cessda saw

Research and Innovation Action

CESSDA Strengthening and Widening

Project Number: 674939 Start Date of Project: 01/08/2015 Duration: 27 months

Deliverable 4.1 – "Trust" workshops report

Dissemination Level	PU
Due Date of Deliverable	01//03/2017
Actual Submission Date	27/10/2017)
Work Package	WP4
Task	T4.3
Type	Report
EC Approval Status	16 November 2017
Version	V1.0
Number of Pages	p.1 – p. 75

Abstract:

This deliverable contains the report of the two "Trust" workshops as well of that of a preceding "CESSDA Expert Seminar". These workshops were held as part of task 4.3 of the CESSDA SaW project plan ("Development Support: achieving the Data Seal of Approval") in 2016 and 2017.

Project funded by the EU Horizon 2020 Research and Innovation Programme under the agreement No.674939

History

Version	Date	Reason	Revised by
V0.1	18/08/2017	First draft	Heiko Tjalsma (DANS)
V0.2	24/08/2017	Second draft with contributions by Mari Kleemola (FSD), Natascha Schumann (GESIS) and Janez Štebe (ADP	Heiko Tjalsma (DANS)
V0.3	29/08/2017	Third draft with contributions by Hervé l'Hours (UKDA)	Hervé l'Hours (UKDA)
V0.4	20/09/2017	Fourth draft with contributions by Hervé l'Hours (UKDA)	Hervé l'Hours (UKDA) and Heiko Tjalsma (DANS)
V1.0	24/10/2017	Final draft	Heiko Tjalsma (DANS)

Author List

Organisation	Name	Contact Information
DANS	Heiko Tjalsma	Heiko.tjalsma@dans.knaw.nl
UKDA	Hervé l'Hours	herve@essex.ac.uk
FSD	Mari Kleemola	Mari.Kleemola@staff.uta.fi
GESIS	Natascha Schumann	Natascha.Schumann@gesis.org
ADP	Janez Štebe	Janez.Stebe@fdv.uni-lj.si

Time Schedule before Delivery

Next Action	Deadline	Care of
Review by the task partners	25/10/2017	DANS
Review by the WP leader	26/10/2017	DANS
Review by the Chair of the Delivery Committee	26/10/2017	CSDA
Review by the Project Coordinator	27/10/2017	CESSDA
Approval and Submission by the Project Coordinator to the European Commission	27/10/2017	CESSDA

Executive Summary

As part of task 4.3 of the CESSDA SaW project plan ("Development Support: achieving the Data Seal of Approval") two "Trust" workshops were held in 2016 and 2017. This deliverable contains the report of these two workshops as well of that of the preceding "CESSDA Expert Seminar 2015". Task 4.3 was carried out by the existing Trust Group of CESSDA (further: Trust Group) as the objectives and activities of this task concurred with those of the Group for the time of the SaW project.

Within the task, two workshops were organised. These workshops were preceded by the CESSDA Expert Seminar 2015, which was held just before the start of the SaW project. At the first one in in June 2016 in The Hague, the concepts of trust and certification were (re-)introduced to a relatively large group of SP's. In the second workshop, in March 2017 in Zagreb, a "gap analysis" based on the test self-assessments (of all the certification requirements) by the SP's was presented. These self-assessments were peer-reviewed and analysed by the Trust Group.

Abbreviations and Acronyms

Annex II	Annex II of the CESSDA Statutes
CTS	CoreTrustSeal
DSA	Data Seal of Approval
OAIS	Open Archival Information System
SP	Service Provider
TDR	Trustworthy Digital Repository
WDS	World Data System

Table of Contents

Table of Contents

List of tables

1. Introduction

As part of task 4.3 of the CESSDA SaW project plan ("Development Support: achieving the Data Seal of Approval") two "Trust" workshops were held in 2016 and 2017. Task 4.3 was carried out by the existing Trust Group of CESSDA (further: Trust Group) as the objectives and activities of this task concurred with those of the Group for the time of the SaW project. Within this task the two workshops were organised. These workshops were preceded by the CESSDA Expert Seminar 2015, which was held just before the start of the SaW project.

At the first workshop in June 2016, the concepts of trust and certification were (re-)introduced to a relatively large group of SP's. In the second workshop, in March 2017, a gap analysis based on all the test self-assessments (of all the requirements) submitted by the SP's was presented. These self-assessments were peer reviewed and analysed by the Trust Group.

2. CESSDA Expert Seminar on Trust in 2015

The seminar was held at DANS in The Hague, November 30th – December 1st, 2015. The two main issues of the seminar were:

A. Creating awareness and knowledge of trust issues generally
B. Exchanging and developing ideas on yet unresolved trust issues (the non-DSA Annex II obligations)

As a result, the report of this expert seminar contained the first draft plan for task 4.3 (delivered in the SaW project as Milestone MS19 "Evaluation of already existing ideas and plans" and Milestone MS20 "Proposal on how to set up the Trust Group").

The timing of this seminar made it possible that its discussions and conclusions could feed into the CESSDA SaW project.

At the Expert Seminar meeting the issue of having both a 'Trust Group' acting in line with other CESSDA groups, and a simultaneous Trust Task as part of the CESSDA SaW project was discussed. It was decided that the best approach was to subsume the Trust Group into the SaW task for the duration of the project to minimize duplication of effort and avoid confusion.

3. CESSDA Trust Workshop June 2016, The Hague

There were three sessions on trust in this SaW workshop. At the first session members of the Trust Group presented a general introduction into the issues of trust and trustworthiness with a particular focus on the ***new*** Common Requirements from DSA/WDS and an overview of the changes. The release of the final approved common requirements took place just before the SaW workshop.

The main message which could be delivered here was that these new requirements mostly contain the same concepts as the old DSA ones, but differently organised and presented. Also, the challenges around the relationship between these guidelines and the Annex II obligations were touched upon.

In the last part of this first session all the participants were invited to raise issues and questions related to trust, trustworthiness, certification and the common requirements. As in 2013 the requirement provided a good common basis for sharing viewpoints and the discussion was fruitful. With regard to compliance and the timing of a TDR application, a number of service providers stressed their uncertain future and funding which could make it virtually impossible to become DSA-compliant within a year, as the SaW project prescribes. Others discussed the resource implications of preparing and making public the evidence required.

In the second session, the timescale and procedure was set out by which participants could seek TDR compliance within the remaining year of the project. Roughly speaking three categories of SP's could be distinguished: those already certified, those in the process of preparing evidence and self-assessments and those starting with a blank slate. Support from the Trust Group and mechanisms to support mutual cooperation were both well received. It was decided to arrange a common online place for communication as part of the Basecamp CESSDA ERIC map, where all SP's working on certification could share their provisional results as well as questions and comments. Also, each SP identified a contact person for trust and certification issues to support more direct, efficient communication and to guarantee continuity.

In the final session, the new guidelines were discussed in more detail in smaller groups. Based on their experience with DSA and their overview of past assessments the members of the Trust Group provided feedback on many of the potential problems and clarified a number of key issues. Both the second and the third sessions were well attended, indicating that most SP's take the trust issue seriously.

4. CESSDA Trust Workshop March 2017, Zagreb

More than 60 participants from 26 European countries participated in the 'Second Training workshop on Trust and Technical Aspects within the CESSDA infrastructure in March 2017 in Zagreb. The event also addressed the Annex II obligation of providing single sign on across CESSDA partners.

To become a CESSDA ERIC member, a service provider it is required to "adhere to the principles of the OAIS reference model and any agreed CESSDA ERIC requirements for operating trusted repositories;" (see obligation 7 of the Annex II, Statutes). The agreed TDR criteria are the CoreTrustSeal requirements, though there is not yet a set period within which SPs must fulfil this obligation.

One result of the expert workshop in 2016 in The Hague was that all partners and candidates should provide a self-assessment against the CoreTrustSeal requirements to the CESSDA Trust group. Members of the working group have undertaken to review all test assessment and give feedback to the participants. This service ensures that all participants receive support and can get an initial impression of where any strengths and weakness in their applications might lay. The overall results were collated into an overview of progress towards TDR certification (gap analysis).

The workshop further demonstrated the benefit of having a common set of requirements against which to benchmark ourselves. Participants communicated between themselves and engaged with the trust support process. Areas where a number of SPs had similar issues were identified and these were discussed and addressed. The completion of a self-assessment or a response to the requirements provided a rich experience across participants which was reflected in discussions and outcomes.

5. Gap Analysis

15 out of 23 participants submitted a test assessment before the Zagreb workshop. Each submission was reviewed by two expert members of the CESSDA Trust group. Part of the review was to determine the level of compliance (from 0 to 4) and to check if the requirements were met by the self-assessment statement and supporting evidence. The reviewers also had the opportunity to comment on each requirement.

Based on these test assessments a gap analysis was created. The average compliance level was in the range of 3 to 3.5, but the results varied across the service providers.

One significant outcome was that providing evidence really is an issue for many institutions.

The lowest scores were achieved for the technical infrastructure and security (both addressed in more detail in the CoreTrustSeal requirements than in the DSA) as well as for requirements concerning continuity of access, documented procedures and preservation plans. The highest scores were achieved for the requirements related to mission/scope of the repository, data reuse, expert guidance and confidentiality / ethics. As observed in prior workshops there is a general problem with a lack of supporting evidence and/or a lack of evidence available in English.

