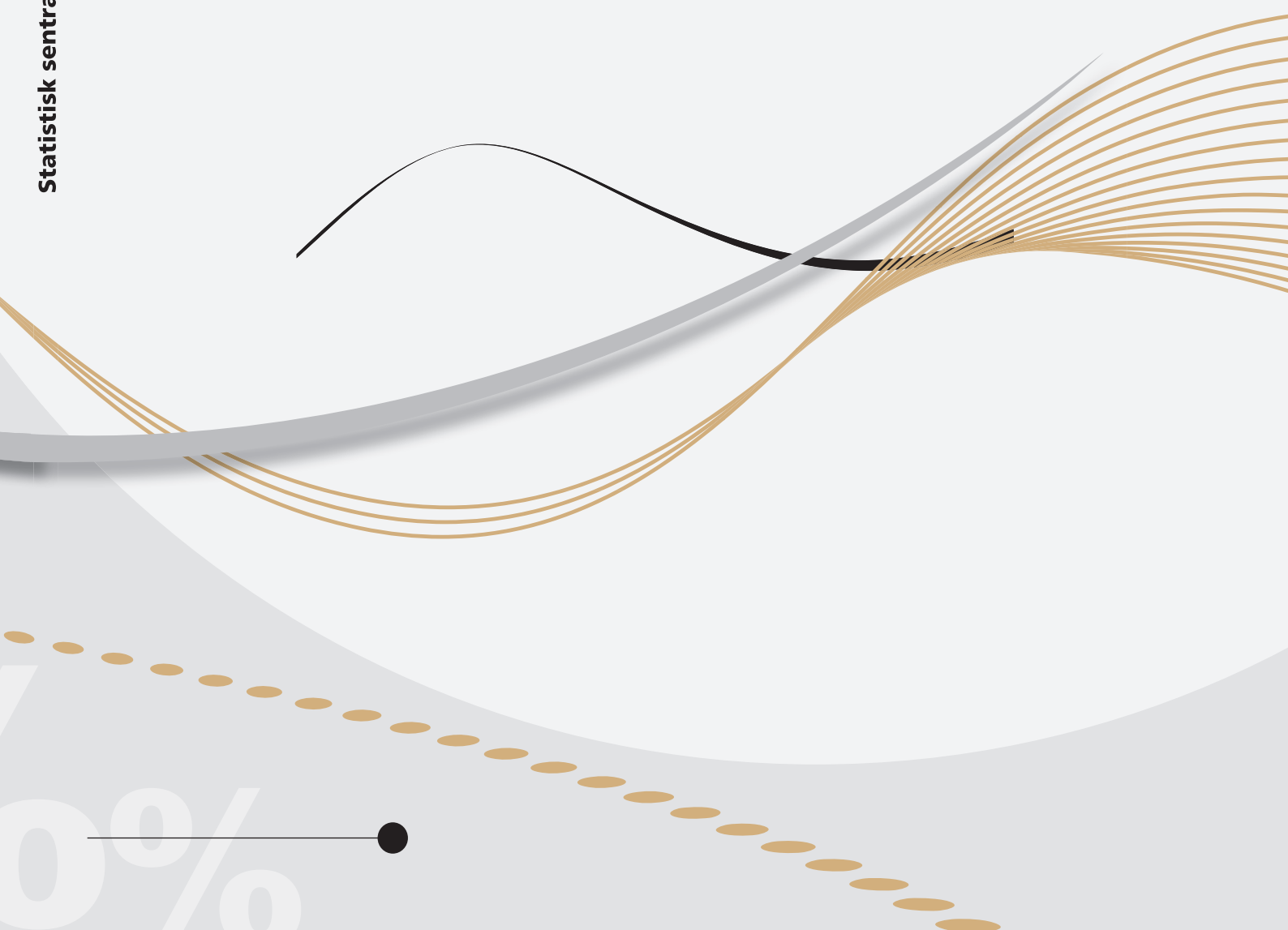




Virksomhetsplan 2016 Risikovurderinger



Virksomhetsplan 2016

Risikovurderinger

I serien Planer og meldinger publiseres dokumenter med et institusjonelt preg og notater med en viss offisiell karakter.

© Statistisk sentralbyrå
Ved bruk av materiale fra denne publikasjonen skal Statistisk sentralbyrå oppgis som kilde.

Publisert mars 2016

Trykk: Statistisk sentralbyrå.

Standardtegn i tabeller	Symbol
Tall kan ikke forekomme	.
Oppgave mangler	..
Oppgave mangler foreløpig	...
Tall kan ikke offentligjøres	:
Null	-
Mindre enn 0,5 av den brukte enheten	0
Mindre enn 0,05 av den brukte enheten	0,0
Foreløpig tall	*
Brudd i den loddrette serien	—
Brudd i den vannrette serien	
Desimaltegn	,

Forord

Virksomhetsplan 2016 Risikovurderinger presenterer overordnede risikovurderinger knyttet til virksomhetsplanen for 2016 og endringer fra tidligere år. Prioriteringer og satsinger for arbeidet i 2016 er samlet i publikasjonen *Virksomhetsplan 2016 Statistisk sentralbyrå*. I tillegg foreligger virksomhetsplaner for avdelingene med risikovurderinger for enkelte områder. Det foreligger også risikovurderinger i prosjektdokumentasjonen for prosjekter i porteføljen.

