Revidering av veiledningsmateriell i Normen

Underlag til Styringsgruppemøte i Normen 25. mars 2021

Sak 23/21 Overordnet plan for oppdatering av veiledningsmateriell 2021

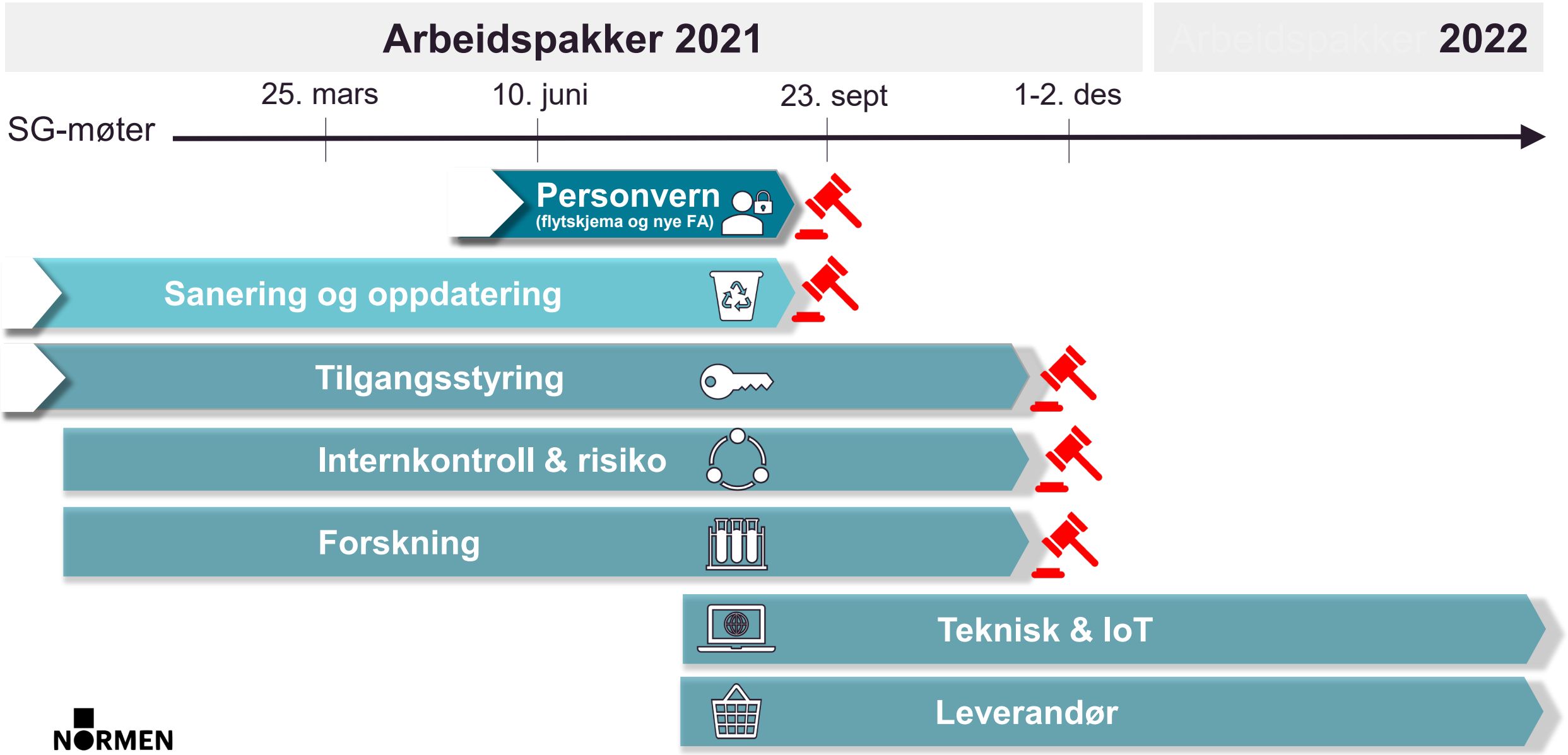
Organisering av revideringsarbeidet

- Prosjektleder: Aasta Hetland (Sekr)
  - Prosjektadministrativ støtte: Carsten Rapp (BDO)

