



Vad krävs för certifiering med Core Trust Seal?

Webbinarium 2026-09-29

14.00 – 15.30



SND

Svensk nationell datatjänst | Göteborgs universitet - Chalmers tekniska högskola - Karolinska Institutet - Kungliga Tekniska högskolan - Lunds universitet - Stockholms universitet - Sveriges lantbruksuniversitet - Umeå universitet - Uppsala universitet



Dagordning

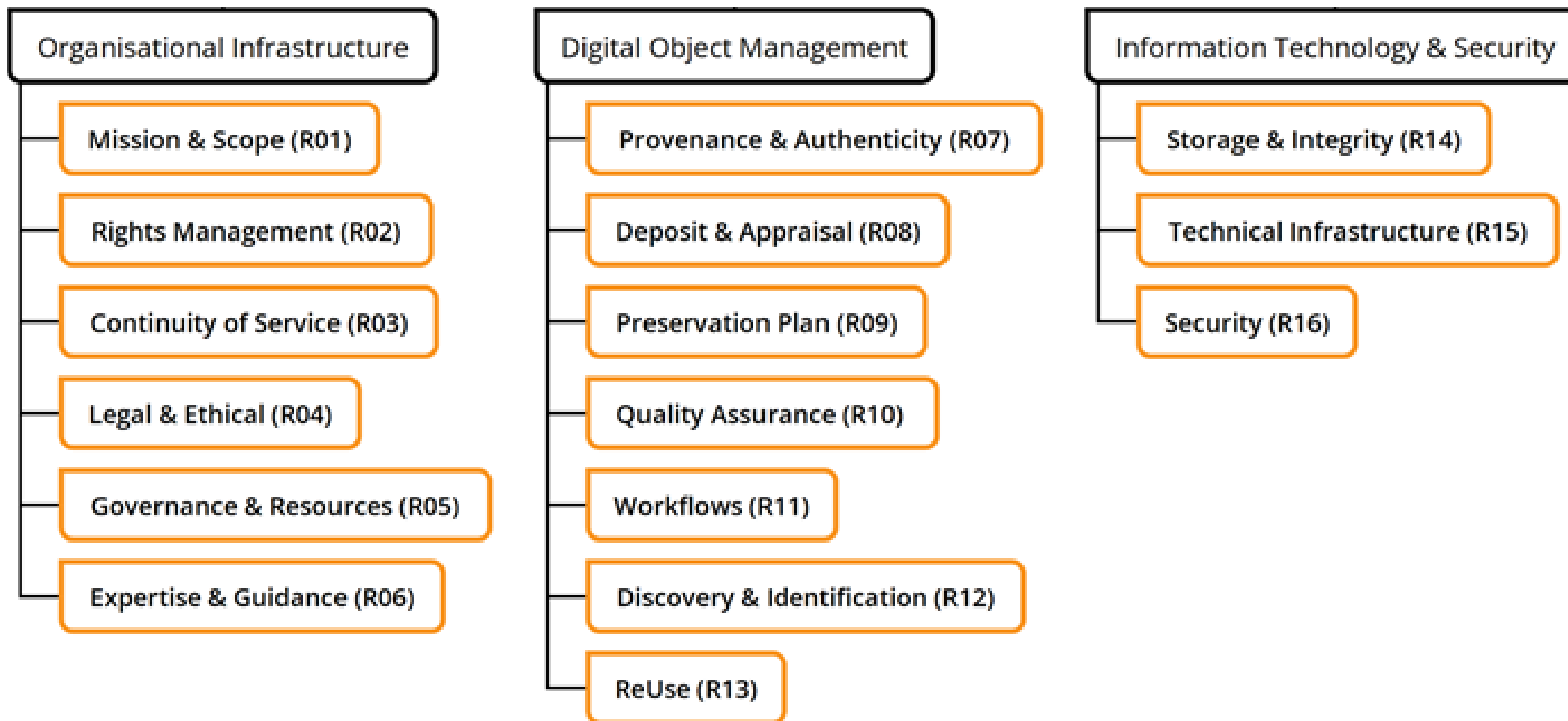
- Introduktion – CoreTrustSeal, vad och varför (bild 3-16)
- Bolincentret för klimatforskning (bild 17-31)
- KI Data Repository (bild 32-48)
- Granskningsprocessen och arbetet "bakom kulisserna" (bild 49-55)
- Frågor och diskussion (bild 56)

Vad är CoreTrustSeal (CTS)



- Internationell, "*community-based*" certifiering av datarepositorier/arkiv
- 16 grundläggande krav ("Core Requirements") med låga trösklar som är oberoende av ämnesområde
- Kostnad: EUR 3000
 - 5 inskick ingår
- Besvarar frågan: Kan man lita på att detta arkiv bevarar digitala data och ger åtkomst till dem över tid?

16 kravområden





Uppdateringar?



- Granskas och uppdateras vart tredje år
- Speglar praxis i ständig utveckling
- Utformas genom öppen samrådsprocess (RDA IG)
- Baseras på erfarenheter från sökande och granskare

Vad har ändrats (2026 – 2028)?

- **Tydlighet:** mindre utrymme för tvetydighet för sökande och granskare
- Starkare betoning på **aktivt bevarande**
- Tydligare sätt att beskriva **ansvaret** för kurering och bevarande, även vid utkontraktering av tjänsten *[outsourcing]*

Vad har förändrats: Från lagring till aktivt bevarande



- Tidigare krav suddade ut gränserna mellan lagring, kurering och bevarande
- Perioden 2026–2028 inför tydliga nivåer för hantering:
 - Endast lagring ("i befintligt skick") – Z
 - Kravuppfyllande vid deponering – D [*deposit compliance*]
 - Initial kurering – C
 - Aktivt bevarande – A
- Enbart säker lagring är inte längre tillräckligt
- I linje med EOSC-FIDELIS / TTRAM

Vad har ändrats: Outsourcing är tillåten, men inte ansvaret.



- Outsourcing innebär inte att ansvaret överförs till den externa tjänsteleverantören
- Repositorier måste tydligt redogöra för:
 - Vem som gör vad
 - Vilka avtal som gäller
 - Hur tillsyn och ansvarsutkrävande säkerställs