Statistisk sentralbyrå, 25. februar 2016

Morten Reymert
Styreleder

Christine Meyer
Adm.dir

Innhold

Forord	3
Risikovurdering for Statistisk sentralbyrå 2016	5
1. Statistikkproduksjonen	8
2. IT	12
3. Økonomiforvaltning og innkjøp	15
4. Sikkerhet	18

Risikovurdering for Statistisk sentralbyrå 2016

Statistisk sentralbyrås hovedmål er å dekke samfunnets behov for offisiell statistikk og utarbeide sentrale analyser og forskning som bygger på denne statistikken.

Måloppnåelsen er avhengig av flere forhold, som evnen til effektiv statistikkproduksjon, kvalitet i produksjonen og at samfunnet har tillit til at SSB opptrer objektivt og ikke misbruker data. Disse forholdene er oppsummert i de europeiske retningslinjene for statistikk. Hensynet til kvalitet og effektiv produksjon er også understreket i SSBs sentrale strategidokumenter og planer.

På et overordnet nivå er effektiv og kvalitetssikret statistikkproduksjon og forskning blant annet avhengig av:

- Gode formidlingsløsninger
- Gode IT-systemer
- God kompetanse
- God organisering
- Gode produksjonsprosesser

I tillegg står SSB overfor administrative krav, blant annet:

- God personalforvaltning
- God økonomistyring
- Gode innkjøpsrutiner
- Gode sikkerhetsrutiner

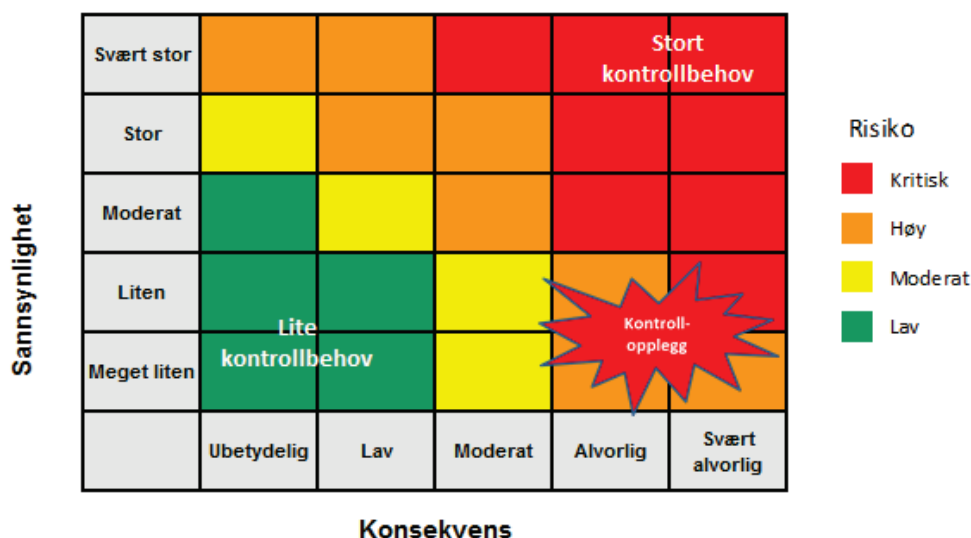
Metode for risikovurdering

Denne rapporten inneholder overordnede risikovurderinger for SSBs virksomhet i 2016. *Operasjonell risiko* omfatter forhold som raskt kan føre til svikt i SSBs løpende produksjon eller tjenesteleveranser, økonomisk tap, tap av liv og helse eller tap av omdømme, som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser.

Risikovurderingene oppsummeres i en fast mal, og i tillegg benyttes risikokart som beskrevet i *Metode for risikovurdering* ([dokument 2009/17](#)). Metoden bygger på DFØs opplegg for risikovurderinger. Risikovurderingene inneholder en kolonne for beskrivelse og forklaring av risiko, en for gradering (kritisk-høy-moderat-lav) av risikoen slik den fremgår i risikokartet og en hvor tiltak og oppfølging av eventuelle tidligere tiltak er kommentert. Under vises risikomatriksen som er benyttet.

For risiko med lav sannsynlighet, men alvorlig/svært alvorlig konsekvens, kan det være uforholdsmessig kostnadskrevende å redusere risikoen ytterligere. Derimot kan en her måtte vurdere behov for bedre beredskap til å håndtere situasjonen dersom uheldige utfall inntreffer, dvs. tiltak som kan redusere konsekvensen og begrense skaden.

Det pågår nå et arbeid med å forbedre prosessen for utarbeidelse av de årlige risikovurderingene og bruken av disse i SSB. Arbeidet involverer hele toppledergruppen og har som mål å få risikovurderingene enda bedre integrert som en del av det øvrige planleggings- og styringsarbeidet i virksomheten. Forbedringsarbeidet er en av flere aktiviteter som gjennomføres i 2016 for å styrke internkontrollen i virksomheten.



