Stockholms universitet

Välkomna!

IT-forum för administrativa chefer

2022-11-29

Presentationer läggs ut på https://www.su.se/medarbetare/it/it-forum.

Mötet spelas in! Maila stina.haase@su.se för tillgång till video.

Stockholms universitet

Välkommen!

Karin Olsson, gruppchef Portföljkontoret

Stockholms universitet

Agenda

- Informationssäkerhet och projekt ESIR
- Nya rapportverktyget – Qlik Sense
- Inspera – införande
- Fokusområde 2023: Säkerställa kvalitet i tjänsteleveranser med tillhörande support
- Avrundning

Stockholms universitet

Informationssäkerhet och ESIR

Stefan Kvarnerås, sektionschef Arkitektur, IT- och informationssäkerhet
Informationssäkerhetschef SU

Stockholms universitet

Vad ska jag prata om

- Vad har hänt med informations- och IT-säkerheten på SU och vad är ESIR
- Lite status om it-säkerhetsläget
- Vad är nästa steg

Hot och risker (konstaterade)

Bristfällig informationssäkerhet

- Osäkra administrativa rutiner
- Osäkra tekniska system
- Okunskap bland medarbetare

Ökat regulatorisk tryck

- MSB:s föreskrifter 2020:6-8
- Säkerhetsskyddslagen
- Regulatoriska krav mot din verksamhet

Datainspektionens tillsyn och sanktioner

- IMYs tillsynsprogram
- Risken för sanktioner

Verksamhetens yttre hotbild

- Avsaknad gemensam hotbild mot organisationens information
- Cyberkriminalitet på stadig uppgång

Universitets förtroende

- Organisationer som inte behandlar uppgifter korrekt riskerar minskat anseende och misstro från användare och medborgare

2. En tillbakablick: Kort introduktion till ESIR[1)]

Projektets syfte är att höja informationssäkerheten vid Stockholms Universitet

- Uppdraget är att både skydda och säkra tillgången till viktiga informationstillgångar genom att lägga grunden till ett systematiskt och effektivt arbete med informationssäkerhet vid Stockholms universitet.
- Projektet ska resultera i ökat säkerhetsmedvetande och en informationshantering som följer MSB:s riktlinjer, tillämpliga delar i standarden SO/IEC 27001 samt universitets övergripande åtgärdsplan för riskhantering.

Bakgrunden är att det finns konkreta risker och hot mot organisationens information

- Granskningar och internrevisioner har visat allvarliga säkerhetsbrister som måste åtgärdas
- Universitets informationsresurser blir allt mer kritiska samtidigt som cyberkriminalitet är på stadig uppgång
- Regulatoriskt tryck med risk för sanktioner och skador på universitets trovärdighet

Projektet har som mål att det ska vara enkelt och intuitivt att arbeta med hög säkerhet

- Dialog och metodstöd som ökar säkerhetsmedvetandet bland ledare och medarbetare
- Etablering av ansvarsfördelning och rutiner som säkerställer ett systematiskt arbete med informationssäkerhet
- Kultur som fokuserar mer på kontinuerlig förbättring och lärande än vilken nivå man är på

Metodstöd och tillämpning är prövat på fyra institutioner i samarbete med IT-avdelningen

- Metoderna och modellerna för att för att höja informationssäkerheten är framtagna i nära samarbete mellan fyra utvalda pilot-institutioner tillsammans med säkerhetsfunktionen inom IT-avdelningen.

Not 1) ESIR är en förkortning av Etablering av Systematiskt Informationssäkerhetsarbete och Resultatstyrning

Lärdomar från de fyra ESIR-piloterna visade på värdet av att skapa gemensamma arbetssätt och verktyg

Varje institution ska inte behöva uppfinna hjulet på nytt

Många upplever informationssäkert som abstrakt, komplext och svårbegriplig

Vi vill så långt som möjligt ha gemensamma checklistor, mallar och centralt support

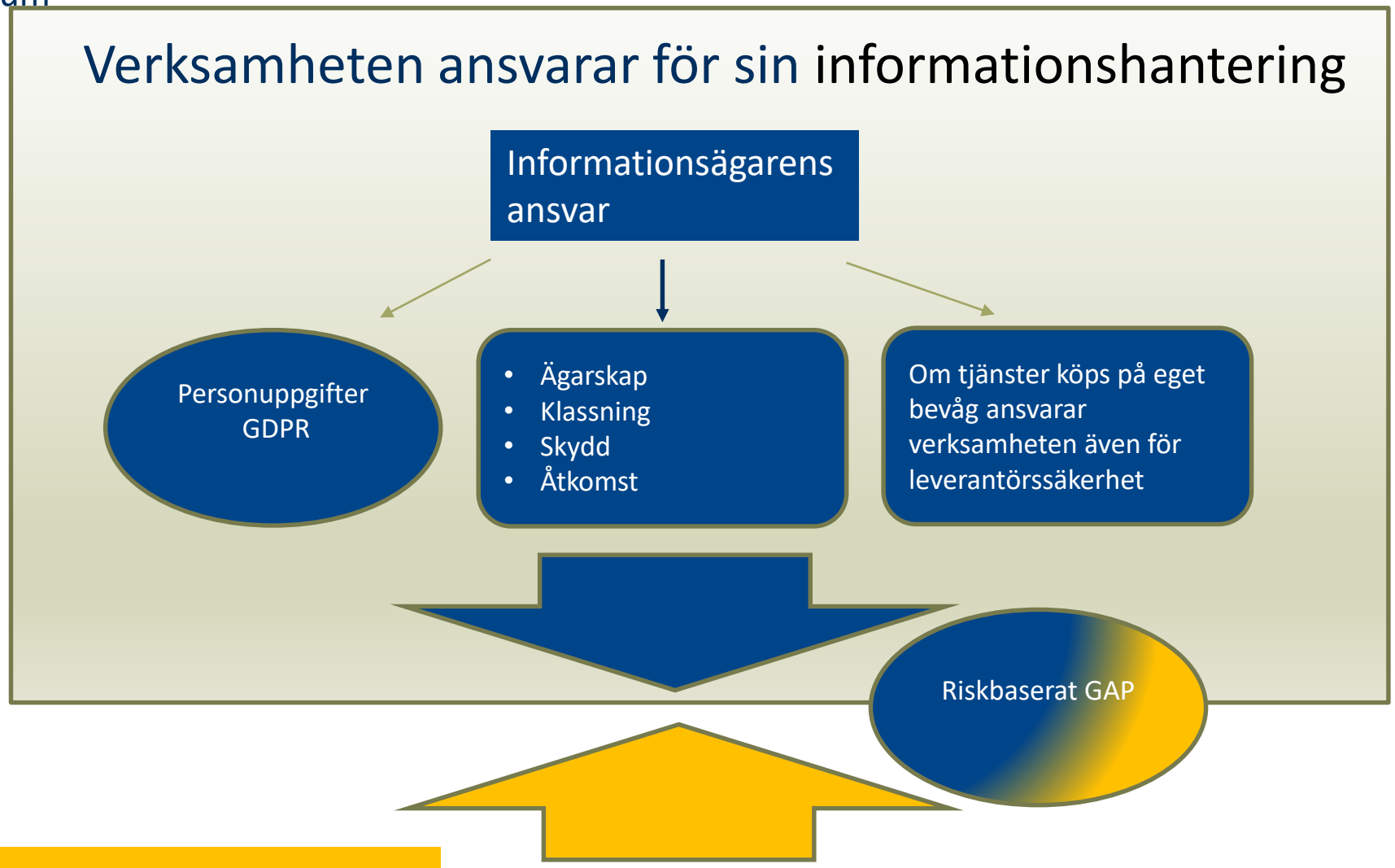
Kulturen i universitetsvärlden är att information i möjligaste mån ska vara tillgänglig för att maximera lärande och kunskapsutveckling

Administrativa chefen är den mest lämpade att samordna helheten

Viktigt att öka medvetandet om informationssäkerhet bland medarbetarna

Institutioner på många sätt unika, men i detta område har vi väldigt liknade behov

Principbild



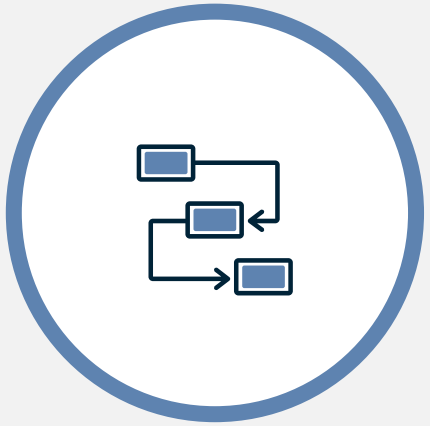
IT-avdelningens ansvar

- Leverans av ”säkra system och lösningar”
- Grundläggande nivå MSBFS 2020:7

SU:s mål: Hantera information på ett säkert sätt

Komplexitet

Informationssäkerhet upplevs av många som ett komplext område med höga krav på verksamhet, teknik och medarbetare



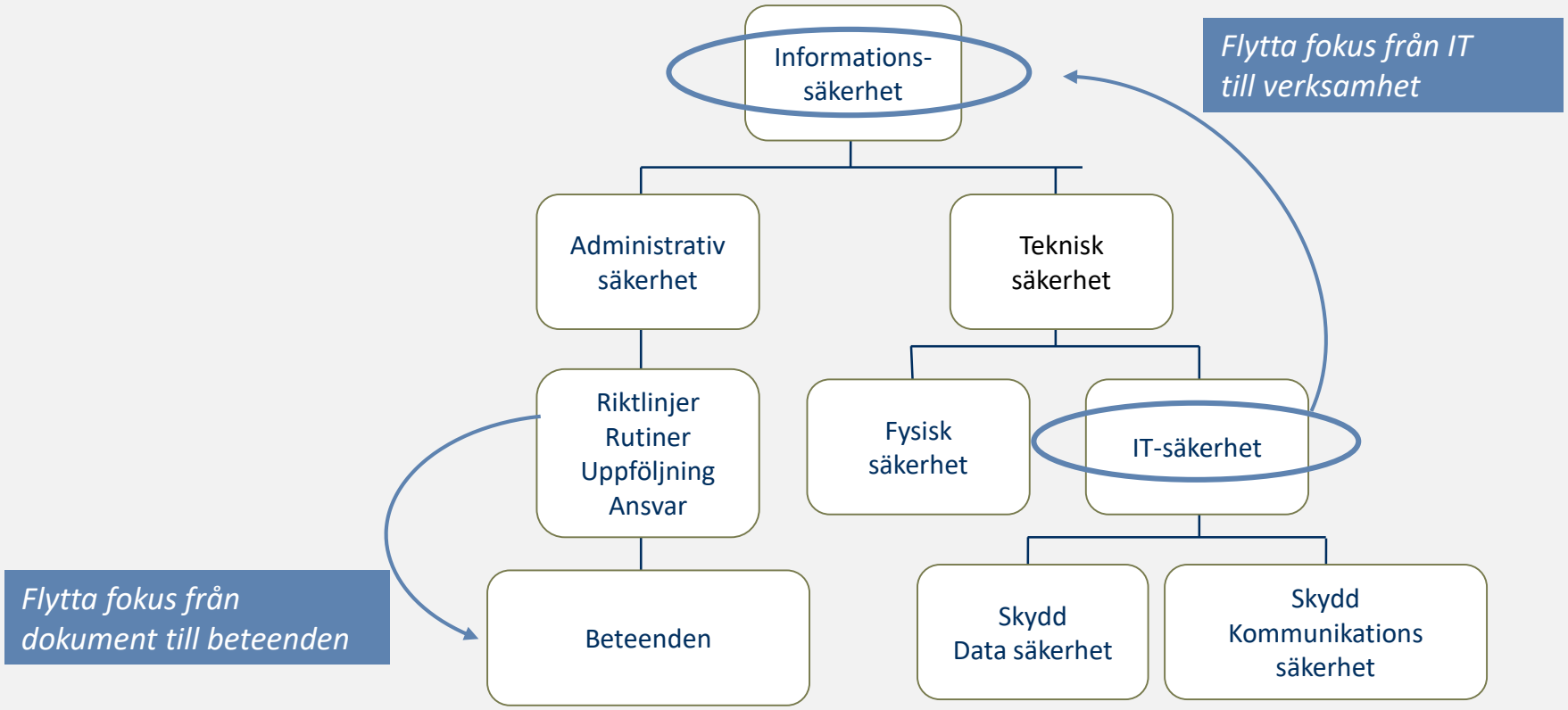
Förenkling

ESIR syftar till att reducera komplexitet utan att helhetssynen förloras så att åtgärder kan sätts in där de skapar mest nytta