Vad har förändrats: Bevarande innefattar förändring



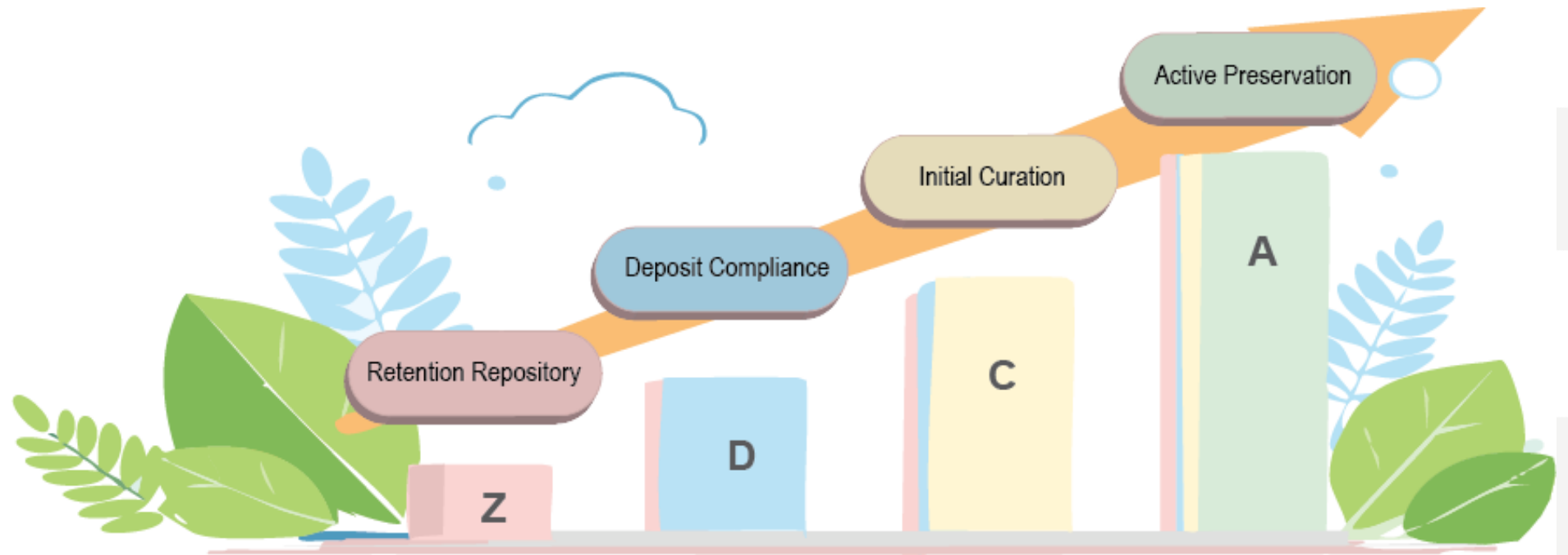
- Bevarande är inte detsamma som att "behålla allt för alltid"
- Arkiv och datalagringstjänster kan:
 - Omvärdera beståndet, inklusive att ta bort data
- Detta påverkar hur åtkomst, citering och PID:er måste dokumenteras

Vad har förändrats: Från policydokument till bevarande i praktiken

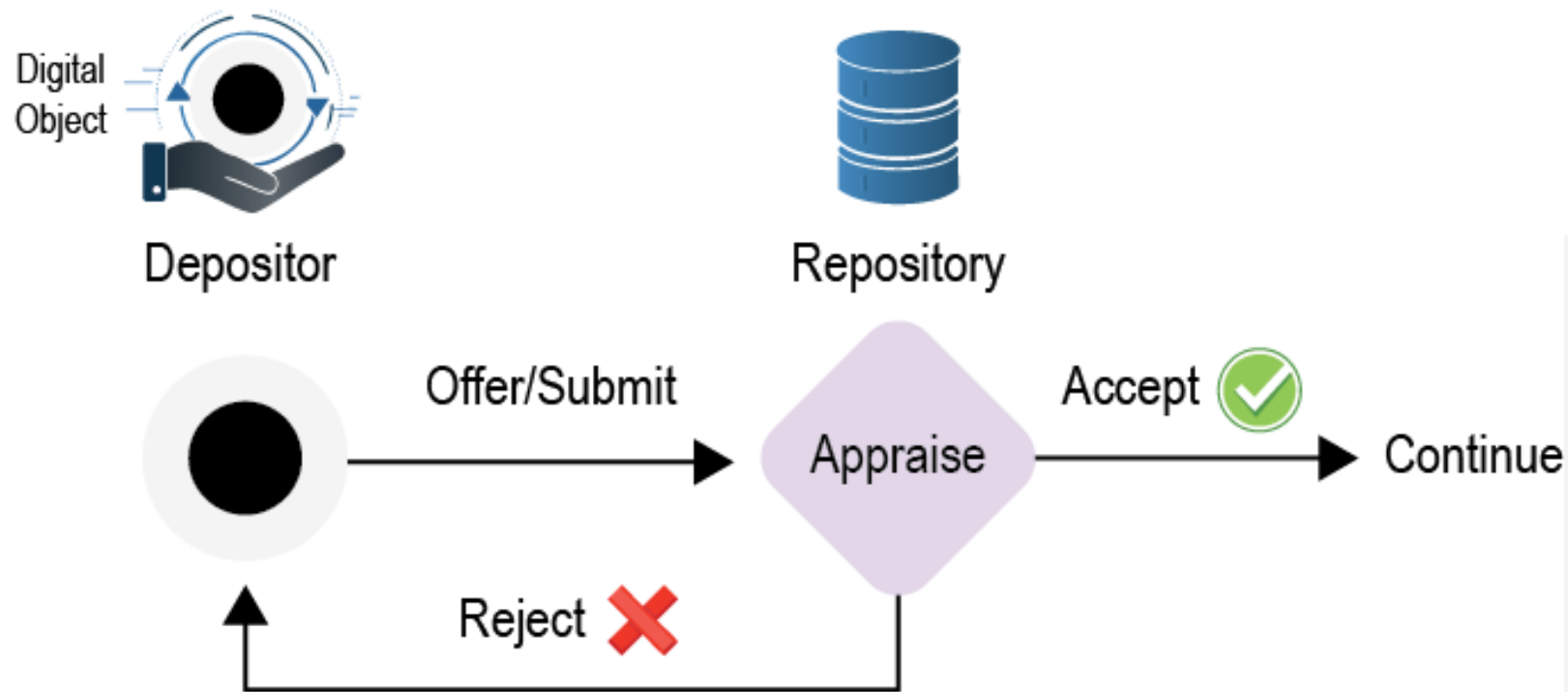


- Det räcker inte längre att ha en policy
- Mindre tolerans för rent ambitiösa påståenden
- Granskare förväntar sig tydligare bevis på arbetsflöden för bevarande, vidtagna åtgärder samt övervakning och granskning