One should take into account that there is a wide range of different types of archives within CESSDA. There are well-established ones provided with a number of staff and resources and others with only a few staff members and small budgets or funded by third parties. Parts of the institutions taking part in the test assessment have already a DSA and others are at the very beginning of the process.

This gap analysis was presented in the first session of the workshop. In addition to procedural issues such as defining our next activities and timelines a roundtable discussion with all participants was conducted to determine progress towards certification and whether aspiring members were able to join in the process. It was clear that not all participants would be able to undertake applications within the project timeframe, some for reasons of preparedness, while others for local planning reasons.

Again, the roundtable illustrated the different circumstances of the participants which also impact the ability to progress to the formal CoreTrustSeal application process (resources, funding, staff, time etc.).

With regard to the status of the test assessment four different groups could be identified:

- Institutions used the test assessment as a preparation for a real (re-) submission of to the CoreTrustSeal in the near future, comments of the reviewer were seen as helpful,
- Institutions used the test assessment to see what issues still have to be addressed; not sure if they would be able to submit CoreTrustSeal applications within CESSDA SaW,
- Institutions used the test assessment as guidelines to build up their archive not intended (yet) to submit to CoreTrustSeal,

- Institutions not used the test assessment at all, mostly for reasons of lacking resources, funding, support from ministry.

The Trust Group followed on from this session with a presentation of comments and issues relating to particular requirements across a range of the self-assessment. The most general comment across the self-assessments was the lack of available (public) evidence, more detailed comments are provided in the table below.

Table 1: Comments most often made by reviewers

Requirements	Frequently comments by reviewers
R0: Context	Outsourcing: Links, contracts, SLA are lacking Clarity to responsibilities Information would better fit in other requirements Designated Community should be described in more detail lack of clarity about organisational unit /collection that is applying (->Organisational structure) Context of evidence is not always clear
R1: Mission/Scope	Missing evidence/explicit statements (formal approval, recognition) Lack of mentioning ”preservation“ as a goal
R2: Licenses	Licenses for dealing with data with disclosure risk Public evidence missing Regulations of use missing Breach policies
R3: Continuity of access	Lacking description of plans and procedures in case no formal succession plan is in place Agreements or other documents to provide evidence Preconditions to hand over data to other institutions Ideas for different scenarios
R4: Confidentially/Ethics	Missing links to documents/procedures Possible effects of the new EU data protection regulation Handling of data with disclosure risk to be described, also for internal data management Description of procedures would be helpful Skills of staff Breach policy
R5: Organizational structure	Funding perspectives

	Description of staff's affiliation in national/international bodies Required skills of staff members
R6: Expert guidance	Is a scientific or user board established? Scope of expert advice Are user surveys conducted? Feedback from users
R7: Data integrity and authenticity	Description of managing changes Are checksums in place? Versioning strategy Definition of significant properties and control of data Which kind of checks are in place? Identifying depositors
R8: Appraisal	Would be a 4 if supported by linked documentation. Is there a collection development policy? Documented list of preferred and/or acceptable formats missing Are there any quality control procedures? Elaborate more precisely
R9: Documented storage procedures	Evidence missing! If there is no public documentation, describe in more detail the internal documentation. Evidence links provided are not sufficient Would benefit from public procedure links
R10: Preservation plan	Cannot be a 4 without some specific reference to the ongoing monitoring and forward migration of formats What licenses or agreements are in place? Add links to documentation Evidence missing
R11: Data quality	Describe how the procedures are documented and what kind of (internal) guidance or instructions exist Provide link(s) to public documentation Explain, how is metadata quality assessed, in particular for social science qualitative / quantitative data Is the Designated Community encouraged to send comments?
R12: Workflows	Are there formal decision processes taken and documented? Do you have written (internal) documentation, describe them Diagrams defining how the local processes map to OAIS would help progress these theoretical concepts Which types of data and corresponding workflows exist?
R13: Data discovery	Are your metadata or data included in any national/international

and identification	data catalogues? Do you have a PID policy? How are DOIs assigned?
R14: Data reuse	Are plans related to future migrations in place? Tech watch would ideally monitor SPSS as an 'appropriate' format for archiving and dissemination, and have a plan in place should the format be identified as 'at risk' Seems everything is in place but some more evidence could be provided What are the mandatory metadata fields?
R15: Technical infrastructure	Evidence not in English should be supported by a brief English explanation Not enough evidence Describe what system documentation is available Technical documentation should reference the partners and areas of responsibility clearly. Are you OAIS compliant? Future plans should be supported by timescales
R16: Security	Disaster and recovery plans missing; risk management plans missing Is any risk analysis applied? Could you say more about risk analysis? Do you have any guidelines or instructions in place? This self-assessment does not cover the items requested in the Guidance under "please describe"

In another roundtable, the successes and challenges were discussed and the participants discussed which of the requirements they had found the easiest to meet and which were the hardest.

Requirements concerning the mission of the repository and ethics and confidentiality were mentioned by many participants as easy to answer. Questions with regard to the continuity of access, security and technical infrastructure were for many difficult to answer. A lack of communication with and information from IT departments hosting the technical service was mentioned, but this may well reflect the non-technical background of attendees. Continuity of access is for most institutions an issue. Only some have an agreement or contract with another institution, in most cases with a higher-level organisation they belong to, in place. Creation of workflow

documentation and the provision of English evidence were both mentioned as additional challenges.

The last session was split up into a common part to find out what would be an ideal evidence to provide for two requirements that were classified as hard to answer: continuity of access (Requirement 3) and security (Requirement 16). In parallel to this group session it was possible for single partners to talk to their reviewers and discuss any comments that were not clear to them. Again, the most discussed questions within these 'surgeries' were about evidence: what is enough, what kind of evidence, how much in English, how much needs to be public?

6. Conclusion

Out of 23 participants in this task 15 self-assessments were sent in., a percentage of 65%. After reviewing these test assessments, the total average score of the compliance level (ranging from 0 to 4) was 3 to 3.5. The results were varying between and in-service provider's.

Providing evidence was the main obstacle for many service providers, in particular concerning the requirements for the technical infrastructure and security. However, evidence was also often weak for the requirements on continuity of access, documented procedures and preservation plans. On the other hand, requirements related to mission/scope of the repository, data reuse, expert guidance and confidentiality/ethics had high scores. Lack of supporting evidence and/or a lack of evidence *available in English* proved to be a difficult point as well.

Based on all the self-assessments the conclusion was that circa 50% of the service providers could be considered as reasonably certain in complying with the certification in the required timeframe of the SaW project, the other 50% however not.