Resultat

Ökat säkerhetsmedvetande och rutiner som säkerställer ett systematiskt arbete med informationssäkerhet

Informationshantering handlar inte bara om teknik, utan också om användares beteende



ESIR provade ett nytt arbetssättet för att öka informationssäkerheten

Pilot Institution	Uppstart och utbildning	Inventering & klassning	Informations-analys	Handlingsplan	Lärande och återkoppling
Asien-, Mellanöstern- och Turkietstudier	✓	✓	✓	✓	✓
Etnologi, Religionshistoria och Genusvetenskap	✓	✓	✓	✓	✓
Juridiska institutionen	✓	✓	✓	✓	✓
Molekylär biovetenskap, Wenner-Grens institut	✓	✓	✓	✓	✓

Stockholms universitet

Framtaget Metodstöd/Verktygslåda har åtta delar

Rollbeskrivningar

Roller med ansvarsbeskrivning inom institution/motsvarande

Masterdata

Modell för inventering och gruppering av information

Informationsanalys

Modell för informationsanalys

Klassning

Guide och checklistor vid informationsklassning

Administrativa Skyddsåtgärder

Guide för administrativa skyddsåtgärder

Riskanalys

Guide och verktyg för riskanalys kopplat till gap i informationsanalys

Handlingsplan

Exempelsamling till handlingsplan

Årshjul

Årshjul och enkät för säkerhetsuppföljning

Stockholms universitet

Rollbeskrivningar

Nyckelroller i verksamheten är informationsägaren och informationssäkerhetssamordnaren

Informationsägare (person/er inom verksamheten)

Övergripande beskrivning	
Vem?	Prefekt/motsvarande är informationsägare men rollen kan också delegeras
Ansvars-område	▪ Klassificerar informationstillgångar utifrån behovet att upprätthålla konfidentialitet, riktighet och tillgänglighet ▪ Tar ställning till huruvida säkerhetsåtgärderna är beaktade och säkerställer att det finns anvisningar och rutiner. ▪ Fastställer lämpliga regler för styrning av åtkomst kopplat till informationstillgången. ▪ Ställer krav på interna/externa leverantörer av IT-tjänster att de skyddar informationen enligt gjord klassning.

Finns inte idag

Informationssäkerhetssamordnare (person inom verksamheten)

Person inom institution/motsvarande, kan tex vara administrativa chefen

- Kontaktperson vid informationssäkerhetsfrågor, dataskydd och incidenthantering/rapportering.
- Säkra att informationsklassning och registerförteckningar mm är upprättade och korrekta.
- Verka för att eventuella brister inom verksamheten upptäcks och åtgärdas.
- Bistå med kompetens t.ex. kring informationssäkerhet eller i sakfrågor kring dataskydd

Referensmodell med masteradata (informationstillgångar) som är grupperad i tre områden (våra förmågor)

Masterdata

Forskningsdata

- Planering
- Forskning
- Intressenter
- Resultat

Utbildningsdata

- Antagning
- Planering
- Genomförande
- Dokumentation

Administrativ data

- Planering
- Ekonomi
- HR/Personal

Övriga adm. data

- Upphandling
- Avtal och projekt
- Kommunikation
- Arkivhandlingar
- Dokumentation

Referensmodellen är framtagen och baserad på arbetet med de fyra pilot-institutionerna samt i ett samarbete med en forskargrupp och biblioteksavdelningen

Stockholms universitet

Masterdata

Katalogen över informationstillgångar underlättar inventeringen genom att visualisera de vanligaste informationsmängderna inom SU (inom akademin)

Forskningsdata

- Forskningsfinansiärer
- Forskningsmedel
- Etikprövning
- Tillstånd
- Forskningsansökan
- Forskningsområden
- Datahanteringsplan
- Forskare
- Forskningspersoner
- Forskningsdeltagare
- Forskningsdata
- Forskningsplan
- Instrument
- Forskningsprojekt
- Forskningsresultat
- Forskningspublikation

Utbildningsdata

- Kontaktuppgifter studenter
- Antagningsbeslut
- Studentintyg
- Läkarintyg studenter
- Beslut om anpassningar
- Studentkorrespondens
- Kursutvärderingar
- Bedömning/betygsunderlag
- Resultatinformation
- Betyg
- Närvaroinformation
- Bemanningsplanering
- Schema
- Litteraturlistor
- Kursplaner
- Lektionsplaner
- Lärarkompens/dokumentation
- Kursinformation
- Undervisningsmaterial
- Tentafrågor
- Tentaskrivningar

Administrativ data

- Verksamhetsplaner
- Ekonomi
- Budget
- Fakturor
- Tillgångar/licensförteckningar
- Förteckningar över tillgångar
- Personalinformation
- Anställningsinformation
- Personalakter
- Bilder på medarbetare
- Intyg, diplom
- Rehab-information
- Utvecklingssamtal
- Lönesamtal
- Löneinformation
- Reseräkningar, kvitton
- Kontaktuppgifter, anhöriga
- Jobbansökningar
- Testamenten
- Gåvobrev

Övrig adm. data

- Upphandlingar
- Avtal och överenskommelser
- Projektinformation
- Möteshandlingar/protokoll
- E-post korrespondens
- Post
- Webbsidor
- Anslagstavlor/skärmar
- Sociala medier
- Användarmanualer
- Riktlinjer och Arbetsrutiner
- Kris och kontinuitetsplan
- Teknisk dokumentation/larm
- Fastighetsritningar
- Dokumentation av IT-system
- Arkivbeskrivningar (vad arkiverat)
- Arkivskåp/handlingar (fysiska)
- Arkiv/handlingar (digitala)
- Diarieförda handlingar

Information inom forskning

Masterdata

Gruppering/Objekt	Informationsmängd	Innehåll
Planering	Forskningsfinansiärer	Beskrivningar av organisation som finansierar forskningen
	Forskningsmedel	Forskningsbidrag eller intäkt från extern finansiär eller SU interna anslag avsedda för forskning
	Etikprövning	Etikprövning för forskning som utförs i Sverige och som involverar människor eller djur.
	Tillstånd	Dokument som styrker rätt att utföra en viss aktivitet som kräver tillstånd
	Forskningsansökan	Ansökan till forskningsfinansiär om finansiering av forskning
Forskning	Forskningsområden	Forskningsområde är forskning inom ett avgränsat ämnesområde, t.ex. naturvetenskap
	Datahanteringsplan	En Datahanteringsplan beskriver hur data som samlas in och/eller skapas i forskningsprojektet
	Forskningsdata	Information som samlas in, bearbetas, analyseras eller produceras för forskningsändamål.
	Forskningsplan	Dokument som beskriver de aktiviteter som ska genomföras I forskningsprojektet
	Instrument	Digitalt eller fysiskt verktyg/utrustning för data insamling och/eller analys
	Forskningsprojekt	Ett projekt med definierad tid och frågeställning som man bedriver forskning i
Intressenter	Huvudman	Lärosätet eller institution som ansvarar för forskningsprojektet
	Forskare	Anställda av SU eller affielerade till SU, som bedriver forskning
	Forskningsperson	Någon som utfrågas, försöksperson m.m.
	Forskningsprojektdeltagare	Forskare eller annan person som är knuten till forskningsprojektet
Resultat	Forskningsresultat	Forskningsresultat är resultatet av en vetenskaplig studie.
	Forskningspublikation	Forskningspublikation är en presentation av forskningsdata, metoder, resultat och slutsatser.
	Patent	Patent är en ensamrätt att utnyttja en uppfinning

Stockholms universitet

Information inom utbildning

Masterdata

Gruppering /Objekt	Informationsmängd	Innehåll
Antagning	Antagningshandlingar	Ansökningar, betyg tidigare utbildningar, behörighetsbedömningar, antagningsbeslut
	Studenter	Studentlistor, kontaktuppgifter mm
	Studentintyg	Studieintyg, resultatintyg mm. till studenter
Planering	Kursplaner	Planer för kurser
	Lärarkompens	Legitimation, dokumenterad kompetens
	Bemanningsplanering	Bemanning, lärare
	Schema	Schema, schemaläggning, lokalbokning
	Kursinformation	Litteraturlistor, betygskriterier, examination mm.
	Undervisningsmaterial	Planeringar, gruppindelningar, examinationer, seminarieuppgifter, powerpoint-underlag mm
	Inspelade föreläsningar	Lagrade inspelningar
	Tentafrågor	Tentauppgifter, frågebanker
Genomförande	Studentkorrespondens	Frågor om undervisning, studievägledning mm
	Närvaroinformation	Information om närvaro
	Inlämningsuppgifter	Studenters inlämningsuppgifter
	Tentor	Studenters tentaskrivningar
Dokumtation	Anpassningar	Beslut om anpassningar, studenter med särskilda behov
	Läkarintyg studenter	Läkarintyg, information om funktionsnedsättning, sjukintyg från stundeter
	Bedömning/betygsunderlag	Betygsmotivering, omdöme om students prestation, resultat
	Betyg	Betyg , examen
	Kursutvärderingar	Utvärderingar från studenter
	Klagomål	Klagomål om utpekade händelser och lärare

Stockholms universitet

Information inom administration

Masterdata

Gruppering/Objekt	Informationsmängd	Innehåll
Planering	Verksamhetsplaner	Mål, strategier, verksamhetsplaner, uppföljning
	Protokoll och minnesanteckningar	Anteckningar om den löpande verksamheten, kallelser, handlingar och protokoll
	Riktlinjer och rutiner	Information om verksamhetens rutiner och arbetssätt
	Kris och kontinuitetsplan	Kris och katastrofplaner, kontinuitetsplaner etc.
Ekonomi	Ekonomi	Redovisning, analyser, rapporter mm
	Budget	Budgetunderlag, kalkyler, budget, prognoser, åtgärdsplaner mm
	Fakturor	E-handel, fakturahantering, fakturadokument och dyl.
	Förteckningar över tillgångar	Inventarier, leasade datorer, mobiler, licenser, mm
	Testamenten	Testamenten, gåvobrev
HR/Personal	Personalinformation	Personaluppgifter, kontaktlistor
	Anställningsinformation	Anställningsbeslut, tjänstledigheter, begäran om entledigande
	Personalakter	Personalakter och information om tidigare och befintlig personal samt
	Funktionsbeskrivningar	Information om medarbetares arbetsuppgifter
	Bilder på medarbetare	Fotografier på medarbetare, tex digitalt
	Intyg, diplom	Bevis, intyg, certifikat, diplom mm
	Rehab-information	Läkarintyg, mail, tjänsteanteckningar, kommunikation med företagshälsa
	Utvecklingssamtal	Dokumentation och anteckningar från utvecklingssamtal, digitalt eller papper
	Lönesamtal	Dokumentation och anteckningar från utvecklingssamtal, digitalt eller papper
	Löneinformation	Löneuppgifter
	Reseräkningar, kvitton	Information om medarbetares resor i tjänsten
	Kontaktuppgifter, anhöriga	Kontaktuppgifter till anhöriga
	Jobbansökningar	Dokumentation om rekrytering och hantering av jobbansökningar

Stockholms universitet

Information inom övrig adm.

