Kravnr	Kravställning	Beskrivning	Generella kommentarer till kravställningen och vägledning		Kontrollpunkter i checklista
1	**Informationsmodellering och klassificering**				
1.1	**Informationsmodell**	Organisationen upprätthåller en informationsmodell för systemet, som omfattar och beskriver samtliga informationsobjekt i systemet.	Organisationen ska ha överblick över och kännedom om all information som ska lagras i och utgör systemet, och kan presentera den i en informationsmodell som är begriplig och fullständig, till exempel utifrån vilken information som utgör allmänna handlingar och kan lämnas ut som sådana.		Informationsmodellen täcker all information i systemet och definierar hur informationsobjekten ser ut.
			Informationsmodellen ska presentera informationsobjekten med koppling till organisationens hela informationsbestånd.		Informationsobjekten i modellen relaterar till handlingstyper i organisationens informationsbestånd.
			Relationen mellan informationsmodell och struktur för användergrupper och roller för systemet kan användas för att identifiera primära och sekundära användare.		Informationsmodellen relaterar till användargrupper och rollmodell.
					Informationsobjekten beskrivs tillräckligt utifrån användarnas behov.
					Informationsmodellen inkluderar all metadata som hanteras i systemet (beskrivande metadata, teknisk metadata och kontextuell metadata).
					Informationsmodellen är tillgänglig och uppdateras vid behov.
1.2	**Informationsvärdering**	Organisationen har värderat informationen i systemet utifrån definierade värden och risker.	Organisationen måste ha förståelse för syftet för insamling av information och hur den ska tillgängliggöras. Sådana insikter gör det möjligt för organisationen att avgöra vilka informationsobjekt som ska förvaltas på lång sikt och vilka som inte ska det.		Alla information i systemet är värderad.
			Värderingen sker utifrån värde för allmänheten (det demokratiska värdet), värde för den arkivbildande organisationen (det organisatoriska värdet) och värde för forskning och kulturarv (det källkritiska värdet).		Informationsvärdet är angivet för alla informationsobjekt i systemet.
			Värdering, klassificering och riskanalyser inom ramen för informationssäkerhetsarbetet bör användas som grund.		Bedömningen som ligger bakom informationsvärderingen är tillräcklig och begriplig för användarna
1.3	**Bevarandeplanering**	Organisationen har upprättade bevarandeplaner att tillämpa för informationen i systemet.	Bevarandeplaneringen bygger på bevarande- och gallringsutredningar för informationen i systemet. Bevarandeplanerna redogör för åtgäder för bevarande under den tid informationen ska finnas tillgänglig. Med åtgärder för bevarande avses här till exempel konvertering och migrering.		Organisationen har upprättat en strategisk bevarandeplanering för informationen i systemet baserad på organisationens bevarande- och gallringsutredning.
			Bevarandeplaneringen ska innehålla fastställda bevarandeperioder för varje informationsobjekt. Bevarandeperioden baseras på informationens värde för organisationen samt nationellt och internationellt regelverk som ska tillämpas. Organisationen måste ha kännedom om regelverk och tillräcklig mognad för att följa det.		Bevarandeplaneringen innehåller information om bevarandeformat och tidpunkt för överföring till bevarande. Det ska finnas en tidspunkt i systemet där informationsobjekt inte kan ändras.

			Fastställda bevarandeperioder ger möjlighet till lämplig lagring genom att behålla och flytta information i och mellan informationssystem under informationens livscykel/livsförlopp.		Alla informationsobjekt har en angiven bevarandeperiod, vilken är kopplad till gällande lagar, förordningar och föreskrifter.
					Bevarandeperiod framgår i systemet. Det finns signaler som anger när åtgärder för bevarande ska vidtas (till exempel åtgärder för konvertering, migrering eller gallring).
2	**Representation, format och metadata**				
2.1	**Sökfält och representation**	Varje informationsobjekt har en synlig representation i systemet, som är möjlig att söka fram genom tillgängliga sökfält.	Med representation avses hur informationsobjektet återges till exempel som en fil.		Varje informationsobjekt representeras genom en unik beteckning.