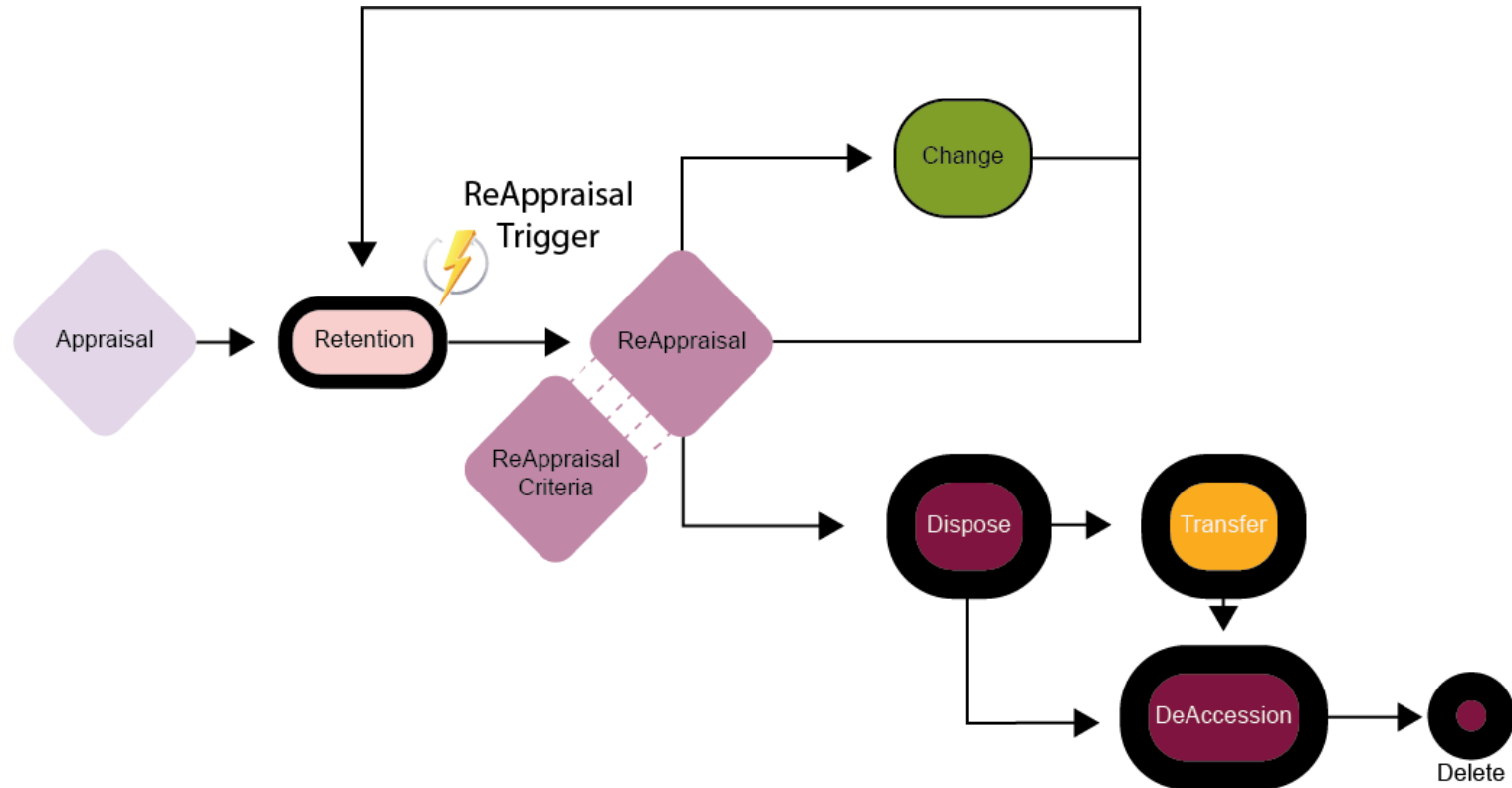
LoRCAP: Level of Retention, Curation and Preservation



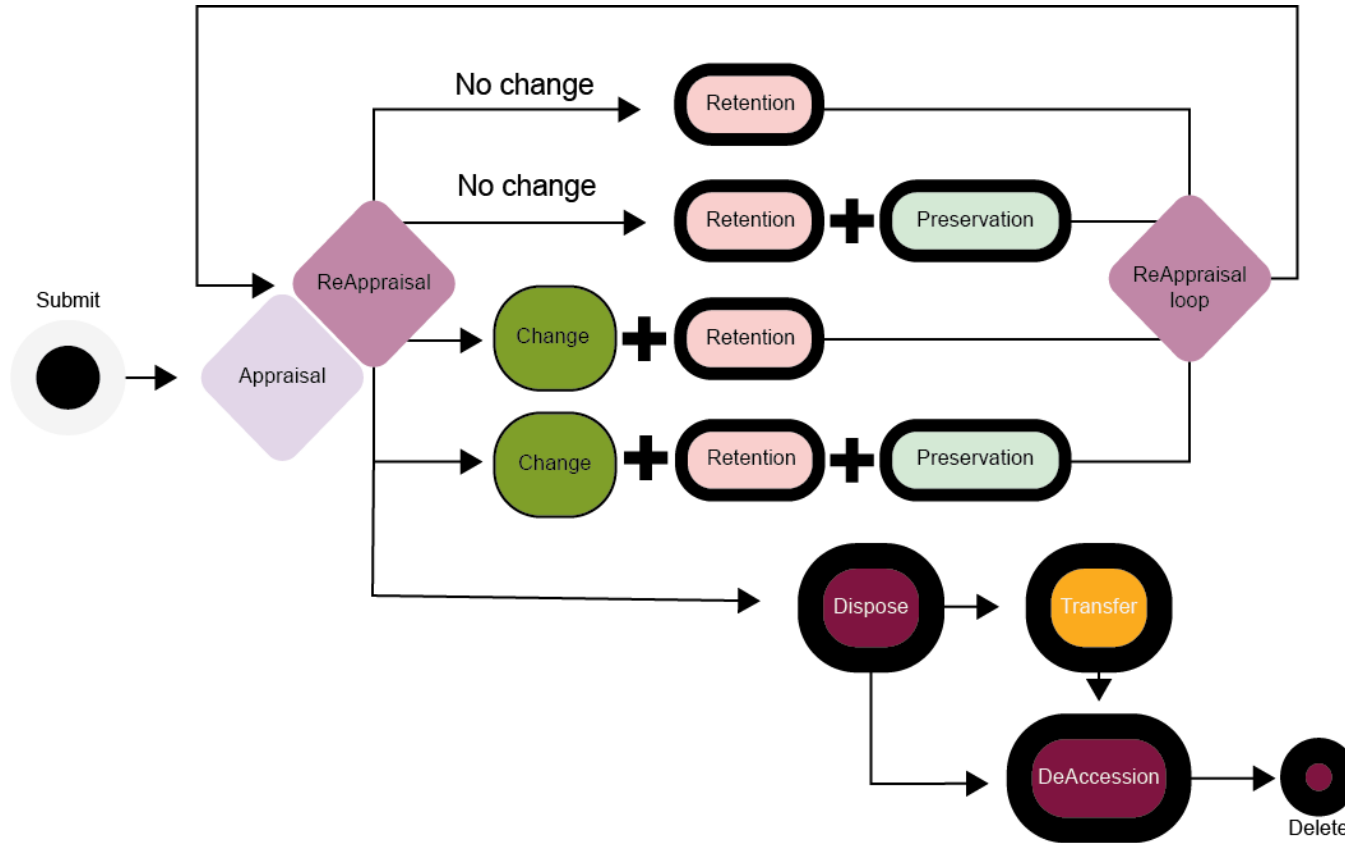
Submission and Appraisal (D)



