KLASSA – SKL:s metodstöd för informationssäkerhet

Markus Ekbäck, SKL

Webbseminarium 181114

KLASSA – SKL:s metodstöd för informationssäkerhet

Sveriges Kommuner och Landsting

KLASSA används för att

- Bestämma skyddsnivåer för konfidentialitet, riktighet och tillgänglighet
- Välja lagrum, t.ex. GDPR, PDL, NIS
- Bedöma befintligt skydd för informationen

KLASSA ger

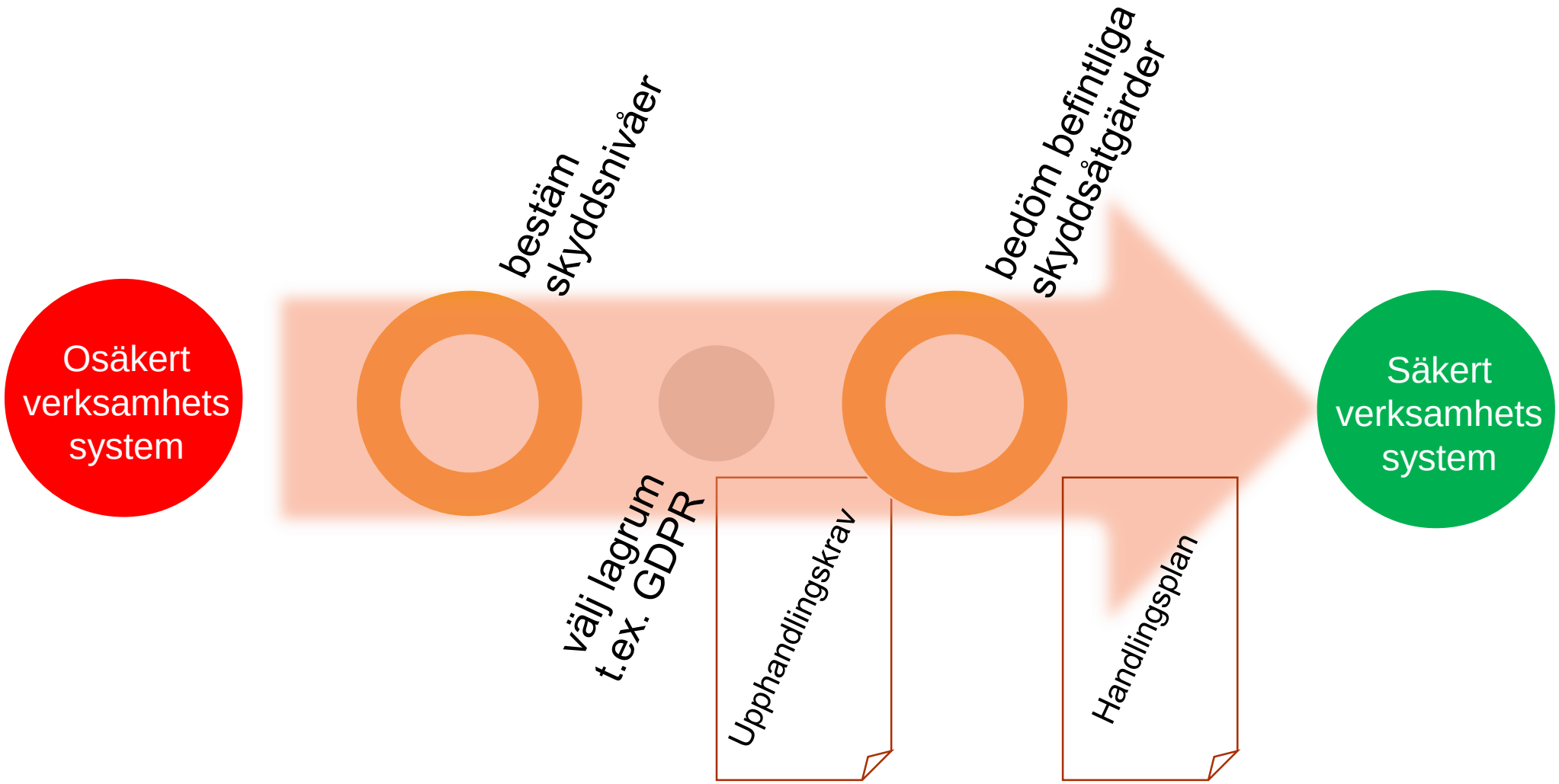
- Upphandlingskrav – säkerhetskrav som ska uppfyllas av leverantören (bör ingå i avtalen)
- Handlingsplan – GAP-analys till den ansvariga verksamhetens förvaltningsplan