- Koordinatorer
  - Arbeidspakke Sanering & oppdatering: Aasta Hetland (Sekr)
  - Arbeidspakke Tilgang: Carsten Rapp, fra 1.4 Herman Vidje (BDO)
  - Arbeidspakke Internkontroll & risiko: Siw T. Johnsen (Sekr)
  - Arbeidspakke Forskning: Thea Rølsåsen (Sekr)
  - Arbeidspakke Teknisk & IoT: TBD
  - Arbeidspakke Leverandør: TBD

- Fageksperter i prosjektgruppen (bidrar i flere av arbeidspakkene):
  - Herman Vidje, Astrid E. Skorpen, Ulrich Isachsen og Carsten Rapp (alle BDO)

Overordnet plan for revidert (og noe nytt) veiledningsmateriell



NORMEN

Enkeltprodukter i arbeidspakkene som forseres («fast track»)

- Mal for (utforming av) veiledninger og FA
  - Hører under *arbeidspakke Oppdatering & sanering*
  - Godkjenning på SG-møtet 25. mars

- FA 29 om hjemmekontor
  - Hører under *arbeidspakke Tilgang*
  - Godkjenning SG på e-post 3. mai

- Vedlegget til Normen med oversikt over kravene
  - Hører under *arbeidspakke Leverandør*
  - Fremlegges på SG-møtet 10. juni

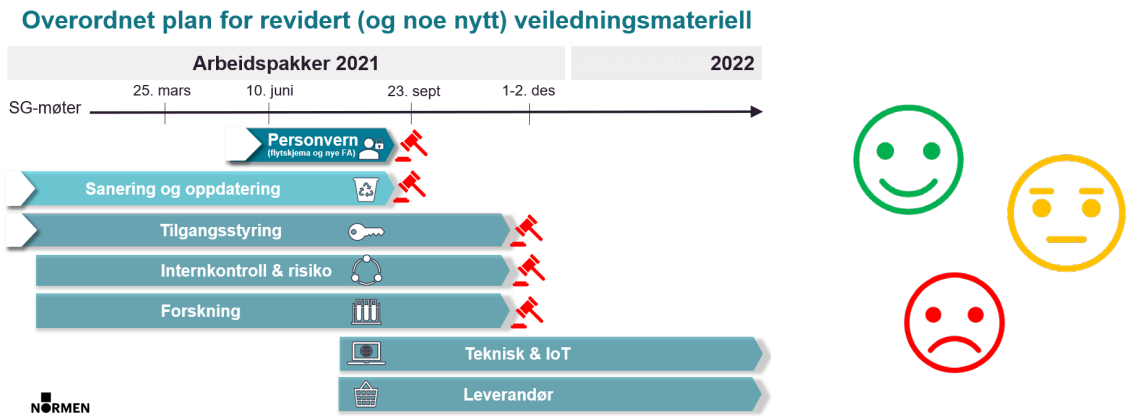
- Veileder om medisinsk utstyr v. 2.0
  - Hører under *arbeidspakke Teknologi & IoT*
  - Fremlegges på SG-møtet 10. juni

Involvering av sektoren

- Sektorinvolvering helt essensielt og en viktig del av planene
- Interessentkartleggingsfase nå
- Referansegrupper
- Diverse arenaer; innspillswebinar, en-til-en, innspill gjennom nyhetsbrev og some, diverse forankrings- og innspillsmøter, andre

Involvering av styringsgruppen for Normen

- SG-møtene brukes til statusrapportering, delkonklusjoner, avklaringer og godkjenning
- Redaksjonskomite brukes i arbeidet
- Identifisert som risiko at SG ikke er nok involvert i prosessen med revisjon
- Risikoreduserende tiltak:
  - Godt underlag til SG i forkant av SG-møtene
  - Månedlig status til SG på e-post med eventuelt innspill og avklaringer