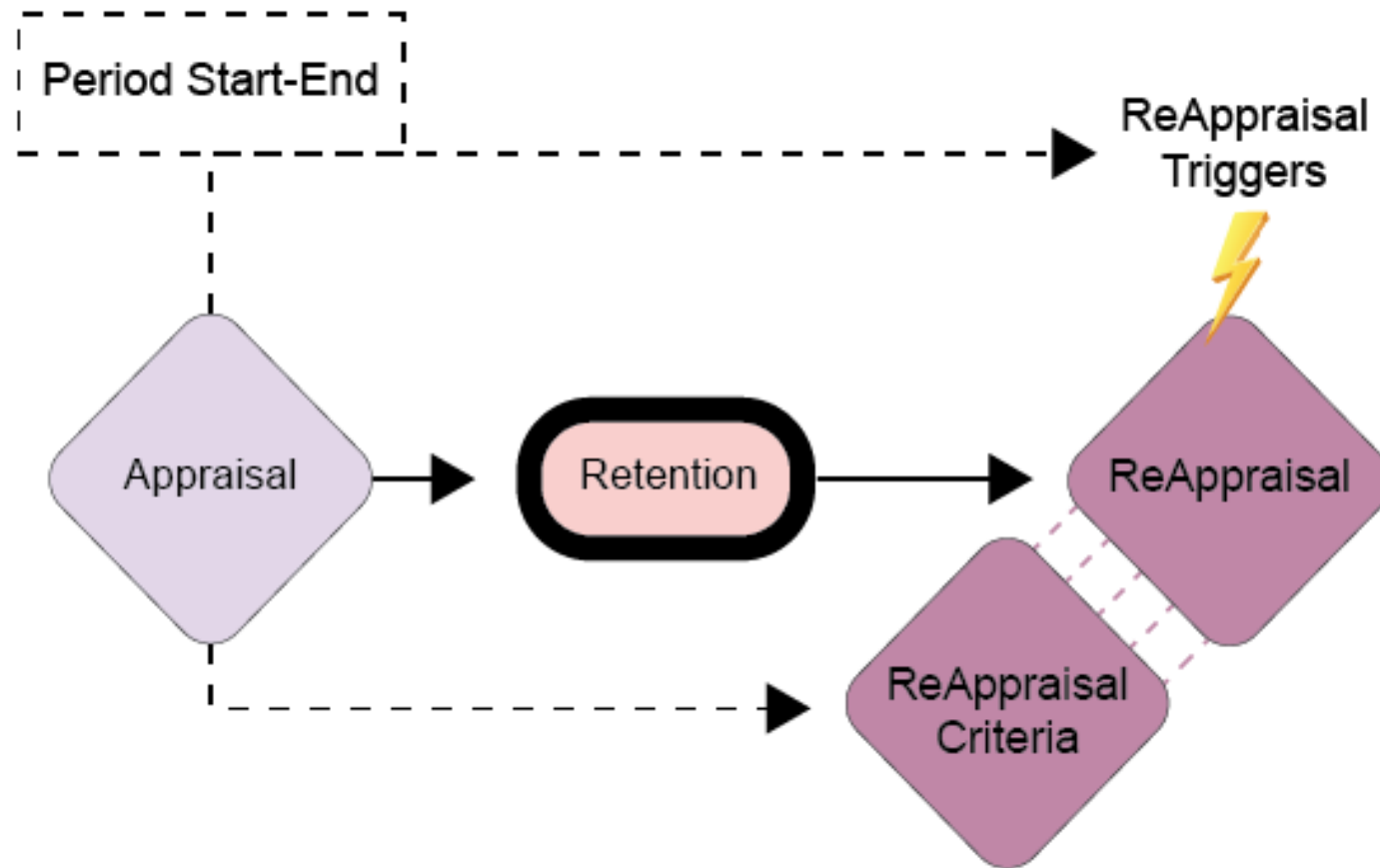
Retention and Reappraisal (C)



Preservation and Reappraisal (A)



Reappraisal triggers and criteria





CTS i korthet



- 16 krav
- Självutvärdering – granskning – revidering – styrelsebeslut
- Certifieringen gäller i 3 år
- Aktivt bevarande, inte bara lagring

CTS-ansökan och Bolincentret

Merlijn de Smit, Stockholms universitet
merlijn.de.smit@su.se



Stockholms
universitet

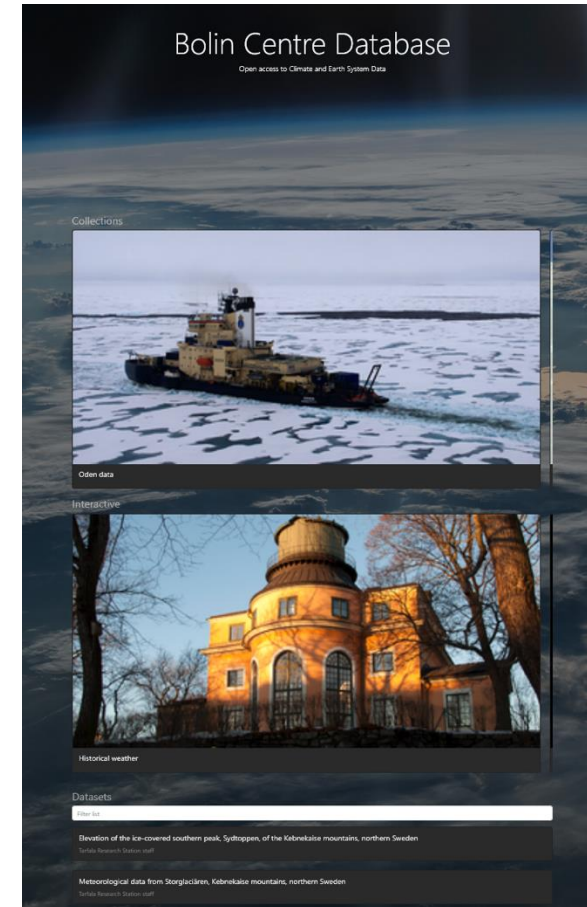
Bolincentrets Databas

Repository för klimat- och jordvetenskapliga data:

- Drivs av Bolincentret (SU+KTH+SMHI)
- Öppen för forskare med anknytning till Bolincentret (eller deltagande organisationer)
- I nuläget 500+ dataset
- Git-repositorium och samlingar för vissa forskningsgrupp eller expeditioner

Styrkor: stark "community" av forskare, hög standard på databeskrivning.

Att jobba på: metadata är utförliga, men inte alltid "interoperabla"



bolin.su.se/data



Bolincentrets databas 2022

Stor databas, med hundratals dataset och samlingar (data från isbrytaren Oden, Tarfala forskningsstation), men:

- Två personer på Bolincentret gör allt i deltid (drift, kurering inkommande dataset, utveckling)
- Infrastruktur körs på en liten server i ett skåp
- Systemet bara tillgänglig från en specifik dator i samma rum

Vad händer om servern brinner ner, livsviktiga datorn kraschar, en nyckelperson får ett jobberbjudande som den kan inte tacka nej till?



