består det av?
2. Hva er endret i forhold til det gamle rammeverket?
3. Strategi og måloppnåelse
4. Rammeverkets komponenter og prinsipper
5. Hva finner vi i rammeverket, ut over det som inngår i Sammendraget?
6. Hva nå?

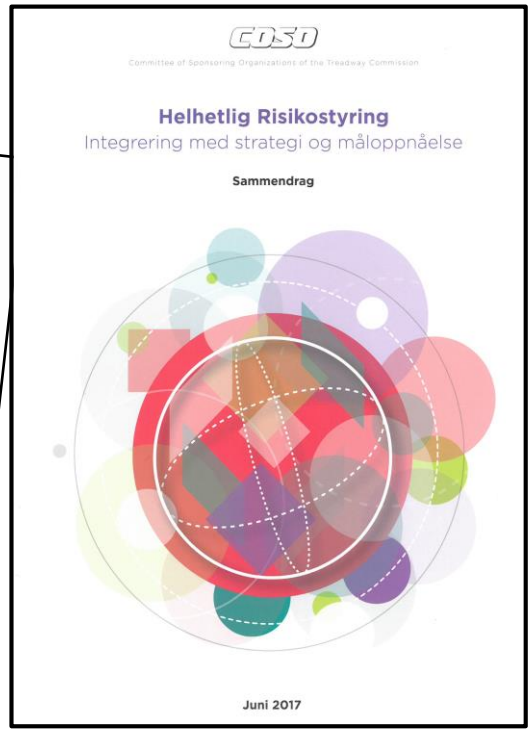
HELSE NORD

Historikk



Original: 2004
Norsk utgave: 2005

Dessuten:
Appendices og FAQ



Norsk utgave: 2018
Men bare Sammendraget

HELSE NORD

Historikk

Det er først og fremst dette vi skal se på i dag

Norsk utgave: 2018
Men bare Sammendraget

HELSE NORD

Norsk versjon av Executive Summary – Sammendrag – er utarbeidet av Fag- og metodekomiteen

Fra referat, møte januar 2018:

Det var også enighet om at en god og forståelig norsk språkdrakt er svært viktig, noe som vil innebære at vi må tillate oss visse omskrivinger og mindre avvik i forhold til originalen.

Spennende og gøy,
men mye arbeid!

HELSE NORD

Hvorfor ny versjon?

- Risikobildet har blitt mer komplekst, og nye risikoer har kommet til og omgivelser er i stadig endring
- Teknologisk utvikling og økt tilgang til data og analyser – viktig støtte for beslutningstaking
- Styre og ledelse har fått økt bevissthet rundt risiko/risikostyring, og ønsker nå bedre risikorapportering
- Ønske om å integrere helhetlig risikostyring i hele virksomheten samt identifisere og håndtere risiko i virksomheten samlet sett
- Øke omfanget av muligheter ved å vurdere både de positive og negative sider ved risiko for å forbedre positive resultater samtidig som negative resultater reduseres
- Forbedre virksomhetens motstandsdyktighet, fleksibilitet og omstillingsevne
- Ønske om å legge større vekt på verdien av risikostyring ved utvikling og implementering av strategi
- Ønske om sterkere fokus på sammenhengen mellom risikostyring og måloppnåelse samt redusere variasjonen i måloppnåelse
- Forbedre ressursutnyttelsen

HELSE NORD

Hva er endret?

Strengt tatt: Det meste!

Vi vil særlig peke på:

- Rammeverkets tittel
- Definisjonen av risikostyring
- Definisjonen av risiko
- Sentrale figurer/illustrasjoner
- Bruken av komponenter og prinsipper

Vi ser nærmere på disse endringene, en etter en:

HELSE NORD

Rammeverkets tittel

- Tidligere: Enterprise Risk Management – Integrated Framework

  (Helhetlig risikostyring – et integrert rammeverk)

- Nå: Enterprise Risk Management – Integrating with Strategy and Performance

  (Helhetlig risikostyring – Integrering med strategi og måloppnåelse)

Altså: Styrket, eller endret, fokus på integrering med strategi og måloppnåelse

Vi kunne ikke være konsekvent i oversettelsen av ordet performance. Det brukes mye om måloppnåelse, men flere steder benyttes det også om gjennomføring

HELSE NORD

Definisjonen av risikostyring

- Tidligere: En prosess, gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten, og håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetens måloppnåelse.
- Nå: The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value.