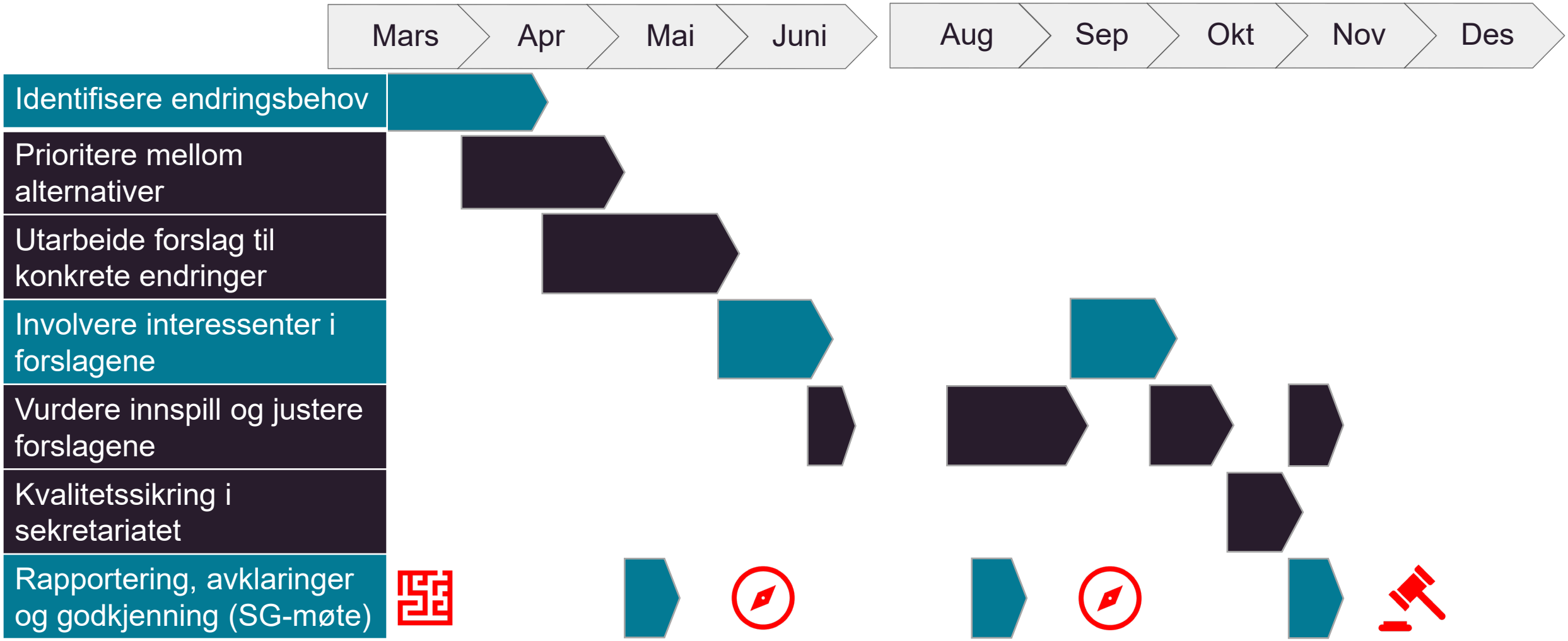


Forlag til vedtak

Styringsgruppen for Normen godkjenner overordnet plan for revisjon av veiledningsmateriell 2021, inkludert materiellet i «fast-track».

Sak 24/21 Plan for veiledningspakke Forskning

Sak 24/21 - Plan for *arbeidspakke Forskning*



NORMEN

Temaer/produkter som inngår i *arbeidspakke Forskning*

- Veileder i personvern og informasjonssikkerhet i forskningsprosjekter
- Flytskjema for arbeid med personvern og informasjonssikkerhet i forskningsprosjekter
- FA 23 avtaler og tillatelser vedr. forskning
- FA 40 informasjonssikkerhet i forskningsprosjekter

Revisjon

Nytt produkt

Vurdering: Selvstendig produkt eller del av veileder forskning

Arbeidsmetodikk og forankring

Arbeidsgruppe(under sammensetning):

- Bidrar med identifisering av behov, problemstillinger og prosess.
- Vil ha løpende kontakt om avklaringer og informasjonsinnhenting.
- Ikke lagt opp til faste møter ennå i kartleggingsfasen, men kan bli aktuelt å strukturere dette ytterligere utover våren.

Referansegruppe(under sammensetning)

- Veileder sendes til referansegruppen i to runder, se plan for arbeidspakke forskning.

Tema- og interessentkartlegging

- Har styringsgruppen innspill til tema, kilder eller hvem som bør involveres?