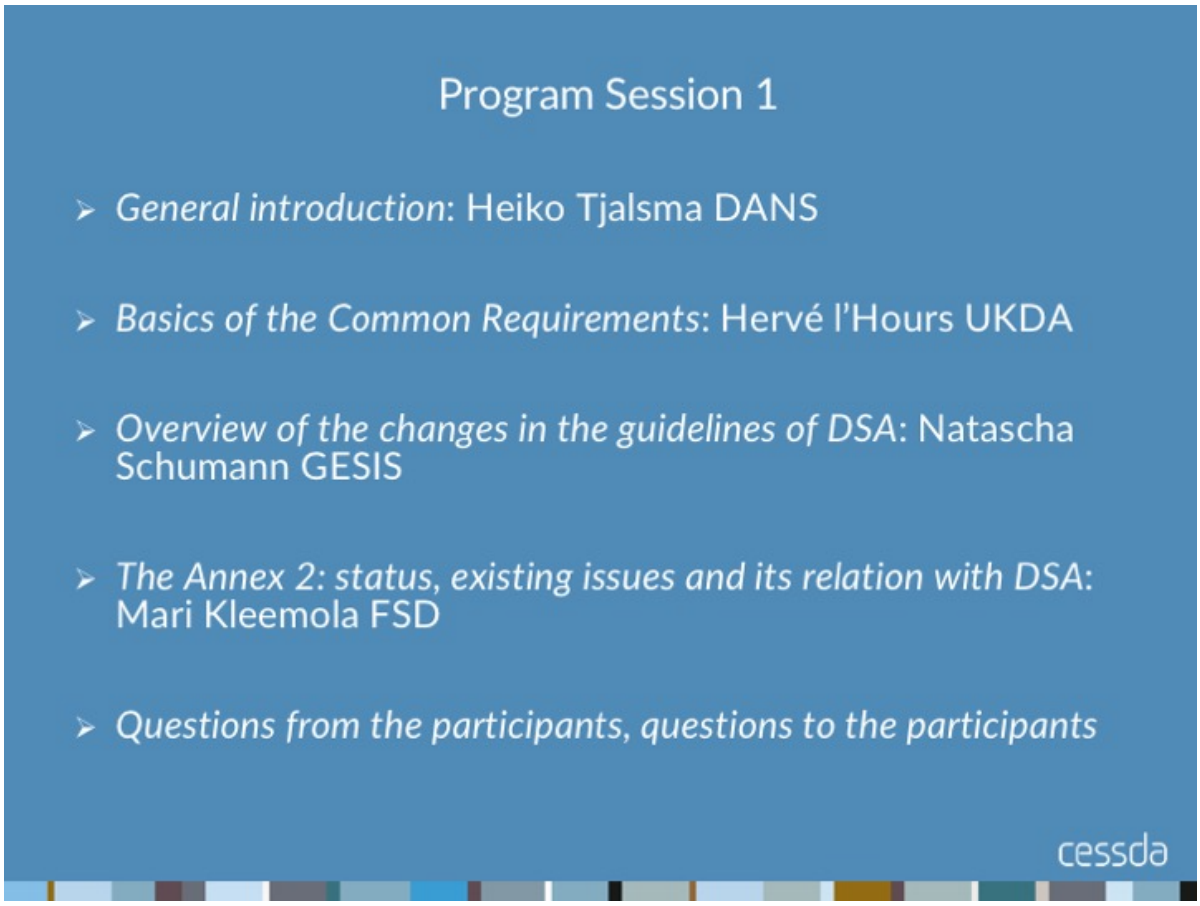
Appendix 1

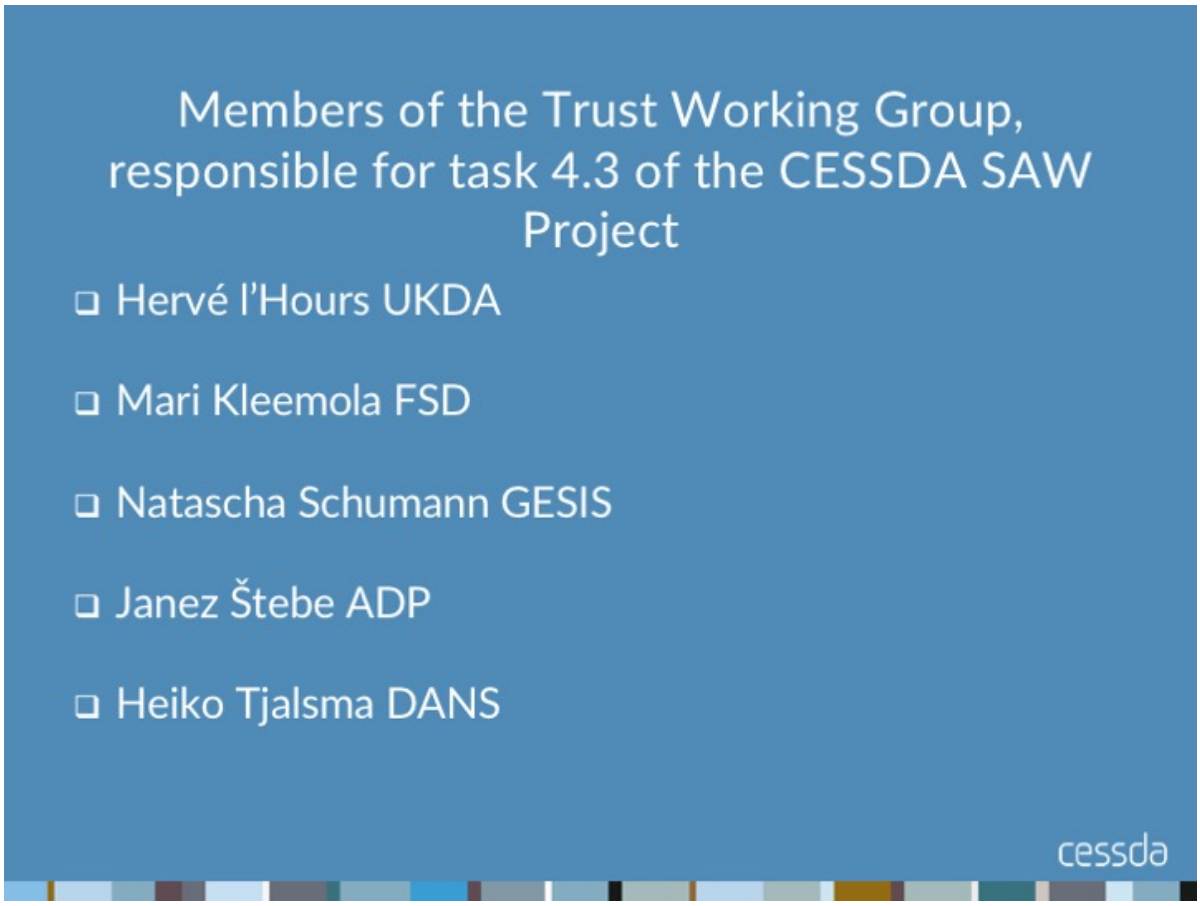
Presentations at the Trust Workshop in The Hague, 16-17 June 2017

Presentations at the Trust Workshop in Zagreb, 1-2 March 2017


CESSDA Trust and Certification
Introduction Trust Session 1
CESSDA SAW Workshop
The Hague, 16-17 June 2016
Heiko Tjalsma
Policy advisor DANS
Chairman Trust Working Group
cessda


Three times Trust in this workshop
• Thursday 9.45 – 11.00 Session 1: General Introduction on Trust and DSA
• Thursday 11.15 – 12.45 Parallel Session 2: DSA self-assessment test procedure and potential problems
• Friday 9.15 – 10.45 and 11.00 – 12.30: Parallel Sessions Consultancy on all trust issues
cessda


Program Session 1
General introduction: Heiko Tjalsma DANS
Basics of the Common Requirements: Hervé l'Hours UKDA
Overview of the changes in the guidelines of DSA: Natascha Schumann GESIS
The Annex 2: status, existing issues and its relation with DSA: Mari Kleemola FSD
Questions from the participants, questions to the participants
cessda


Members of the Trust Working Group, responsible for task 4.3 of the CESSDA SAW Project
Hervé l'Hours UKDA
Mari Kleemola FSD
Natascha Schumann GESIS
Janez Štebe ADP
Heiko Tjalsma DANS
cessda


Tasks Trust Working Group
Support and Training for the DSA Certification, the mandatory Trusted Digital Repository status for all SPs as a basis for trust
Review of the Annex 2 Obligations Compliance
Certification Watch
cessda