  Altså: Den tidligere, litt omstendelige definisjonen, med klare krav/føringer til prosessen, er erstattet med en noe enklere versjon. Nå fokuseres det på de elementer/egenskaper som må være på plass, og som må integreres med strategi og måloppnåelse, for at risikostyringen skal bidra til at verdier skapes og realiseres.

HELSE NORD

Definisjonen av risiko

- **Tidligere**: Det at en hendelse kan inntreffe og påvirke måloppnåelse negativt
- Nå: The possibility that events will occur and effect the achievement of strategy and business objectives

Man har altså fjernet presiseringen av at det dreier seg om *negativ* påvirkning på måloppnåelse. Med denne definisjonen vil også de mulige *positive* virkningene/ muligheter falle inn under begrepet risiko.

HELSE NORD

Sentrale figurer

FØR:

NÅ:

Én figur: STRATEGI SATT INN I SAMMENHENGEN

Strategi i sammenheng: Figuren viser at formål m.m. danner utg.punktet for hvilke risikoer man kan akseptere når man tar stilling til strategier, at det er en mulighet for at strategien og målsettingene ikke samsvarer med formål m.m., at det følger risiko med den strategien man velger, og at det ligger risiko innebygget i hvordan man følger den valgte strategi.

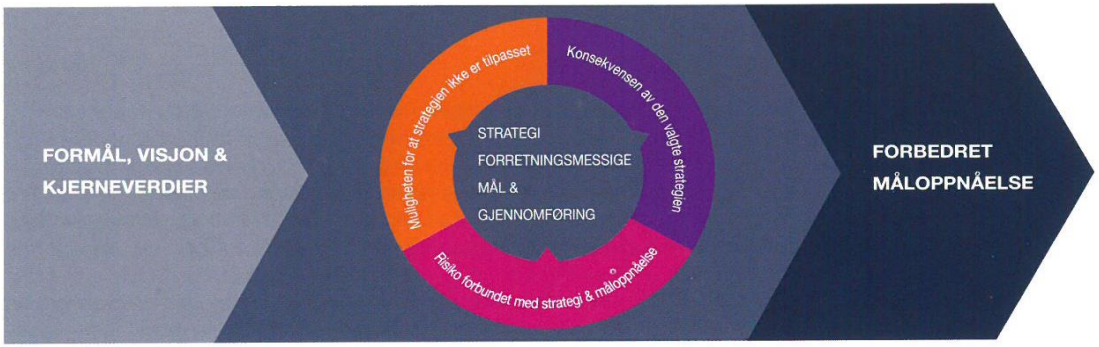
HELSE NORD

Sentrale figurer

FØR:

NÅ:

Én figur: STRATEGI SATT INN I SAMMENHENGEN



En annen figur: HELHETLIG RISIKOSTYRING

Helhetlig risikostyring: De fem «båndene» representerer fem komponenter, som har klare fellestrekk med komponentene i den gamle kuben. Komponentene er da relevante/viktige hele veien fra formål m.m. er besluttet – ved strategiske valg og fastsettelse av forretnings-messige mål, i gjennomføringsfasen og helt frem til forbedret verdiskaping er oppnådd.

HELSE NORD

Komponenter og prinsipper

- **Tidligere**: Åtte komponenter

Komponentene var beskrevet og forklart i rammeverket, men det var ikke definert konkrete prinsipper til hver komponent, slik det ble gjort i COSOs *internkontrollrammeverk* fra 2013

- **Nå**: Fem komponenter, med klare fellestrekk med disse åtte, hver av dem støttes av et sett **prinsipper** – fra tre til fem per komponent, totalt 20 prinsipper

HELSE NORD

Fem komponenter

1. **Virksomhetsstyring og kultur:** Virksomhetsstyring bidrar til etablering av organisasjonskultur, styrker betydningen av helhetlig risikostyring og fastsetter ansvaret for oppfølging av den. Kultur omhandler etiske verdier, ønsket atferd og forståelse for risiko i enheten.