KLASSA är

- Fritt tillgängligt för SKL:s medlemmar
- Använt av 206 kommuner och 6 landsting *(okt 2018)* – över 4000 handlingsplaner har gjorts

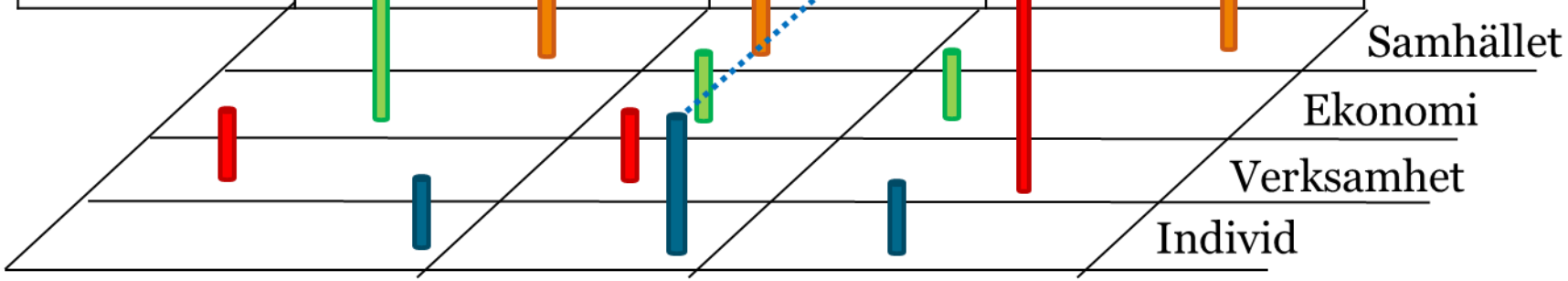
Webb: klassa-info.skl.se
Frågor: klassa@skl.se

Tre steg i KLASSA (processen)



Så genomför vi en informationsklassning

Aspekt / Nivå	Konfidentialitet	Riktighet	Tillgänglighet
Allvarlig	K3	R3	T3
Betydande	K2	R2	T2
Måttlig	K1	R1	T1
Ingen	K0	R0	T0



Resultatet av informationsklassningen i detta exempel är: **K2R1T3**
Verksamhetens krav är högst för tillgänglighet, sedan för konfidentialitet och lägst för informationens riktighet

Källa: informationssäkerhet.se

Skadenivåer

- Nivå 0 – ingen eller försumbar skada
- Nivå 1 – måttlig skada, exempelvis minskad förmåga att genomföra verksamhetens uppdrag, effektiviteten är påvisbart reducerad
- Nivå 2 – betydande skada, exempelvis tillgänglighetsstörningar, brott mot regelverk, rättsliga krav och avtal, eller förlust av skapat förtroende
- Nivå 3 – allvarlig skada, exempelvis massiv informationsförlust, verksamhetsförlust, oöverskådliga konsekvenser, eller fara för liv och hälsa

Skadenivåer konfidentialitet
– begränsningar i åtkomst till information

- Nivå 0 – inga svårigheter för verksamheten, ingen eller liten påverkan på samhällsviktiga funktioner
- Nivå 1 – inga större svårigheter för verksamheten att nå målen, störningen kan noteras eller upplevas ge lindriga besvär
- Nivå 2 – trolig risk för kännbar påverkan (t.ex. ekonomiskt), andra myndigheter/organisationer kan påverkas, konsekvenser för enskilda individer
- Nivå 3 – stora svårigheter för verksamheten, samhällsviktiga funktioner påverkas, allvarlig kränkning av den personliga integriteten