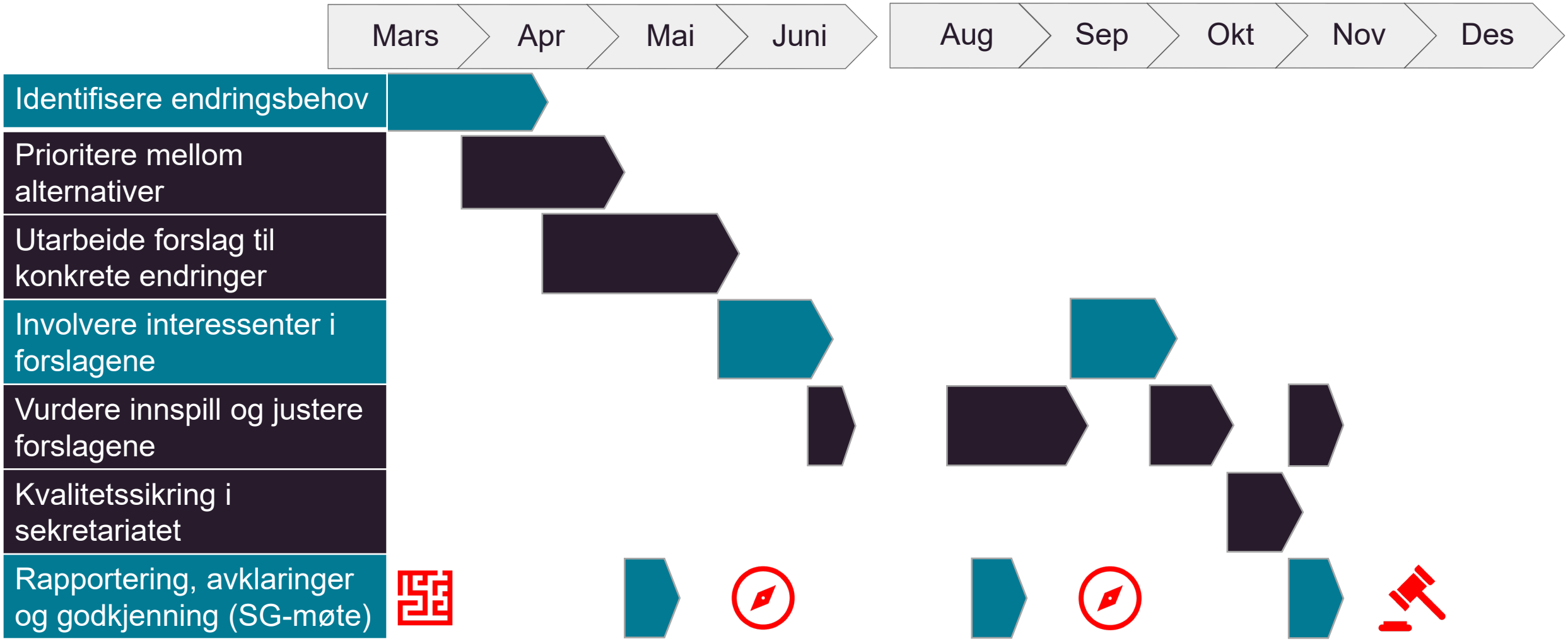
Forslag til vedtak

Styringsgruppen godkjenner plan for veiledningspakke forskning, med veilederen Veileder i personvern og informasjonssikkerhet i forskningsprosjekter, og tilhørende flytskjema og eventuelle faktaark.

