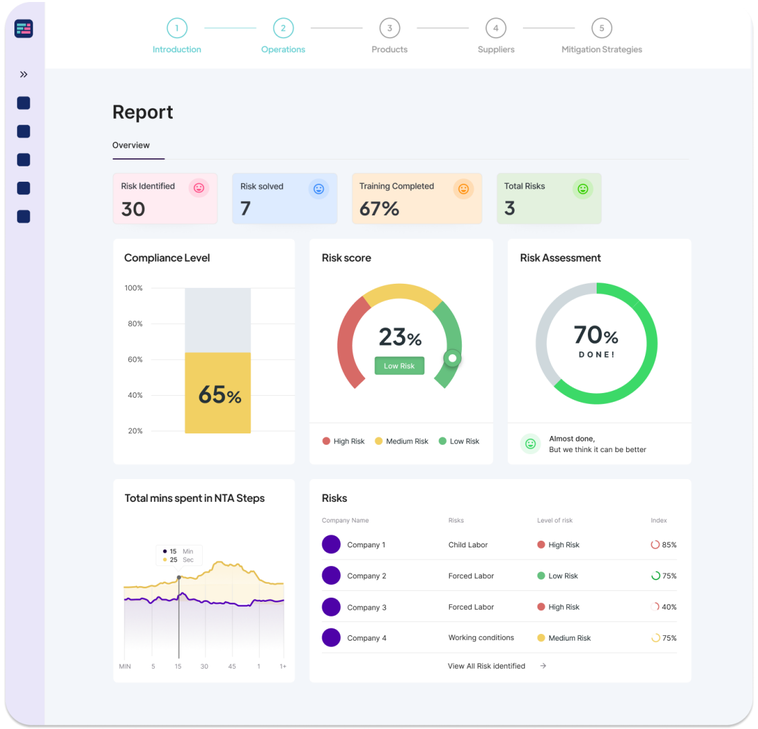
FORTIFAI

Hvordan definere KPIer og bruke data for mer proaktiv compliance?

Janne Britt Saltkjel, 24. november 2023

Agenda

- Utvikling og status for Compliance i Norge
- CSRD og ESRS' krav til governance (compliance)
- Hva er KPIer (- og hva skal vi med det)
- Eksempler på rapportering
- Case
- Muligheter mht bruk av data



Compliance i Norge - 20 års jubileum

Ikke uttømmende oversikt

Hvor går veien videre?

Panama papers

2000 2003 2023

Sarbanes Oxleys Act (Sox) (2002)

Lovgivning mot korrupsjon styrket

Regnskapsloven presiserer styreansvar mht virksomhetsstyring

2. / 3. linje blir pålagt finansforetak over en viss størrelse (forvaltningskapital>10 mrd)

Forsterket AML (2015-2020)

MiFIDII (2018)

GDPR (2018)

PSD2 (2019)

