

	Konfidentialitet Skyddsomål att innehållet i informationsobjekt (eller ibland dess existens) inte får göras tillgängligt eller avslöjas för obehöriga	Riktighet Skyddsomål att information inte förändras, vare sig obehörigen, av misstag eller på grund av funktionsstörning	Tillgänglighet Skyddsomål där informationstillgångar skall kunna utnyttjas i förväntad utsträckning och inom önskad tid	Spårbarhet Skyddsomål där det ska vara möjligt att i efterhand härleda hur uppgifter har behandlats och av vem
1	Röjande av uppgifterna medför ingen, försumbar eller måttlig skada för verksamheten eller enskilda personliga förhållanden. Systemet innehåller i huvudsak allmänna offentliga handlingar. Systemet är avsedd för bred spridning/ publicitet. Systemet innehåller inte personuppgifter. Den enskilde kan själv ansvara för uppgifterna	Information som obehörigen, av misstag eller på grund av funktionsstörningen ändrats medför ingen, försumbar eller måttlig skada för verksamheten eller enskilda personliga förhållanden. Systemet innehåller uppgifter som med begränsad insats kan återställas. Förändringarna bedöms inte leda till negativ publicitet för verksamheten eller skadeståndsanspråk.	Ett avbrott medför ingen, försumbar eller måttlig skada för verksamheten eller enskilda personliga förhållanden. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas endast i begränsad omfattning av otillgänglighet i systemet. Systemet kan vara otillgängligt i ett par dygn med måttlig inverkan på myndighetsutövningen.	Att spårbarhet saknas medför endast ingen, försumbar eller måttlig skada för verksamheten eller enskilda personliga förhållanden. Möjligheten att härleda vad som har hänt i systemet vid förändringar av uppgifter, incident eller säkerhetsincident bedöms vara oviktigt.
2	Röjande av uppgifterna kan medföra kännbar skada för verksamheten eller enskilda personliga förhållanden. Systemet innehåller arbetshandlingar som kan bli föremål för sekretess enligt OSL, information avsedd för internt bruk eller personuppgifter enligt PUL.	Information som obehörigen, av misstag eller på grund av funktionsstörningen ändrats medför kännbar skada för verksamheten eller enskilda personliga förhållanden. Systemet ingår i myndighetsutövningen eller innehåller uppgifter som omfattas av krav på oavslöshet, tex lagrum där riktighetskrav anges. Förändringar av uppgifter bedöms kunna leda till negativ publicitet för verksamheten eller skadeståndsanspråk.	Ett avbrott medför kännbar skada för verksamhetens förmåga att bedriva sin myndighetsutövning (kärnverksamheten) eller enskilda personliga förhållanden. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en betydande omfattning av otillgänglighet i systemet. Systemet kan vara otillgängligt i ett par timmar utan negativ inverkan på verksamheten.	Att spårbarhet saknas medför kännbar skada för verksamheten eller enskilda personliga förhållanden. Möjligheten att härleda vad som har hänt i systemet vid förändringar, incident eller säkerhetsincident bedöms vara viktigt. Spårbarhet ska finnas för att påvisa på vilket sätt information har behandlats i systemet och av vem.
3	Röjande av uppgifterna kan medföra allvarlig skada för verksamheten eller enskilda personliga förhållanden. Systemet innehåller information som är föremål för sekretess enligt OSL, känsliga personuppgifter, andra lagrum eller tystnadsplikt. Systemet kan innehålla uppgifter om ekonomiska transaktioner, persondossier med skyddade uppgifter (elevregister, brukarregister) eller uppgifter som omfattas av säkerhets- och bevakningssekretess.	Information som obehörigen, av misstag eller på grund av funktionsstörningen ändrats medför allvarlig skada för verksamheten eller enskild. Systemet innehåller uppgifter där hanteringen styrs av specifika lagparagrafer, känsliga personuppgifter eller hälso sjukvård. Förändringar av uppgifter bedöms leda till allvarlig påverkan för egen eller annan organisation eller för enskild individ och kan sannolikt leda till skadeståndsanspråk.	Ett avbrott medför allvarlig skada för verksamhetens förmåga att bedriva sin myndighetsutövning (kärnverksamheten) eller enskild. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en allvarlig/katastrofal omfattning av otillgänglighet i systemet. Systemet kan vara otillgängligt i upp till en timme per år utan negativ inverkan på verksamheten.	Att spårbarhet saknas medför allvarlig skada för verksamheten eller enskild. Möjligheten att härleda vad som har hänt i systemet vid förändringar, incident eller säkerhetsincident bedöms vara mycket viktigt. Spårbarhet ska finnas för alla specificerade händelser i systemet, att titta på tex. närståendes information är ett brott och ska generera ett larm. Revisionskrav, lagar eller förordningar ställer krav på spårbarhet och/eller oavslöshet.
4	Röjande av uppgifterna kan medföra allvarlig skada för rikets säkerhet Systemet innehåller information som omfattas av sekretess och rör rikets säkerhet och som där påverkan av informationen ger oöverskådliga konsekvenser och är katastrofala för verksamhetens förmåga att fullfölja sitt uppdrag, eller där omfattande fara för liv och hälsa föreligger.	Information som obehörigen, av misstag eller på grund av funktionsstörningen ändrats kan antas medföra allvarlig skada eller skada för rikets säkerhet som inte är ringa. Information som kan bli sekretess enl. KAP 15 § 1-2 (hemliga uppgifter enligt rikets säkerhet). Information som skulle kunna nyttjas för spioneri, sabotage, förberedelse för terroristbrott eller andra brott som kan hota rikets säkerhet.	Ett avbrott påverkar nationell kritisk infrastruktur och kan antas medföra allvarlig skada för centrala samhällsfunktioner. Den egna medför allvarlig skada för verksamhetens förmåga att bedriva sin myndighetsutövning (kärnverksamheten) eller enskild. Den egna verksamhetens och andra organisationers förmåga att upprätthålla ett centralt samhällsansvar påverkas i allvarlig/katastrofal omfattning av otillgänglighet i informationssystemet/infrastrukturen	Att spårbarhet saknas kan antas medföra allvarlig skada eller skada för rikets säkerhet som inte endast är ringa. Möjligheten att härleda vad som har hänt med informationen vid förändringar, incident eller säkerhetsincident bedöms vara av yttersta vikt