Flaggskeppsprojekt

Säkra databasens framtid genom att:

- Involvera forskningsdatagruppen på SU med dagliga arbetet kring databasen (t.ex. kurering)
- Uppgradera infrastrukturen och flytta den till ett mer central och säker ställe
- Dokumentera krav på metadata, kureringsrutiner samt tekniska infrastruktur för att kunna överföra kompetens
- Ta fram en Terms and Conditions mellan BCD och forskare

Förbereda en CoreTrustSeal ansökan

Detta strukturerar vårt arbete med att ta åtgärder för att säkra databasens framtid och ger oss ett klart mål. Mycket av vad vi ska göra är det som krävs för en CTS-ansökan, t.ex.:

- **Rights management (R02):** ömsesidiga rättigheter och förpliktelser ska dokumenteras
- **Continuity of Service (R03):** kontinuiteten genom tid ska garanteras genom tillgång till personal och kompetensdelning
- **Technical infrastructure (R15)**



Hinder på vägen

Fördröjning, på grund av:

- Vissa nyckelpersoner lediga under längre tid
- Personalomsättning i forskningsdatagruppen – men också hos centrala samarbetspartners (IT-avd.)
- Sjösättning ny infrastruktur: vi har en ”lätt” version (microk8s) och en full kubernetes-system som är anpassad till GitOPS. Långa förhandlingar om implementering av fullständiga systemet resultatlösa
- **Skelett i garderoben!** Vissa aspekter av teknisk infra/lagring inte så säkra som vi trodde



Bolincentrets databas 2026

- Forskningsdatagruppen helt inblandade i kurering, forskarkontakt, osv.
- Ny infrastruktur i drift i "lätt" version med inloggningsfunktion, kureringsgränssnitt, inte längre beroende på specifik dator. Fullständiga versionen kan implementeras när SU:s tekniska infrastruktur är redo för detta
- Flytt till SUB-IT på gång
- Utförlig dokumentation för metadata, kurering, osv. för både forskare och kuratorer



CTS-ansökan, var är vi?

Utkast till ansökningsdokumentet finns, och vi är OK när det gäller:

- ✓ Levels of curation and active preservation
- ✓ Rights management (R02)
- ✓ Continuity of service (R03) – men avvecklingsplan saknas!
- ✓ Legal & ethical (R04) samt Governance & Resources (R05)
- ✓ Expertise & Guidance (R06) samt Provenance (R07)
- ✓ Deposit & Appraisal (R08)
- ✓ Quality assurance (R10), Workflows (R11), Discovery (R12) and Reuse (R13) samt Security (R16)

Saker som återstår:

- ✗ Preservation plan (R09): vi gör vad vi kan när det gäller t.ex. filformat, men behöver jobba på metadataexport samt skördning till researchdata.se. Digital arkivlösning på SU saknas.
- ✗ Storage and integrity (R14): otydligheter i ansvarsfördelning mellan oss och externa leverantörer, håller på åtgärdas
- ✗ Technical infrastructure (R15): ska och kan dokumenteras, men på vilken nivå?



Levels of curation and active preservation

Logical-technical measures include updating hard- and software environments, archival and dissemination formats of digital objects, and metadata.

Semantic measures include updating the content of metadata elements and other semantic artefacts such as controlled vocabularies and ontologies if necessary. It may include responsibility for editing the structure and content of deposited data.

It is recognised that a repository may offer different levels of curation to different digital objects. It is important that this is clear to depositors, users, and to CoreTrustSeal Reviewers.

The levels may be cumulative as they progress from Deposit Compliance (D), through Initial Curation (C), to Active Preservation (A). A repository may offer different levels of curation and preservation for different digital objects depending on the type of data and curation and preservation terms agreed with the depositor. For each level selected add some concise information on how the respective levels are reached e.g. automatic checks of metadata, intellectual checks and editing of documentation, file format identification, transformation to preservation file formats, etc. To qualify for the CoreTrustSeal a repository must deliver Active Preservation to at least some of their holdings. Common approaches to active preservation can include transformations to new data formats and metadata schemas, and updates to (meta)data content so that digital objects remain understandable and technically usable by the community.

- Vi **hårdkurerar** metadata, t.ex. databeskrivning på fil- och variabelformat – men vi kan behöva lätta på detta lite i framtiden för att hålla arbetsbördan hanterbar!
- Vi utför **active preservation** i t.ex. kontrollerad vokabulär (GMCD-nyckelord och en del ”interna” regler och konventioner), filformat (öppna och hållbara), versionering (alla versioner bevaras), **men:**
- Rutiner för **obsolescence checking** saknas (fast införandet av nya infrastrukturen och migrering var en sådan check i praktiken), metadata måste bli mer interoperabel.
- Ingen skördning till arkivformat i nuläget (ingen e-arkiv för forskningsdata på SU)

Storage and integrity (R14)

Storage & Integrity (R14)

R14. The repository applies documented processes to ensure data and metadata storage and integrity.

Self-Assessed Compliance Level:

Response

Guidance

In addition to maintaining 'archival' copies of digital objects, repositories need to store data and metadata from the point of deposit, for curation and preservation, and for access by users. For each storage location, measures should be in place to ensure that unintentional or unauthorised changes can be detected and correct versions of data and metadata recovered.

The response statement and evidence should include references to the following items:

- Processes and documents to ensure that the repository staff have a clear understanding of all storage locations and how they are managed.
- The repository's strategy for multiple copies.
- The risk management techniques used to inform the strategy.
- Procedures for handling and monitoring deterioration of storage media.
- Procedures to ensure that data and metadata are only deleted as part of an approved and documented process.
- Any checks (i.e. fixity checks) used to verify that a digital object has not been altered or corrupted from deposit to use.

Storage and integrity measures should be covered here (R14) and not as part of Technical Infrastructure (R15) or Security (R16) responses. Details of how intentional changes to the data and metadata are logged should be covered under Provenance & Authenticity (R07).

Vi använder en extern leverantör för lagring av data och metadata, men:

- Det visade sig att inga säkerhetskopiering gjordes (detta är åtgärdad)
- Osäkerhet kring t.ex. kontrollsummor och andra säkerhetsåtgärder – göra själv?
- Lösningen är en mer eller mindre inofficiell lösning som täcks dåligt av befintliga avtal
- Långsiktigt: också lokal lösning för lagring. Men detta tar tid!

Teknisk infrastruktur (R15)

Responses and evidence should focus on demonstrating that the repository solution, including hardware and software is well managed and appropriate to the needs of the repository functions and the Designated Community of users.

The response statement and evidence should include references to the following items:

- The repository software used for deposit, curation, preservation and access management. Whether it is community supported, open source, or locally developed.
- Any IT service management approach followed and the functions this approach specifies (e.g. systems documentation, software inventories, code repositories, infrastructure development planning).
- Any international, community or other technical infrastructure standards in place and how compliance is monitored.
- The version control systems used for repository generated software.
- Measures taken to ensure that availability, bandwidth, and connectivity are sufficient to meet the needs of the Designated Community.
- Processes in place to monitor and manage the need for technical change, including in response to the changing needs of Preservation (R10), and Reuse (R13) by the Designated Community.

Vi har ett egenutvecklad system som i nuläget använder en "lätt" kuberneteslösning (microk8s) men som kan lätt skalas upp till en fullständig lösning – detta kräver dock en miljö som IT på SU inte i nuläget kan leverera. Systemet är dock bra och kan dokumenteras, men:

- Jag kan själv ta fram en beskrivning som är begriplig för de mesta men kommer att sakna detaljer, eller
- Jag kan låta vår utvecklare ta fram en beskrivning som bara en IT-specialist kan förstå, eller
- Något däremellan?