Risikovurderinger i publikasjonen

Følgende risikovurderinger er presentert i denne publikasjonen:

- Statistikkproduksjonen samlet
- IT
- Økonomiforvaltning, herunder innkjøp og faren for misligheter
- Sikkerhet

Risikovurderingene er gjennomført i forbindelse med utarbeidelse av virksomhetsplanene for 2016, i perioden august-desember 2015. I tillegg til disse risikovurderingene har alle porteføljeprosjektene slike vurderinger i prosjektdokumentasjonen. Enkelte risikovurderinger på mer detaljert nivå vil også bli presentert i avdelingenes virksomhetsplaner. I 2015 ble det gjennomført en egen vurdering av risiko for feil i publisert statistikk, basert på en gjennomgang av fire sentrale statistikker. En oppdatering når det gjelder risiko for feil i publisert statistikk for 2016 er lagt under kap. 1.

Den fagdirektøren som er ansvarlig for det enkelte fagområdet er i utgangspunktet ansvarlig for tiltakene. For statistikkproduksjonen totalt gjelder dette alle fagdirektørene på statistikksiden, mens IT-direktør har et ansvar på tvers av avdelingene for tiltak knyttet til IT. Alle tiltak beskrevet i disse risikovurderingene skal også være beskrevet i avdelingenes virksomhetsplaner der de passer inn.

Under følger oversikt over kritiske eller høye risikofaktorer knyttet til områdene som er vurdert i rapporten. Nærmere beskrivelser av de ulike risikofaktorene står under hvert kapittel:

- 1 **Statistikkproduksjon**
 - Risiko for mangelfull kapasitet mht. nødvendig kompetanse
 - Risiko for reduksjon av markedsfinansierte oppdrag
 - Risiko for driftsstopp/systemfeil i IT-systemer
 - Risiko knyttet til organisering av arbeidet
 - Risiko for sviktende tilgang til data fra administrative registre og spørreundersøkelser
- 2 **IT**
 - Manglende ressurser i driftsseksjonen
 - Ondsinnet dataangrep som følge av økt eksponering av nettverk og tjenester mot omverden
 - Utdatert hardware og software

- Begrenset kapasitet til forvaltning av IT-systemene og fagapplikasjoner
- Mangler samordnet og helhetlig prioritering av utviklingsoppgaver i IT
- Mangelfull ressursstyring i IT
- Mangelfull kompetanse til gjennomføring av utviklingsprosjekter

3 **Økonomiforvaltning og innkjøp**

- Ingen risiko som er vurdert til kritisk eller høy

4 **Sikkerhet**

- Manglende integritet og konfidensialitet – interne forhold
- Manglende tilgjengelighet
- Risiko for omfattende brann, oversvømmelse eller naturkatastrofe
- Manglende sikkerhetskompetanse og bevissthet
- Terror

1. Statistikkproduksjonen

Mål: Opprettholde den løpende produksjonen og formidlingen av statistikk med en kvalitet minst på dagens nivå.

Endring:

Risiko knyttet til kompetanse vurderes fortsatt som høy. Innsparinger har over flere år skjedd ved naturlig avgang og ved sterke begrensninger i eksternt rekruttering. Det er iverksatt tiltak som omstilling og kompetansekartlegging. På kort sikt gir SSBs økonomiske situasjon at man i 2016 kan benytte innleid eksternt kompetanse ved behov.

Risiko for svikt i markedsfinansierte oppdrag vurderes nå som høy. Risiko for manglende oppdragsfinansiering av EU-pålagte undersøkelser kan på sikt gå ut over annen statistikkproduksjon.

Vi står fremdeles overfor lang feilrettingstid i infrastrukturen og risikoen for driftsstopp/systemfeil vurderes som høy (jf. kap.2).

Risikovurderingen knyttet til den interne organiseringen av arbeidet vurderes fortsatt som høy. Avdeling for IT er omorganisert og det er nå nedsatt en arbeidsgruppe som skal vurdere fremtidig organisering av statistikkproduksjonen og foreslå ny organisasjonsmodell i SSB.

Risiko for sviktende datatilgang, både fra administrative registre og gjennom lav oppslutning om spørreundersøkelser, vurderes fortsatt som høy. Det er videre økt risiko som følge av overgangen til Altinn. Overgangsperioden innebærer økt risiko for at vi ikke får de dataene vi skal ha, samt at deler av omleggingen har blitt forsinket. Omleggingen viser seg også å være mer ressurskrevende enn først antatt. Replanlegging av prosjektet har redusert risikoen noe, men ikke vesentlig da tidsplan er til mars 2017 og mange leveranser gjenstår.