			En sökfunktion bör fungera utifrån såväl metadata som fulltext. Sökvägarna till respektive informationsobjekt bör baseras på resultatet från kartläggningen av användarnas behov av att återsöka informationen utifrån olika kriterier.		Informationsobjekt är sökbara genom en funktionalitet som tillåter sökmöjligheter utifrån informationsobjektens metadata samt utifrån fulltext.
			All sökfunktionalitet i systemet ska ha testats.		Sökfälten har utformats utifrån definierade användargrupper.
					En specifik sökning ger samma resultat vid upprepade sökningar.
					Det är möjligt att kombinera flera parametrar vid samma sökning.
					Det är möjligt för behöriga att fritextsöka i hela informationsbeståndet.
					Systemet kan erbjuda en samlad, komplett representation av ett informationsobjekt för behörig användare.
2.2	**Formatval**	Informationsobjekten kan lagras och exporteras i öppna, standardiserade eller föreskrivna format.	Säkerställ att format som tillåts i systemet används i enlighet med sina specifikationer. Säkerställ att konvertering till format för långtidsbevarande sker så snart som möjligt, och att dessa är anpassade efter tidsperspektiv och bevarandeplanering.		Varje informationsobjekt är i eller kan konverteras till öppna, standardiserade eller föreskrivna format.
			Med öppet format menas icke-proprietära format. Med proprietära format menas sådana som endast kan läsas i program som utvecklats av samma ägare.		Systemet ska generera en förteckning över dess förekommande format och vilka öppna format de kan konverteras till. Förteckningen ses över regelbundet och uppdateras vid utvecklingsinsatser och inför avveckling.
			All funktionalitet rörande begränsningar och konverteringar av filformat i systemet ska ha testats.		Det finns implementerade verktyg för att konvertera och validera format.
					Det ska finnas en begränsning av vilka filformat som är tillåtna i systemet.
2.3	**Metadata**	Metadata finns kopplad till varje informationsobjekt och är möjlig att exportera tillsammans med informationsobjektet. Metadata är möjlig att återsöka via sökfält.	Kvaliteten på och tillräcklig mängd metadata i systemet är avgörande för informationens sökbarhet och autenticitet. Kravställningen på metadata måste vara känd och implementerad. Ju mer manuell tillförsel av uppgifter i form av metadata som görs, ju mer utvecklade måste rutiner för detta vara.		Informationen i systemet förses med metadata enligt den standard som implementerats eller annars på det sätt verksamheten beslutat.
			Metadata är en del av de informationsobjekt som definieras genom den informationsmodell som tillämpas för systemet.		Implementerad metadatastandard har dokumenterats.
			All funktionalitet i systemet ska ha testats.		Metadata som kommer ur krav från verksamheten har definierats och beretts plats.

					Metadata som kommer ur lagkrav har definierats och beretts plats.
					Metadata är sökbar via sökfält.
					Metadata kan exporteras ur systemet separat eller i tillsammans med information som den beskriver på ett strukturerat sätt.
3	**Gallring och export**				
3.1	**Gallring**	Informationsobjekten gallras varken tidigare eller senare än som angivits i bevarandeplanen. Gallringen i systemet dokumenteras.	Med gallring avses här att destruera allmänna handlingar såväl som annan information.		Informationsobjekten i systemet kan gallras. Befogenhet att gallra styrs genom behörigheter.
			Gallringsfrister ska finnas tillgängliga i relation till varje informationsobjekt. Säkerställ att rätt instans har fattat besluten om gallring.		Delar av informationobjekt kan gallras utifrån de beslut om gallring som gäller för informationen.
			All gallringsfunktionalitet i systemet ska ha testats.		Utvalda informationsobjekt i systemet kan undantas från gallring (t.ex. gallra filer men behålla viss metadata, eller gallra personuppgifter men behålla övrig metadata).
					Loggar kan gallras helt eller delvis.
					Hela eller valda delar av metadata kan gallras.