2. **Fastsettelse av strategi og mål:** Helhetlig risikostyring, strategi og fastsettelse av mål er elementer som virker sammen i strategiplanprosessen. Risikoappetitt blir fastsatt og avstemt mot strategien; virksomhetens mål setter strategien ut i praksis og danner samtidig grunnlag for å identifisere, evaluere og respondere på risiko.

3. **Gjennomføring:** Risiko som kan påvirke oppnåelsen av strategiske og operasjonelle mål må identifiseres og evalueres. Risikoer prioriteres ut fra alvorlighetsgrad i forhold til risikoappetitt. Organisasjonen velger deretter risikohåndtering og benytter et porteføljesyn på hvor mye risiko den kan pådra seg. Resultatene av denne prosessen rapporteres til relevante interessenter.

4. **Gjennomgang og revurdering:** Ved å gjennomgå enhetens måloppnåelse kan en organisasjon ta stilling til hvor godt komponentene i den helhetlige risikostyringen virker over tid og ved betydelige endringer, samt identifisere behov for revurderinger.

5. **Informasjon, kommunikasjon og rapportering:** Helhetlig risikostyring krever en kontinuerlig prosess for å innhente og dele nødvendig informasjon, både fra interne og eksterne kilder, som kommuniseres i hele organisasjonen.

HELSE NORD

Komponenter med prinsipper

1. Virksomhetsstyring og kultur:

1. **Styret fører tilsyn med risiko** — Styret fører tilsyn med strategien og utøver sine virksomhetsstyringsforpliktelser som støtte for ledelsen i arbeidet med å gjennomføre strategien og nå virksomhetens mål.

2. **Etablerer driftsstrukturer** — Organisasjonen etablerer driftsstrukturer i arbeidet med å gjennomføre strategien og nå virksomhetens mål.

3. **Definerer ønsket kultur** — Organisasjonen definerer den atferd som karakteriserer enhetens ønskede kultur.

4. **Er opptatt av og viser forpliktelse til kjerneverdier** — Organisasjonen er opptatt av og viser forpliktelse til enhetens kjerneverdier.

5. **Rekrutterer, utvikler og beholder medarbeidere med ønskede egenskaper** — Organisasjonen er opptatt av å bygge menneskelig kapital som er i samsvar med strategien og virksomhetens mål.

HELSE NORD

Komponenter med prinsipper

2. Fastsettelse av strategi og mål:

6. **Analyserer omgivelsene virksomheten opererer i** – Organisasjonen vurderer potensielle virkninger omgivelsene kan ha på risikoprofilen.

7. **Definerer risikoappetitten** – Organisasjonen definerer risikoappetitten som en del av prosessen med å skape, bevare og realisere verdi.

8. **Evaluerer alternative strategier** – Organisasjonen evaluerer alternative strategier og den potensielle innvirkning disse kan ha på risikoprofilen.

9. **Formulerer virksomhetens mål** – Organisasjonen vurderer risiko når den på ulike nivåer etablerer virksomhetens mål, som er i samsvar med strategien og støtter opp om den.

HELSE NORD

Komponenter med prinsipper

3. Gjennomføring:

10. **Identifiserer risiko** – Organisasjonen identifiserer risiko som påvirker gjennomføringen av strategien og oppnåelse av virksomhetens mål.

11. **Vurderer alvorligheten av risiko** – Organisasjonen vurderer hvor alvorlig risikoen er.

12. **Prioriterer risikoer** – Organisasjonen prioriterer risikoer som grunnlag for beslutninger om hvordan disse skal håndteres.

13. **Iverksetter risikohåndtering** – Organisasjonen identifiserer og velger hvordan risikoen skal håndteres.

14. **Utvikler porteføljesyn** – Organisasjonen utvikler og evaluerer et porteføljesyn på risiko.