Masterdata

Gruppering /Objekt	Informationsmängd	Innehåll
Upph./Avtal/Proj,	Upphandlingar	Upphandingsdokumement, utvärderingar, protokoll mm
	Avtal	Avtal med andra leverantörer, externa finansiärer, samarbetspartner
	Projektinformation	Projektplaner, bemanning, dokumentation, protokoll mm
Kommunikation	E-post korrespondens	Inkommande och utgående e-post som är lagrad och/eller ännu ej tagits omhand
	Post	Fysisk post, postboxar, postrum etc.
	Webbsidor	Interna och externa webbsidor
	Anslagstavlor/skärmar	Anslagstavlor, informationsskärmar
	Sociala medier	LinkedIn, Facebook, Instagram m.fl.
Arkivhandlingar	Arkivbeskrivningar	Vad som är arkiverat
	Diarieförda handlingar	Myndighetsdokument, inkomna och upprättade handlingar, verksamhetsbeslut
	Lokala arkiv (fysiskt)	Kassaskåp med handlingar
	Lokalt arkiv (digitalt)	Filservrar och digital lagringsplatser med dokument (ex Box)
Dokumentation	Användarmanualer	Manualer och handledningar till system etc.
	Teknisk dokumentation/larm	Dokumentation och information om larm, etc.
	Fastighetsritningar	Ritningar och fastighetsbeskrivningar
	Dokumentation av IT-system	Systemdokumentation, diftdokumentation, informationsklassningar, rutiner etc.
	Registerförtecking GDPR	Förteckning över personuppgiftsbehandlingar och syftet
	Förteckning informationsklassing	Förteckning och informationsobjekt med vidhängande klassning och ägarskap

Stockholms universitet

Analys över informationshantering i verksamheten

Informationsanalys

Övergripande analysprocess

- Analys av Information som hanteras
- Grupperas som tillgångar och fördelas inom förmågor (masterdata)
- Informationsklassning
- Skydd
- GAP/Risk

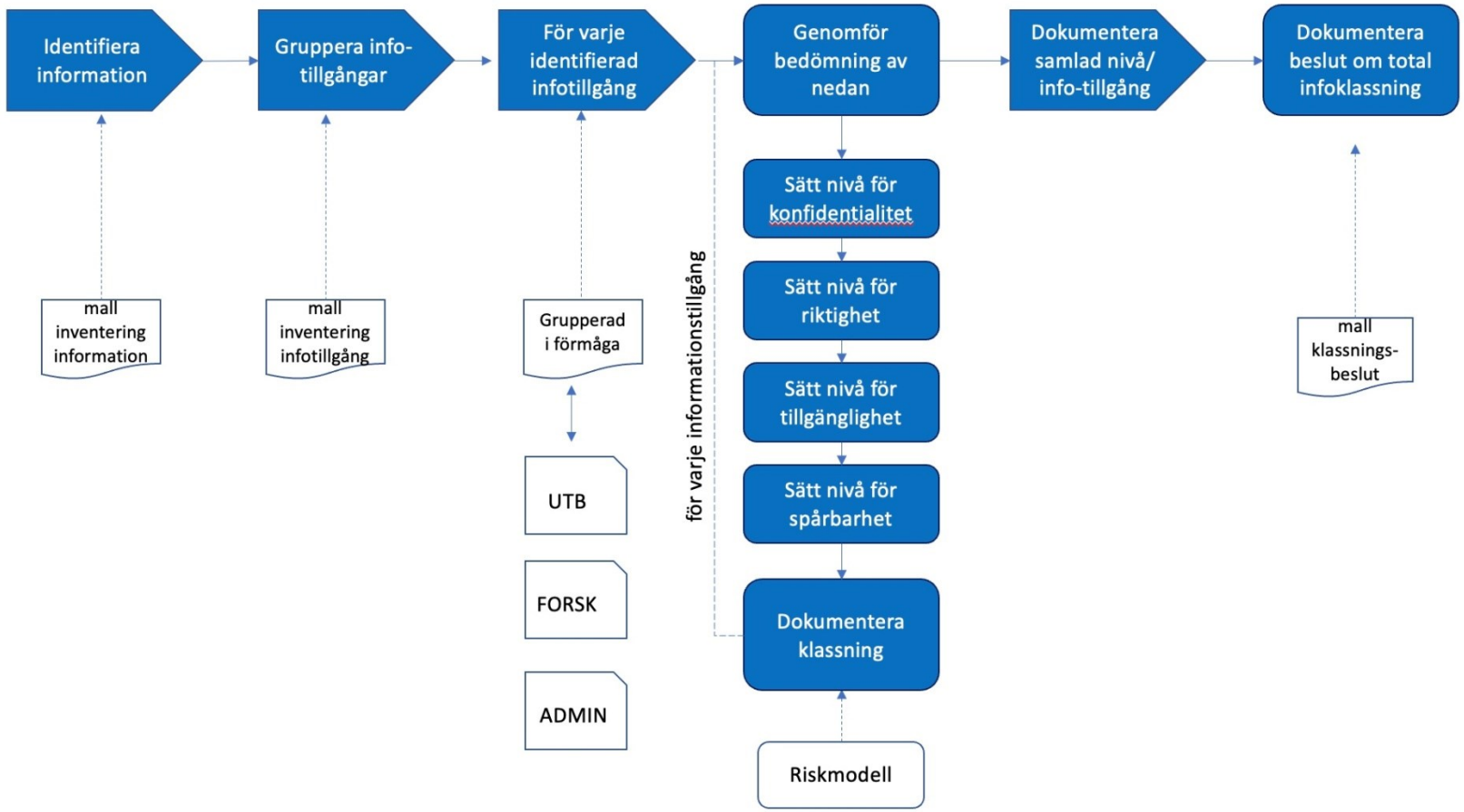
Övriga processer

- Hantering av nya person-uppgiftsbehandlingar/PU register
- Informationsklassning av information i system/register informationstillgångar
- Säkerhetskrav vid upphandling av system/tjänster
- Säkerhetskrav vid större projekt /verksamhetsförändringar
- Säkerhetskrav vid nya Partnerskap/leverantörsrelationer
- Utformning och hantering av tekniska skyddsåtgärder

Stockholms universitet

Klassning

Klassning av inventerade informationsobjekt görs med stöd av en guide som säkrar rätt skyddsnivå



Not 1) Exempel är checklista för personuppgifter

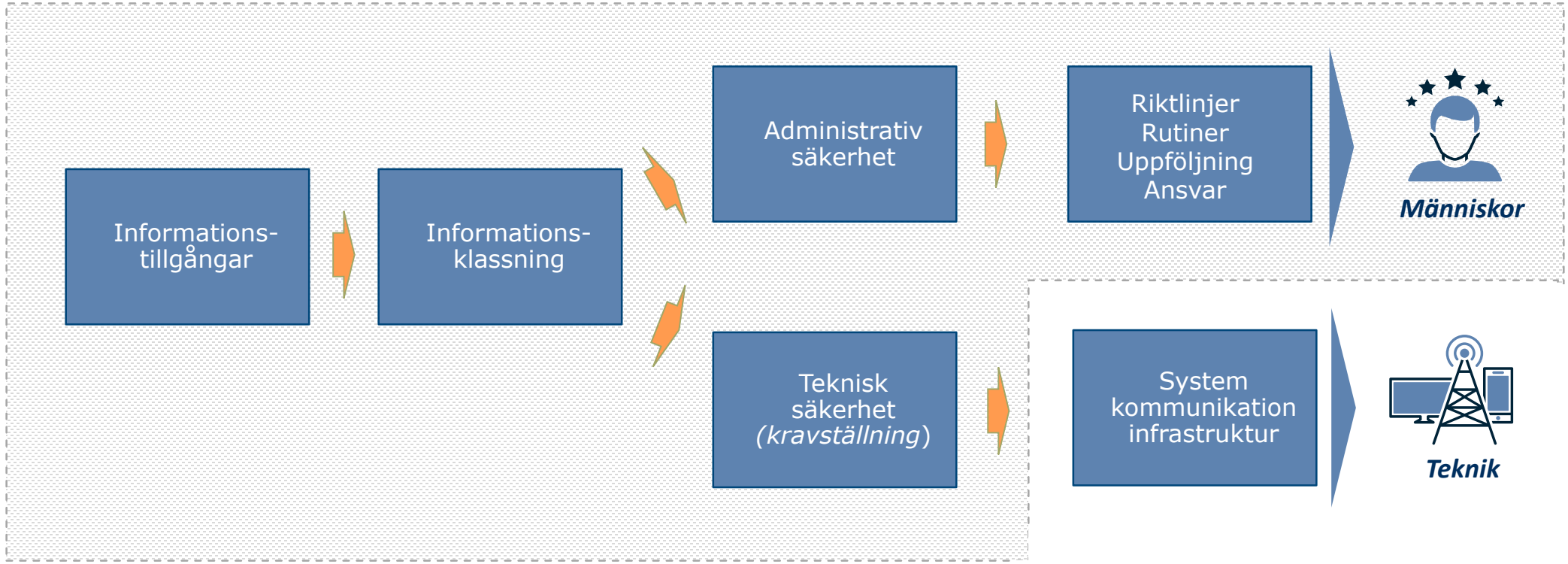
Stockholms universitet

Klassningsmatris SU

Version 1.0

		Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet
4	Hög skyddsnivå	**K4** Information där förlust av konfidentialitet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R4** Information där förlust av riktighet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T4** Information där förlust av tillgänglighet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**S4** Information där förlust av spårbarhet innebär **allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
3	Utökad skyddsnivå	**K3** Information där förlust av konfidentialitet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R3** Information där förlust av riktighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T3** Information där förlust av tillgänglighet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**S3** Information där förlust av spårbarhet innebär **betydande** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
2	Grundläggande skyddsnivå	**K2** Information där förlust av konfidentialitet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R2** Information där förlust av riktighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T2** Information där förlust av tillgänglighet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**S2** Information där förlust av spårbarhet innebär **måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
1	Ingen skyddsnivå	**K1** Information där förlust av konfidentialitet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**R1** Information där förlust av riktighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T1** Information där förlust av tillgänglighet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.	**T1** Information där förlust av spårbarhet inte medför någon negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

Informationsklassningen identifierar risker att åtgärda



Stockholms universitet

Administrativa Skyddsåtgärder

Rutiner för de mest skyddsvärda informationsobjekten säkras upp med med hjälp av en särskild checklista

Informations-klass	Typ av administrativ hantering									
	Generell tillämpning	Privata enheter	Delning av information	Åtkomst	Videomöte	Lagring och delning	E-post hantering	SMS och chatt	Digitala media (USB)	Pappers-dokument
K1 – Ej konfidentiell Öppen										
K2 – Konfidentiell Intern										
K3 – Konfidentiell medel										
K4 – Konfidentiell Hög										

Får **ej** hanteras på privat utrustning t.ex. dator eller smartphone, på privata e-postkonton eller i molntjänster som inte godkänts för ändamålet av SU.

Endast med behöriga. Säkerställ att samtalet inte överhörs av obehöriga.