Åpenhetsloven

EU Taxonomy

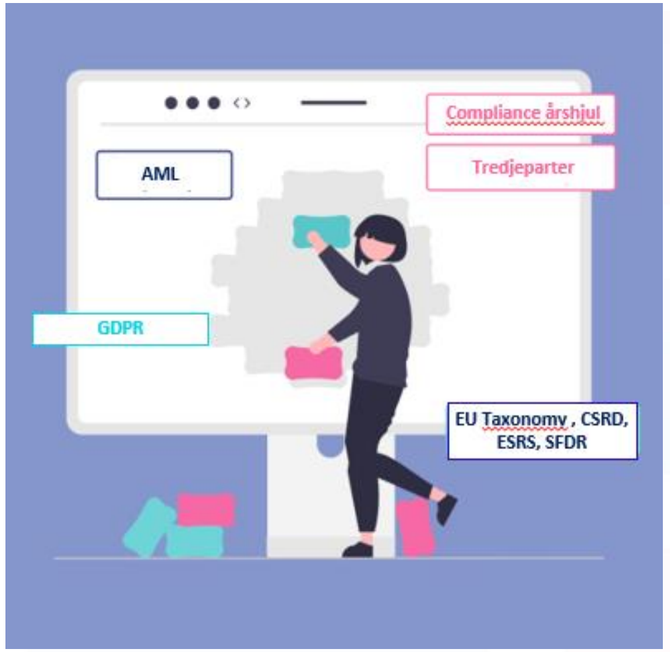
SFDR

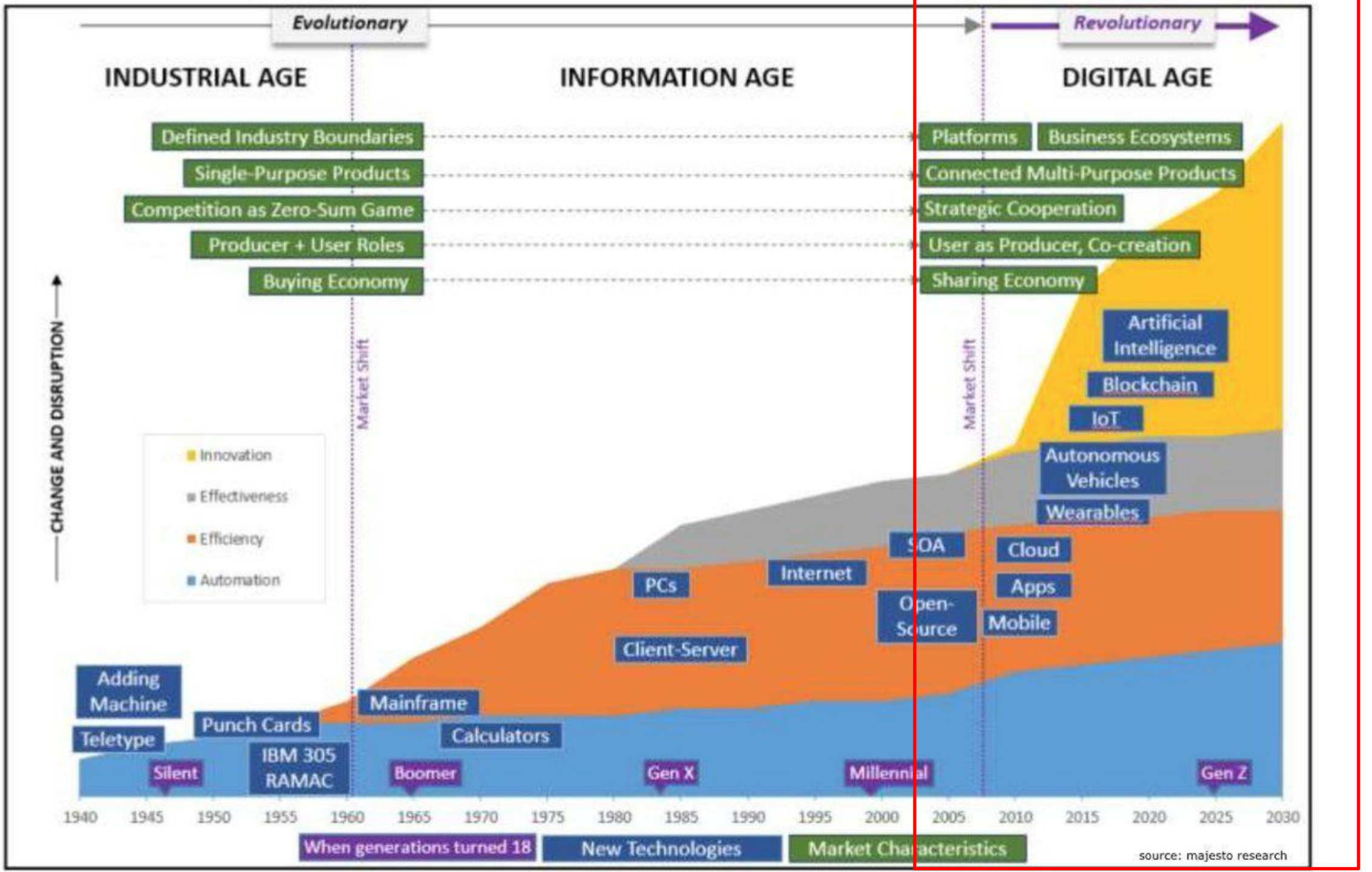
CSRD

CSDDD

Status for compliance i dag

- Økt regulatorisk press de siste årene med bl.a. AML, GDPR og ESG
- Reflekteres også i kundekrav som treffer virksomheter som ikke er direkte omfattet av loven
- Compliance blir en “lisence to operate”
- Knapphet på kompetanse i markedet og knapphet på ressurser I compliancefunksjoner
- Fortsatt ganske manuelt, men nye løsninger og bruk av data kan effektivisere arbeidet




Evolutionary
Revolutionary
INDUSTRIAL AGE
INFORMATION AGE
DIGITAL AGE
Defined Industry Boundaries
Single-Purpose Products
Competition as Zero-Sum Game
Producer + User Roles
Buying Economy
Platforms
Business Ecosystems
Connected Multi-Purpose Products
Strategic Cooperation
User as Producer, Co-creation
Sharing Economy
Market Shift
Market Shift
CHANGE AND DISRUPTION
Innovation
Effectiveness
Efficiency
Automation
Artificial Intelligence
Blockchain
IoT
Autonomous Vehicles
Wearables
Cloud
Apps
Mobile
SOA
Internet
PCs
Open-Source
Client-Server
Adding Machine
Teletype
Punch Cards
IBM 305 RAMAC
Mainframe
Calculators
Silent
Boomer
Gen X
Millennial
Gen Z
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
When generations turned 18
New Technologies
Market Characteristics
source: majesto research

Bærekraftsrapporteringskrav til Governance - G'en i ESG

CSRD: Bærekraftsrapportering i henhold til ESRS

Part of the management report	[draft] ESRS codification	Title of [draft] ESRS
1. General information	[draft] ESRS 2	*General disclosures*, including information provided under the Application Requirements of [draft] topical ESRS listed in [draft] ESRS 2 Appendix D.
2. Environmental information	[draft] ESRS E1	*Climate change*
	[draft] ESRS E2	*Pollution*
	[draft] ESRS E3	*Water and marine resources*
	[draft] ESRS E4	*Biodiversity and ecosystems*
	[draft] ESRS E5	*Resource use and circular economy*
3. Social information	[draft] ESRS S1	*Own workforce*
	[draft] ESRS S2	*Workers in the value chain*
	[draft] ESRS S3	*Affected communities*
	[draft] ESRS S4	*Consumers and end-users*
4. Governance information	[draft] ESRS G1	*Business conduct*

Må ses I sammenheng med ESRS 1 General principles og [draft] ESRS 2 General requirements.