Skadenivåer riktighet

– informationen ska vara tillförlitlig, korrekt och fullständig

- Nivå 0 – inga svårigheter för verksamheten, ingen eller liten påverkan på samhällsviktiga funktioner
- Nivå 1 – inga större svårigheter för verksamheten, störningen kan noteras eller upplevas ge lindriga besvär
- Nivå 2 – trolig risk för kännbar påverkan (t.ex. ekonomiskt), andra myndigheter/organisationer kan påverkas, konsekvenser för enskilda individer
- Nivå 3 – stora svårigheter för verksamheten, samhällsviktiga funktioner påverkas, individers liv och hälsa äventyras

Skadenivåer tillgänglighet

– informationen ska kunna nyttjas efter behov, i förväntad utsträckning samt av rätt person med rätt behörighet

- Nivå 0 – inga svårigheter för verksamheten, ingen eller liten påverkan på samhällsviktiga funktioner
- Nivå 1 – inga större svårigheter för verksamheten, störningen kan noteras eller upplevas ge lindriga besvär
- Nivå 2 – trolig risk för kännbar påverkan (t.ex. ekonomiskt), andra myndigheter/organisationer kan påverkas, konsekvenser för enskilda individer
- Nivå 3 – stora svårigheter för verksamheten som påverkas i allvarlig/katastrofal omfattning, samhällsviktiga funktioner påverkas, individers liv och hälsa äventyras

Exempel på upphandlingskrav (avtalsbilagor)

Sveriges Kommuner och Landsting

#	Krav	ISO kapitel	ISO kravområde	Kon.	Rik.	Til.
3501	Leverantören ska för de delar av verksamheten som berörs i leveransen ha ett **ledningssystem** för informationssäkerhet (LIS) som baseras på SS-EN ISO/IEC27001:2017 eller motsvarande.	A.6.1 Intern organisation	A.6.1.1 Informationssäkerhetsroller och ansvar	2	2	2
3504	Leverantören ska ha en **policy** som beskriver hur de anställda får **arbeta på distans** avseende drift, förvaltning och support av de levererade tjänsterna.	A.6.2 Mobila enheter och distansarbete	A.6.2.2 Distansarbete	2	2	
3505	Leverantören ska ha processer och rutiner på plats för relevant **bakgrundskontroll av personal.**	A.7.1 Före anställning	A.7.1.1 Bakgrundskontroll	2	2	
3506	Leverantören ska ha avtal om **tystnadsplikt** med sina anställda. Tystnadsplikten ska omfatta information om leverantörens kunder. Via avtal ska leverantören även säkerställa tystnadsplikt för underleverantörer.	A.7.1 Före anställning	A.7.1.2 Anställningsvillkor	2		
3507	Leverantören ska för sin personal regelbundet genomföra **utbildningar** för ökad medvetenhet **kring informationssäkerhet** samt hålla sig uppdaterad kring beställarens policys, regler och rutiner.	A.7.2 Under anställning	A.7.2.2 Medvetenhet, utbildning och fortbildning vad gäller informationssäkerhet	2	2	2
3510	Leverantören ska ha **dokumenterade regler, rutiner och roller** som beskriver tillåten användning av de resurser som ingår i leveransen.	A.8.1 Ansvar för tillgångar	A.8.1.3 Tillåten användning av tillgångar	2		
3512	Leverantören ska under kontraktstiden, dock minst vart tredje år, ha genomfört en **riskbedömning för systemet**. Identifierade brister ska åtgärdas enligt en dokumenterad plan och kunna redovisas för beställaren.	A.8.2 Informationsklassning	A.8.2.1 Klassning av information	2	2	2

7 Personalsäkerhet

7.1 Före anställning

Mål: Att säkerställa att anställda och leverantörer förstår sitt ansvar och är lämpliga för de roller de är tilltänkta för.

7.1.1 Bakgrundskontroll

Säkerhetsåtgärd

Bakgrundskontroll på alla sökande för anställning bör utföras i enlighet med relevanta författningar och etiska krav och bör stå i proportion till verksamhetskraven, klassificeringen av information som de ges behörighet till och de upplevda riskerna.