HELSE NORD

Komponenter med prinsipper

4. Gjennomgang og revurdering:

15. **Evaluerer vesentlige endringer** – Organisasjonen identifiserer og evaluerer endringer som i vesentlig grad kan påvirke strategien og virksomhetens mål.

16. **Gjennomgår risiko og måloppnåelse** – Organisasjonen gjennomgår enhetens måloppnåelse og vurderer risiko.

17. **Tilstreber forbedring av den helhetlige risikostyringen** – Organisasjonen tilstreber kontinuerlig forbedring av den helhetlige risikostyringen.

HELSE NORD

Komponenter med prinsipper

5. Informasjon, kommunikasjon og rapportering:

18. Drar nytte av informasjonssystemer – Organisasjonen drar nytte av enhetens informasjons- og teknologisystemer for å understøtte den helhetlige risikostyringen.

19. Kommuniserer risikorelatert informasjon – Organisasjonen bruker kommunikasjonskanaler til å understøtte den helhetlige risikostyringen.

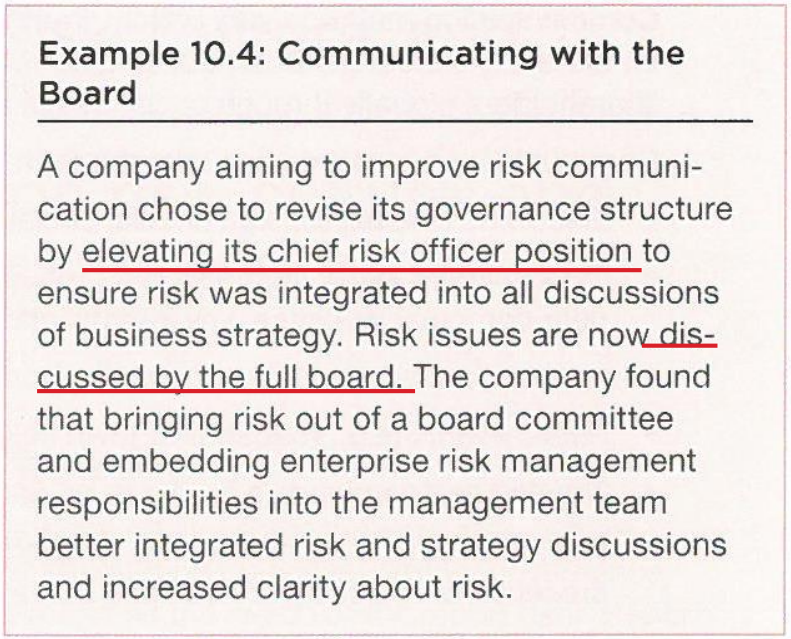
20. Informerer om risiko, kultur og måloppnåelse – Organisasjonen informerer om risiko, kultur og måloppnåelse på flere nivåer og på tvers av enheten.

HELSE NORD

Hva mer finner vi i COSO ERM-pakken?

I **selve heftet** («hovedboken») finner vi:

- Del 1: En grundigere gjennomgang av temaene som omtales i Sammendraget:
  - Begreper og definisjoner
  - Strategi, målsettinger og måloppnåelse
  - Integrering av risikostyring
  - Komponenter og prinsipper
- Del 2: Rammeverket:
  - Gjennomgang av hver enkelt komponent og alle underliggende prinsipper. Inneholder en rekke eksempler og figurer
- Del 3: Ordliste



Example 10.4: Communicating with the Board

A company aiming to improve risk communication chose to revise its governance structure by elevating its chief risk officer position to ensure risk was integrated into all discussions of business strategy. Risk issues are now discussed by the full board. The company found that bringing risk out of a board committee and embedding enterprise risk management responsibilities into the management team better integrated risk and strategy discussions and increased clarity about risk.