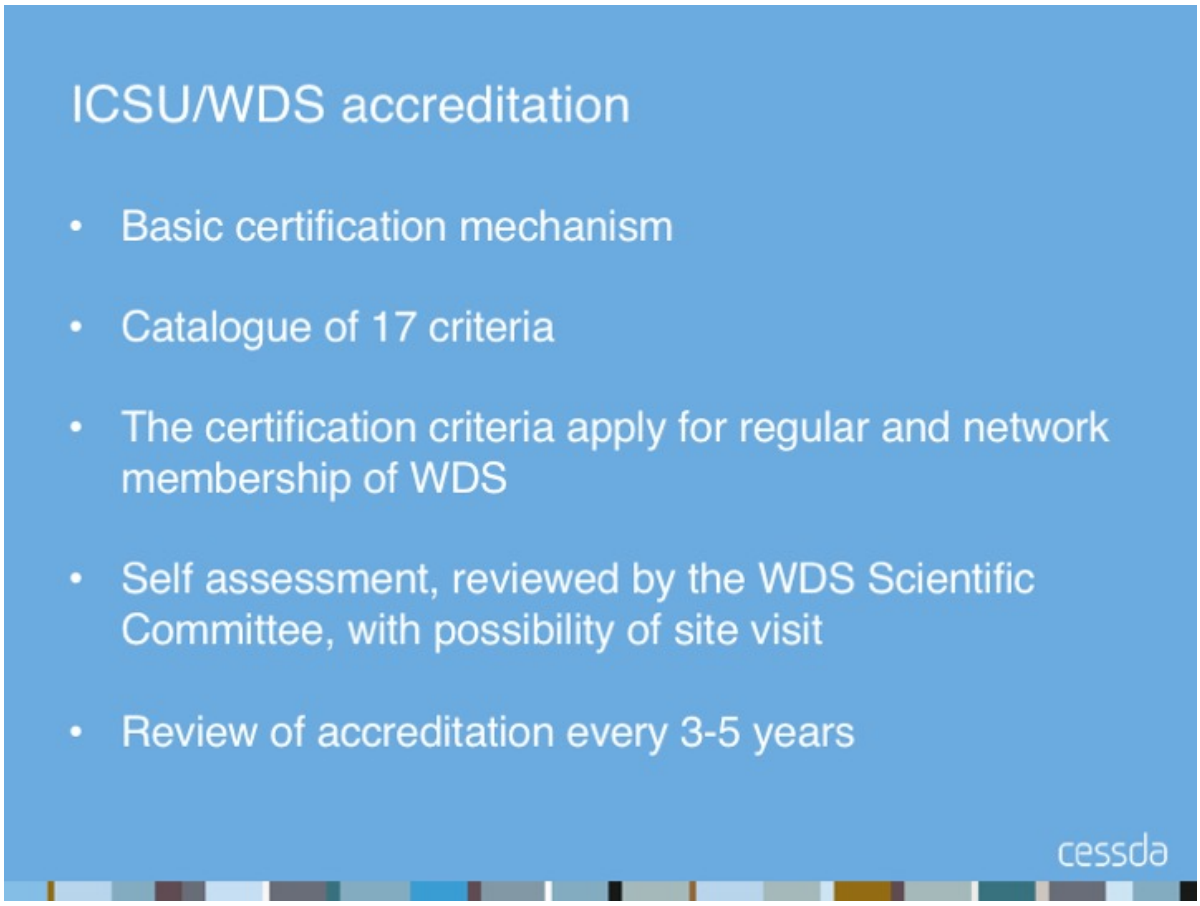

cessda
—in your circle of trust.
website: www.cessda.net / twitter:
@CESSDA_Data

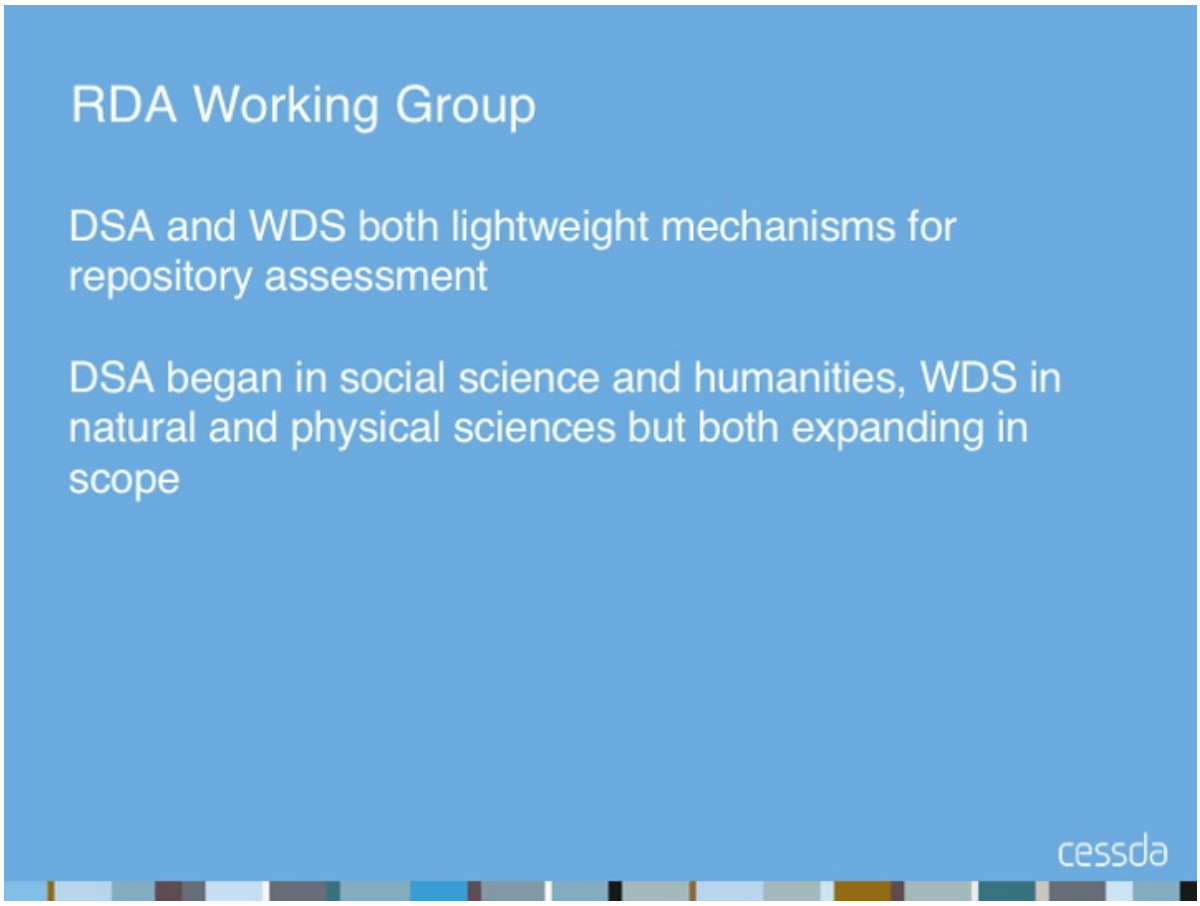

CESSDA SAW
Data Seal of Approval (DSA)
Introduction to the Common Requirements
DANS, The Hague, 16 June 2016
Hervé L'Hours
UK Data Service
cessda

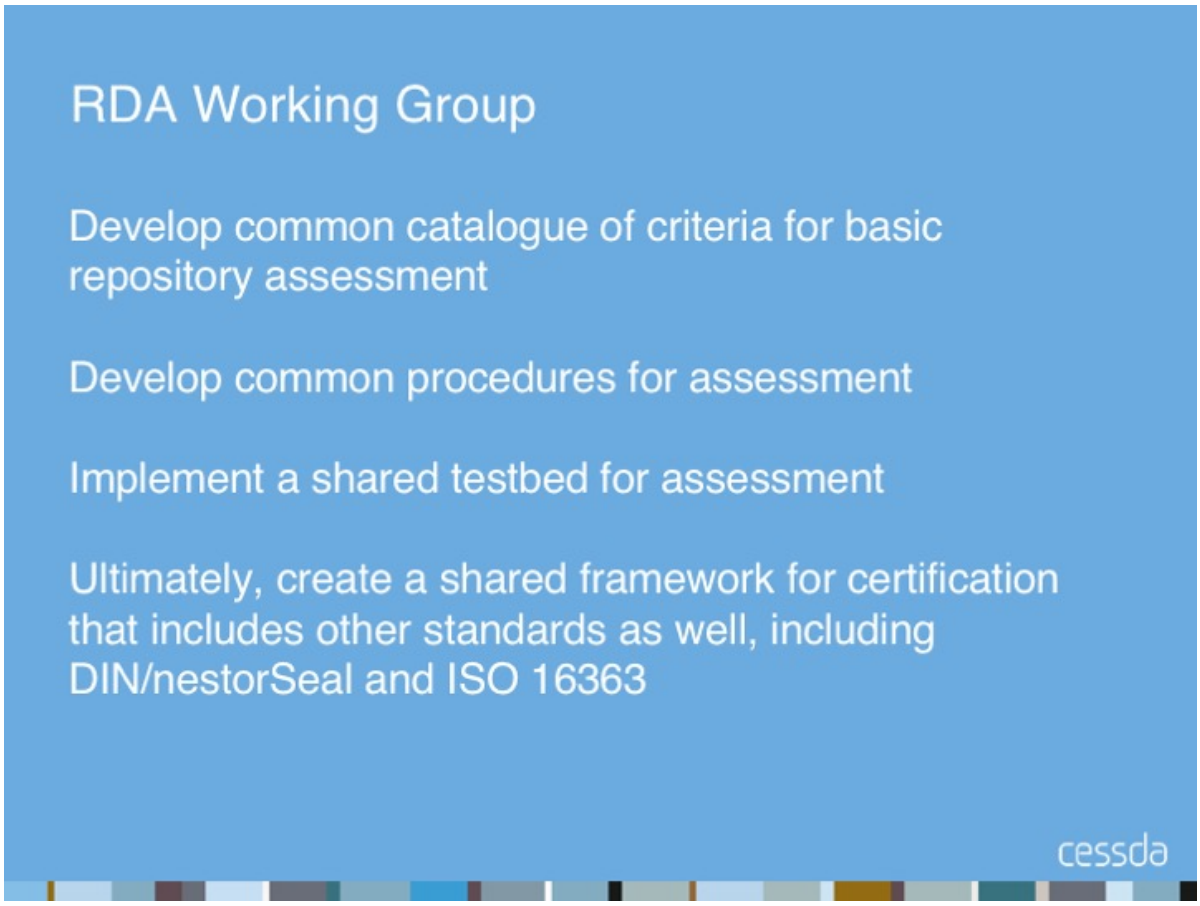

Common Requirements Overview
• Data Seal of Approval (DSA) Board
• World Data System (WDS)
• Aligned Common Requirements
• Valid from September 2016
• Replace existing version of the DSA Guidelines
cessda


Framework of Certification
Basic Certification is granted to repositories which obtain DSA certification
Extended Certification is granted to Basic Certification repositories which in addition perform a structured, externally reviewed and publicly available self-audit based on DIN 31644/nestorSeal
Formal Certification is granted to repositories which in addition to Basic Certification obtain full external audit and certification based on ISO 16363
cessda

