FINANSDEPARTEMENTET

Risikoanalyse i arkivarbeidet – Ta sjansen?

Jorunn Bødtker, 23. mars 2010

Begreper

Norsk standard 5814:2005 og ISO 27002

Risiko: Muligheten for å lide tap eller skade

- Risikostyring: Koordinerte aktiviteter for å styre og kontrollere en virksomhet med hensyn til risiko
- Risikovurdering: Samlet prosess som består av risikoanalyse og risikoevaluering
- Risikoanalyse: Systematisk bruk av informasjon for å identifisere kilder og anslå risiko
- Risikoevaluering: prosess for å sammenligne anslått risiko med gitte risikokriterier for å bestemme risikoens betydning
- Risikohåndtering: Prosess for å velge og iverksette tiltak som skal endre risiko

Ulike lover – ulike krav til risikohåndtering

Noen eksempler

- Eforvaltningsforskriften
- Esignaturforskriften
- Esignaturloven
- Forskrift om risikostyring og internkontroll
- Forvaltningsloven
- Helsepersonelloven
- Helseregisterloven
- IKT-forskriften
- Kommuneloven
- personopplysningsforskriften
- Personopplysningsloven
- Reglement for økonomistyring i staten
- Sikkerhetsloven m/forskrifter

Arkivregelverket - eksempel

FOR 1999-12-01 nr 1566: Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver.

Kapittel IX: Elektronisk arkivering av saksdokumenter

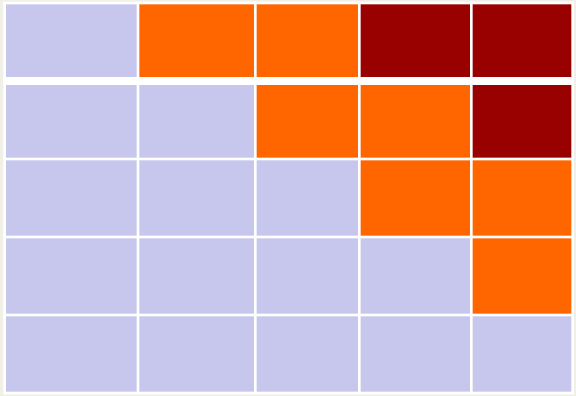
- B. Krav til systemer, formater og lagringsmedier
- C. Krav til organisering og rutiner

Arkivarbeidet – risikovurdering både i drift og utviklingsarbeid

- Analyse av den daglige driften
- Analyse – før innføring av nye prosjekter

- Akseptabelt risikonivå er en ledelsesbeslutning!

Risikomatrise



Sannsynlighet/konsekvens

meget lav/lav/moderat/høy/meget høy

hendelser (nummerert)

Hendelse: Ufullstendig offentlig postjournal

- Mulige årsaker: Manglende eller sein journalføring, særlig av e-post adressert til den enkelte ansatte
- Sannsynlighet: Høy
- Konsekvens: Moderat - avhengig av hva saken gjelder. Tap av omdømme, kritikk fra presse, tilsynsmyndighet eller granskere
  - Tiltak for å redusere *sannsynligheten* for hendelsen:
    - Brukeropplæring, informasjon, mer brukervennlige systemer, etablering av felles rutiner for journalføring og arkivering
  - Tiltak for å redusere *konsekvensen* av hendelsen:
    - ”Legge seg flat med én gang” – journalføre og produsere ny versjon av offentlig journal

Hendelse: Feilutsendelse av e-post (taushetsbelagte eller unntatte opplysninger)

- Mulige årsaker: ”menneskelig feil”, dårlige systemer
- Sannsynlighet: Lav
- Konsekvens: Moderat / høy avhengig av hva saken gjelder. Erstatningssøkmål, tap av omdømme, kritikk fra presse, tilsynsmyndighet eller granskere
  - Tiltak for å redusere *sannsynligheten* for hendelsen:
    - Sperre i systemene mot å sende ut forhåndsklassifiserte dokumenter, soneløsning, forsinkelse i e-post, slå av gjettefunksjon, to-leddet ekspedering, ”arbeid i fred og ro”
  - Tiltak for å redusere *konsekvensen* av hendelsen:
    - Tilbakekalle e-post, varsle internt om hendelsen, varsle eksternt om hendelsen