	Risiko	Grad	Tiltak	Frist
1	<p>Kompetanse</p> <p>➤ Risiko for mangelfull kapasitet mht. nødvendig kompetanse.</p> <p>Konsekvens: Kan medføre at kvaliteten på statistikker svekkes, eller at statistikker i ytterste konsekvens må nedlegges</p>	Høy	<p>a. Omstilling gir rom for økt grad av eksternt rekruttering som sikrer tilgang til kritisk kompetanse.</p> <p>b. Kompetansekartlegging, hospitering og intern rotasjon bidrar til at kompetanse utnyttes på tvers i organisasjonen.</p> <p>c. Lean-gjennomgang i seksjoner og standardisering av prosesser gir bedre muligheter for utnyttelse av medarbeidernes kompetanse.</p> <p>d. Bruk av innleid kompetanse på kritiske områder etter behov.</p> <p>e. Tydelige karriereveier og utviklingsmuligheter for medarbeidere med nøkkelkompetanse.</p>	<p>a. Hvert tertial</p> <p>b. Kompetansekartlegging 30.4 og 30.9</p> <p>c. Løpende og ifbm lean-oppfølgning av gevinster</p> <p>d. Konsulenter på IT</p> <p>e. Løpende ihht personalstrategi</p>
2	<p>Kvalitet i statistikken</p> <p>➤ Risiko for alvorlige feil i statistikken</p>	Lav	<p>a. Risiko for alvorlige feil i statistikken vurderes som lavt, jf. beskrivelse</p>	<p>a. Ingen nye tiltak.</p>

	<ul style="list-style-type: none"> ➤ Avvik i Nasjonalregnskapet 	Høy	<p>på slutten av kap.1.</p> <ul style="list-style-type: none"> b. En egen tiltaksplan for å korrigere de avvikene som er oppdaget i Nasjonalregnskapet er under utarbeidelse. 	<ul style="list-style-type: none"> b. Frister iht. plan, ikke endelig p.t.
3	<p>Finansiering</p> <ul style="list-style-type: none"> ➤ Risiko for reduksjon av markedsfinansierte oppdrag. - Offentlige virksomheter får reduserte budsjetter som påvirker oppdragsmengden i SSB ➤ Risiko for manglende oppdragsfinansiering av EU-pålagte undersøkelser <p>Konsekvens: EU-forordnet statistikk, som tidligere er blitt finansiert som markedsoppdrag, kan måtte tilføres midler over statsoppdraget, og det vil gå ut over annen statistikkproduksjon</p>	Høy	<ul style="list-style-type: none"> a. Stillingskontroll og stram budsjettstyring opprettholdes i 2016 b. Tilpasse kostnadsnivået til nye rammer over tid ved bruk av økonomiske reserver og nedbemanning c. Avklare finansieringsmodell for EU forordnede undersøkelser som medfører høye kostnader på eks. datafangstsiden 	<ul style="list-style-type: none"> a. Løpende b. 06-2016. Budsjettrevisjon. c. 03-2016
4	<p>IT-systemer</p> <ul style="list-style-type: none"> ➤ Risiko for driftsstop/systemfeil <p>Konsekvens: Det kan oppstå vansker med å få publisert statistikker, statistikker blir ikke publisert på riktig tidspunkt, statistikker kan få svakere kvalitet</p>	Høy	<ul style="list-style-type: none"> a. Økte investeringer og prioritering av IT (se konkrete tiltak i kap.2) 	<ul style="list-style-type: none"> a. Se frister i kap.2
5	<p>Organisering av arbeidet</p> <ul style="list-style-type: none"> ➤ Risiko for at organiseringen hemmer effektiv produksjon ➤ Risiko for at tverrgående prosesser ikke blir ivaretatt og suboptimalisering <p>Konsekvens: Mindre effektiv statistikkproduksjon som kan gi lavere kvalitet, aktualitet og problemer med å følge opp nye brukerbehov</p>	Høy	<ul style="list-style-type: none"> a. Nedsatt arbeidsgruppe som skal vurdere dagens organisering og foreslå ny organisasjonsmodell b. Gjennomføre fase 2 av Lean som skal omhandle tverrgående prosesser og følge opp Lean- gjennomgangene c. Utvikle porteføljestyringen 	<ul style="list-style-type: none"> a. 02-2016 b. 06-2016 c. Løpende

6	<p>Datatilgang</p> <ul style="list-style-type: none"> ➤ Risiko for sviktende tilgang til dataregistre. Risiko for at statistikkgrunnlag forringes eller forsvinner som følge av forenklingarbeider i andre etater <p>Konsekvens: Det kan oppstå vansker med å få utarbeidet statistikker; det kan ta tid å få ny statistikk, basert på andre kilder, på lufta; statistikker kan få svakere kvalitet, det kan oppstå brudd i tidsserier, etc.</p>	Høy	<ul style="list-style-type: none"> a. Nært samarbeid med registreiere b. Tett oppfølging av forenklingarbeidet i det offentlige c. Tett oppfølging av nye registre for å sikre at SSB får tilgang til data d. Tiltak for å øke brukerkompetansen på nedlasting av data fra APIer 	<ul style="list-style-type: none"> a. Løpende b. Løpende c. Løpende d. 12-2016
7	<p>Datatilgang</p> <ul style="list-style-type: none"> ➤ Risiko for lave svarprosjenter <p>Konsekvens: Kvaliteten på statistikker kan bli svekket, både pga høyt frafall men også på grunn av skjevheter og økt usikkerhet i resultatene. Kostnader til datafangt kan øke dersom man ikke setter inn riktig tiltak tidlig. etc.</p>	Høy	<ul style="list-style-type: none"> a. Sikre tilgang til kontaktinformasjon i Altinn b. Tiltak for å samordne og fordele oppgavebyrden c. Ta i bruk nye kommunikasjonsformer overfor oppgavegiverne d. Etablere samarbeid med postens meldingsformidler for de oppgavegiverne som har reservert seg overfor digital kommunikasjon e. Etablere strategi overfor oppgavegivere som ikke er privatpersoner og som mangler kontaktinformasjon i Altinn 	<ul style="list-style-type: none"> a. Løpende b. 12-2016 c. 12-2016 d. 10-2016 e. 06-2016