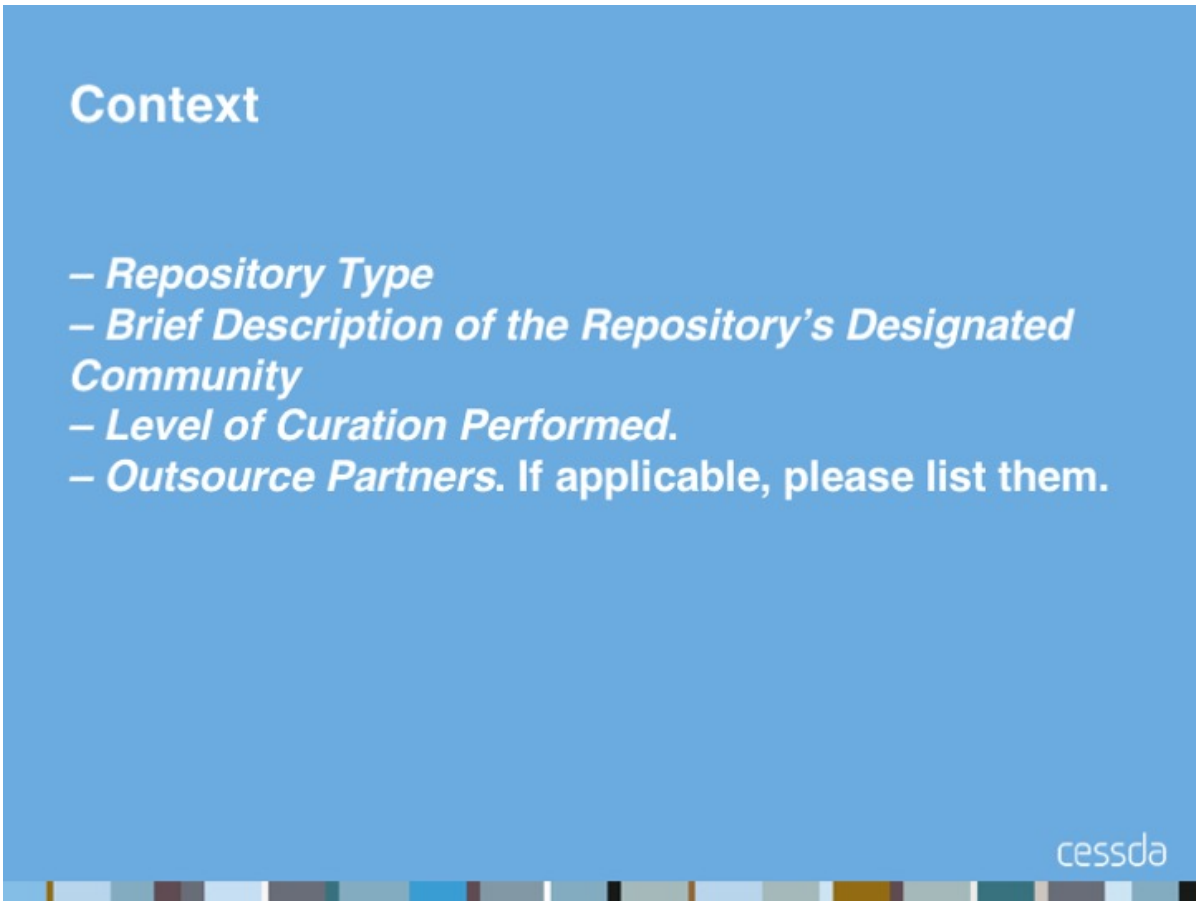

Data Seal of Approval
•Basic, lightweight certification mechanism
•16 guidelines for Trustworthy Digital Repositories
•Guidelines that relate to Data Producers, Data Repositories, and Data Consumers
•Self-assessment, with no site visit
•Peer review process supervised by DSA Board
•DSA granted for a period of two years
•Online tool for self-assessment and review
cessda

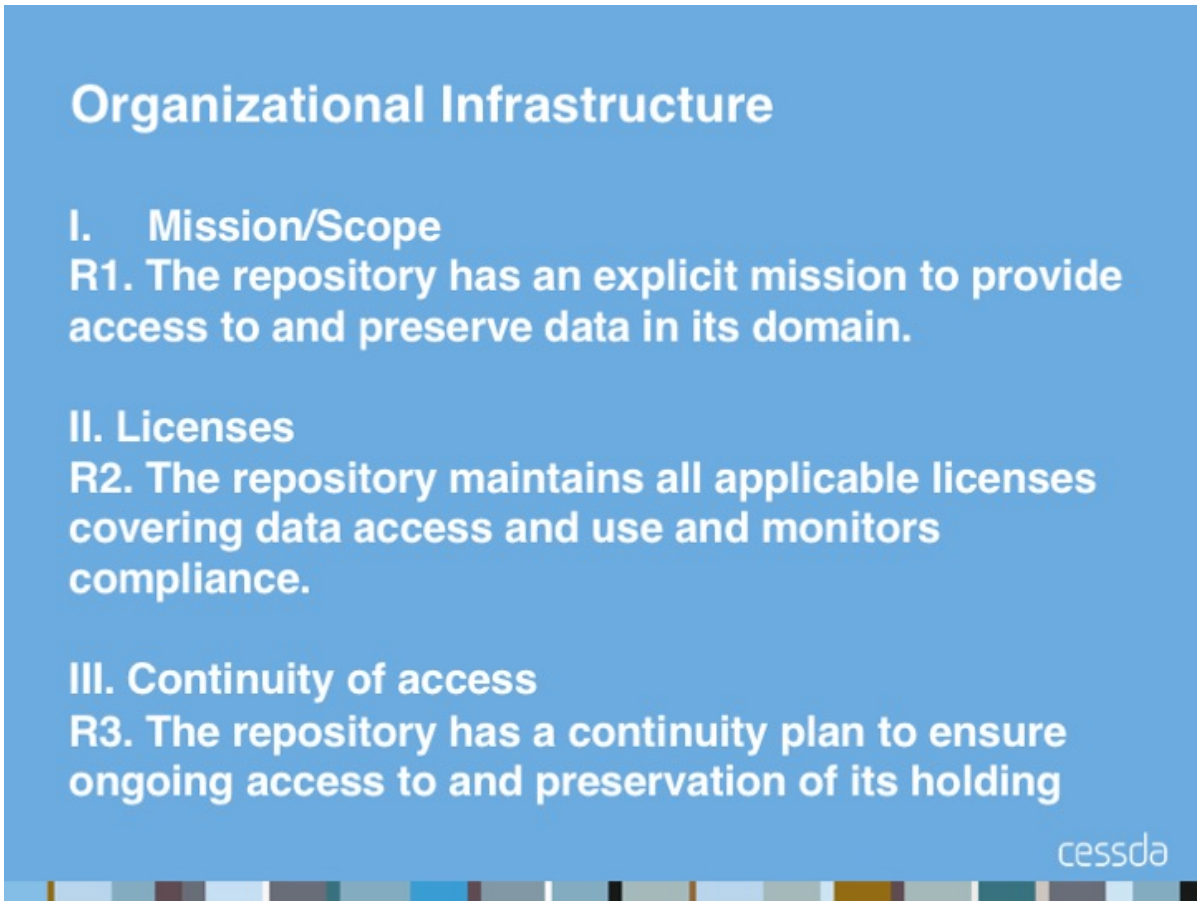

ICSU/WDS accreditation
• Basic certification mechanism
• Catalogue of 17 criteria
• The certification criteria apply for regular and network membership of WDS
• Self assessment, reviewed by the WDS Scientific Committee, with possibility of site visit
• Review of accreditation every 3-5 years
cessda


RDA Working Group
DSA and WDS both lightweight mechanisms for repository assessment
DSA began in social science and humanities, WDS in natural and physical sciences but both expanding in scope
cessda

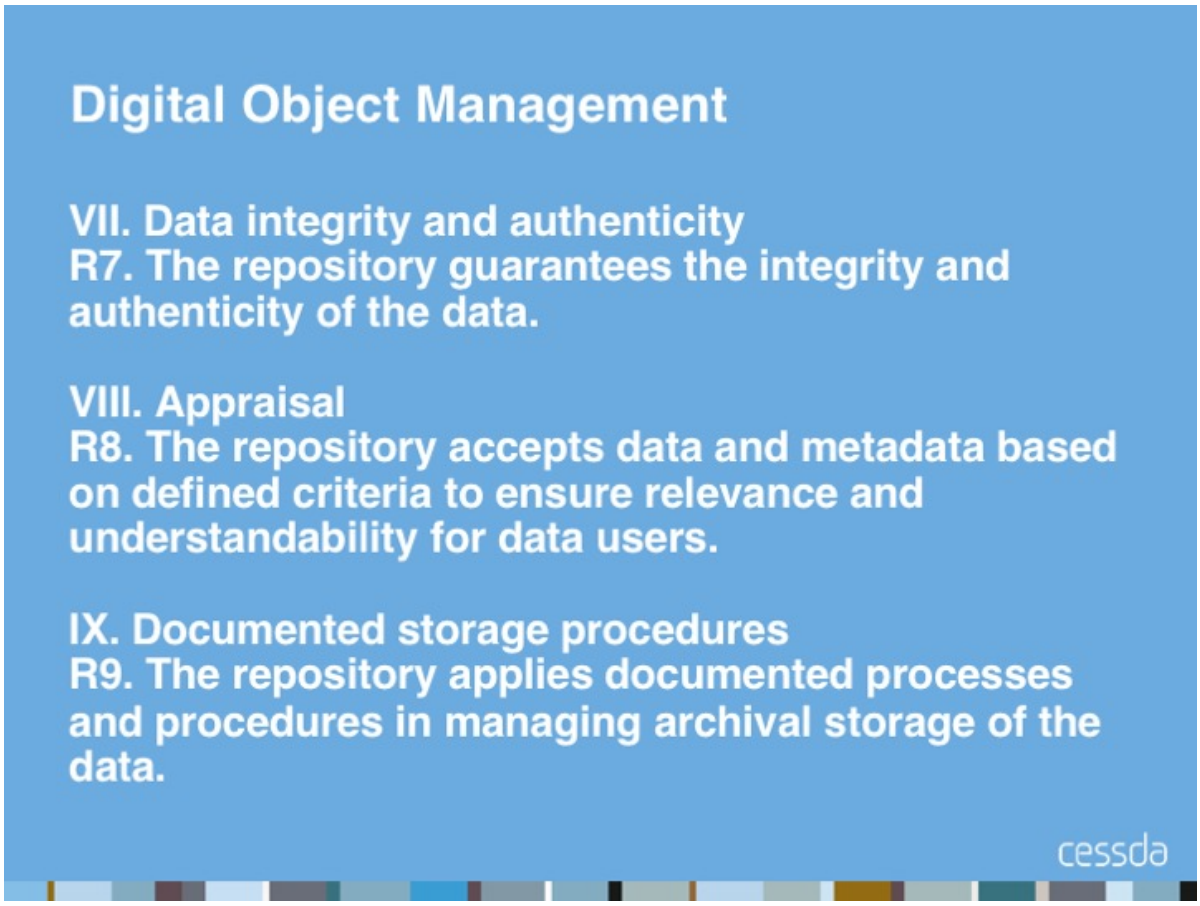

RDA Working Group
Develop common catalogue of criteria for basic repository assessment
Develop common procedures for assessment
Implement a shared testbed for assessment
Ultimately, create a shared framework for certification that includes other standards as well, including DIN/nestorSeal and ISO 16363
cessda