Hendelse: Feilpublisering av dokumenter på nett

- Mulige årsaker: ”menneskelig feil”, dårlige systemer og rutiner
- Sannsynlighet: Lav
- Konsekvens: Moderat / høy avhengig av hva saken gjelder. Erstatningssøkmål, tap av omdømme, kritikk fra presse, tilsynsmyndighet eller granskere
  - Tiltak for å redusere *sannsynligheten* for hendelsen:
    - Opplæring, informasjon, rutiner, forsinkelser i publisering, to-leddet publisering, forhåndsvisning
  - Tiltak for å redusere *konsekvensen* av hendelsen:
    - Slette på nettsted
    - Ta kontakt med søkemotorene

Hendelse: Arkiv- og saksbehandlingssystemet ikke tilgjengelig

- Mulige årsaker: Feil eller feil ved retting/oppdatering av systemet. Mangelfull testing og pilotdrift. Mangelfulle rutiner ved drift. Feil på applikasjons- eller databaseserver.
- Sannsynlighet: Moderat
- Konsekvens: Moderat / Høy avhengig av omfang, varighet og tidspunkt.
  - Tiltak for å redusere *sannsynligheten* for hendelsen:
    - Bedre IKT-infrastruktur, clusterløsning, kopiere (deler av) databasen til test- eller kursdatabasen, etablere gode driftsrutiner internt og ha avtaler med kompetent tredjepart.
  - Tiltak for å redusere *konsekvensen* av hendelsen:
    - Hente på forespørsel dokumenter fra test- eller kursdatabasen, utlevere originaldokumenter (inngående post), hente ut lokalt lagrede filer
-

Eksempel – risikooppfølging i et anskaffelsesprosjekt

- Avdelingene bidrar ikke med avtalte prosjektressurser
  - Forankring i styringsgruppen.
  - Direkte kontakt med styringsgruppens deltakere.
- For stram tidsplan til evaluering- og forhandlingsfasen for å oppnå ønsket kvalitet
  - Endring av milepæler med forankring i styringsgruppen.
  - Følge opp fremdrift
- Prosjektets deltakere har ikke riktig kompetanse til å foreta evaluering- og forhandlingsoppgavene
  - Involvere personer med kompetanse fra kravspesifikasjonsarbeidet samt bruk av spisskompetanse ved behov.
- Avdelingene ønsker ikke å binde seg til ny løsningen.
  - Involvere avdelingene i alle faser av prosjektet inklusiv en aktiv styringsgruppe.

Eksempel – anskaffelsesprosjekt (forts.)

- Manglende samordning med IKT–prosjekt
  - Kontinuerlig dialog med prosjektet for å sikre implementering av ny elektronisk saksbehandlerløsning
- Velger en løsning som er på vei ut/velger løsning basert på gale kriterier
  - Involvere spisskompetanse i evalueringsarbeidet.
- Tilbyderne forstår ikke leveransens omfang
  - Klargjøre dette i forhandlingsmøtene
  - Strukturert og gjennomarbeidet konkurransegrunnlag
- Velger komplisert system med høy brukerterskel.
  - Legger stor vekt på brukervennlighet ved tildeling av kontrakt.

Nyttig informasjon - eksempler

- Senter for statlig økonomistyring (SSØ)
  http://www.sfso.no/templates/Page____141.aspx

- Datatilsynet – Risikovurdering av informasjonssystem
  http://www.datatilsynet.no/upload/Dokumenter/veiledere/Risikoveileder_pdf.pdf
- Nasjonal sikkerhetsmyndighet (NSM)
  https://www.nsm.stat.no/Documents/Veiledninger/ROS_2004_veiledning.pdf