Ska krypteras

Ska låsas in i säkerhetsskåp när de ej är under direkt uppsikt.

Stockholms universitet

Konsekvensnivåer - kategorier och nivåer

version 1.0 2022

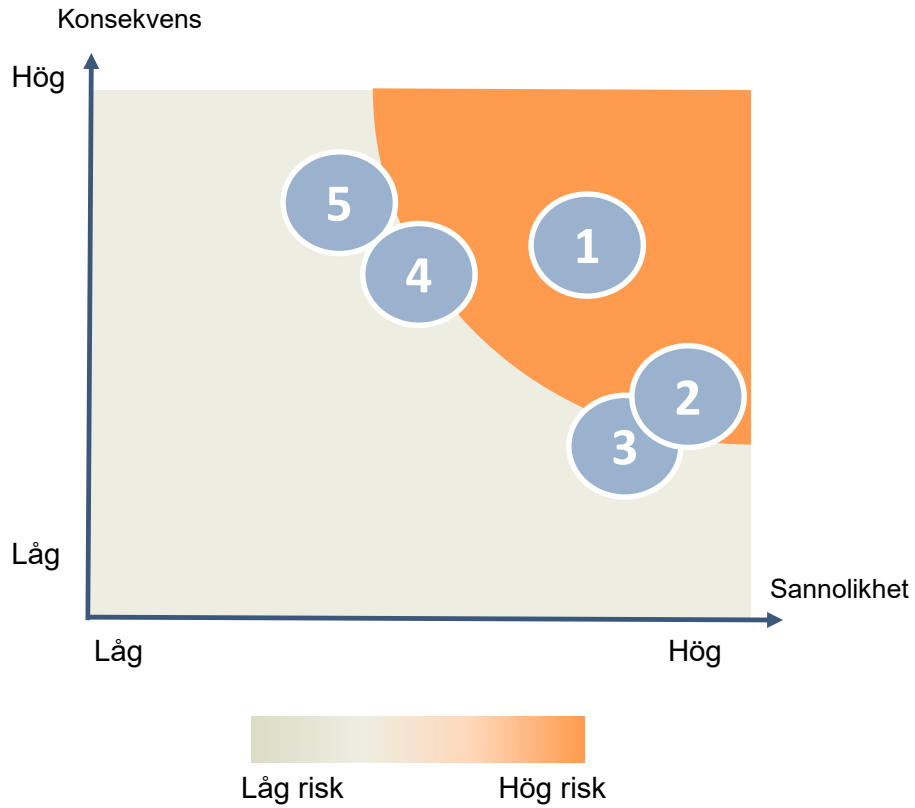
	Nivåer	Kategorier: Ekonomi och finanisering	Verksamhet	Varumärke och Förtroende	Individ	Miljö och hållbarhet	Juridik
4	Hög skyddsnivå	Mycket stor påverkan, över 10 msek	Hela verksamheter står stilla. Stor skada riskeras på egendom inom SU. Stor mängd personer, fler än 500. Allvarliga problem att uppnå verksamhetsmål. Långtids forskning påverkad eller förstörd. Omfattande påverkan på HelpDesk/ServiceCenter.	Negativ debatt i större omfattning i TV, radio och rikspress. Stor påverkan på universitets trovärdighet. Stor påverkan på samarbetspartners och externa intressenter.	Fara för liv. Allvarliga bestående emotionella eller fysiska problem. Allvarligt påverkat eller förstört anseende som forskare. Studenter/forskare/medarbetare väljer att lämna SU.	Allvarliga miljö- och/eller hållbarhetskador som kräver omfattande återställningsarbete. Irreversibel miljö- och/eller hållbarhetsskada. Miljöskada som bryter mot lagar och regler. Långvarig störning (ljud, ljus, lukt, framkomlighet).	Hot om avsked eller fängelse efter brott mot lagar, förordningar eller avtal. Höga viten, skadestånd eller sanktioner.
3	Utökad skyddsnivå	Stor påverkan, 5 - 10 msek	Ett större antal personer påverkas, 100 – 500. Allvarlig påverkan på ett fåtal personer. Visstids forskning påverkad eller förstörd. Märkbart höjd belastning på HelpDesk/ServiceCenter.	Negativ debatt i större omfattning i lokala medier. Påverkan på universitets trovärdighet. Potentiell påverkan på samarbetspartners och externa intressenter.	Övergående emotionella eller fysiska problem. Påverkat anseende som forskare. Individer hotar med att lämna SU.	Miljö- och/eller hållbarhetsskada som kräver återställningsarbete. Miljö- och/eller hållbarhetsskada som bryter mot lagar och regler. Långvarig mindre störning (ljud, ljus, lukt, framkomlighet).	Vite, skadestånd, sanktioner eller varning efter brott mot lagar, förordningar eller avtal.
2	Grundläggande skyddsnivå	Liten påverkan, 100 tsek – 5 msek	Viss mängd personer påverkas, 10 – 100. Betydande påverkan på ett fåtal personer. Ingen större belastning för HelpDesk/ServiceCenter.	Intern kritik som kräver åtgärd, t ex internt möte.	Irritation, oro eller obehag hos individer, men ingen kvarvarande påverkan.	Måttlig miljö- och/eller hållbarhetsskada där effektiva motåtgärder snabbt kan sättas in. Kortvarig störning (ljud, ljus, lukt, framkomlighet).	Varning eller erinran efter försumlighet mot lagar eller avtal.
1	Ingen skyddsnivå	Ingen eller liten påverkan, < 100 tsek	Enstaka personer påverkas. Enstaka system eller systemfunktioner påverkas. Enstaka systemkonton missbrukas.	Intern kritik som enkelt kan besvaras tillfredsställande.	Möjlig irritation hos individ.	Liten miljö- och/eller hållbarhetsskada som enkelt kan åtgärdas. Kortvarig liten störning (ljud, ljus, lukt, framkomlighet).	Egen anmälan av incident.

Stockholms universitet

Riskanalys

Avvikelserna som identifierats under informationsanalysen sammanställs med hjälp av riskverktyget

Riskmatris



Riskbeskrivning

Risk	Beskrivning
1	
2	
3	
4	
5	

Illustrativt exempel

Risk att viktig information och/eller personuppgifter inte hanteras på ett säkert sätt pga. att medarbetare inte har en grundläggande kompetens och medvetenhet om regelverk avseende informationshantering.

Stockholms universitet

Informationsanalys

Informationsanalysen görs med hjälp av ett enkätverktyg som mäter mognadsnivån i informationshanteringen

1. Lokal IT-miljö/ användning

2. Organisation med roller och ansvar

3. Arbete med informationshantering

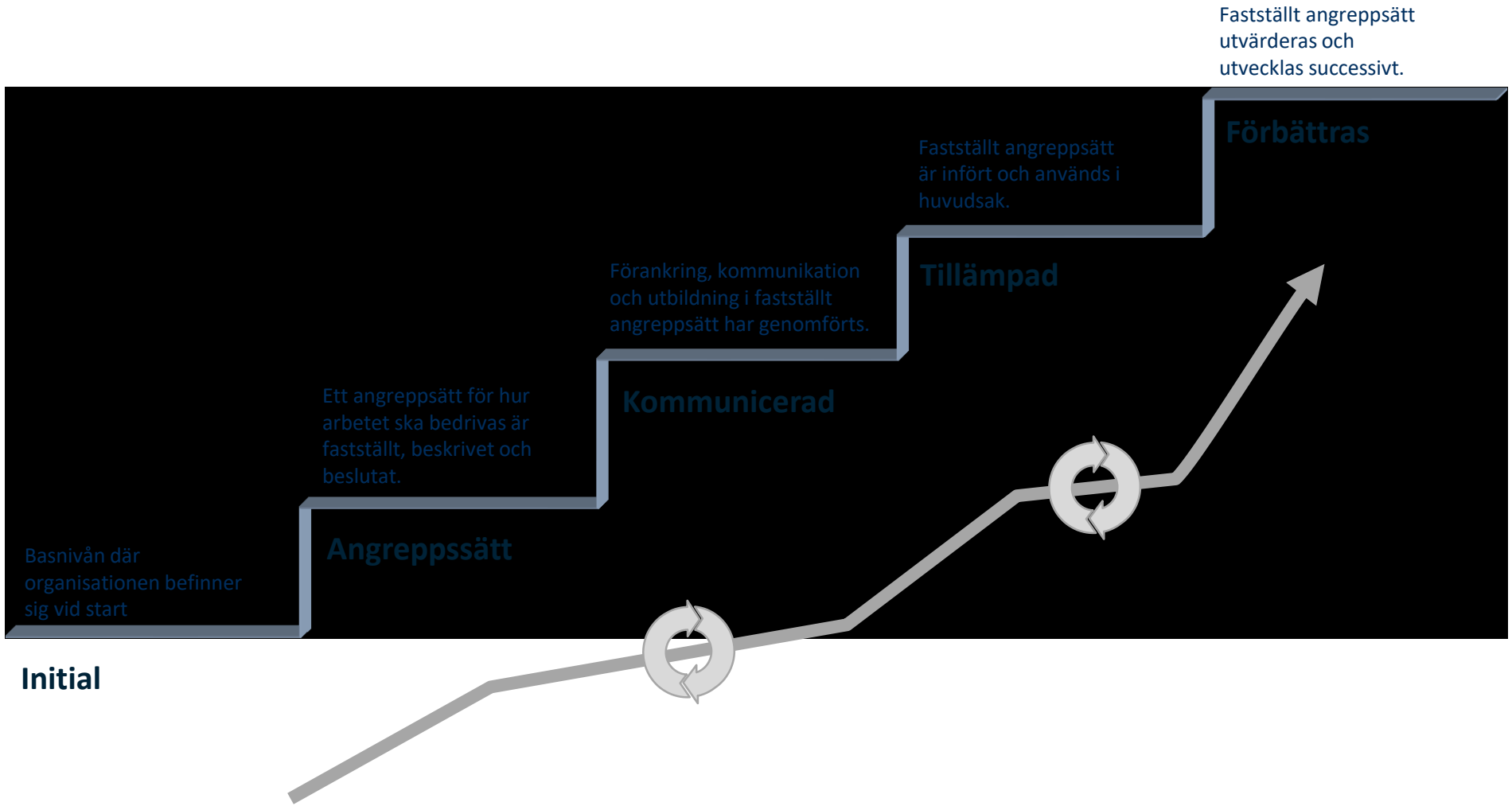
4. Informationshanterings-medvetande

5. Medarbetaransvar

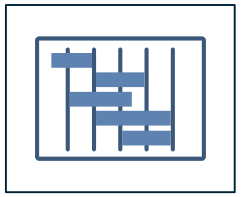
Informationsanalysen konkretiseras i fem delområden