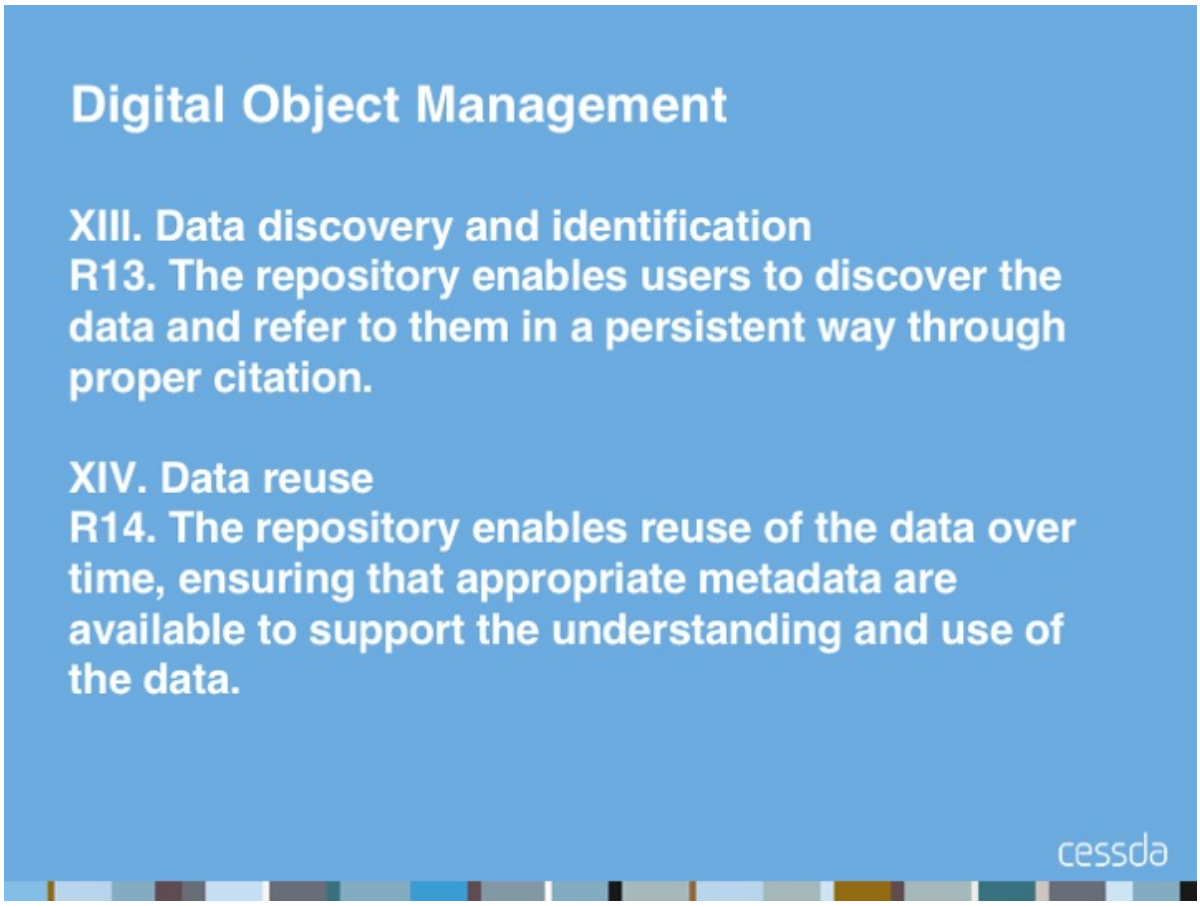

RDA Working Group
Simplification of the array of certification options and showing the value to be gained from a certification procedure requiring relatively low investment of time and effort
A combined standard will benefit the larger community of scientific data users because more repositories will be certified; leading to greater trust in these institutions and more data sharing
cessda

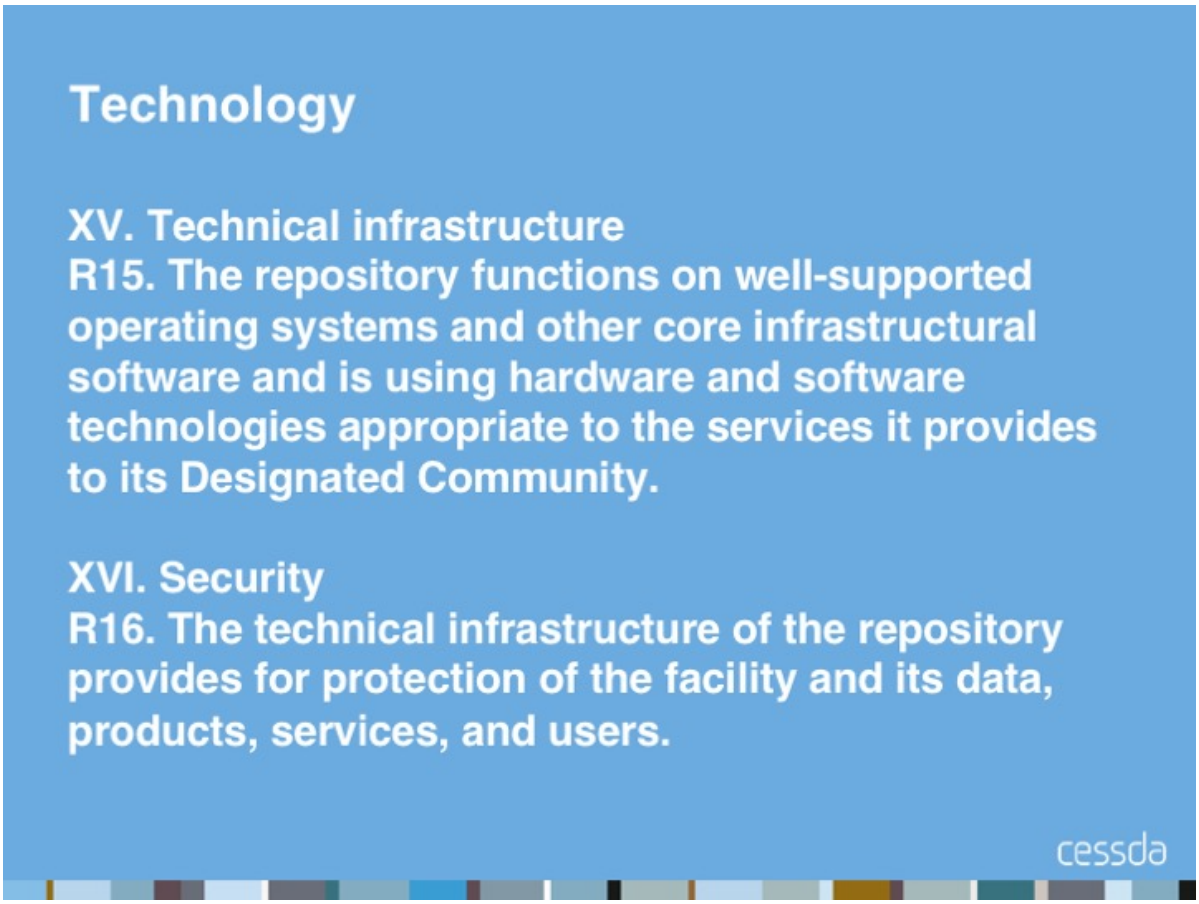

Context
– Repository Type
– Brief Description of the Repository's Designated Community
– Level of Curation Performed.
– Outsource Partners. If applicable, please list them.
cessda


Organizational Infrastructure
I. Mission/Scope
R1. The repository has an explicit mission to provide access to and preserve data in its domain.
II. Licenses
R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.
III. Continuity of access
R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holding
cessda