ESRS G1-1 Business conduct and corporate culture

Formålet er å skape forståelse for

- hvordan ledelse og styret utvikler, fremmer og overvåker bedriftskulturen
- virksomhetens evne til å dempe negative påvirkning og maksimere positiv påvirkning, og overvåke og styre relaterte risikoer

→ Må beskrive mekanismer for å identifisere, rapportere og granske varsler om mulig kritikkverdige forhold, korrupsjon og misligheter, samt hvilke områder som har høyest risiko

Basis for KPIer kan være:

- Code of conduct, policier og prosedyrer - utarbeidet og implementert
- Gjennomført opplæring og kommunikasjon
- Kvalitet i gjennomførte risikovurderinger
- Gjennomføring av tiltak for å styre risiko
- Håndtering av varslingssaker

ESRS G1-2 Management of relationship with suppliers

Formålet er å få forståelse for selskapets styring av innkjøpsprosessene samt rettferdig behandling av leverandører.

→ Må beskrive håndtering av leverandører, herunder risikoer og leverandør-kjedens påvirkning på bærekraftsforhold, sosiale og miljømessige kriterer for valg av leverandører, samt prosedyrer for å unngå forsinket betaling til små leverandører.

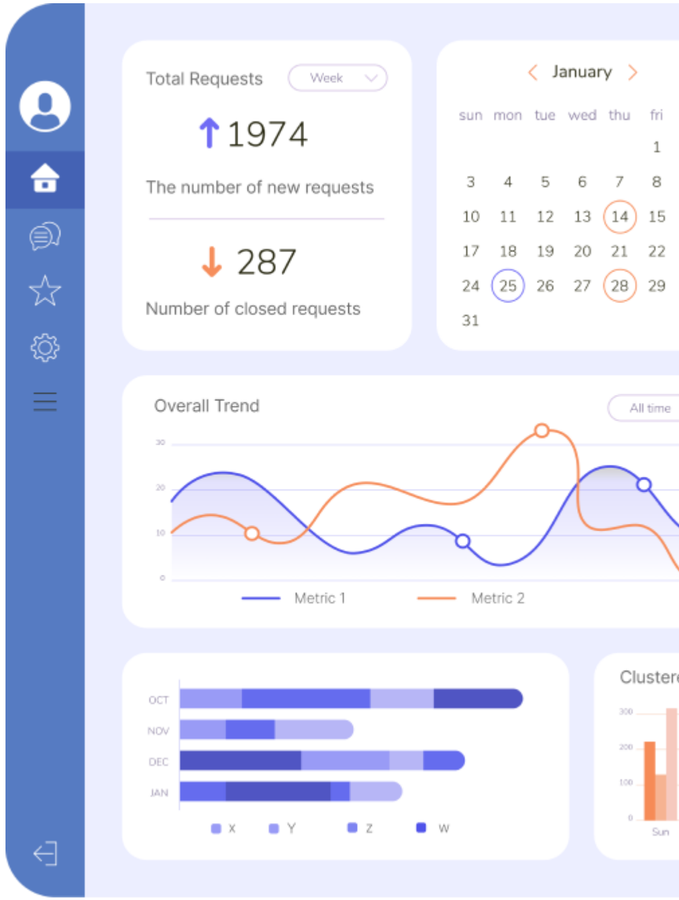
Basis for KPIer kan være:

- Policier og prosedyrer for innkjøp, inkludert valg av leverandører
- Gjennomførte IDDer og utvikling i leverandørportefølje
- Resultater fra åpenhetsloven (mht sosiale forhold)
- Resultater fra miljørapportering fra tredjeparter (CO2, GHG)
- Leverandørrevisjoner
- Purringer

ESRS G1-3 Prevention and detection of corruption and bribery

Formålet er å sikre åpenhet rundt prosedyrer for å forebygge, avdekke, og håndtere mistanker om korrupsjon. Inkluderer opplæring og informasjon internt og til leverandører.

Må beskrive prosedyrer for å antikorrupsjon, hvorvidt granskningsteam er uavhengig og hvordan granskningsresultater rapporteres.



Basis for KPIer kan være:

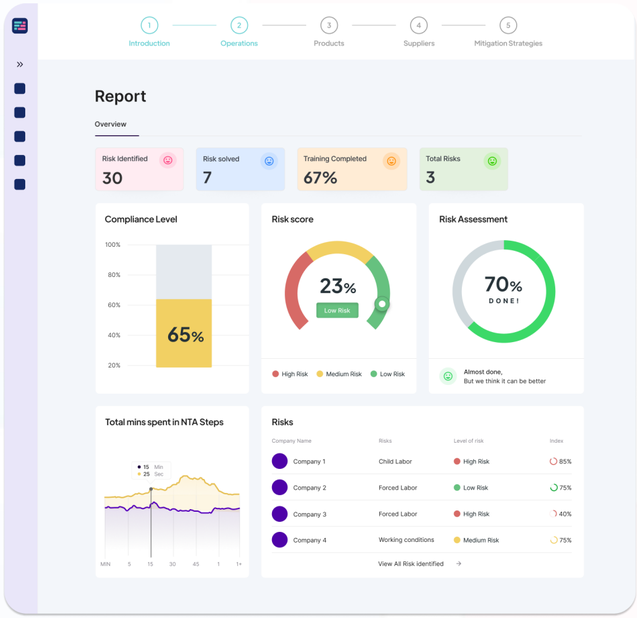
- Policyer og prosedyrer – utarbeidet og implementert
- Opplæring, kommunikasjonstiltak, -verktøy og -kanaler
- Incentivordninger – feks til selgere
- Bruk av kontraktsklausuler
- Saker behandlet og evaluering av disse

KPIer og bruk av data

Compliance – mandat og verdibidrag

Hva trenger ledelsen og styret av informasjon fra Compliance for å ta gode beslutninger?