Stockholms universitet

Självskattningen i enkäten har fem nivåer



Stockholms universitet



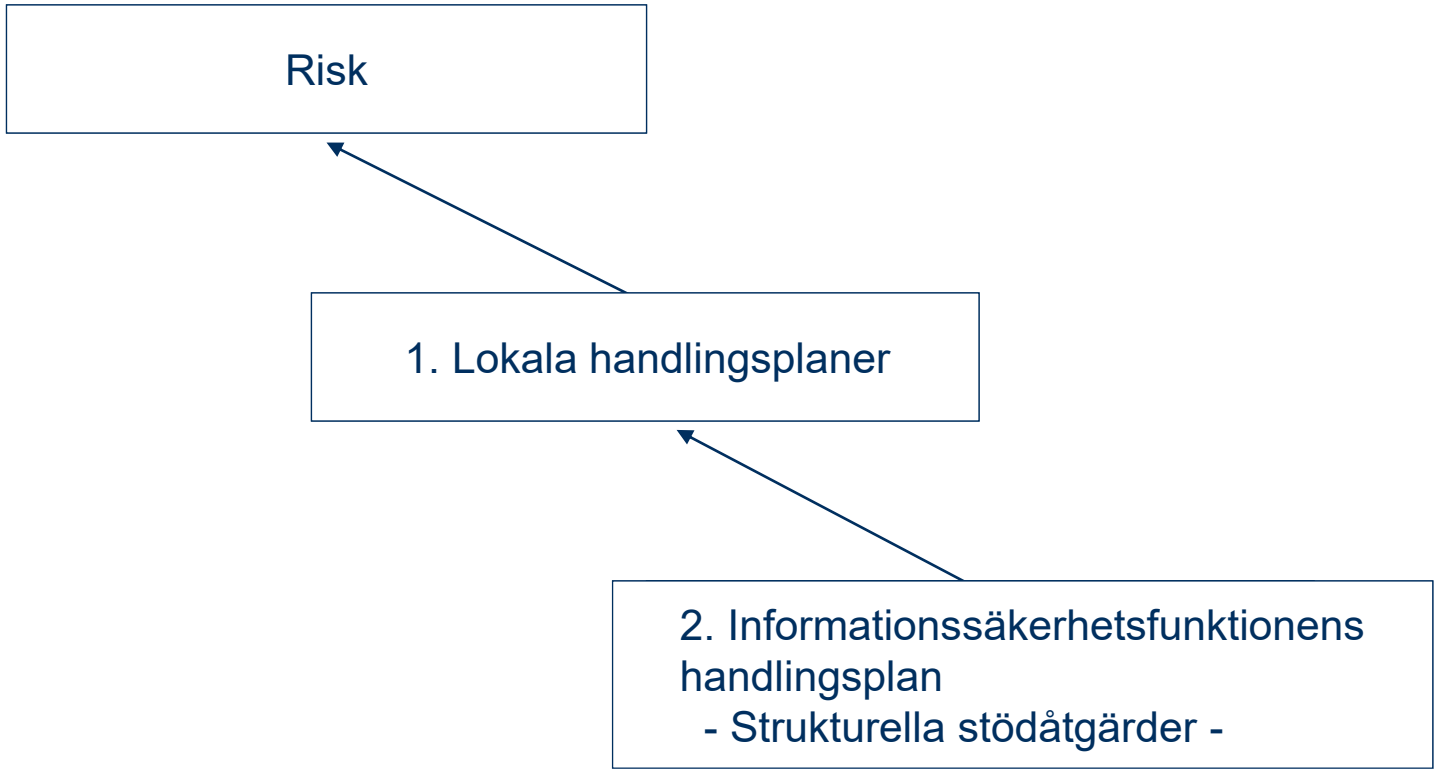
Handlingsplan

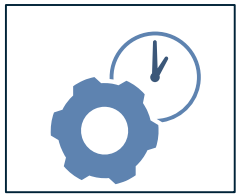
Högsta riskerna med vidhängande åtgärder överförs till en handlingsplan med utpekat ansvar och färdigdatum

Illustrativt exempel

Id	Iakttagelse	Risk	Åtgärd/Leverabel	Ansvarig	Klart	Stöd centralt
#1	Medarbetares kompetensutveckling avseende informationshantering och personuppgifts-hantering säkras ej i enlighet med gällande krav.	• Risk att viktig information och/eller personuppgifter inte hanteras på ett säkert sätt pga. att medarbetare inte har en grundläggande kompetens och medvetenhet om regelverk avseende informations-säkerhet/Dataskydd.	Säkerställ att medarbetare som hanterar viktig information och/eller personuppgifter i sitt arbete har nödvändig utbildning att säkra regelefterlevnad.	Prefekt	22nnnn	Säkerhetspolicy vid Stockholms universitet SU kostnadsfria online-utbildningar
#2	Allvarliga informations-säkerhetshändelser rapporters inte alltid.	• Risk att informationssäkerhets-händelser inte rapporteras och sårbarheter inte åtgärdas. • Risk för att bevis försvinner • Risk för förtroendeskada när regelverk inte efterlevs	Etablera ansvar och rutin lokalt för rapportering av av person-uppgiftincidenter och incidenter till MSB (Ska göras till It-avd av DSA eller motsvarande)	Adm.chf	22nnnn	Processbeskrivning (finns på intranätet) Central funktion som tar emot och vidarerapportera incidenter
#3	Det saknas en aktuell och fullständig registerförteckning över förekommande personuppgift-behandlingar.	• Risk att bristande regelefterlevnad orsakar vitesföreläggande. • Risk att personuppgifter inte hanteras på ett säkert sätt och kan förloras, hamna i orätta händer och att de vid begäran ej kan lämnas ut eller raderas	Upprätta/färdigställa registerförteckning över förekommande personuppgiftbehandlingar.	Adm.chef	22nnnn	Masterdatamodell Ta fram angreppsätt och mallar för att identifiera och dokumentera register-förteckningar

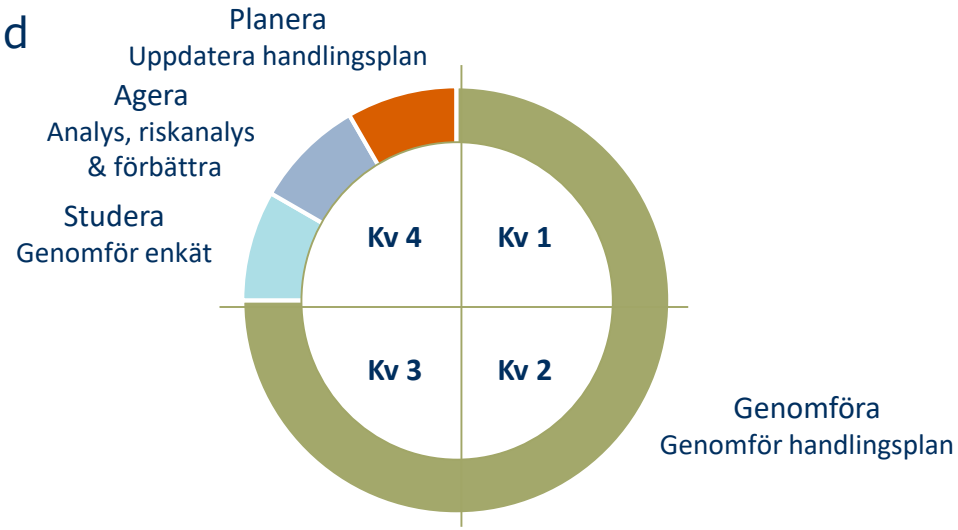
De lokala handlingsplanerna är understödda av strukturella projektåtgärder





Med hjälp av årshjul och återkommande mätningar säkerställs det kontinuerliga förbättringsarbetet

- Årshjulet bygger på förbättringshjulet PGSA [1)] och ger de övergripande aktiviteterna för året som syftar till att över tid utveckla och förbättra arbetet med informationssäkerhet.
- Årshjulet börjar i kvartal 4 med
  - fastställande av nuläge (uppföljningsenkät)
  - analys baserat på nuläge och uppdaterad riskanalys
  - planering och uppdatering av handlingsplan för genomförande kommande år
- Under kvartal 1 till 3 genomförs den handlingsplanen
- Vid större förändringar, exempelvis förändrade arbetssätt, organisatorisk förändring eller införande av nya it-system/tjänster kan det vara aktuellt att genomföra ”studera, agera och planera”.



[1)] Årshjulet bygger på Demings förbättringshjul PDSA översatt till PGSA

Arbetsgång för bredinförande för säker informationshantering

Utveckla förståelse — Reducera risker

1	2	3	4	5
Inledande möte **Prefekter/motsvarande och administrativa chefer**	**inventera och klassa information**	**Informationsanalys** **Genomföra enkät och analysera svar**	**Handlingsplaner informationssäkerhet**	**Årlig uppföljning** **Uppföljningsenkät och översyn**
Inledande möten för att annonsera och skapa medvetenhet	▪ Inventera information ▪ Klassa inventerad information ▪ Introducera enkät	▪ Genomför enkät ▪ Analys av enkätsvar och gjord klassning ▪ Förbered riskanalys och handlingsplaner	▪ Genomgång enkät ▪ Riskanalys ▪ Utarbeta handlingsplan utifrån nuläge och börläge	▪ Uppföljningsenkät ▪ Översyn att klassning är aktuell ▪ Riskanalys ▪ Uppdatera handlingsplan
Fakulteter och förvaltningen	2 - 3 tillfällen	Ca 50 institutioner + 15 avd.	1 tillfälle	Ca 505 institutioner + 15 avd.

Stockholms universitet

Dokumentförteckning

Kommunikationspaket

- Masterkommunikation

Stödjande dokument

- Referensmodell masterdata
- Informationshantering
- Enkät informationshanteringssanalys
- Riskanalys och handlingsplan
- Mätning och uppföljning

Upprättade dokument (mallar)

- Informationsförteckning och klassning
- Enkät Informationshanteringssanalys
- Riskanalys och handlingsplan

Upprättade dokument (exempel)

- Informationsförteckning och klassning
- Registerförteckning GDPR
- Riskanalys och handlingsplan

Underlag styrdokument

Stockholms universitet

Vad har hänt med omprioritering av informations- och IT-säkerhetsarbetet utifrån omvärldsläget

Åtgärdslista sid 1(5)

Område	Krav	P	K	Leverabler	Status IT 2022-03	Status IT 2022-10	Status SU 2022-03	Status SU 2022-10	Notering
Ansvar	Krav att för varje system tydliggöra befattning som ansvarar för att införa och förvalta säkerhetsåtgärder	na	R	Uppdatera rollbeskrivning (systemägare)	Klart	Klart	NA	NA	
		na	F	Etablera ansvar och rutin för etablering	Pågår	Pågår.	NA	NA	Klart 2023-01
Omvärlds-bevakning och riskbe-dömning	Omvärldsbevakning identifiering och hantering av hot och sårbarheter i myndighetens informationssystem.	M	R	Regelverk för omvärldsbevakning	Kvarstår	Pågår	NA	NA	Klart 2022-12
		M	F	Etablera rutiner och ansvar för omvärldsbevakning	Kvarstår	Pågår	NA	NA	
	Riskbedömning för enskilda system och för produktionsmiljön i sin helhet.	H	R	Regelverk och stöd för informationsklassning	Kvarstår	Pågår	NA	NA	
		H	D	Informationsklassning varje system	Kvarstår	Kvarstår	Kvarstår	Kvarstår	
		M	F	Etablera rutiner och ansvar för kontinuerlig informationsklassning	Kvarstår	Kvarstår	Kvarstår	Kvarstår	
Dokumentation av IT miljön	Dokumentation över varje system	M	R	Regelverk för dokumentation, systemkarta och beroenden	Kvarstår	Pågår	NA	NA	
		L	D	Dokumentering av beroenden, varje system	Kvarstår	Pågår	Utreds	Kvarstår	
Kravställning och kontroll	Krav på säkerhet vid utveckling, anskaffning och utkontraktering	L	R	Kravkatalog	Kvarstår	Klart	Klart	Klart	
		L	F	Etablera ansvar och process för kravkatalog	Kvarstår	Kvarstår	Kvarstår	Kvarstår	

P = Prioritet; H=Hög, M=Medel, L=Lägre

K = Kategorier; R= Regelverk, D=Dokumentera, T=Teknik åtgärd, F= Förändra/etablera

Stockholms universitet

Åtgärdslista sid 2(5)