Generella frågor

Vi gör vissa saker bra, vissa saker inte så bra. Vissa saker som vi trodde var bra har visat sig inte så bra – men vi hittar lösningar som iaf. fungerar just nu.

Men hur ska vi tänka med vår CTS-ansökan?

- Ska vi betona våra styrkor och släta över svagheter (vi nämner dem förstås men kanske med lite mindre detalj) eller
- Ska vi vara väldigt öppna om de biter som är inte så starka och om hur vi planerar att åtgärda dem?



Utmaningar: människor, inte bara tekniken

- **Personalomsättning:** i ett projekt som tar längre tid hinner folk byta jobb, få barn, osv. Detta gäller också viktiga kontaktpersoner hos samarbetspartners. Kompetensöverföring och rutiner för detta (som också krävs i CTS-ansökningar) är av största vikt.
- **Personberoende:** Vårt repositorium är utvecklat in-house, och detta leder till att mycket viktig kunskap finns hos 1 person. Externa tekniska lösningar kan delvis åtgärda detta men är inte alltid (lätt) tillgängliga för myndigheter. Åter igen: kompetensöverföring.



Utmaningar: *est enim in perpetuo motu*

- **Otydlighet i ansvarsfördelning** mellan oss och extern leverantör. Saker som vi trodde fanns på plats fanns inte på plats – detta hade vi behövt kolla upp direkt i början!
- **Rullande tåg:** om en projekt rörande utveckling av ett repositorium och CTS-ansökan tar längre tid förändras förutsättningar också. Det kan komma nya CTS-krav, vissa tekniska åtgärder kan bli föräldrade men det kommer också nya möjligheter. Viktigt att vara flexibel och inte stirra sig blind på en optimal lösning som kanske aldrig förverkligas.



Sammanfattningsvis

Vår projekt handlar samtidigt om utveckling av ett repositorium (gällande underliggande tekniken men också personal, dokumentation, arbetsflöde) och att skriva färdigt ett CTS-ansökan.

- Detta var ju hela idén: att använda förberedelsen av en ansökan som ramverk för att utföra arbetet för att säkerställa framtiden av databasen.

Men:

- Införandet av en ny teknisk infrastruktur (i sig helt nödvändig) fördröjde vissa åtgärder (t.ex. dokumentation, flytt) som var nödvändiga för att förbereda själva ansökan.

Alltså:

- **Om ni gör som oss** och vill CTS-certifiera ett repositorium "under utveckling", se till att **det tekniska är på plats** och ni kan koncentrera er på **dokumentation, personaltillgång** och **arbetsflöden** ("continuity of service").

Och slutligen...

Om ni arbetar med externa leverantörer för (delar av) drift av repositoret, se till att:

- Det finns klarhet om ömsesidig ansvar när det gäller tekniska åtgärder innan början
- Allt detta finns på pappret!

Detta kan låta som en självklarhet – men det är inte alltid så självklar på ett större, mycket decentraliserat lärosäte där institutioner/avdelningar har själv mycket ansvar för tekniska lösningar och upphandlingar.



Certifiering av KI Data Repository

Vad krävs för certifiering
med Core Trust Seal? SND-
webinarium 2026-09-29



"[Mirage in the Desert](#)" by [Michael Gwyther-Jones](#) is licensed under [CC BY 2.0](#).

KI Data Repository

- SND DORIS för metadataregistrering
- Researchdata.se för metadataexponering
- Lokal lagring



**Karolinska
Institutet**

Beslut

2025-04-10

Sida: 1 (3)

Dnr: 1-494/2025

Universitetsdirektör

**Beslut om KI Data Repository som KI:s institutionella
repositorium för tillgängliggörande och bevarande av
forskningsdata**

Beslut

För KI Data Repository (KI DR) ska följande gälla:

- att KI DR ska fungera som KI:s institutionella repositorium för tillgängliggörande och bevarande av forskningsdata.

Varför certifiera?

- För att KI DR ska kunna möta såväl interna behov som externa krav krävs att repositoret drivs i enlighet med etablerad praxis för styrning, metadatahantering, informationssäkerhet och långtidsbevarande.
- Trovärdighets gentemot KI:s forskare
- Trovärdighet gentemot tidskrifter och förlag
- Trovärdighet för KI som ansvarig för datahantering gentemot KI:s samarbetspartners, ex. inom konsortier
- En institutionell internrevision av datahanteringspolicies, bevarandep Praxis, efterlevnad av lagar, IT- och informationssäkerhet och långsiktig hållbarhet med hjälp av CoreTrustSeal-kraven

Ansökan togs fram i samverkan mellan:

- KI Data Access Unit,
- KI:s enhet för Arkiv och registratur,
- KI:s juridiska enhet,
- Objektledare verksamhet och Objektledare IT för objektet
- Forskningsstöd på KI,
- samt med stöd från Sektionschef IT och Sektionschef forskningsdatatjänster vid Svensk Nationell Datatjänst (SND)

Ansökningsprocess Core Trust Seal – tid och

2021

- Första CTS-ansökan, avslås
- Brister: KI möter inte krav på beskrivning av repositoriets uppdrag, interna organisation samt relation till Svensk Nationell Datatjänst (SND), och bevarandeplanering.

2023–2025

- Ansökan återupptas inom ramarna för projektet KI Data Repository Fas 1
- Inom projektet åtgärdas flera av de brister som identifierats i repositoriets organisation genom införande av uppdragsbeskrivning och utredning om långsiktig finansiering.
- Eftersom plan för långsiktigt bevarande av forskningsdata inte åtgärdas under projektiden skjuts CTS-ansökan upp

2025–2026

- Ansökan återupptas inom projektet KI DR ICE, med uttalat fokus att åtgärda kvarvarande brister i repositoriets långsiktiga planerande och organisation för bevarande av forskningsdata samt att slutföra ansökan.
- Inom ramarna för KI DR ICE utformas en bevarandeplan, vilken också innehåller en handlingsplan för fortsatta åtgärder inom verksamhet och IT-förvaltning.