- Regulatoriske krav og utvikling
  - Direkte og indirekte (via kunder)
- Hendelser, risiko og retning
  - Virksomhetens eksponering og utvikling
- Ressursbruk, effekt og eventuelle utfordringer
  - Hva får virksomheten ut av compliance



KPIer – Key Performance Indicator

- Skal si noe om effektiviteten og resultatene av complianceprogrammet i forhold til målsetting
- Er ikke det samme som en KRI (– men bør rapportere begge deler)
- Må være sterkt påvirkbar (- ellers er det ikke «performance»)
- God score på KPI skal gi lavere risk
- Kan alt ha en KPI? -Mulighetsrommet øker når man utvider fra kvantitative til også kvalitative kriterier
- Bruk de data du har – både kvalitative og kvantitative – **ikke bare fra compliance, men hele virksomheten**

KPIer tar utgangspunkt i målsetting

For eksempel:

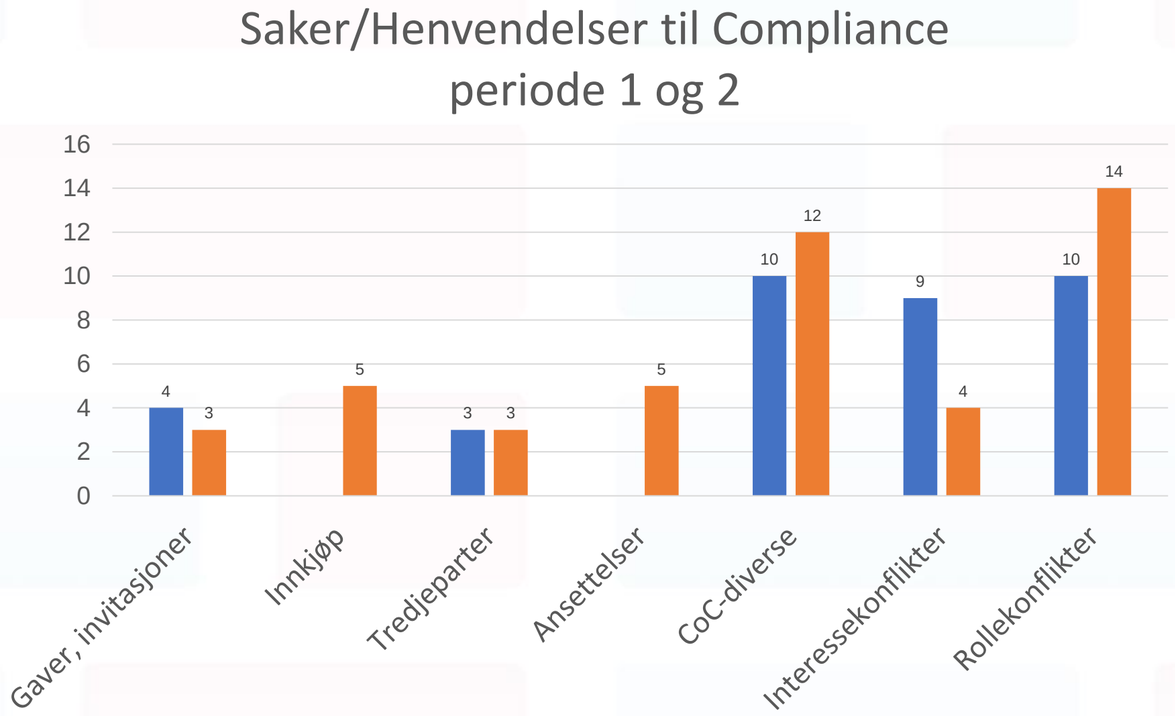
- Mål: Effektiv forebygging, avdekking og håndtering av <korrupsjonsrisiko>

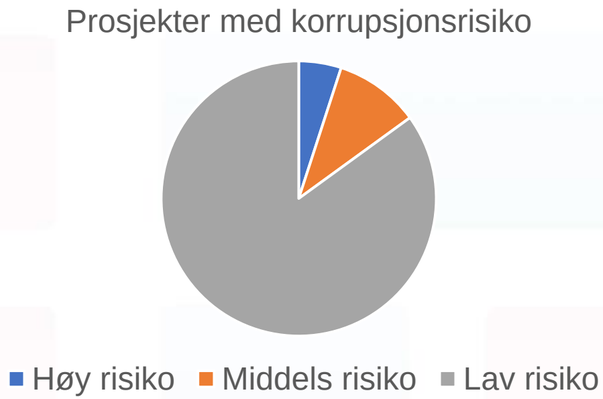
Krever at:

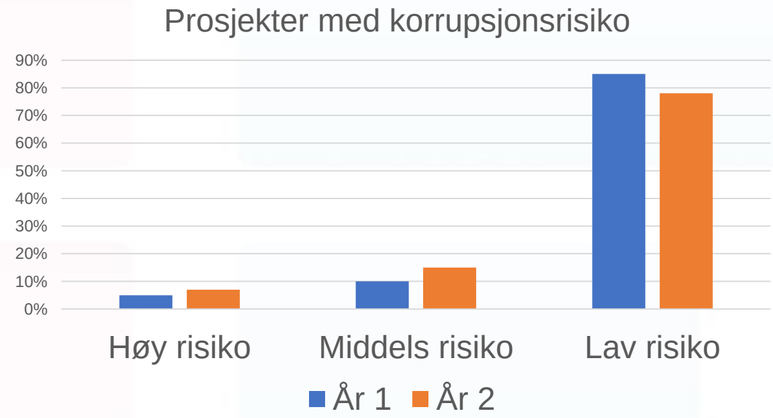
- Prosedyrer og prosesser er hensiktsmessige utformet. Dvs at kontrolltiltak for antikorrupsjon er integrert i relevante prosesser som prosjektstyring, innkjøp, markedsføring, anbud, kundepleie, ansettelser
  - > KPIer på oppdaterte rutiner og prosesser, monitorering regulatorisk utvikling og korrupsjonsrisikoer

- Prosessene er riktig praktisert. Organisasjonen skal være profesjonell og disiplinert i bruken av prosedyrer og verktøy for antikorrupsjon → KPIer på praksis, opplæring, (leder-) kommunikasjon, monitorering/stikkprøver, revisjoner og forbedring