Område	Krav	P	K	Leverabler	Status IT 2022-03	Status IT 2022-10	Status SU 2022-03	Status SU 2022-10	Notering
IT-miljöer	Krav på separerade IT-miljöer; utveckling, test, utbildning och produktion	na	R	Regelverk för olika miljöer	Kvarstår	Pågår	NA	NA	Klart 2022-12
		na	T	Separation av IT-miljöer	Kvarstår	Pågår	Utreds	Kvarstår	
	Krav på avidentifierad data i icke-produktionsmiljö	H	T	Avidentifiering av testdata i IT-miljöer	Kvarstår	Kvarstår	Utreds	Kvarstår	
Nätverk	Uppdelning i nätverkssegment och filtrering av nätverkstrafik	H	R	Regelverk för nätsegmentering	Kvarstår	Pågår	NA	NA	Klart 2022-12
		M	T	Segmentering enl. regelverk	Kvarstår	Kvarstår	Utreds	Kvarstår	*(påbörjat utifrån informell modell) Vakans för utförare*
		H	F	Göra brandväggshantering *(saknas uppföljning/avbeställningar)*	Kvarstår	Kvarstår	Utreds	Kvarstår	
Behörighets–hantering	Krav på lösenordshantering och 2-faktorsautentisering.	H	R	Regelverk för lösenordshantering *(behöver justeras med 2 faktor)*	Kvarstår	Pågår	NA	NA	Klart 2022-12
		H	T	Förstudie 2-faktor	Kvarstår	Pågår	NA	NA	
		H	T	Införande av 2-faktor	Kvarstår	Kvarstår	NA	NA	
		na	F	Etablera ansvar och rutiner för behörighetshantering	Klart	Klart	Utreds	Pågår	

Stockholms universitet

Åtgärdslista sid 3(5)

Område Syse	Krav	P	K	Leverabler	Status IT 2022-03	Status IT 2022-10	Status SU 2022-03	Status SU 2022-10	Notering
Kryptering	Krav på regler för kryptering och införa DNSSEC på interna DNS servrarna.	L	R	Regelverk för kryptering	Kvarstår	Kvarstår	NA	NA	Klart 2022-12
		M	T	Lösning och införande av DNSSEC på DNS servrar	Kvarstår	Pågår	NA	NA	Vakans för utförare
		L	F	Etablera ansvar och rutiner för kryptering i servermiljö	Kvarstår	Pågår	Utreds	Kvarstår	
		H	T	Myndigheten bör införa möjlighet att verifiera myndigheten som avsändare respektive mottagare av e-post. (DKIM, SPF)	Kvarstår	Klart	Klart	Klart	
Säkerhets-konfigurering	Krav på skydda informationssystem mot obehörig åtkomst, tex blockera systemfunktioner som inte behövs.	H	R	Checklistor och mallar för ”härdning” (CIS benchmark)	Kvarstår	Kvarstår	Utreds	Kvarstår	
		H	T	Konfigurera härdning *(påbörjat utifrån informell modell)*	Kvarstår	Kvarstår	Utreds	Kvarstår	
		M	F	Etablera ansvar och rutiner för härdning	Kvarstår	Kvarstår	Utreds	Kvarstår	
Säkerhets-tester och granskningar	Krav att säkra att säkerhetstester och granskningar möjliggör identifiering av sårbarheter	L	R	Regelverk för regelbundna säkerhetstester	Kvarstår	Pågår	NA	NA	Klart 2022-12
		H	T	Teknisk lösningar för larmsättning av patchningsnivåer	Kvarstår	Pågår	Utreds	Kvarstår	
		M	T	Lösning för att utföra tekniska säkerhetstester inkl. scanning	Pågår	Pågår	NA	NA	
		L	F	Etablera ansvar och rutiner för säkerhetstester/gransk.	Kvarstår	Pågår	NA	NA	

Stockholms universitet

Åtgärdslista sid 4(5)

Område	Krav	P	K	Leverabler	Status IT 2022-03	Status IT 2022-10	Status SU 2022-03	Status SU 2022-10	Notering
Ändrings-hantering	Krav på att säkerställa att förändringar genomförs på ett strukturerat och spårbart sätt.	L	D	Dokumentera regelverk för patch-hantering (enligt befintligt arbetssätt)	Kvarstår	Pågår	Utreds	Kvarstår	
Korrekt och spårbar tid	Krav på korrekt och spårbar till universell tid, UTC(SP)	na	T	Införa korrekt och spårbartid i produktionsmiljö	Klart	Klart	Klart	Klart	
Säkerhets-loggning och övervakning	Krav att säkerställa spårbarhet i informationssystem, logga följande säkerhetsrelaterade händelser	M	R	Regelverk för loggning och övervakning	Kvarstår	Pågår	NA	NA	Klart 2022-12
		na	T	Ta fram och inför tekniska lösningar för loggning av konton/rättigheter och övervakning	Klart	Klart	Utreds	Kvarstår	
		M	F	Justera ansvar och rutiner för loggning och övervakning	Kvarstår	Kvarstår	Utreds	Kvarstår	
Skydd mot skadlig kod	Krav på användning av mjukvara som ger skydd mot skadlig kod	H	R	Regler för övervakning och användning av mjukvara som ger skydd mot skadlig kod	Kvarstår	Klart	Utreds	Klart	
		H	T	Etablera ansvar och rutiner för övervakning och hantering av skadlig kod	Kvarstår	Pågår	Utreds	Kvarstår	

P = Prioritet; H=Hög, M=Medel, L=Lägre

K = Kategorier; R= Regelverk, D=Dokumentera, T=Teknik åtgärd, F= Förändra/etablera

Stockholms universitet

Åtgärdslista sid 5(5)

Område L	Krav	P	K	Leverabler	Status IT 2022-03	Status IT 2022-10	Status SU 2022-03	Status SU 2022-10	Notering
Skydd av utrustning	Krav på att skydda utrustningen som hanterar informationssystem,	na	R	Regler för besökshantering (*saknas krav på spårbarhet besök)*	Klart	Klart	Utreds	Utreds	
		L	R	Regler för hantering av mobila enheter (dator och mobil) utanför fysiska lokaler	Kvarstår	Kvarstår	NA	NA	
		L	F	Etablera ansvar och rutiner för skydd	Kvarstår	Kvarstår	Utreds	Utreds	
Redundans och återställning	Krav att säkra tillgänglighet till information och informationssystem vid incidenter och avvikelser	M	R	Regler för återställning och redundans *(hur uppdatera/förtydliga återställning)*	Kvarstår	Kvarstår	NA	NA	
		M	D	Ta fram återställningsplaner (för varje system)	Kvarstår	Kvarstår	Utreds	Kvarstår	
		M	F	Etablera rutiner och ansvar för redundans och återställning	Kvarstår	Kvarstår	Utreds	Kvarstår	
Säkerhets-kopiering	Krav att återställa information som förlorats eller förvanskas genom att regelbundet säkerhetskopiera information	M	R	Regler för säkerhetskopiering, behöver uppdateras	Kvarstår	Kvarstår	NA	NA	
		M	F	Uppdatera rutiner och ansvar för säkerhetskopiering (enligt regler och informationsklassning)	Kvarstår	Kvarstår	NA	NA	

P = Prioritet; H=Hög, M=Medel, L=Lägre

K = Kategorier; R= Regelverk, D=Dokumentera, T=Teknik åtgärd, F= Förändra/etablera

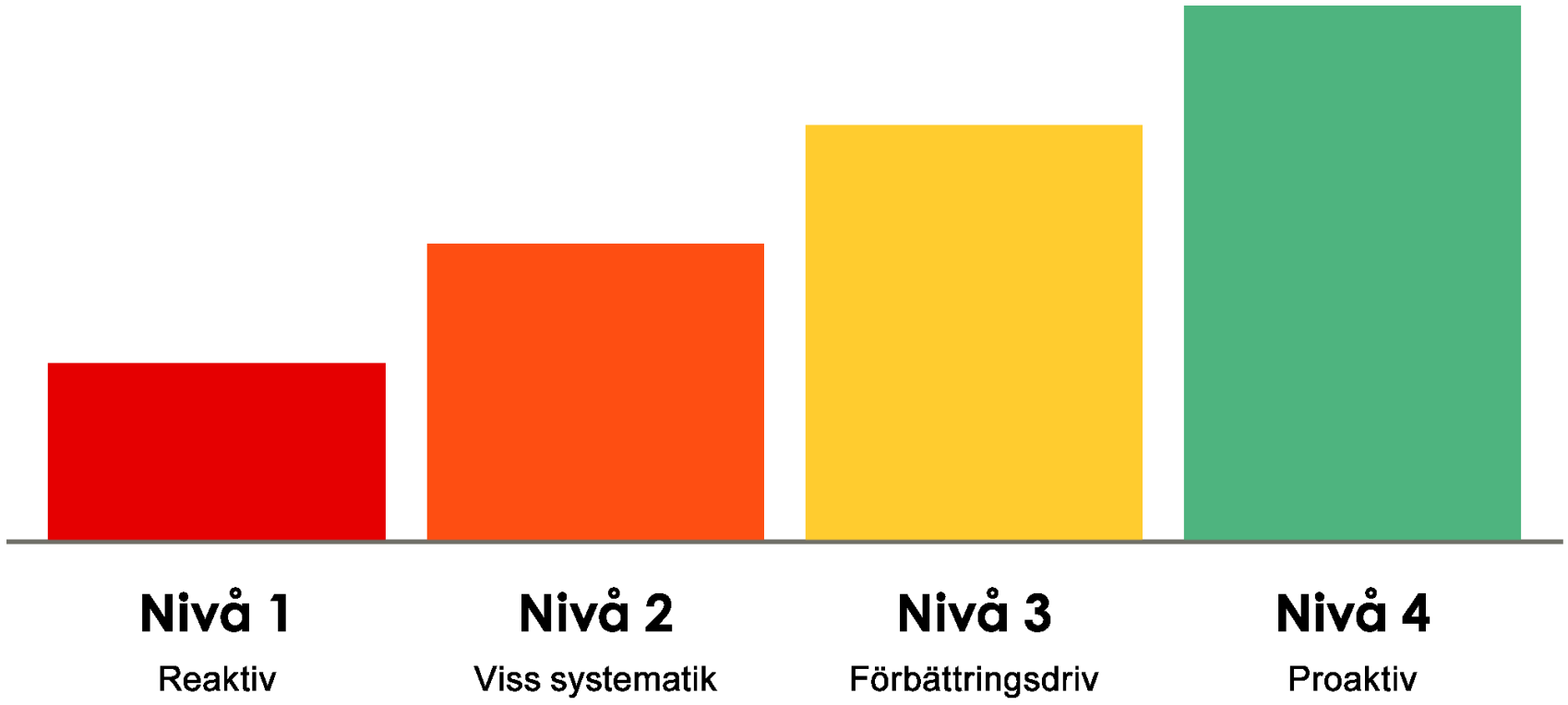
Stockholms universitet

Mognadsmätning för Informationssäkerhet – uppdelat i centrala sex perspektiv

- Riskhantering
- Informationsklassning
- Incidenthantering
- Upphandling
- Kompetens
- Uppföljning