Sak 25/21 Plan for veiledningspakke Internkontroll og risiko

25.3.2021

Plan for *arbeidspakke Internkontroll & risiko*

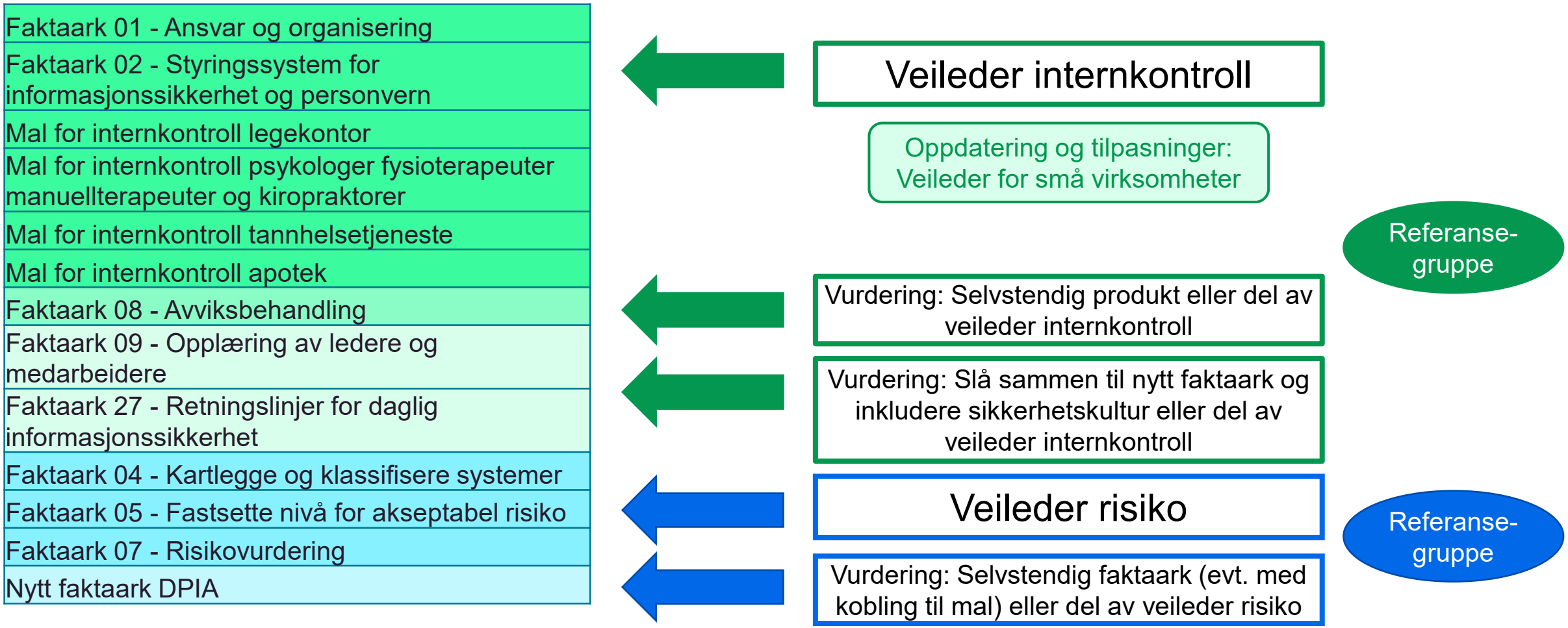


NORMEN

Temaer/produkter som inngår i *arbeidspakke Internkontroll & risiko*

- Faktaark 01 Ansvar og organisering
- Faktaark 02 Styringssystem for infosik og personvern
- Faktaark 04 Kartlegge og klassifisere systemer
- Faktaark 05 Fastsette nivå for akseptabel risiko
- Faktaark 07 Risikovurdering
- Faktaark 08 Avviksbehandling
- Faktaark 09 Opplæring av ledere og medarbeidere
- Faktaark 27 Retningslinjer for daglig infosik
- Faktaark (nytt) om personvernkonsekvensvurdering (DPIA)
- Veileder for små helsevirksomheter
- Mal for internkontroll legekontor
- Mal for internkontroll psyk. fysiot. manuellter. og kirop.
- Mal for internkontroll tannhelsetjeneste
- Mal for internkontroll apotek

