|  |  |  |
| --- | --- | --- |
| Bilag 8: Eksempel på risikovurderingsrapport – bør justeres til organisations kontekst før brug |  |  |
|  |  |

# Risikovurdering af [system]

I forbindelse med [indkøb/udbud/udvikling] af it-systemer i [organisationen] skal der gennemføres en risikovurdering af det planlagte system.

Ejer af procedure: [kontor/enhed]

Dato for ikrattrældelse: [dato]

Godkendt af: [Informationssikkerhedsudvalget]

Næste planlagte revision: [dato]

[Eller:

Som et led i informationssikkerhedsarbejdet i [organisationen], skal systemer i drift risikovurderes med passende mellemrum.]

Jf. [organisationens] informationssikkerhedspolitik, udarbejdes risikovurderinger på informationssikkerhedsområdet med det formål at:

* [Anfør krav til risikovurdering jf. organisationens informationssikkerhedspolitik]

I denne rapport beskrives resultaterne af risikovurderingen. Risikovurderingen er foretaget ud fra spørgerammen i skema [xx] med deltagelse af repræsentanter fra [kontor(er)/enhed(er)].

## Beskrivelse af systemet

I forbindelse med risikovurderingen er der udarbejdet en beskrivelse af systemet og dets formål. Beskrivelsen er vedlagt i bilag [xx] og kan opsummeres som følgende:

* [Systemets formål – hvilken proces understøtter den]
* [Type af data, der behandles i systemet, og hvilke informationer det omhandler]
* [Infrastrukturelle lag, som anskaffelsen vedrører]
* [Hvem der skal hoste systemet ekstern leverandør/SIT]
* [Hvis systemet er en cloud-anskaffelse, angives det også]
* [Evt. hvor mange brugere der forventes at være af systemet]
* [Øvrig information]

## Proces for risikovurderingen

Processen og metoden for risikovurderingsarbejdet er fastlagt i bilag [xx].

[Kontor/enhed] har faciliteret risikovurderingen via en række workshops med deltagelse fra de øvrige fagkontorer. Workshoppene har indeholdt følgende trin:

### Konsekvensvurdering

[Metoden beskrives]

### Trussels-, sårbarheds-, og sandsynlighedsvurdering

[Metoden beskrives]

### Risikoberegning

[Metoden beskrives]

## Resultater

### Konsekvensvurdering

[Resultaterne for konsekvensvurderingen beskrives]

### Vurdering af konsekvenser for [organisation] ved brud på F-I-T

Konsekvensvurderingen viser, at informationssikkerhedsbrud på [system] i værste fald kan få [angiv højeste konsekvensniveau] konsekvenser for [organisationen].

Vurderingen viser overordnet at:

Fortrolighedsbrud:

* Det er vurderet, at et fortrolighedsbrud (fx ved [gengiv kort relevant scenarie]) kan få [angiv højeste konsekvensniveau]konsekvenser for [organisationens] [gengiv konsekvenstyper].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

Integritetsbrud:

* Det er vurderet, at et integritetsbrud (fx ved [gengiv kort relevant scenarie]) kan få [angiv højeste konsekvensniveau]konsekvenser for [organisationens] [gengiv konsekvenstyper].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

Tilgængelighedsbrud:

* Det er vurderet, at et tilgængelighedsbrud (fx ved [gengiv kort relevant scenarie]) kan få [angiv højeste konsekvensniveau]konsekvenser for [organisationens] [gengiv konsekvenstyper].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

### Vurdering af konsekvenser for registrerede personer ved brud på F-I-T

For de registrerede vurderes det, at et informationssikkerhedsbrud i værste fald kan få [angiv højeste konsekvensniveau] konsekvenser for den registrerede. Det høje konsekvensniveau er forbundet med [uddyb sammenhæng mellem konsekvensniveau og mængden og typen af persondata].

Fortrolighedsbrud:

* Det er vurderet, at et fortrolighedsbrud i værste fald kan få [angiv højeste konsekvensniveau*]* [uddyb konsekvenstyper] konsekvenser for den registrerede [kort beskrivelse af scenarie].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

Integritet:

* Det er vurderet, at et integritetsbrud i værste fald kan få [angiv højeste konsekvensniveau*]* [uddyb konsekvenstyper] konsekvenser for den registrerede [kort beskrivelse af scenarie].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

Tilgængelighed:

* Det er vurderet, at et integritetsbrud i værste fald kan få [angiv højeste konsekvensniveau*]* [uddyb konsekvenstyper] konsekvenser for den registrerede [kort beskrivelse af scenarie].

Vurderingen af den enkelte parameter uddybes i bilag [xx].

*Sårbarheds- og sandsynlighedsvurdering*

Illustrationen nedenfor viser en oversigt over, hvordan de samlede vurderede sårbarheder fordeler sig som risici på overordnet set [antal] risikoniveauer.

[redegør for evt. omstændigheder eller forbehold i vurderingen, som er væsentlige for de fremkomne resultater]

### I tabel 1 opsummeres de sårbarheder, som er vurderet at have et middel risikoniveau eller højere. Den fulde oversigt med bemærkninger og begrundelser fremgår af bilag [xx] (spørgeramme):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Nr.** | **Sårbarhed** | **Sandsynlighed** | **Fortrolighed** | **Integritet** | **Tilgængelighed** | **Risiko** | **Igangsat risikomitigerende aktiviteter** |
| Sx |  |  |  |  |  |  |  |
| Sx |  |  |  |  |  |  |  |

## Konklusion

[Fremhæv konklusionerne fra risikovurderingen]

## Sikkerhedsmæssige foranstaltninger

Nedenfor i tabel 2 er opstillet forslag til sikkerhedsforanstaltninger i forhold til de risici, der er nævnt i tabel 1. Det er [kontor/enheds] vurdering, at de foreslåede sikkerhedsforanstaltninger, vil kunne nedbringe de enkelte risici til et acceptabelt niveau. [Kontor/enhed] anbefaler dog samtidigt, at der fortsat er særligt opmærksomhed på de konkrete risici ved opfølgningen på denne risikovurdering.

### Tabel 2: Anbefalede sikkerhedsforanstaltninger

|  |  |  |
| --- | --- | --- |
| Anbefalingsnr. | Sårbarhed | Anbefalede sikkerhedsforanstaltninger/tiltag |
| Ax |  |  |
| Ax |  |  |

## Håndtering af risici

[Udfyldes af fagkontoret, når det er besluttet, hvilke risici, der ønskes håndteret, og evt. på hvilken måde. Beslutning om accept af risici samt manglende handling begrundes]