Eksempel til prinsipp 19 – Kommuniserer risikorelatert informasjon

HELSE NORD

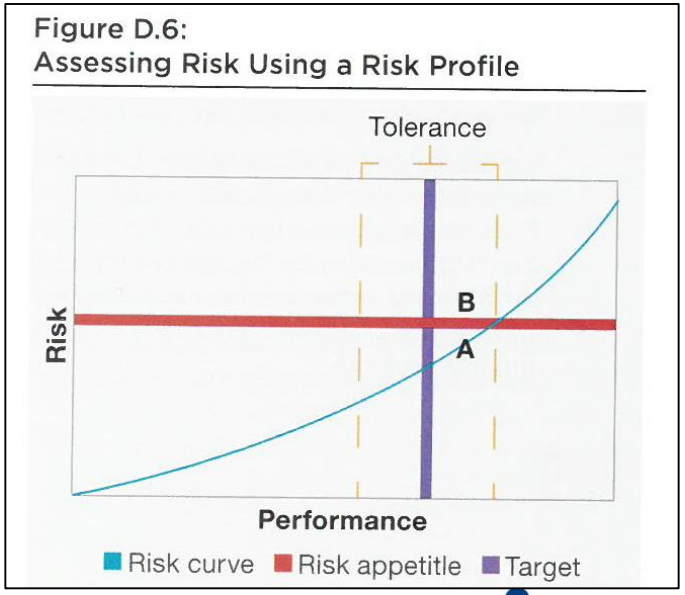
Hva mer finner vi i COSO ERM-pakken?

I **Appendices** finner vi:

- A: Project Background and Approach for revising the Framework
- B: Summary of Public Comments
- C: Roles and Responsibilities for Enterprise Risk Management
  - Board of Directors and Dedicated Committees
  - Management and the Three Lines of Accountability
- D: Risk Profile Illustrations

Fra FAQ: *The **risk profiles** demonstrate how the type and severity of risk can change in response to changes in the level of performance for a given strategy or business objective*.

Eksempel:



Hva mer finner vi i COSO ERM-pakken?

I **FAQ (Frequently Asked Questions)** ligger bl.a.:

- Additional Information about the Documents
- Updates to the Documents
- Key Changes – hvor det man mener er de 10 mest vesentlige endringene listes opp og forklares

Hva nå?

Til sist: hva vil det nye rammeverket bety for virksomheter som allerede har et risikostyringsopplegg på plass, i samsvar med «gamle» COSO ERM (ev. DFØs Veileder og Metodedokument, eller IIA Norges Veileder)?

- Det er ingen «plikt» til å ta det nye rammeverket i bruk
- Lite eller ingenting i de gamle rammeverkene er i direkte strid med det nye. Men:
  - Det nye COSO ERM-rammeverket har elementer/poenger som sannsynligvis ikke er godt hensyntatt i opplegg etablert i samsvar med de gamle rammeverkene, og
  - Noe av det som er lagt vekt på i etablert opplegg vil kanskje fremstå som mindre vesentlig når man følger logikken i nye COSO ERM.

Derfor et velment innspill til sist:

HELSE NORD

Hva nå? (forts.)

Vurdér det etablerte risikostyringsopplegget nøye opp mot *COSO ERM – Integrating with Strategy and Performance*. Vær bl.a. obs på følgende:

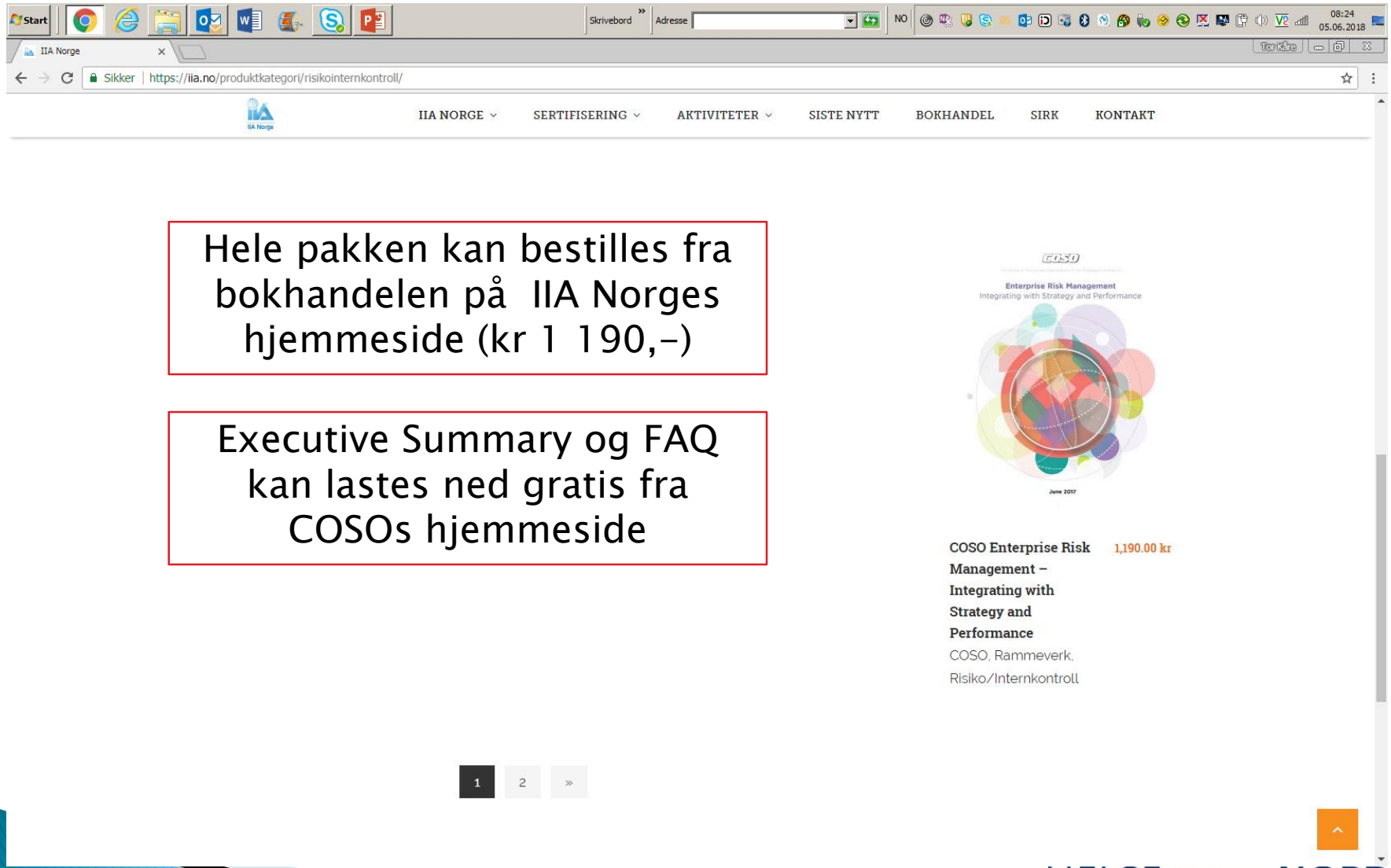
- Bør det gjøres noe med hvordan virksomhetens **strategi** håndteres i risikostyringen vår?
  - Her er det gjort vesentlige endringer i nye COSO ERM
- Legger risikostyringsopplegget vårt tilstrekkelig vekt på risikoens **positive** side («oppsiderisikoen») – mulighetene for å forbedre måloppnåelsen gjennom å ta (økt) risiko?
  - Dette vektlegges atskillig sterkere i nye COSO ERM
- Er det viktige **prinsipper** i det nye rammeverket som blir mangelfullt ivaretatt i dagens opplegg?
  - Komponentene er ikke vesentlig forandret, men det ligger mye nyttig veiledning i de 20 prinsippene, som er nye.

HELSE NORD

Hvordan skaffer jeg meg rammeverket?

Hele pakken kan bestilles fra bokhandelen på IIA Norges hjemmeside (kr 1 190,-)

Executive Summary og FAQ kan lastes ned gratis fra COSOs hjemmeside



Mangelfull risikovurdering og katastrofal risikostyring?

Eller bare et eksempel på tiltaket «pursue risk» ?

Takk for oppmerksomheten!