Certifiering i projektform

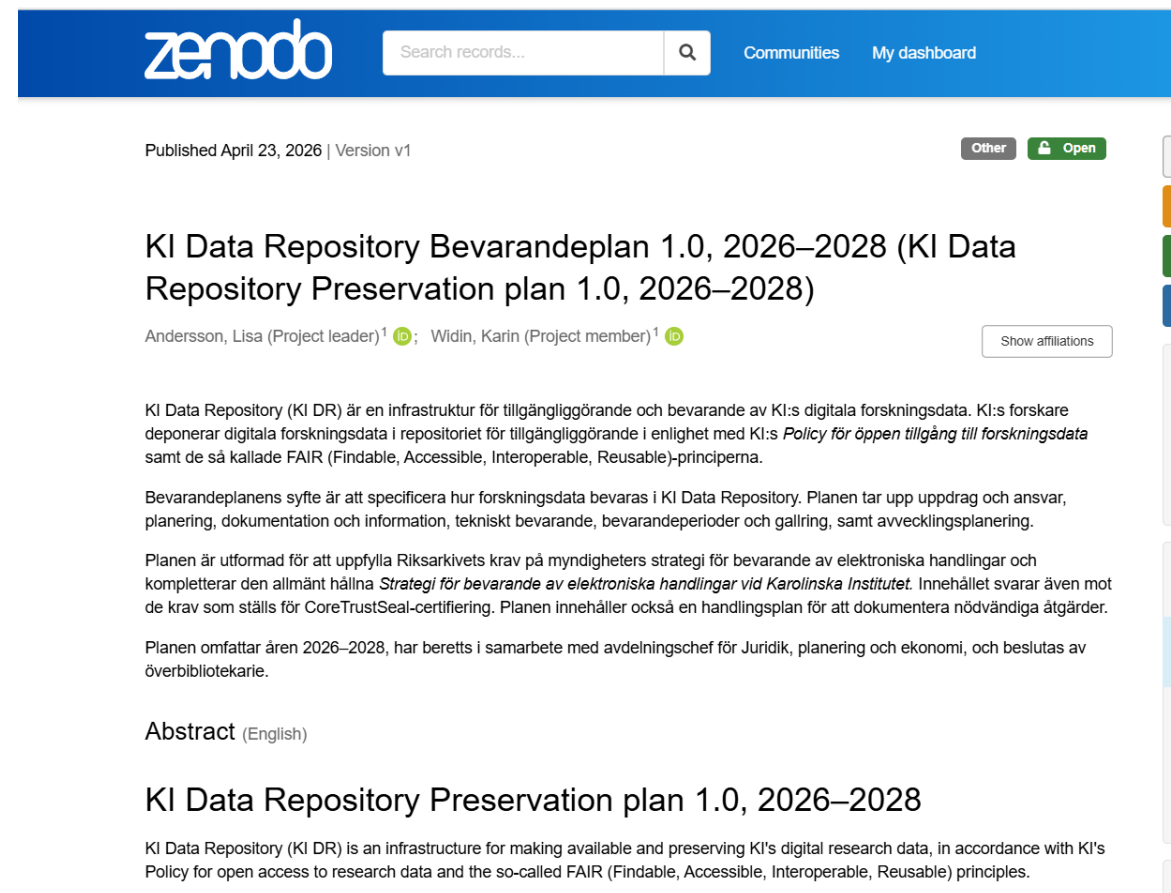
- analys av befintliga rutiner och tekniska lösningar
- genomförande av eventuella anpassningar,
- noggrann dokumentation,
- inskickande av certifieringsansökan och förslag på upplägg för fortsatt arbete kring certifiering

Inventering – vad saknas?

- Vägval 2025-11-25

Requirement no.	Status	Action required
0 Background information & Context	Implemented	N/A
1 Mission & Scope	Implemented	N/A
2 Rights Management	Implemented	Handläggningsordning för utlämning
3 Continuity of Service	In progress	- Bevarandeplan inkl. Avvecklingsplanering - Avtal med successor
4 Legal & Ethical	Implemented	N/A
5 Governance & Resources	Implemented	N/A
6 Expertise & Guidance	Implemented	N/A
7 Provenance and authenticity	In progress	"fixity checks", ingår i delprojekt "Integrera"
8 Deposit and appraisal	In progress	Bevarandeplan, spec. datakurering och gallring/bevarande
9 Preservation plan	In progress	Bevarandeplan
10 Quality assurance	Implemented	N/A
11 Workflows	Implemented	N/A
12 Discovery and identification	Implemented	N/A
13 Reuse	Implemented	N/A
14 Storage and integrity	Implemented	N/A
15 Technical infrastructure	Implemented	N/A
16 Security	Implemented	N/A

- Andersson, L., & Widin, K. (2026). KI Data Repository Bevarandeplan 1.0, 2026–2028 (KI Data Repository Preservation plan 1.0, 2026–2028). Zenodo.
<https://doi.org/10.5281/zenodo.20488688>



The screenshot shows the Zenodo interface for a specific dataset. At the top is a blue header with the Zenodo logo, a search bar, and links for 'Communities' and 'My dashboard'. Below the header, the record details are displayed. The title is 'KI Data Repository Bevarandeplan 1.0, 2026–2028 (KI Data Repository Preservation plan 1.0, 2026–2028)'. The authors are listed as 'Andersson, Lisa (Project leader)' and 'Widin, Karin (Project member)'. The publication date is 'Published April 23, 2026 | Version v1'. The abstract is in English and describes the KI Data Repository (KI DR) as an infrastructure for making available and preserving KI's digital research data, in accordance with KI's Policy for open access to research data and the so-called FAIR (Findable, Accessible, Interoperable, Reusable) principles. The abstract also mentions that the plan is designed to fulfill the requirements of the Rikssarkivets strategy for the preservation of electronic documents and that it complements the general policy for the preservation of electronic documents at Karolinska Institutet.

zenodo Search records... Q Communities My dashboard

Published April 23, 2026 | Version v1 Other Open

KI Data Repository Bevarandeplan 1.0, 2026–2028 (KI Data Repository Preservation plan 1.0, 2026–2028)

Andersson, Lisa (Project leader)¹ ; Widin, Karin (Project member)¹

Show affiliations

KI Data Repository (KI DR) är en infrastruktur för tillgängliggörande och bevarande av KI:s digitala forskningsdata. KI:s forskare deponerar digitala forskningsdata i repositoriets för tillgängliggörande i enlighet med KI:s *Policy för öppen tillgång till forskningsdata* samt de så kallade FAIR (Findable, Accessible, Interoperable, Reusable)-principerna.

Bevarandeplanens syfte är att specificera hur forskningsdata bevaras i KI Data Repository. Planen tar upp uppdrag och ansvar, planering, dokumentation och information, tekniskt bevarande, bevarandeperioder och gallring, samt avvecklingsplanering.

Planen är utformad för att uppfylla Rikssarkivets krav på myndigheters strategi för bevarande av elektroniska handlingar och kompletterar den allmänt hållna *Strategi för bevarande av elektroniska handlingar vid Karolinska Institutet*. Innehållet svarar även mot de krav som ställs för CoreTrustSeal-certifiering. Planen innehåller också en handlingsplan för att dokumentera nödvändiga åtgärder.

Planen omfattar åren 2026–2028, har beretts i samarbete med avdelningschef för Juridik, planering och ekonomi, och beslutas av överbibliotekarie.

Abstract (English)

KI Data Repository Preservation plan 1.0, 2026–2028

KI Data Repository (KI DR) is an infrastructure for making available and preserving KI's digital research data, in accordance with KI's Policy for open access to research data and the so-called FAIR (Findable, Accessible, Interoperable, Reusable) principles.