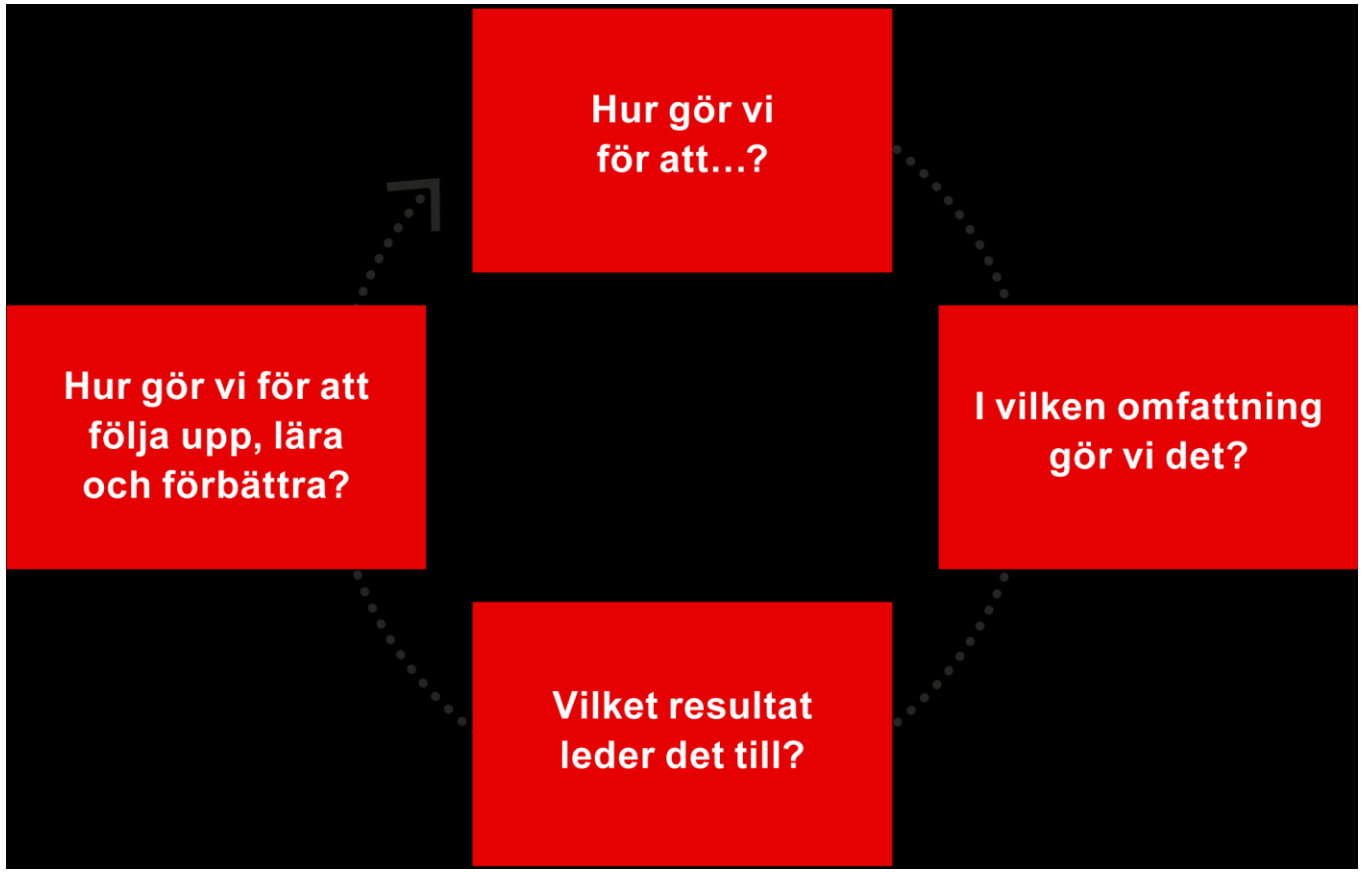
Stockholms universitet

Mognadsdialogen



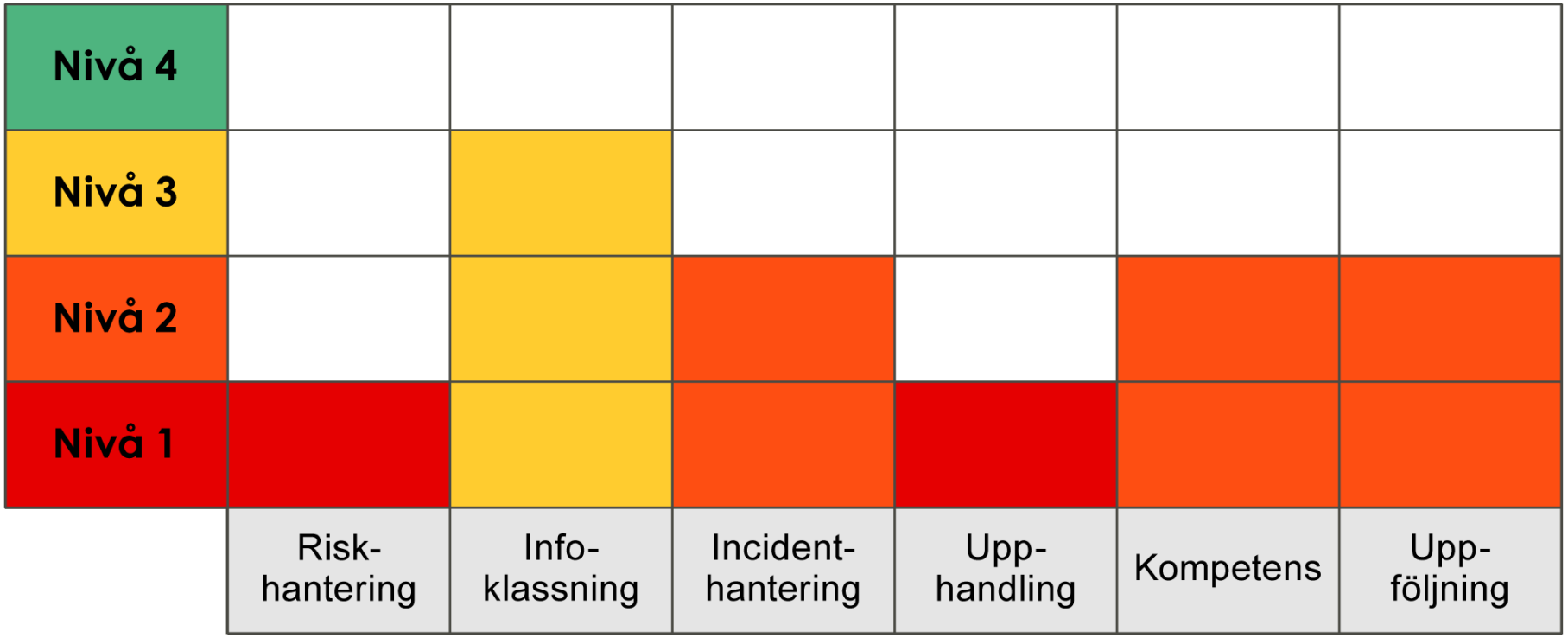
Stockholms universitet

Det systematiska arbetssättet - fångas upp i frågorna



Stockholms universitet

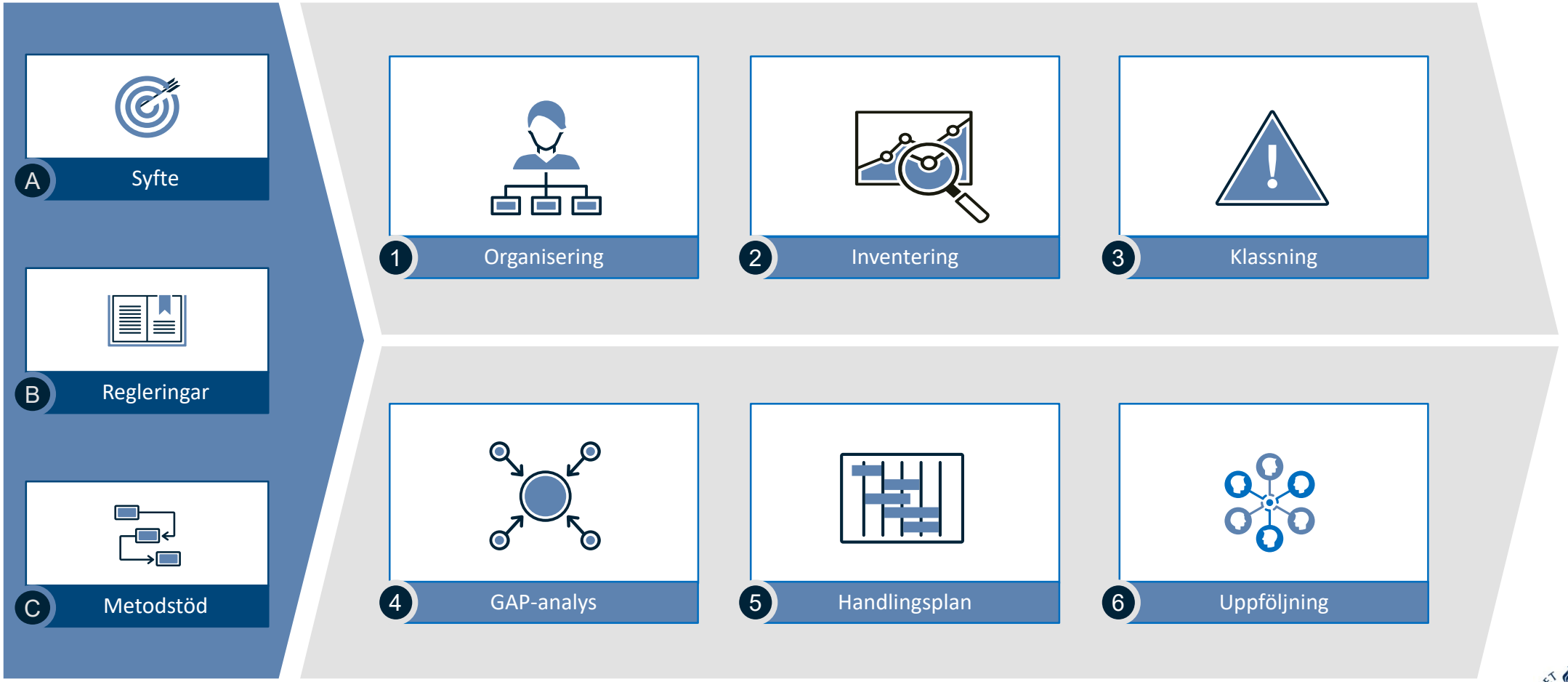
Mognadsdialogen
- exempel på resultat



Stockholms universitet

	Nivå 1	Nivå 2	Nivå 3	Nivå 4
Kännetecken/kultur	**Reaktiva**	**Viss systematik**	**Förbättringsdriv**	**Proaktiv, förutseende**
Arbetssätt	Saknar i huvudsak gemensamma medvetet valda arbetssätt inom området. Lösryckte arbetssätt finns men ofta otydliga, okända eller hänger inte ihop. Låg insikt om behov av struktur inom området.	Några gemensamma, medvetet valda arbetssätt inom området. Arbetssätten hänger inte alltid ihop (samordnade). Insikt om behov av struktur och systematik finns.	Flera gemensamma, medvetet valda arbetssätt. Arbetssätten hänger ihop (samordnade). Bygger struktur och systematik. Roller och ansvar finns. Högt driv för struktur och systematik	Genomtänka, medvetet valda, väl samordnade arbetssätt inom området. Mycket systematiska och proaktiva. Arbetssätten utgår tydligt från intressenternas krav, behov och förväntningar. Roller och ansvar är adekvata och fungerar väl.
Tillämpning	Var och en arbetar efter eget huvud och situationen styr. Vissa arbetssätt tillämpas sporadiskt.	Arbetssätten används i begränsad omfattning, dvs inte i alla relevanta processer och situationer. Arbetssätt kan nyligen ha införts eller håller på att införas. Inte kända hos alla.	Arbetssätten är kända. Arbetssätten används i god omfattning i de flera relevanta processer/situationer.	Arbetssätten är välkända, används i alla relevanta processer/situationer.
Resultat	Inga långsiktiga resultat samlas in, eller jämförs över tid. Enstaka resultat och ekonomiresultat har fokus. Saknar mål.	Enstaka resultat samlas in och jämförs över tid men hänger ofta inte ihop med formulerade mål. Enstaka goda resultat. Resultaten kan sällan härledas till arbetssätten.	Flertalet resultat samlas in och jämförs över tid. Vissa uthålliga positiva resultat, vilka kan kopplas till formulerade mål. Jämför inte resultat med andra. Viss osäkerhet om resultat kan härledas till arbetssätten.	Flera relevanta resultat som visar positiva trender kopplade till formulerade mål. Positiva, uthålliga resultat, även i jämförelse med andra organisationer. Resultat kan tydligt härledas till arbetssätten. Resultatfokus
Följa upp, lära och förbättra	Reaktiv. Fokus på problemlösning och korrigerande åtgärder. Saknar insikt, men pratar OM uppföljning. Följer inte upp, utvärderar och lär inte över tid.	Enstaka arbetssätt och processer följs upp, resultat (mest tillämplighet) analyseras. Förbättringar sker ofta ad hoc eller genomförs inte systematiskt. Börjar få insikt – driver på samverkan och teamarbete.	Flera arbetssätt/processer följs upp, resultaten (mest ändamålsenlighet) analyseras och leder till förbättringar. Viss osäkerhet om orsak och verkan. Lärande börjar få fokus för förbättringar. Hög insikt, nyfikenhet och ifrågasättande.	Proaktiv. Relevanta arbetssätt/processer följs upp, analyseras och förbättringar sker, metodiskt och agilt utifrån att öka effektivitet. Högt fokus på lärande i hela organisationen.

Upplägg för säker informationshantering



Stockholms universitet

Detaljering – processen analys av informationstillgångar, steg 1 - 3

1 Organisering

- Utse/allokera lokala roller
  - Informationsägare
  - Informationssäkerhets-samordnare.
- Inläsning av metodstöd och ev. tidigare gjorda informationsanalyser.
- Planera arbetet med att genomföra analys av informationstillgångar.

- Rollbeskrivningar (lokala)
- Processbeskrivning analys

2 Inventering

- Inventera vilken information/data institutionen/motsvarande hanterar och lagrar, både digitalt och fysiskt, samt ange informationsägare.
- Informationsdomäner inom en institution är:
  - Forskningsdata
  - Utbildningsdata
  - Administrativ data
  - Övrig adm. data

- Referensmodell masterdata
- Guide informationsklassning

3 Klassning

- Klassa inventerade informations-objekt med hjälp av anvisningarna i metodstödet för informationsklassning.
- Klassningen görs baserat på fyra risknivåer i dimensionerna:
  - Konfidentialitet (K)
  - Riktighet (R)
  - Tillgänglighet (T).

- Guide informationsklassning

Detaljering – processen analys av informationstillgångar, steg 4 - 6

4 GAP-analys

- Gå igenom beslutad informationsklassning
- Analysera och dokumentera eventuella gap, särskilt för informationsobjekt med högt riskvärde i gjord informationsklassning.
- Studera även klassade objekt med hjälp av det stödjande dokumentet administrativa skyddsåtgärder för hantering av information

- Analys
- Guide administrativa skyddsåtgärder

5 Handlingsplan

- Värdera noterade gap från säkerhetsanalysen i riskmodellen och bestäm hantering.
- Uppdatera handlingsplanen från riskanalysen med riskägare, ansvarig för åtgärder och datum när åtgärden ska vara på plats.
- Ta gärna hjälp av tidigare redan gjorda riskanalyser/handlings-planer

- Riskmodell samt guide riskanalys
- Riskanalysverktyg (Excel)

6 Uppföljning

- Följ upp den beslutade handlingsplanen inom beslutat tidsintervall
- Följ upp eventuella kvarstående risker med riskägaren
- Följ upp eventuellt beslutade undantag

- Guide Årshjul

I nästa steg kommer informationssäkerhetsarbetet:

- **Återuppta arbetet i november och erbjuda seminarium, föreslagen längd 55 min, målgrupp alla informationsägare**
- **Det åligger informationsägaren/institutionen att ta sitt ansvar och ta kontakt med informationsssäkerhetsfunktionen för att få stöd i genomförandet**
  - **Sannolikt så behövs det 1-2 mötestillfällen/institution för att göra informationsförteckningen komplett**
- **Progressen i detta arbete måste avrapporteras av informationssäkerhetsfunktionen till universitetsledningen i lämpligt fora**