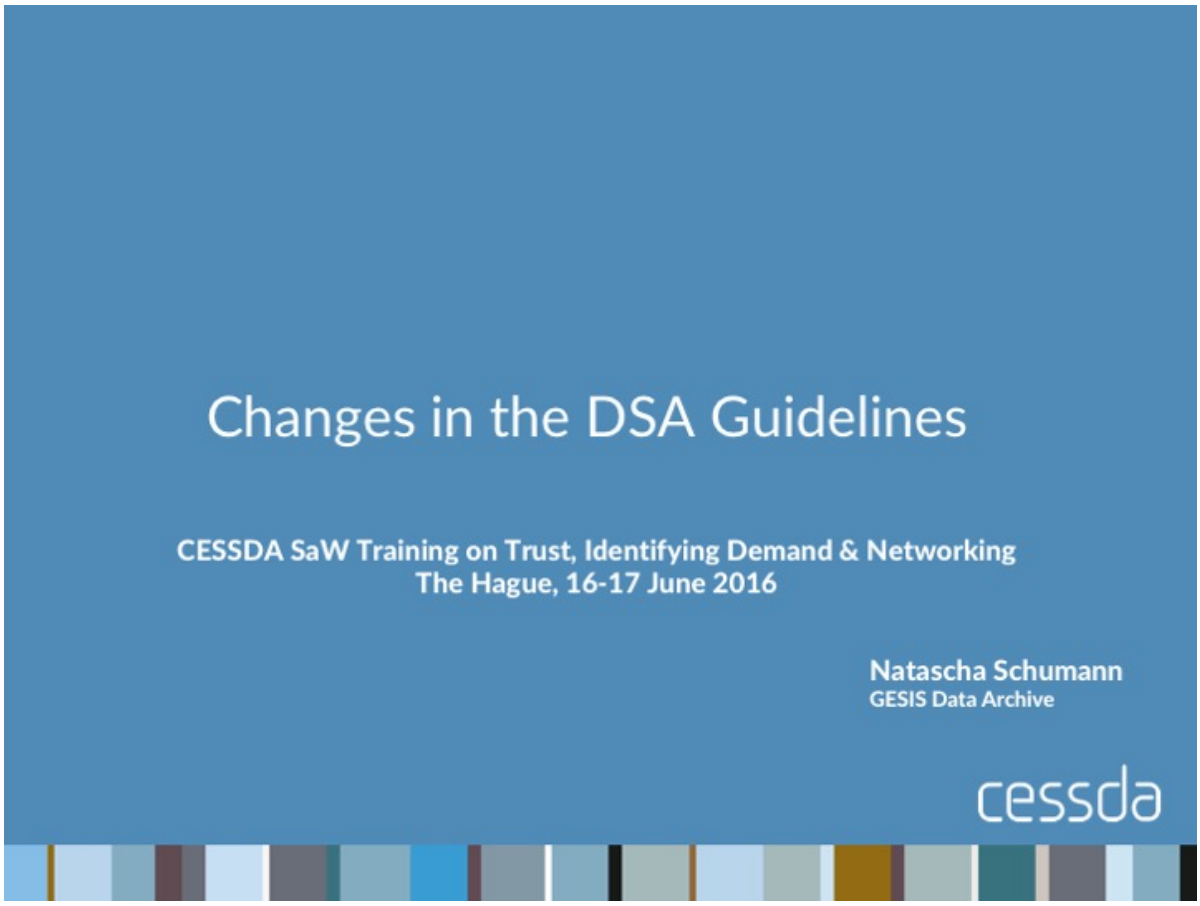

Organizational Infrastructure
IV. Confidentiality/Ethics
R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.
V. Organizational infrastructure
R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.
VI. Expert guidance
R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant)
cessda


Digital Object Management
VII. Data integrity and authenticity
R7. The repository guarantees the integrity and authenticity of the data.
VIII. Appraisal
R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.
IX. Documented storage procedures
R9. The repository applies documented processes and procedures in managing archival storage of the data.
cessda


Digital Object Management
XIII. Data discovery and identification
R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.
XIV. Data reuse
R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.
cessda


Technology
XV. Technical infrastructure
R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.
XVI. Security
R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.
cessda


Thanks
cessda

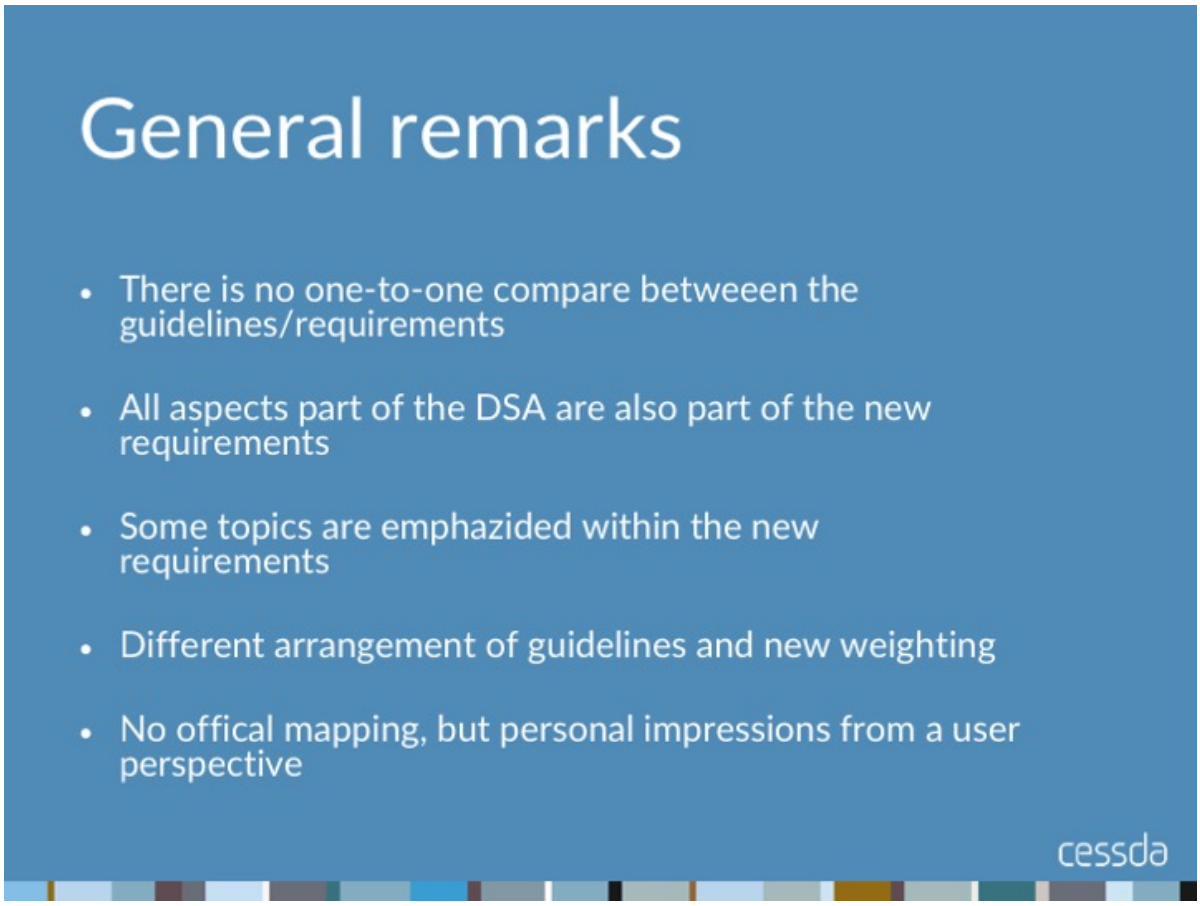

Changes in the DSA Guidelines
CESSDA SaW Training on Trust, Identifying Demand & Networking
The Hague, 16-17 June 2016
Natascha Schumann
GESIS Data Archive
cessda

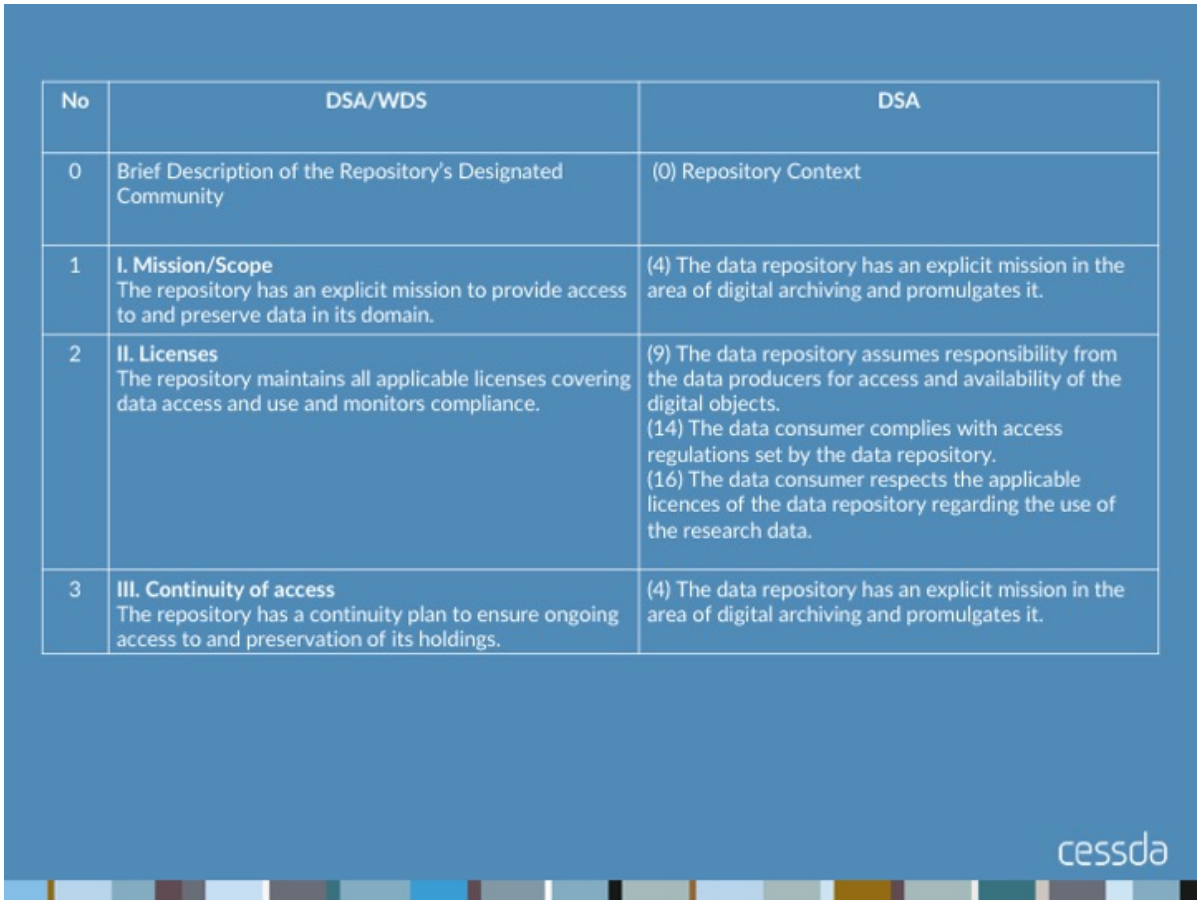

Overview
• Different Structure
• Compliance Level
• Old Guidelines vs new and common Requirements
cessda