					Gallringsregler kan implementeras automatiskt i systemet utfrån gällande gallringsbeslut och kan ändras vid behov.
					Gallringsvillkor kan kopplas till händelser i systemet (t.ex. att gallringsfristen räknas 3 år efter avslutad anställning, eller 10 år efter upphört avtal).
					Gallringsrapport kan skapas (manuell eller automatiserad) efter verkställd gallring enligt verksamhetens krav.
					Data från genomförd gallring kan återskapas under specificerade förhållanden (dvs. under den tid som organisationen kravställt) och beskrivning av hur den kan återskapas finns. Funktionaliteten är endast tillgänglig för specifika roller.
					Data från genomförd gallring kan inte återskapas efter en viss tidsperiod.
3.2	**Export**	Export till annat verksamhetssytem eller system för bevarande sker enligt bevarandeplanering baserad på ekonomiskt hållbar förvaltning och informationssäkerhetnivå.	Informationsobjekten med kopplad metadata kan exporteras till ett annat informationssystem i öppna, standardiserade eller föreskrivna format.		Exportfunktion finns som täcker samtliga informationsobjekt i systemet.
			All exportfunktionalitet i systemet ska ha testats.		Export kan göras på flera informationsobjekt samtidigt.
					Informationsobjekten ska kunna exporteras i öppna, standardiserade eller föreskrivna format och strukturerade enligt den standard som ska tillämpas.
					Export sker systematiskt genom uttag av standardiserade informationspaket.
					Strukturella samband mellan informationsobjekt upprätthålls vid export.
					Exporterade informationsobjekt tas inte bort från källsystemet förrän dess kvalitet och åtkomst har säkrats.
					Exporten är reversibel under specificerade förhållanden (den tid som organisationen kravställt) och det finns dokumenterat på vilket sätt.
					En rapport över genomförd export skapas manuellt eller automatiserat.

4	**Begränsningar och säkerhet**				
4.1	**Behörighet**	Rätten till tillgång till informationsobjekten i systemet regleras genom behörighetssystem.	Utgå från den informationsklassificering som verksamheten baserar sina riskbedömningar på och som definierar behörighetsnivåerna och systemets behörighetsmodell.		Systemets behörighetsnivåer och behörighetsgrupper följer organisationens informationssäkerhetsklassificering.
			All funktionalitet rörande behörighetsstyrning i systemet ska ha testats.		Behörigheterna är utvärderade i förhållande till informationssäkerhetsklassificeringen.
					Behörighetsnivåerna i systemet är definierade och finns dokumenterade i en behörighetsmodell eller rollmodell.
					Behörighetsnivåer och behörighetsgrupperna är tillgängliga i systemet.
					Informationsobjekt i systemet är tillgängliga för alla som enligt organisationens regelverk och policyer ska ha behöriget. Om ett informationsobjekt innehåller skyddsvärda eller sekretesskyddade uppgifter, tillåter systemet att det går att hantera en begränsad representation av informationsobjektet.
					Systemet har stöd för anonymisering och pseudonymisering.
					Behörighetsstyrda aktiviteter loggas i systemet.
					Loggarna över behörighetsstyrda aktiviteter följs upp och utvärderas kontinuerligt.
4.2	**Säkerhet**	Systemet hanteras i enlighet med tillämpliga informationssäkerhetsbestämmelser.	Med säkerhet avses informationssäkerhet inkluderande IT-säkerhet och cybersäkerhet.		Lagar, regler och interna styrdokument som rör informationssäkerhet ska kunna tillämpas i systemet.
			Säkerställ att kunskap finns i AbD-undersökningen om vilka säkerhetsbestämmelser som ska tillämpas.		Organisationens tillämpning av regelverket kring informationssäkerhet, till exempel i egna policyer eller riktlinjer, ska vara uppdaterade.
			All funktionalitet rörande säkerhet i systemet ska ha testats.		Informationen som ska hanteras i systemet har varit föremål för en nyligen gjord informationssäkerhetsklassificering.
					Informationssäkerhetsarbetet genomgår en årlig översyn och utvärdering.