Risikokart statistikkproduksjonen

Sannsynlighet	Svært stor					
	Stor					
	Moderat			1,3		
	Liten			2	4,5,7	
	Meget liten				6	
		Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig

Konsekvens

Risiko for feil i publisert statistikk

Det ble i 2015 gjennomført en egen vurdering av risiko for feil i publisert statistikk, basert på en gjennomgang av fire sentrale statistikker (konsumprisindeksen, kvartalsvis befolkningsstatistikk, detaljomsetningsindeksen og utenrikshandel med varer). Jevnt over ble risikoen vurdert som lav.

På bakgrunn av en ny, mindre omfattende gjennomgang høsten 2015 vurderes risikoen for alvorlige feil i publisert statistikk fortsatt som lav. Det er også en positiv utvikling mot færre registrerte feil. I første halvår 2015 var det ingen alvorlige feil, mot tre første halvår 2014 og fem i første halvår 2013. For mindre alvorlige feil var tilsvarende tall henholdsvis 22 i 2015, 21 i 2014 og 66 i 2013.

2. IT

Mål: IT skal sikre stabil drift ut fra organisasjonens definerte leveransenivå. IT-systemene skal gi effektive og standardiserte arbeidsprosesser, samt ivareta krav i lovverket og krav til nasjonal og internasjonal rapportering. IT-systemene skal støtte SSB sin virksomhet- og informasjonsarkitektur. Alle systemer skal leveres i tråd med interne og eksterne brukeres prioriterte behov og krav til kvalitet.

IT-avdelingen skal drives effektivt gjennom gode styringsmodeller, oversiktlig ressursstyring og kompetansebygging.

Risiko	Grad	Tiltak / Oppfølging	Frist
<p>1 Manglende ressurser i driftsseksjonen</p> <p>Konsekvens: Lang rettetid ved feil - forsinkelser i statistikk produksjonen.</p>	Høy	<p>Eksisterende tiltak</p> <ul style="list-style-type: none"> • proaktiv overvåking • automatisert feilhåndtering • pågående bemanningsøkning i driftsseksjonen <p>Forslag til tiltak:</p> <ul style="list-style-type: none"> • Utvide beredskaps- og vaktordningen • Sørg for moderne og tidsriktige SW- og HW-løsninger¹ 	<p>08-2016</p> <p>Løpende etter behov</p>
<p>2 Tjenestenektangrep (DOS/DDOS²)</p> <p>Konsekvens: Angrep på nettverket som gjør systemene midlertidig utilgjengelige – forsinkelser i statistikk-produksjonen.</p>	Modert	<p>Forslag til tiltak:</p> <ul style="list-style-type: none"> • Nærmere vurdering av sannsynlighet og konsekvens, i samråd med forretningssiden i SSB • Ev. vurdere tilgjengelige tjenester for å redusere og fjerne denne type trusler. 	<p>08-2016</p> <p>10-2016</p>
<p>3 Ondsinnnet dataangrep som følge av økt eksponeringen av nettverk og tjenester mot omverden</p> <p>Konsekvens:</p> <ul style="list-style-type: none"> • Datatyveri. • Potensielt skadelig trafikk i nettverket. • Tilliten til SSB svekkes. • Redusere viljen til å avgi data til SSB. • ID-tyveri • Svindel med børssensitiv informasjon • Utilgjengelige tjenester 	Kritisk	<p>Eksisterende tiltak:</p> <ul style="list-style-type: none"> • Streng soneinndeling • Passive sikkerhetsmekanismer i nettverket (brannmur, WEBproxy etc.) <p>Forslag til tiltak:</p> <ul style="list-style-type: none"> • Logging og overvåking av nettverkstrafikk, enten med egne ressurser eller ved kjøp av tjenester til dette formålet • Utvide spektre av sikkerhetsmekanismer, nye brannmurer, aktiv kontroll av enheter som kobles til nettverket • Definere hvordan brannmurregler dokumenteres og implementere dette i driftsorganisasjonene. Lage og implementere rutine for kontroll og godkjenning av hvem som har tilgang. Etablere 	<p>09-2016</p> <p>09-2016</p> <p>04-2016</p>