Handlingsplan KI DR till följd av CTS

Implementera bevarandeinformation till deponerande forskare	Bör	2026	Funktionsansvarig KI DR	Klar
Integrera informationsvärderingen från blanketten Bevarande eller gallring av forskningsdata i deponeringsflödet till KI DR alternativt extrahera ur datahanteringsplan	Bör	Inväntar SND:s åtgärder i DORIS	Funktionsansvarig KI DR, i samarbete med SND	Ej påbörjad
Implementera bevarandemetadata vid metadatainmatning	Bör	Inväntar SND:s åtgärder i DORIS	Funktionsansvarig KI DR, i samarbete med SND	Ej påbörjad
Testa process för att hämta metadata för arkivbehov från DORIS	Bör	Inväntar SND:s åtgärder i DORIS	Funktionsansvarig KI DR, i samarbete med Arkiv och registratur	Ej påbörjad
Utforma mall för gallringsunderlag	Bör	2027	Funktionsansvarig KI DR, i samarbete med Arkiv och registratur	Ej påbörjad
Pröva gallringsprocess	Bör	2027	Funktionsansvarig KI DR, i samarbete med Arkiv och registratur	Ej påbörjad

Handlingsplan KI DR till följd av CTS

Viruskontroll av filer som laddas upp från externa klienter	Skall	2027	Objektledare Forskningsstöd	Ej påbörjad
Checksummor på filnivå för att garantera dataintegritet	Bör	För öppna data i samband med införande av lagringsadapter. Bevaka gällande skyddsvärda data.	Objektledare Forskningsstöd	Ej påbörjad
Kontinuerliga kontroller av filer för att säkerställa att accepterade och föredragna filformat fortfarande är lämpliga för långtidsbevarande (migrering sker vid behov)	Bör	2027	Funktionsansvarig KI DR i samarbete med Objektledare Forskningsstöd Möjlig utvecklingsaktivitet inom KI DASH Bevarande	Ej påbörjad
Etablera process för formatmigrering	Bör	När process för kontroll av filer etablerats	Objektledare Forskningsstöd, i samarbete med Funktionsansvarig KI DR Möjlig utvecklingsaktivitet inom KI DASH Bevarande	Ej påbörjad
Testa process för formatmigrering	Bör	När process för formatmigrering etablerats	Objektledare Forskningsstöd, i samarbete med Funktionsansvarig KI DR Möjlig utvecklingsaktivitet inom KI DASH Bevarande	Ej påbörjad
Etablera back-up för lagring	Skall	När kall lagring etablerats	Objektledare Forskningsstöd	Påbörjad

Review #4, vad saknas fortfarande?

- clarification on where the **responsibilities of each organisation begin and end throughout the data lifecycle**, including ingest, preservation, access, dissemination, and long-term stewardship
- clarification of how these **responsibilities are distributed in practice**. Specifically, which responsibilities lie with the individual researcher, which are assumed by the KI Data Repository, and which remain under the authority of the Head of Department? For example, who is ultimately **responsible for verifying compliance with legal, ethical, and information security requirements** before data are accepted into the repository?
- Are the **DataCite and SND metadata schemas sufficient for describing the datasets** stored in the KI data repository? Alternatively, does the repository rely on an internal, domain-specific metadata model to provide richer dataset descriptions and support advanced discovery, filtering, selection, and reuse by end users?
- does the repository plan to adopt or integrate **ontology-based metadata management solutions to improve the semantic description, discoverability, and interoperability of its datasets**? For example, are platforms such as OntoPortal Alliance (<https://ontoportal.org/about/>) being considered to support the use of controlled vocabularies, ontologies, and rich domain-specific thesauri? Such semantic annotation capabilities could significantly enhance dataset discovery, interoperability, and reuse within the broader European health data ecosystem.
- **The European Health Data Space (EHDS)** is an EU regulation that entered into force in 2025 to harmonize electronic health data sharing across member states. To our knowledge, Sweden is actively preparing its decentralized healthcare infrastructure for rollout, driven centrally by the Swedish eHealth Agency alongside national research and public health bodies. How is KI data repository integrated in such organisation ?

Topp 5 tips från oss

- 1) Börja tidigt med inventering av status vs. krav
- 2) Involvera alla relevanta experter inom och utanför organisationen.
- 3) Dokumentera och anpassa befintliga institutionella rutiner till CoreTrustSeal-kraven.
- 4) I ansökningstexten: fokusera på bevis (beskrivning av praxis) som stärker era påståenden (policies).
- 5) Se ansökan som en möjlighet att stärka styrningen av bevarande och tillgängliggörande av forskningsdata.

Målbild



"[Carrizo Plain National Monument](#)" by [blmcalifornia](#) is marked with [Public Domain Mark 1.0](#).

Slutrapport om arbetet med delprojekt Certifiera

<https://zenodo.org/records/20553190>

Kontakt

- Lisa.Andersson@ki.se



**Karolinska
Institutet**



Vad händer sedan?



SND

Svensk nationell datatjänst | Göteborgs universitet - Chalmers tekniska högskola - Karolinska Institutet - Kungliga Tekniska högskolan - Lunds universitet - Stockholms universitet - Sveriges lantbruksuniversitet - Umeå universitet - Uppsala universitet



Granskningsprocessen i korthet



- Application Management Tool (AMT)
 - Formulär
- 2 anonyma granskare
- "Triage"
- Full granskning

Triage



- Snabbgranskning!
- Är ansökan "in scope"?
 - R0: Klart definierad "Designated community"?
 - R09: Bevarandeplan?
 - R08: Aktivt bevarande?
 - R13: Återanvändbart?
- Möjliga utfall:
 - Avvisad
 - Begäran om komplettering
 - Fullständig granskning

Reviewing Tips: Triage - is the applicant in scope?





Full granskning



- Genomgång av alla 16 kravområden
- Två utfall per krav
 - Accepterad
 - Komplettering krävs

Krävs komplettering?



- Om en del som står för ett område inte uppfyller helt, alt. det saknas information.
- Bifogade dokument saknas
- Länkar fungerar inte
- Förklaring krävs med info om vad som efterfrågas.
- Gärna referens till Guide eller Utökad guide



Feedback



Går till sökande och CTS board

Bör klargöra om det är något som

- Är absolut nödvändigt
- Är "bra att ha", eller är ett förtydligande
- Är för framtiden
- Är "*In progress*" ok?

Tidslinje



Who?	What?	When?
Applicant	Submission of self assessment – version 1	Within three months of adding the applicant's details to the tool.
Reviewers	Review of self-assessment	Within two months after payment of the fee or submitting the self-assessment when pre-payment applies.
Board	Assessment of reviews and response to the applicant	Within two weeks
Applicant	Submission of self assessment – version 2 to 5	Within three months of receiving the reviewers feedback.
Reviewers	Review of self-assessment – version 2 to 5	Within two months after submitting the self-assessment.
Board	Assessment of reviews versions 2 to 5 and response to the applicant	Within two weeks
Board	Approval of the self assessment and notification of applicant	Within two weeks after board approval
Board	Decline of the self assessment and notification of applicant	Within one month after board approval.



Frågor?



SND

Svensk nationell datatjänst | Göteborgs universitet - Chalmers tekniska högskola - Karolinska Institutet - Kungliga Tekniska högskolan - Lunds universitet - Stockholms universitet - Sveriges lantbruksuniversitet - Umeå universitet - Uppsala universitet