Tematisk fokus i *arbeidspakke Internkontroll & risiko*



Tema- og interessentkartlegging

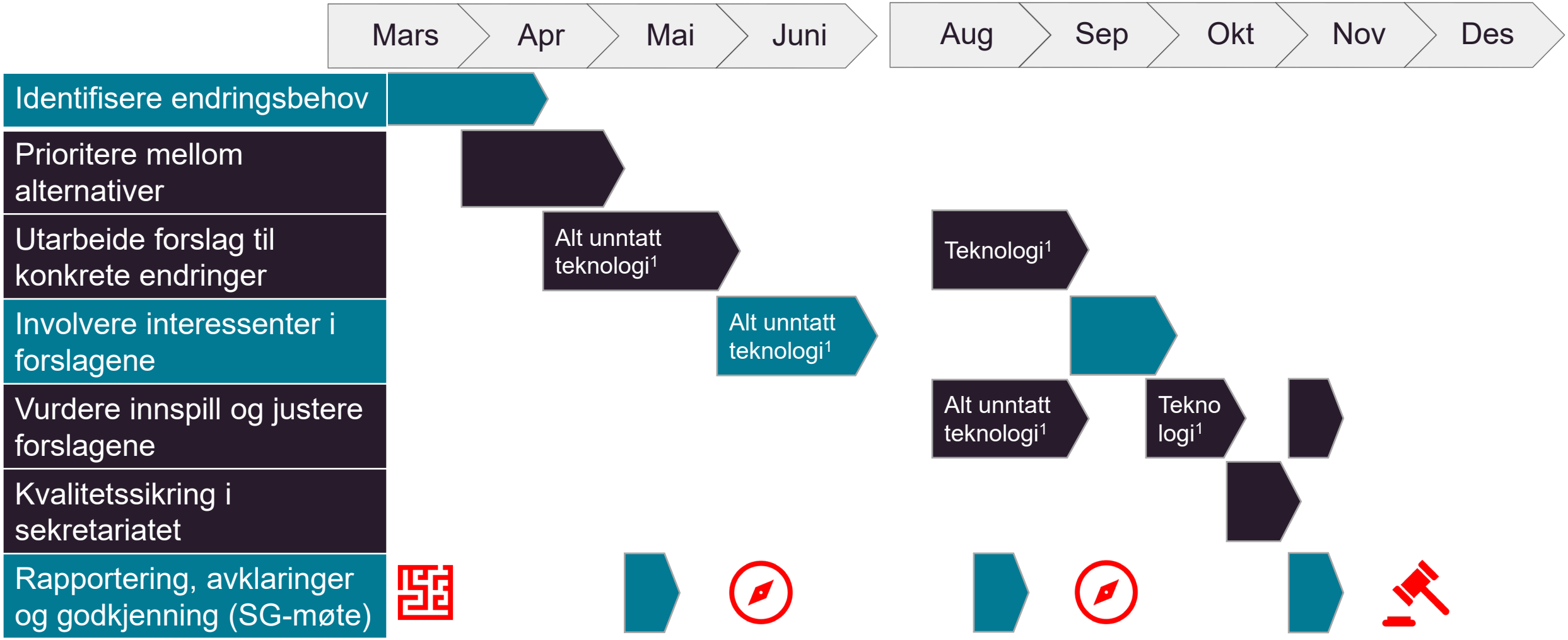
- Har styringsgruppen innspill til tema, kilder eller hvem som bør involveres?

Forlag til vedtak

Styringsgruppen for Normen godkjenner planen for Internkontroll og risiko med to veiledere: internkontroll og risiko, med eventuelle faktaark i tillegg.

Sak 26/21 Plan for veiledningspakke Tilgang

Plan for *arbeidspakke Tilgang*



: *Dialog med SG og andre interessenter*

Fotnote 1: Teknologitemaene er delvis skilt ut i egne bolker fordi fageksperten er lite tilgjengelig før august

NORMEN

Temaer/produkter som inngår i *arbeidspakke Tilgang*

- Veileder tilgangsstyring
- Veileder med avtaleeksempler for samarbeid om felles journal
- Veileder fjernaksess
- Veileder tilgang mellom virksomheter
- FA 14 tilgangsstyring
- FA 15 logging og oppfølging av logger
- FA 25 lagringstid og sletting av opplysninger
- FA 29 hjemmekontor (denne forseres i et «fast track», se aller siste plansje under)
- FA 31 passord og passordhåndtering
- FA 47 autorisasjonsregister
- FA 49 krav ved bruk av PKI ved ekstern kommunikasjon
- FA 50 innsyn i hendelsesregistre

Initielt fokus i *arbeidspakke Tilgang*

- Hovedtemaene i veiledningsmateriellet bør ta utgangspunkt i Normens krav
  - For tilgang innebærer det kravene til *autorisering*, *autentisering* og *kontroll av tilgang*

- Med bakgrunn i utviklingen innen sikkerhet og IKT, bør følgende undertemaer fokuseres på:
  - Praktisk tilgangsstyring i helse- og omsorgsvirksomheter, tilgangsstyring i fagsystemer og tilhørende administrative prosesser
  - Tilgang mellom virksomheter, herunder vurdere sammenslåing av veilederen for dette med veilederen for tilgangsstyring
  - Teknologiske endringer som får betydning
    - Påloggingsmekanismer inkl. passord og mekanismer for multifaktor-autentisering, tilgang ifm. skytjenester, tilgang ifm. hjemmekontor, fjernaksess og mobilt utstyr, sentralisert styring og bruk av (en) identitet og tilgang til kildekode til mekanismer for f.eks. autentisering, samt teknologi i sektoren (f.eks. velferdsteknologi og medisinsk utstyr) der det forutsettes bruk av administrative tilganger i verktøy og utstyr for at det skal virke