¹ SW= Software, HW= Hardware

² DOS=Denial-of-Service, DDOS= Distributed Denial-of-Service

			rutiner for etterlevels-kontroll.	
4	Utdatert SW og HW Konsekvens: <ul style="list-style-type: none"> Eksisterende sikkerhetshull i utdatert SW/HW utnyttes til ondsinnet dataangrep. Ustabile og trege systemer Datatyveri Lang rettetid 	Kritisk	Se også tiltak under punktene 1 og 3 Forslag til tiltak: <ul style="list-style-type: none"> Etablere klar policy på frekvens for oppgradering og patching av anskaffet programvare Definere og implementere rutiner og prosedyrer for systematisk rullering av HW Skaffe nødvendige ressurser til gjennomføring av tiltakene på permanent basis, ref. tiltak under punkt 1. 	08-2016 06-2016 06-2016
5	Begrenset kapasitet til forvaltning av IT-systemer og fagapplikasjoner som benyttes i statistikkproduksjonen Konsekvens: <ul style="list-style-type: none"> Lang rettetid ved feil i statistikkproduksjon Begrenset mulighet til å understøtte nye utviklingsbehov i statistikkproduksjonen Forhindrer effektivisering av statistikkproduksjonen Høy drift- og forvaltningskost over tid 	Høy	Forslag til tiltak: <ul style="list-style-type: none"> Sikre rett prioritet av kritiske forvaltningsoppgaver. Sikre rett bemanning gjennom: <ul style="list-style-type: none"> Kartlegging av system- og applikasjonsporteføljen Kartlegging av kompetanse- og kapasitetssituasjon pr. applikasjon og system. På bakgrunn av kartlegging skal kritiske behov for økning av kompetanse og kapasitet identifiseres og tiltaksplaner utarbeides. 	06-2016 12-2016
6	Mangler samordnet og helhetlig prioritering av utviklingsoppgaver i IT Konsekvens: <ul style="list-style-type: none"> Forsinkelser av IT-leveranser. Kostnadsoverskridelser i leveransene Ineffektiv ressursbruk IT-kapasitet anvendes ikke i tråd med strategiske prioriteringer i SSB 	Høy	Forslag til tiltak: <ul style="list-style-type: none"> Etablering av helhetlig styringsmodell for SSBs prioritering av anvendelse av IT-ressurser. 	10-2016

7	Mangelfull ressursstyring i IT Konsekvens: <ul style="list-style-type: none"> IT-kapasitet anvendes ikke i tråd med strategiske prioriteringer i SSB Forsinkelser av IT-leveranser. Kostnadsoverskridelser i leveransene Ineffektiv ressursbruk 	Høy	Forslag til tiltak: <ul style="list-style-type: none"> Sentralisering av bestillingsmottak og ansvar for ressursstyring i IT Etablering av felles metodikk og verktøystøtte for ressursstyring i IT. 	09-2016 09-2016
8	Mangelfull kompetanse til gjennomføring av utviklingsprosjekter Konsekvens: <ul style="list-style-type: none"> Forsinkelser i gevinstuttak Kostnadsoverskridelser i leveransene Ineffektiv utnyttelse av IT-kapasitet 	Høy	Eksisterende tiltak: <ul style="list-style-type: none"> Opplæring av prosjektledere i SSBs prosjektmetodikk. Forslag til tiltak: <ul style="list-style-type: none"> Sentralisering av ansvar for forvaltning og utvikling av prosjektmetodikk i SSB. Etablering av metodikk for kvalitetssikring av etterlevelse av metode for prosjektstyring i SSB. Opplæring av sentrale ressurser i eierstyring av prosjekter. 	04-2016 09-2016 06-2016

Risikokart IT

Sannsynlighet	Svært stor					
	Stor			5,6,7		
	Moderat			1,8		3
	Liten			2		4
	Meget liten					
		Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
Konsekvens						

3. Økonomiforvaltning og innkjøp

Mål: Pålitelig og oversiktlig økonomiforvaltning, effektive anskaffelser i henhold til gjeldende regelverk og i samsvar med SSBs innkjøpsstrategi.

Endring: Det er i 2015 innført klarere ansvarsforhold innen arbeidsoppgaver på økonomiområdet. Risikoen for feil i regnskapet er dermed redusert. DFØ har gjennomført sin omorganisering, og vi anser ikke risikoen knyttet til kompetanse og bemanning som høy, da SSB benytter standardssystemer og det er enkelt å rekruttere nye personer om nødvendig. Risiko knyttet til kompetanse og bemanning på økonomiområdet er derfor redusert til liten.

Vi har i risikovurderingen vurdert feil i eksternregnskap og regelbrudd til moderat, men har likevel en rekke tiltak for å forbedre områdene. Det samme gjelder for anskaffelsesområdet, som har et såomfattende og komplisert regelverk at sannsynligheten er stor for at man kan glippe på overholdelsen.

	Risiko	Grad	Tiltak / Oppfølging	Frist
1	Kompetanse og bemanning ➤ Risiko for lite ressurser og manglende kompetanse i regnskap og bruk av Agresso med tilhørende system ➤ Manglende ressurser hos DFØ Konsekvens: Kortvarig produksjonsutfordring, økonomisk ulempe ved eventuell innleie.	Lav	a. Kompetanseutvikling av medarbeidere, bla. i bruk av Agresso b. Definere roller og ansvar i forbindelse med utføring av økonomioppgaver c. Jevnlige statusmøter med DFØ og tett oppfølging av bestillinger	a. Løpende b. 05-2016. Nye stillingsbeskrivelser c. Løpende