Eksempel fra risikorapportering

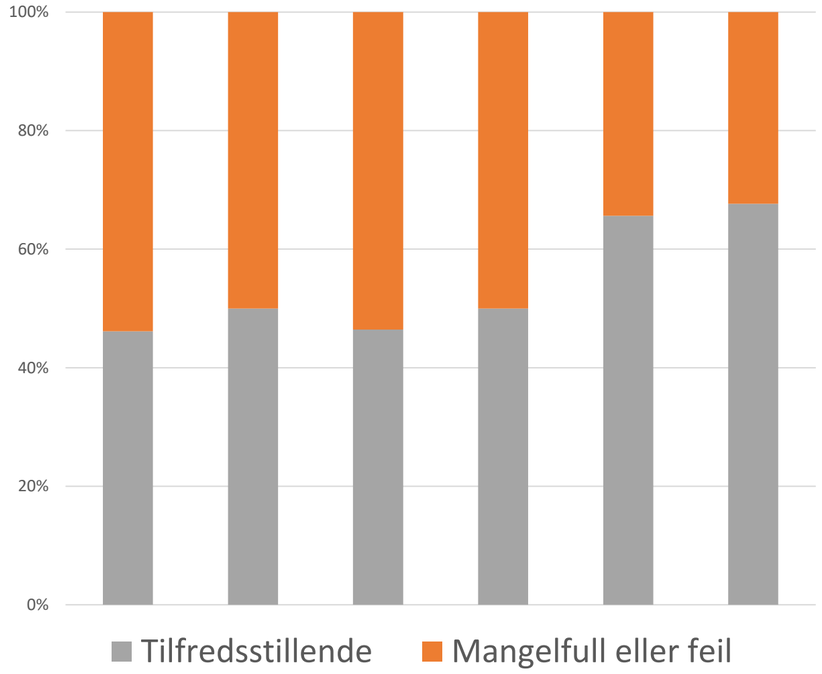


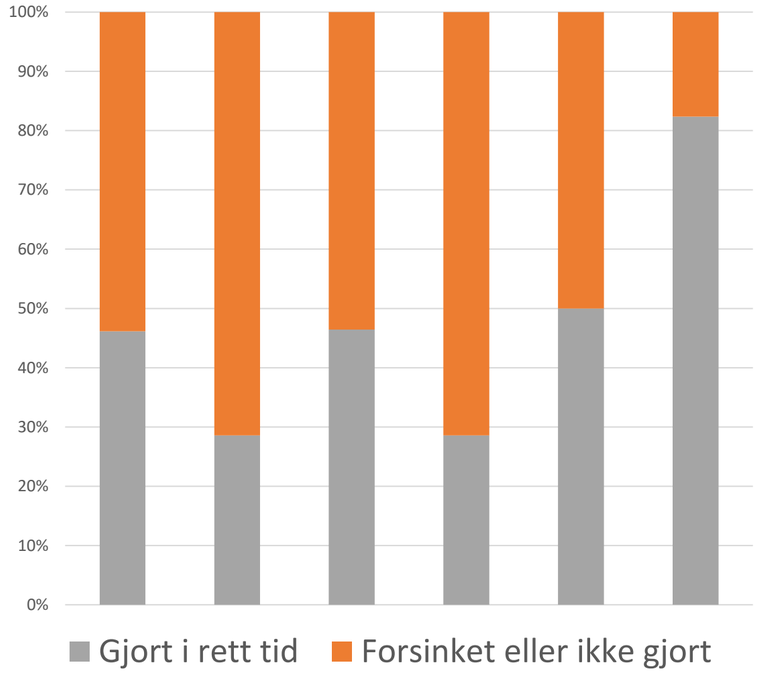


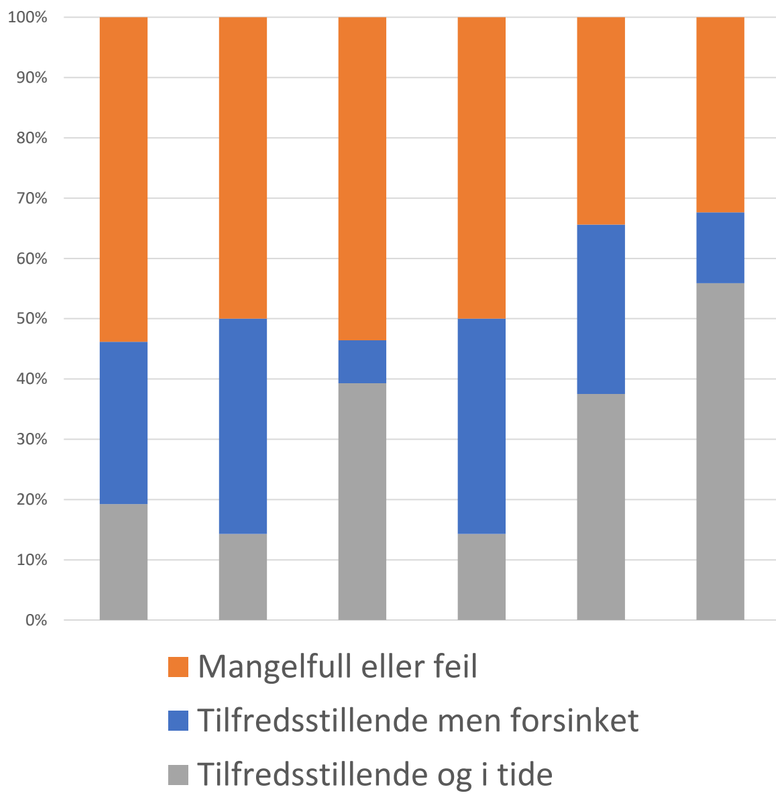


Observasjon:
Tre drivere som fører til henvendelser; spørsmål fra kunde, at enkeltpersoner blant ansatte eller ledere er opptatt av dette, eller at Compliance nylig har vært på besøk.

Eks. fra rapportering av effekt fra compliance program







Aktuelle KPIer:

- Utvikling i gjennomførte vurderinger: KPI: 90 % med akseptabel kvalitet
- Utvikling i identifiserte tiltak: 90 % i rute
- Hvor mange har fått opplæring? KPI: 95 %
- Hvor ofte har compliancetema blitt frontet i internkommunikasjon i avdelingen? KPI: Kvartalsvis

Case: Effektiv rapportering for proaktiv styring

- Sentral complianceenhet ønsker mer innsikt i i datterselskaper for bedre rapportering til styret
- Har begrenset mandat til å instruere datterselskaper (må gå via styret)
- Ønsker å identifisere indikatorer som kan gi nyttig og relevant styringsinformasjon, men som ikke krever mye ekstra innsats eller nye systemer
- Undersøker muligheten for å bruke eksisterende datakilder

Case: Aktuelle områder / tema for rapportering

Risikovurderinger	Leverandører og tredjeparter	Prosjektrisikoer
Utlegg - representasjon, sponsing, gaver	Sertifiseringer, revisjoner	Opplæring og kulturbygging
Monitorering	Varsler og granskninger	Hendelses-register

Case: Prioriterte områder

Risikovurderinger

- Identifisering
- Klassifisering
- Respons / tiltak
- Involvering av interessenter
- Regulatoriske endringer

Eks. på datakilder:
Førstelinjes risikovurderinger
Compliance' risikorapportering
Internrevisjon – log
Tredjeparter (innkjøp)
Gjennomførte tiltak

Utlegg og godkjenninger

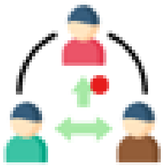
- Interessekonflikter
- Donasjoner
- Gaver
- Lobby
- Utlegg representasjon
- Markedsføring

Eks. på datakilder:
Økonomi/regskapsdata
Banktransaksjoner
Ordrer
Gaveoversikt
Saker til Compliance

Opplæring, kultur

- Tonen på toppen
- Opplæring
- Kommunikasjon

Eks. på datakilder:
Opplæring
Internkommunikasjon-målinger
- konsern og divisjoner
Kulturmålinger
Medarbeiderundersøkelser



Tredjeparter

- Integritets-undersøkelser
- Sanksjoner
- Transaksjoner
- Kontraktsvilkår
- Hendelses-rapportering
- Revisjoner

Eks. på datakilder:
Innkjøp
Prosjektrapportering
Økonomi
Internrevisjon

Varsling og granskninger

- Innmeldte saker
- Klassifisering
- Prosess for håndtering
- Utfall
- Kommunikasjon

Eks på datakilder:
Varslingssystem
Medarbeiderundersøkelser
Rettslige prosesser
Medieomtale

Representasjon og godkjente kostnader

Målsetting: Kun kostnader og aktiviteter som ikke er egnet til å påvirke

Eksempler på kriterier for å nå målet:

- Gode retningslinjer som ansatte kjenner til
- Kontroll av uvanlige posteringer
- Kontroll av betalinger mot uvanlige land og skatteparadiser
- Kontroll av leverandører med postboksadresser (autosøk)

Eksempel på KPIer:

- Representasjonsutlegg godkjent totalt, og på forhånd: 100%
- Sponsoraktivitet har vært i henhold til internt regelverk
- Betalinger til bankkonti i skatteparadiser rapportert til compliance
- Gjennomførte IDDer av leverandører eller partnere ajour / ingen backlog

Varsling og granskninger – hva er egnet KPI?