Initielt fokus i *arbeidspakke Tilgang*

- Betydningen av nye og endrede rettskilder bør undersøkes nærmere
  - Tilgang (pålogging) fra land utenfor EU/EØS
    - Konsekvensene Schrems II-avgjørelsen i EU-domstolen vil ha for fjernaksess
  - Autentiseringsnivåer som tilsvarer selvdeklareringsforskriften for eID
    - Jf. eIDAS-forordningen og lov om elektroniske tillitstjenester, som gjelder for offentlige myndigheter og tilbydere av bl.a. eID og elektronisk signatur
  - Bestemmelser i pasientjournalforskriften som er relevante for tilgang
    - Denne forskriften har erstattet forskrift om tilgang mellom virksomheter, som det gjeldende veiledningsmateriellet viser til
  - Endringene i Helsepersonelloven §§ 29 flg.
    - Både vedtatte endringer og forslag til nye bestemmelser om kunstig intelligens som har vært på høring

Initielt fokus i *arbeidspakke Tilgang*

- Relevant innhold i nye og endrede veiledninger, standarder og andre rammeverk bør gjennomgås for mulig inspirasjon fra, harmonisering med og henvisning til
  - Elementer i Program samhandling, bl.a. felles tillitsmodell, i regi av Direktoratet for e-helse
  - NSMs grunnprinsipper for IKT-sikkerhet kap. 1.3 og 2.6 og evt. annet veiledningsmateriell fra NSM
  - ISO/IEC 27002 kap. 9
  - Centre for Internet Security (CIS) guidelines CSC 4 Controlled Use of Administrative Privileges, CSC 14 Controlled Access Based on the Need to Know og CSC 16 Account Monitoring and Control
    - Disse veilederne er detaljerte og praktiske, og handler om “hvordan”
  - Australian Government Information Security Manual
    - Denne er nå i et helt ny utgave og kan gi nyttig inspirasjon

- Det bør vurderes om det for noen undertemaer skal brukes henvisninger til noen av de ovennevnte dokumentene, i stedet for eller som et supplement til egenutviklet veiledningsmateriell under Normen

Tema- og interessentkartlegging

- Har styringsgruppen innspill til tema, kilder eller hvem som bør involveres?

Forlag til vedtak

Planen for veiledningspakken Tilgang godkjennes av Styringsgruppen for Normen

Sak 27/21 FA Hjemmekontor

Faktaark 29 Hjemmekontor

- FA 29 om hjemmekontor
  - Hører under *arbeidspakke Tilgang*
  - Godkjenning SG på e-post 3. mai

- Aktuelt faktaark nå og vi antar også fremover
- Høyt nedlastingstall

NORMEN

Initiell vurdering av FA 29 om hjemmekontor

- Inndeling og hovedtemaer i gjeldende versjon av FA 29 er som følger:
  - Forutsetninger: Datalagring, konfigurasjon, bruk av og eierskap til utstyr, kommunikasjon
  - Vurderinger før etablering av hjemmekontor: Risikovurdering og tekniske tiltak
  - Krav til bruk av hjemmekontor: Administrative prosedyrer (basert på risikovurderingen)
  - Avvikling av hjemmekontor: Tilbakelevering, overføring til privat bruk, sletting/makulering

Initiell vurdering FA 29 om hjemmekontor

- Det er mange relevante temaer og momenter som er omtalt i faktaarket
- Innretningen, innholdet og detaljgraden i faktaarket bør tilpasses etter hvem som er hovedmålgruppen(e)
- Det bør derfor revurderes hvem som er hovedmålgruppen(e) for (det nye) faktaarket
  - Store virksomheter med mye egen IT-kompetanse, sentraliserte løsninger og standardisert konfigurasjon?
  - Små virksomheter med lav IT-kompetanse, lokale løsninger og varierende konfigurasjon?
  - Bare *virksomheter* (som skal gi føringer til sine medarbeidere) eller også *enkeltmedarbeidere direkte*?

Initiell vurdering FA 29 om hjemmekontor

- Vurdere sammenslåing, en indre sammenheng eller en avgrensning mellom FA 29 og FA 30 om sikring av mobilt utstyr (unødvendig overlapp bør unngås)
  - I dag er det antakelig få rene «hjemme-PCer». En og samme datamaskin kan brukes på flere arbeidsplasser, på hjemmekontoret og på møter og reiser i inn- og utland.