2	<p>Feil i eksternt regnskapet</p> <ul style="list-style-type: none"> ➤ Mange delsystem og forsystemer til Agresso og manglende/dårlige systemløsninger ➤ Feil kontering og bokføring i Basware og Agresso ➤ Feil ved utbetaling til leverandør ➤ Manglende fakturering til kunder, særlig knyttet til oppdragsinntekter ➤ SSB har både kontant og periodisert regnskap, feil i avstemming mellom disse <p>Konsekvens: Konsekvenser for omdømme og mulige økonomiske konsekvenser (ved feilutbetalinger etc).</p>	Moderat	<ul style="list-style-type: none"> a. Utvikle økonomi-controllerfunksjonen b. Tett oppfølging og samarbeid med DFØ og andre statlige etater c. Avstemming og kontroll av kontoer d. Utarbeide gode rapporter som kan følges opp på alle nivåer e. Oppfølging og analyse av oppdragsinntekter f. Gjennomgang av kontrakter med kunder 	<ul style="list-style-type: none"> a. 07-2016. b. 2 møter i økonomiforum pr år c. Løpende d. 04-2016 e. 06-2016 f. 06-2016
3	<p>Regelverk og rutiner</p> <ul style="list-style-type: none"> ➤ Risiko for at regelverk og rutiner ikke følges <p>Konsekvens: I ytterste konsekvens kan dette påvirke omdømmet (FIN, DFØ, etc).</p>	Moderat	<ul style="list-style-type: none"> a. Gjennomført internkontrollpilot b. Gjennomgang og vedlikehold av rutiner c. Opplæring i Økonomireglementet 	<ul style="list-style-type: none"> a. 12-2016 b. 12-2016 c. Løpende (kurs DFØ)
4	<p>Mislighold</p> <ul style="list-style-type: none"> ➤ Risiko for misligheter utover det som er nevnt i risikoen om informasjonssikkerhet (kap.4. punkt 1). <p>Dette gjelder risiko for misligheter knyttet til innkjøp, reiseregninger, telefoner, rekvisita m.m., herunder også korrupsjon.</p> <p>Konsekvens: Økonomiske konsekvenser, omdømme og personalsak.</p>	Lav	<ul style="list-style-type: none"> a. Utvikling av økonomi-controllerfunksjonen b. To personer sjekker hver faktura og reiseregning c. Oppfølging av alle anskaffelser d. Kontroller knyttet til sluttgodkjenning av fakturaer og kontroll av utbetalinger e. Innarbeide en hensikts-messig fullmakts-struktur 	<ul style="list-style-type: none"> a. 07-2016 b. Løpende og innført c. 05-2016: Nytt system house of control d. Sluttkontrollen er innført. Løpende. e. Ferdig i 2015, oppdateres løpende.

5	<p>Anskaffelser</p> <ul style="list-style-type: none"> ➤ Risiko for at regelverk og rutiner ikke følges ➤ Risiko for feil i anskaffelsesprosessene ➤ Risiko for dårlige avtaler ➤ Risiko for at SSB saksøkes på grunn av feil i anskaffelsesprosess ➤ Risiko for negativ omtale i media på grunn av omgåelse av regelverket ➤ Risiko for manglende sporbarhet fra bestilling til faktura <p>Konsekvens: Økonomiske konsekvenser, omdømme og manglende tillit i leverandørmarkedet.</p>	Moderat	<ul style="list-style-type: none"> a. Vedta nye, oppdaterte rutiner for innkjøp og få disse forankret og implementert i organisasjonen b. Benytte e-handelsløsninger aktivt på de innkjøp hvor det er egnet c. Sentralisere mer av innkjøpsarbeidet, herunder anbud og bestillinger 	<ul style="list-style-type: none"> a. Vedtatt, implementeres innen 1.7 pga ny ansattelse b. Utført og løpende c. 07-2016
---	--	---------	--	---

Risikokart økonomiforvaltning og innkjøp

Sannsynlighet	Svært stor					
	Stor					
	Moderat		3,5			
	Liten		1,4	2		
	Meget liten					
		Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
		Konsekvens				

4. Sikkerhet

Mål: Tilfredsstillende sikkerhet i SSB

Endring: En ny Risiko- og sårbarhetsanalyse er planlagt gjennomført i oktober og november 2015. Resultatene fra denne vil i stor grad påvirke vår risikoanalyse på sikkerhetsområdet og risikovurderingene for 2016 vil oppdateres på bakgrunn av dette.

	Risiko	Grad	Tiltak / Oppfølging	Frist
1	<p>Manglende integritet og konfidensialitet³ – interne forhold.</p> <p>Uautorisert tilgang til/ endring av data fra interne</p> <ul style="list-style-type: none"> • Feilsending av mail • Annen lekkasje av data <p>Konsekvens:</p> <ul style="list-style-type: none"> • Tilliten til SSB svekkes • Reduserer viljen til å avgi data til SSB • Svindel med børs-sensitiv informasjon 	Kritisk	<p><u>Med hensikt:</u></p> <p>a. Ved stopp av arbeidsforhold: Avstemming mellom SAP og AD⁴ halvårlig løpende.</p> <p>b. Vurdere behovet for nye tiltak mot utro tjenere ila 2015/2016.</p> <p>c. Ved intern flytting: Tydeliggjøre ansvar og rutiner for LDA⁵/ seksjonsleder vedr. avstemming og tilgang til egne data.</p> <p><u>Med/uten hensikt:</u></p> <p>a. Teste sporingen i filslusa.</p> <p>b. Bestemme nivå for logging og gjenfinning i logger. Deretter gjennomføre prosjektet for forbedring av logger sammen med IT-avdelingen.</p>	<p>a. Løpende</p> <p>b. 04-2016</p> <p>c. 05-2016</p> <p>a. Utført</p> <p>b. 09-2016</p>
2	<p>Manglende integritet og konfidensialitet – eksterne forhold</p> <p>Uautorisert tilgang til/ endring av data fra eksterne</p>		<p>a. Jf. tiltak under risikovurdering for IT, id3.</p>	<p>a. Se kap.2.</p>