Målsetting: En åpenhetskultur og en ansvarskultur og at kritikkverdige forhold håndteres forsvarlig og så tidlig som mulig

Eksempler på kriterier for å nå målet:

- Hensiktsmessige og dekkende prosedyrer, prosesser og verktøy
- Ansatte må vite om prosedyrene og varslingskanalen og ha tillit til disse
- Responsen må være rask
- …og treffsikker – riktig kategorisering (for eksempel skille på arbeidsmiljø og misligheter)
- Saksbehandlingen må være effektiv og i tråd med prosedyre
- Varsler og de det varsles om må være ivaretatt
- Konklusjonene må være tilfredsstillende underbygget og stå seg i en eventuell rettslig vurdering

KPIer kan være:
Medarbeidere kjenner prosedyrene: 90 %
Responstid: < 24 timer
Kategorisering riktig: 100% av tilfellene
Tidsfrister overfor tilsynsmyndigheter overholdt (for eksempel personvernbrudd): 100%
Kvalitativ vurdering av behandlede saker og gjennomførte granskninger: Evaluering i etterkant

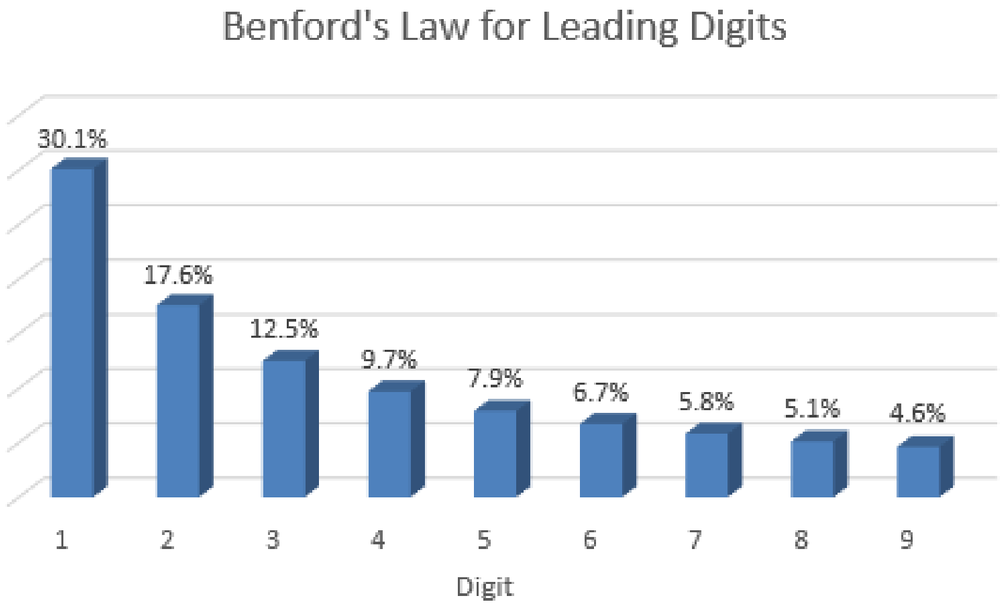
Eksempler på relevante datakilder

Økonomi:

- Transaksjoner til utenlandske banker
- Mange transaksjoner tett under fullmaktsbeløp
- Anomalier i transaksjonsmønstre
- Benford analyse

Salg og marked

- Markedstiltak; gave- og sponsoroversikter brutt ned på selskap
- Anomalier i salgstall – utvikling
- Incentiver for og kontroll av agenter; salgsstatistikk
- Utvikling i reklamasjoner og kundeklager – sammenstilt med for eksempel salgstall



Benfords lov: I et stort utvalg av transaksjonsdata, vil spredningen av første tall følge grafen over. Dvs flest beløp vil begynne på 1, litt over halvparten så mange vil begynne med 2 osv.

Manipulerte transaksjoner vil som regel ikke replikere dette mønsteret. Avvik fra et slikt mønster kan tyde på konstruerte transaksjoner.

Eksempler på relevante datakilder

Innkjøp

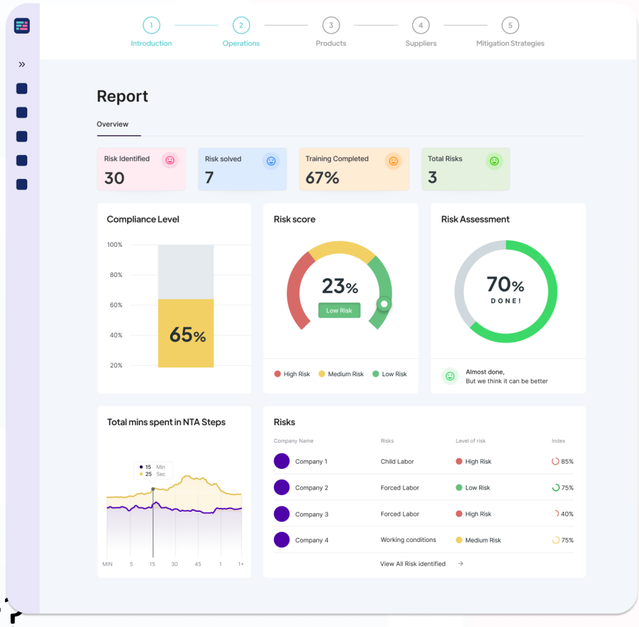
- Leverandørregister – uttrekk basert på adresser, bankforbindelse, integritetsundersøkelse
- Kontraktstyringssystem -
- Databehandlingsprotokoll mot nye leverandører og databehandleravtaler
- Test av tiltak knyttet til håndtering av interessekonflikter