Stockholms universitet

Stockholms universitet

Nya rapportverktyget

Jesper Bergqvist, Controller Planeringssekretariatet
samt projektledare Qlik Sense

Bakgrund

Nuvarande beslutsstöd

- Integrerat verksamhetsstöd (IVS)
- Samtliga anställda har behörighet
- Ca 100 rapporter
  - Ca 25 ekonomi
  - Ca 25 personal
  - Ca 35 utbildning
  - Ca 15 övrig uppföljning (printomat etc)
- Planeringssekretariatet produktansvariga. I dagsläget 2 beslutsstödsutvecklare på IT-avdelningen.
- Anledning till bytet

Nytt beslutsstöd

- Qlik Sense (BI-verktyg) system för datavisualisering som gör det möjligt att skapa flexibla interaktiva visualiseringar.
- Behörighet och rapporttillgång
- Initialt samma rapporter som finns i IVS ska kunna tas fram i Qlik Sense
- Prioritering data/information om Personal, Utbildning och Ekonomi
- Planeringssekretariatet produktansvariga. I dagsläget 2 beslutsstödsutvecklare på IT-avdelningen.

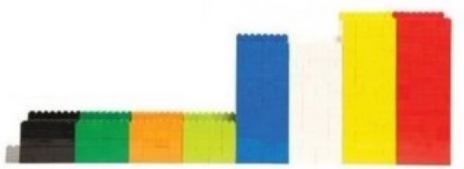
Beslutsstöd/Business intelligence (BI)

- Ett samlingsbegrepp för olika metoder och verktyg för att samla in, sortera, strukturera, visualisera och analysera stora mängder data.
- Data från olika källsystem (tex Raindance, Primula, Ladok) samlas in via ett datalager där informationen sorteras och struktureras och därefter visualiseras.
- Informationen presenteras så att det blir lättare att överblicka hur verksamheten utvecklas och samtidigt som det går att fördjupa sig i data för att förstå varför utvecklingen går i en riktning.


samla in


sortera


strukturera


visualisera


Förstå och förklara

Syfte/Mål

- Bättre analysmöjligheter
- Bättre möjligheter att fatta bra beslut
- Frigöra resurser från IVS
- Bättre och modernare arkitektur i Qlik Sense

Status idag

Utbildning – ett flertal rapporter är framtagna i Qlik Sens testmiljö och har kvalitetssäkrats under hösten. Ett fåtal rapporter saknas jämfört med vad som finns i IVS, bl.a. fyra rapporter kopplat till forskning.

Personal – merparten av rapporterna som finns i IVS går att få fram i Qlik Sense.

Ekonomi – Tre rapporter är framtagna i Qlik Sense; Balansräkning, Resultaträkning och EKUP.

Stockholms universitet

Inspera

Markus Forslund, Projektledare

Bakgrund

- Ge lärare större frihet att konstruera digital examination
- Öka rättssäkerhet genom att all examination i verktyget är anonymiserad och tillgänglighetsanpassad
- Effektivisera administration av examination genom t.ex. att integrera med Ladok, och Ouriginal/Urkund
- Öka kvaliteten på examination på Stockholms universitet

Fördelar med Inspera

- Snabb utveckling (på gång assessment paths, rubricks etc) följ utvecklingen
- Många fler frågetyper
  - 14 automatiskt rättade och 6 manuellt
- Fler typer av innehåll
  - Bild, film, ljud, länkar, excel, word, spss
- Möjlighet att samarbeta med andra lärosäten
- Flexibel användning
  - Öppen bok, med särskilda resurser, eller sluten
  - Salstenta, duggor, hemtenta
  - Bedömning och återkoppling till studenter
  - PC/Mac, eller surfplatta (sisådär)
- Minskad administration
  - Integrerad med Ladok
  - Den bedömda tentan går att skicka ut direkt till studenter
  - Automatisk gallring enligt RALS
  - Mallar
  - Frågebank
  - Möjlighet till automatisk arkivering (när SU har e-arkiv)
- Ingen extra kostnad utöver stolspriset
- Engagerat nätverk inom SUNET

Tidsplan

INFÖRANDET AV INSPERA VID SU

VT22	Pilotinstitutioner använder Inspera för hemtentor och BYOD salstentor
Sommar 2022	Centrala tentamenssalar byggs om
HT22 A+B	• Exia i centrala tentamenssalar • Inspera som BYOD salstenta för piloter • Medarbetare börjar med självstudie-kursen och institutioner börjar använda Inspera för hemtentor
VT23	• Inspera används i centrala tentamenssalar • Exia fortsätter på öppet nät
HT23	Exia avvecklas

Olika roller

Författare

Skapa frågor (uppgifter) och innehåll i en tenta (uppgiftsgrupper)

Admin

Lägga upp tentamenstillfälle, har alla behörigheter

Bedömare

Rättar och bedömer inlämnade svar

Tentamensvärd

Se översikt över pågående tentor samt studenter

VIKTIGT MED RELEVANT BEHÖRIGHET!
BEHÖRIGHET FÖRUTSÄTTER KURS

Stockholms universitet

Allmänt

- Viktiga datum
  - 15 september 2022 lansering självstudiekurs - det går nu att börja förbereda sig för lansering och Inspera kan användas för hemtentamen
  - 23 januari 2023 lansering centrala tentamenssalar
  - Exia öppet mot internet efter 23 januari 2023
  - Exia stängs för nya tentor inför ht 2023
- Inspera-koordinator
- Nyttja möjligheten med Examinationslyftet

Stockholms universitet

Fokusområde 2023

Säkerställa kvalitet i tjänsteleveranser med tillhörande support

Karin Olsson, gruppchef Portföljkontoret

Stockholms universitet

Säkerställa kvalitet i tjänsteleveranser med tillhörande support (1)

Nuläge

- Det finns i nuläget otydligheter i några av de tjänsteområden som IT-avdelningen ansvarar för och vilken service och support som ingår i de olika tjänsterna, samt vilka svarstider verksamheten kan förvänta sig.
- Detta skapar dels olika förväntansbilder och i förlängningen oklarheteter och frustration i verksamheten.

Säkerställa kvalitet i tjänsteleveranser med tillhörande support (2)

Nyläge

- IT-avdelningen kommer nu ta ett helhetsgrepp avseende tjänsteinnehåll, supportnivåer och svarstider. Fokus kommer läggas på IT-accessen, Arbetsplatstjänsten (SUA) samt Lokalt IT-stöd.
- Målsättningen är att förtydliga våra tjänsteleveranser och därmed också förbättra vår IT-service och supportfunktion
- Arbetet har precis påbörjats, och kommer därefter vara ett av avdelningens särskilda fokusområden för 2023.
- Vi kommer att återkomma närmare efter årsskiftet gällande innehåll och upplägg på ovanstående arbete.
- Frågor eller funderingar: Vänd dig till IT-chef Karin Tegefjord

Stockholms universitet

Tack för idag!
God jul och Gott nytt år!
Vi ses 2023!

IT-avdelningen återkommer med datum för första IT-forum VT23