- Det bør undersøkes hvor utbredt det er at små virksomheter selv konfigurer datamaskinene versus at leverandører av utstyret gjør det, og hva små virksomheter trenger av veiledning for å stille de rette kravene til leverandører

- Gjennomgå relevante veiledere om hjemmekontor (og mobilt datautstyr) fra andre, til inspirasjon
  - Herunder vurdere om det finnes gode veiledere om *hvordan* de *teknologiske* tiltakene kan eller bør innføres, som det kan henvises til i faktaarket.

Tema- og interessentkartlegging

- Har styringsgruppen innspill til tema, kilder eller hvem som bør involveres?

Maler og dokumentinformasjon for veiledere og faktaark

Underlag til Styringsgruppemøte i Normen 25. mars 2021

Forslag til vedtak

Styringsgruppen beslutter at veiledningsmateriellet skal inneholde informasjonen som følger av slidene i denne presentasjonen («Beslutningssak som fast informasjon i veiledningsmateriellet»). Sekretariatet gis fullmakt til å utforme hensiktsmessige maler med denne informasjonen.

Generelt for både faktaark og veiledere

- Bruke hashtagger på tema og virksomhetstype, eventuelt andre viktige sorterings-/filtrering-/nøkkelord
  - Dette jobbes videre med i arbeidet med videreutvikling av www.normen.no
- Aktiv bruk av fotnoter istedenfor referanselister
- «Godkjent av styringsgruppen for Normen» og peker til forvaltningsmodellen må løftes fram i både faktaark og veiledere

Gammel faktaark-tabell

Formål	Dokumentere at dataansvarlig har iverksatt tilstrekkelige tiltak og at behandlingene utføres innefor nivå for akseptabel risiko. Virksomhetene er pålagt å vurdere sannsynlighet for og konsekvens av sikkerhetsbrudd, og basere sikkerhetsarbeid på resultater fra slike vurderinger målt opp mot nivå for akseptabel risiko.		
Ansvar	Dataansvarlig er ansvarlig for at det gjennomføres risikovurdering av behandlingen av helse- og personopplysninger.		
Gjennomføring	Risikovurdering skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandlinger som kan påvirke sikkerheten.		
Omfang	Alle virksomheter i helsesektoren skal gjennomføre risikovurdering. Risikovurdering skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger.		
Målgruppe Dette faktaarket er spesielt relevant for:	Virksomhetens leder/ledelse Forskningsansvarlig Prosjektleder forskning Sikkerhetsleder	Ansatt / medarbeider Forsker Personvernombud	IKT-ansvarlig Databehandler Leverandør
Hjemmel	• Personvernforordningen artikkel 32 • Forskrift om tilgang til helseopplysninger mellom virksomheter § 5		
Referanser	• Risikovurdering av informasjonssystem Datatilsynet, Oppdatert: 15.02.02, Opptrykk: 06.03.09 • Norm for informasjonssikkerhet, kap 3.3 Risikovurdering • Faktaark 5 – Nivå for akseptabel risiko • www.difi.no med modell for risikovurdering		

Forslag ny faktaark-tabell

Tema for faktaarket	Med faste punkter. Beskrivelse av hva FA er og hvordan det er bygget opp; maler, eksempelrutiner, intro til tema, om faktaarket har en prosessorientert tilnærming,
Målgruppe	Deskriptiv beskrivelse med faste punkter og eksempelsetninger
Krav i Normen	Kap. 4.2-4.4 Kap 5.3.6
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Lov, forskrift, ISO, NSM, CSA ol

Ikke sikkert at dette skal i tabellform.

NORMEN

Veiledernes kapittel 1

- Tema for veilederen
- Målgrupper
- Krav i Normen
- Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk
- Bakgrunn (med punkter på hva som skal med; utviklingstrek, regulatoriske krav)
- Avgrensninger
- «Utvikling av veilederen» (Forankring beskrives deskriptivt, ikke navn men roller/profesjoner og virksomhet dersom det er viktig for veilederen
- Leseveiledning

Samme informasjon som i faktaarkene

Dersom nødvendig

Veilederne – foran og bak veileder-tekst

- Det må stå på forsiden hvilket år veilederen sist ble oppdatert
- Info «Om Normen» på tittelbladet

- Endringshistorikken plasseres bak veileder-tekst
- Definisjoner plasseres bak veileder-tekst

Veilederne – foran og bak

- Det må stå på forsiden hvilket år veilederen sist ble oppdatert
- Info «Om Normen» på tittelbladet

- Endringshistorikken plasseres bak veileder-tekst
- Definisjoner plasseres bak veileder-tekst