HR

- Medarbeiderundersøkelser
- Kulturmålinger
- Håndtering av personalmessige interessekonflikter

Kommunikasjon

- Kommunikasjon på intranett – hva blir lest, regionale forskjeller, språkbarrierer?
- Mediamålinger

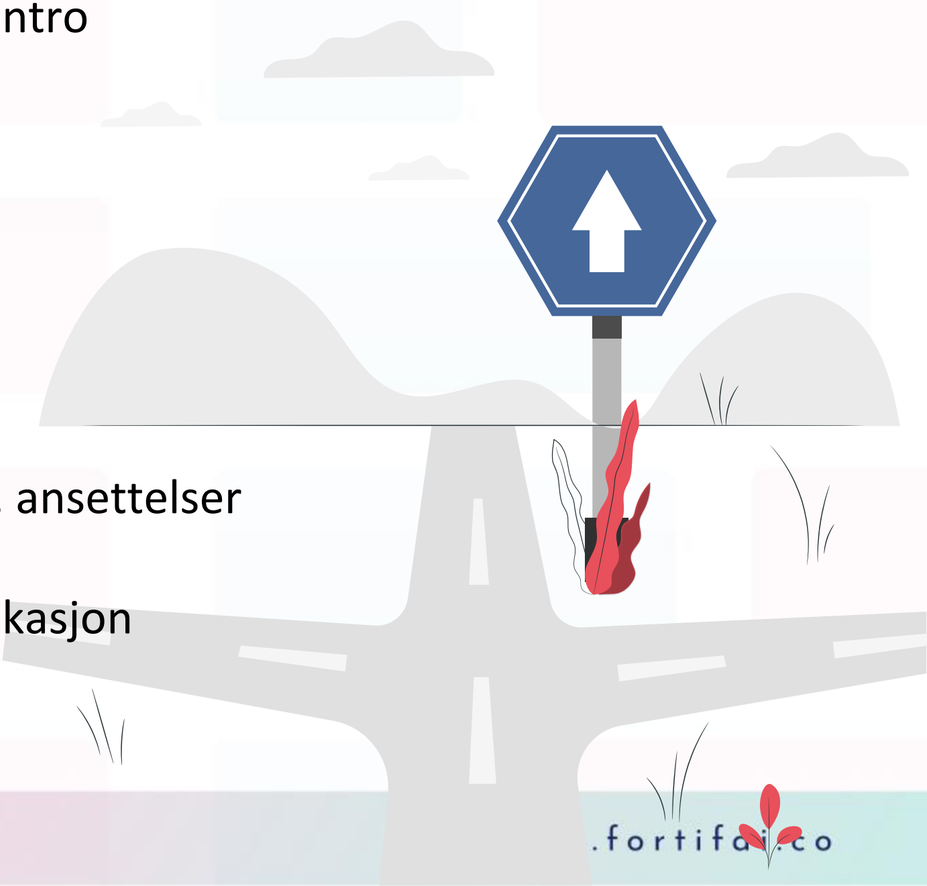


Råd til veien videre for mer datadrevet compliance

- Start med det du kan og samarbeid med andre funksjoner – begynn tidlig

- Ta utgangspunkt i eksisterende kilder, f.eks.
  - Økonomi – regnskap, bank- og korttransaksjoner, leverandørreskontro
  - Innkjøp – innkjøpssystem, leverandørregister, kontraktsystemer
  - Salg – kontrakter med kunder og tredjeparter, lage oversikt over representasjon
  - HR – medarbeiderundersøkelser
  - Kommunikasjon – artikler og materiell, målinger
  - Avvikshåndteringsystem – mønstere, klustere

- Integrer compliancetiltak i eksisterende prosesser, feks leverandørkrav, ansettelser og onboarding, lederutviklingsprogrammer, ansettelsesprosesser, medarbeiderundersøkelser, due diligence ved oppkjøp, internkommunikasjon



Noen lenker til inspirasjon

- Innovation in Compliance with Tom Fox on Apple Podcasts
- Resources | Podcast (lextegrity.com)
- Culture Intelligence - Platform for Culture-driven business growth (data for å måle kultur)
- Kommersiell avtalesjekk (lexolve.com)
- ESRS on Business Conduct (draft): Download (efrag.org)
- Fortifai – Your ESG co-pilot – her kommer det mer

Fortifai

Abbey Lin

Co-Founder
Sales & Marketing, Strategy, Product Development

Janne Britt Saltkjel

Co-Founder
Sales, Finance, Product Development

En Abdulahu

Founding team
Tech Manager, Product Development

Tormod Tingstad

Board Member
Sales and Legal

Geir Henning Pettersen

Board Member
Engineering Tech

Ledere og fageksperter med lang operasjonell erfaring

Spørsmål?

Rådgivning: js@evolutio.no (www.evolution.no)

Systemstøtte og -utvikling: abbey@fortifai.co