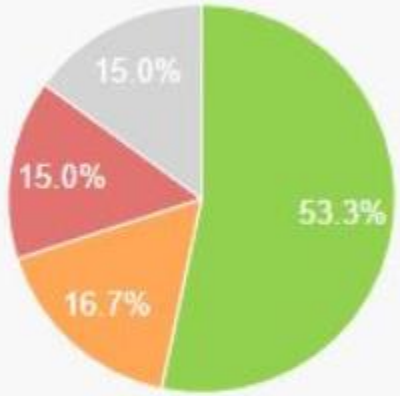
Resultat per system

Sveriges Kommuner och Landsting

Resultat

Uppfyller helt | Uppfyller delvis | Uppfyller inte alls | Ej relevant | Ej besvarade

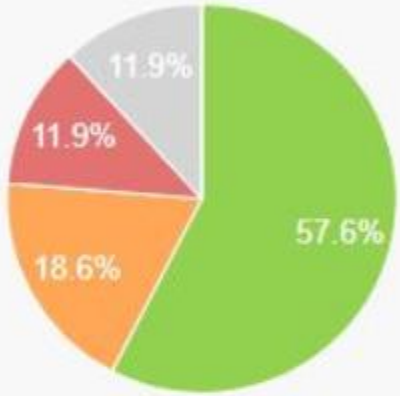
Konfidentialitet (2)



Dina svar

Uppfyller helt: 32
Uppfyller delvis: 10
Uppfyller inte alls: 9
Ej relevant: 9
Ej besvarade: 0

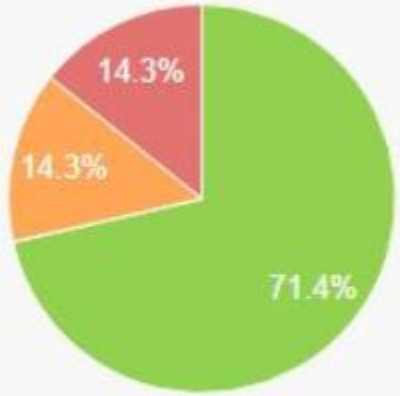
Riktighet (2)



Dina svar

Uppfyller helt: 34
Uppfyller delvis: 11
Uppfyller inte alls: 7
Ej relevant: 7
Ej besvarade: 0

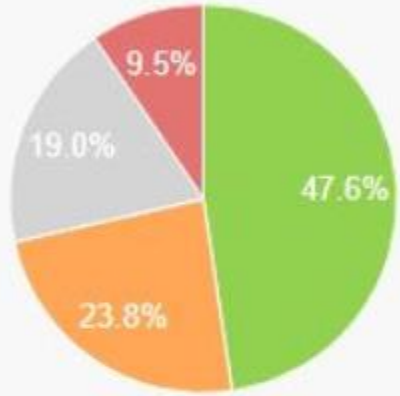
Tillgänglighet (1)



Dina svar

Uppfyller helt: 5
Uppfyller delvis: 1
Uppfyller inte alls: 1
Ej relevant: 0
Ej besvarade: 0

Lagrum



Dina svar

Uppfyller helt: 10
Uppfyller delvis: 5
Uppfyller inte alls: 2
Ej relevant: 4
Ej besvarade: 0

Klassa v 3.5 systemkravkarta

KLASSA Systemkravkarta - 2018

		Total uppfyllnad		Konfidentialitet		Riktighet		Tillgänglighet		Spårbarhet	
Handlingsplan	Datum	Uppfyller hel	Uppfyller delvis	Uppfyller hel	Uppfyller delvis	Uppfyller hel	Uppfyller delvis	Uppfyller hel	Uppfyller delvis	Uppfyller hel	Uppfyller delvis
Treserva v2	2015-06-01	49%	26%	47%	19%	49%	28%	51%	31%	49%	27%
Diariet (Public 360)	2015-06-11	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
eArkiv	2015-07-22	4%	2%	3%	2%	3%	3%	12%	0%	5%	2%
e-post Exchange	2018-04-30	75%	15%	61%	21%	74%	21%	85%	10%	88%	6%
Kontorscenter KC-systemet	2017-06-01	75%	15%	61%	21%	74%	21%	85%	10%	88%	6%
Västkom Journalsystem	2016-09-27	59%	21%	58%	22%	60%	21%	56%	21%	62%	20%

Nytt i version 3.5 är att en organisations olika handlingsplaner kan presenteras och bearbetas som helhet

Tre steg i KLASSA – enkelt som ABC