³ Informasjonssikkerhet i SSB (fra sikkerhetshåndboken i SSB, side 6) omfatter sikring av:

- Konfidensialitet - at informasjonen kun er tilgjengelig for autoriserte personer og/eller systemer og at det på forhånd er foretatt en gyldig identifisering og autentisering.
- Integritet - at informasjonen ikke blir endret eller slettet på uautorisert måte.
- Tilgjengelighet - at informasjonen eller dataressurser er til stede, stabile og anvendelige for brukere etter behov.

⁴ SAP er lønns- og personalsystem, AD = Active directory

⁵ LDA= Lokal dataadministrator

3	<p>Manglende tilgjengelighet</p> <ul style="list-style-type: none"> • Strømstans <p>Brudd på tverrsamband Dette punktet tar ikke for seg manglende tilgjengelighet på enkeltjenester – kun at større deler av infrastrukturen faller ut.</p> <p>Konsekvens: Nedsatt tilgjengelighet på datatjenester, lavere produktivitet.</p>	Høy	<p>a. Teste nødstrøm (Oslo og Kongsvinger) og teste at reservedatarom kan overta produksjon av datatjenester. Eventuelt iverksette tiltak.</p> <p>b. Teste «restore»</p>	<p>a. 05-2016</p> <p>b. Løpende</p>
4	<p>Fysisk sikkerhet</p> <p>Risiko for omfattende brann, oversvømmelse eller naturkatastrofe</p> <p>Konsekvens: I ytterste konsekvens tap av liv. Ellers manglende tilgjengelighet på datatjenester, lavere produktivitet.</p>	Høy	<p>a. Evakueringsøvelser i Oslo og Kongsvinger i 2016</p> <p>b. Videreføre avtale om alternative lokaler</p>	<p>a. Løpende</p> <p>b. Løpende</p>
5	<p>Fysisk sikkerhet</p> <p>Innbrudd med tyveri av materielle ting uten tilgang til data</p> <p>Konsekvens: Økonomisk konsekvens for SSB (vurdert som liten).</p>	Lav	<p>a. Ingen nye tiltak</p>	
6	<p>Manglende sikkerhetskompetanse og bevissthet</p> <p>Dette gjelder først og fremst mangelfull kompetanse om sikkerhet blant medarbeiderne, både for å unngå sikkerhetsbrudd og for å følge opp ev. slike.</p> <p>Konsekvens: Kan medføre omdømmetap dersom sensitive data kommer på avveie, ellers manglende produktivitet.</p>	Høy	<p>a. Vurdere en øvelse ila 2016</p> <p>b. Vurdere weblæringskurs for alle ansatte i 2016.</p>	<p>a. 12-2016</p> <p>b. 09-2016</p>
7	<p>Terror</p> <ul style="list-style-type: none"> • SSB rammes av et terrorangrep gjennom et generelt angrep på statlige virksomheter • SSB rammes av et terrorangrep spesielt rettet mot SSB • SSB rammes av et fysisk angrep fra en oppgavegiver • SSB rammes av et terrorangrep der SSB 	Høy	<p>a. Gjennomgang av sikkerhetsløsninger i Oslo. Iverksette eventuelle tiltak.</p> <p>b. Gjennomgang av retningslinjer for kontakt med media. Iverksette eventuelle tiltak.</p> <p>c. Videreføre avtale om alternative lokaler</p> <p>d. Vurdere øvelse ila 2016</p>	<p>a. Løpende</p> <p>b. 12-2016</p> <p>c. Løpende</p> <p>d. 12-2016</p>

	ikke inngår i målgruppen			
	Konsekvens: I ytterste konsekvens tap av liv. Ellers manglende tilgjengelighet på datatjenester, lavere produktivitet.			

Risikokart sikkerhet

Sannsynlighet	Svært stor					
	Stor					
	Moderat					
	Liten		5		3,6	1
	Meget liten					4,7
		Ubetydelig	Lav	Moderat	Alvorlig	Svært alvorlig
	Konsekvens					

Statistisk sentralbyrå

Postadresse:
Postboks 8131 Dep
NO-0033 Oslo

Besøksadresse:
Akersveien 26, Oslo
Oterveien 23, Kongsvinger

E-post: ssb@ssb.no
Internett: www.ssb.no
Telefon: 62 88 50 00



Statistisk sentralbyrå
Statistics Norway