Structure

DSA (16 Guidelines)	DSA/WDS (18 Requirements)
Data producers (3 Guidelines)	Organizational Infrastructure
Data repository (10 Guidelines)	Digital Object Management
Data users (3 Guidelines)	Technology
	Additional Information & Applicant Feedback

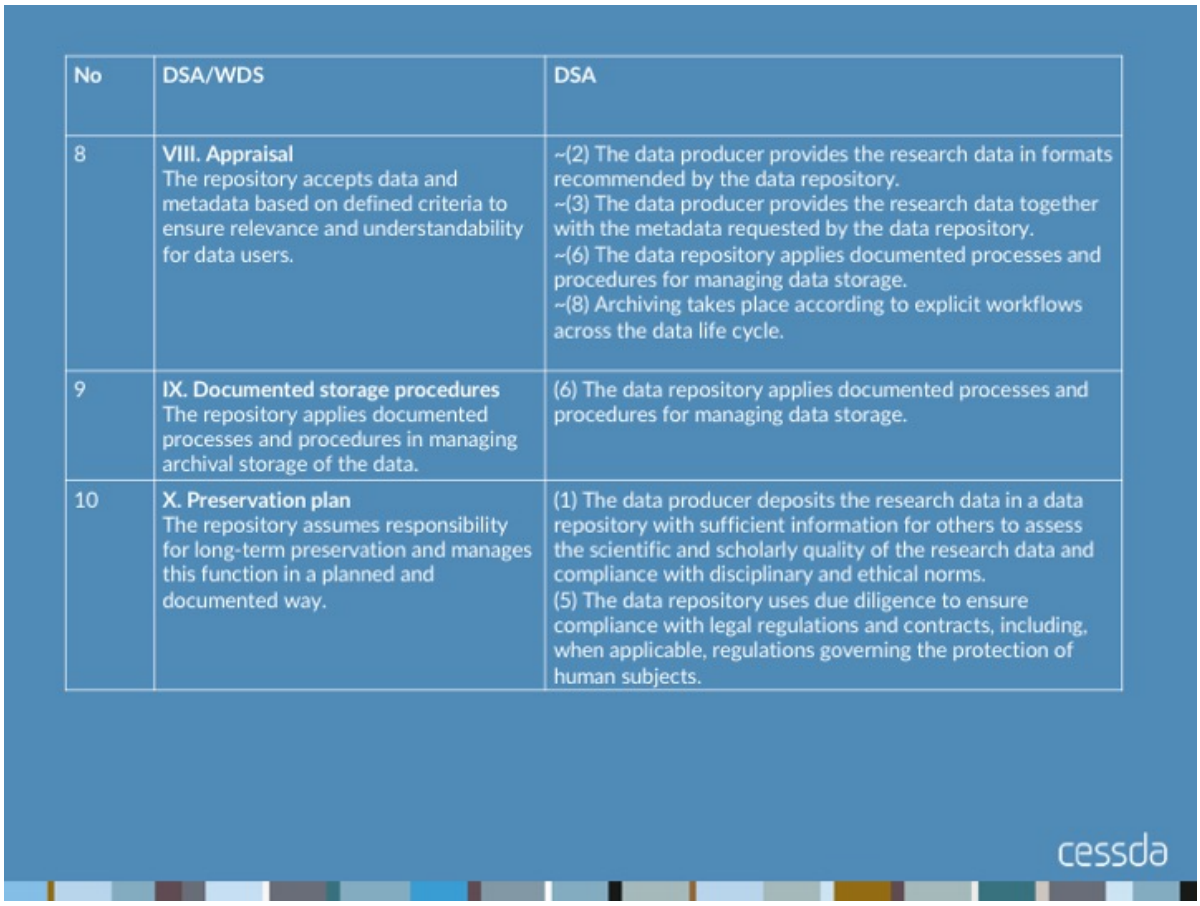

Compliance Level
0 – Not applicable
1 – The repository has not considered this yet
2 – The repository has a theoretical concept
3 – The repository is in the implementation phase
4 – The guideline has been fully implemented in the repository
cessda


General remarks
There is no one-to-one compare betweeen the guidelines/requirements
All aspects part of the DSA are also part of the new requirements
Some topics are emphazided within the new requirements
Different arrangement of guidelines and new weighting
No offical mapping, but personal impressions from a user perspective
cessda

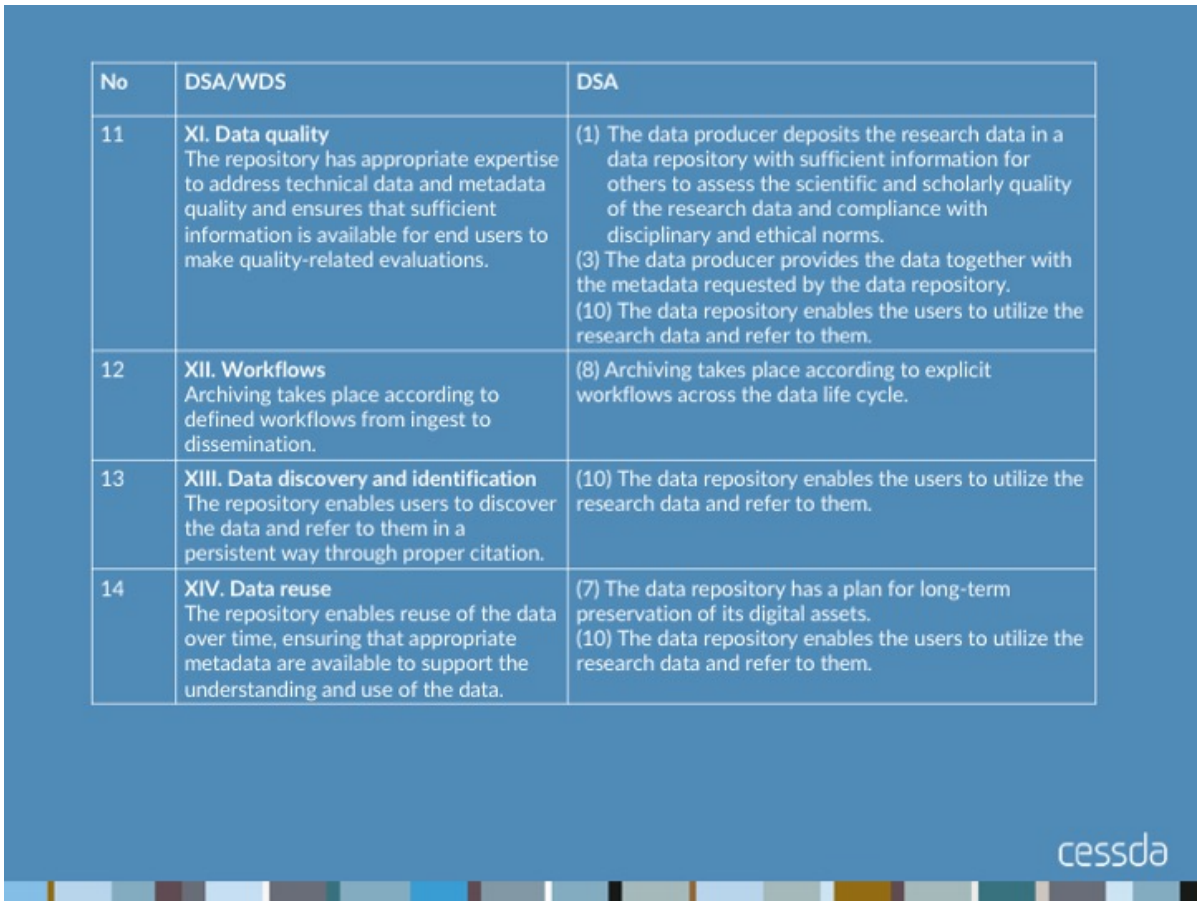


No	DSA/WDS	DSA
0	Brief Description of the Repository's Designated Community	(0) Repository Context
1	**I. Mission/Scope** The repository has an explicit mission to provide access to and preserve data in its domain.	(4) The data repository has an explicit mission in the area of digital archiving and promulgates it.
2	**II. Licenses** The repository maintains all applicable licenses covering data access and use and monitors compliance.	(9) The data repository assumes responsibility from the data producers for access and availability of the digital objects. (14) The data consumer complies with access regulations set by the data repository. (16) The data consumer respects the applicable licences of the data repository regarding the use of the research data.
3	**III. Continuity of access** The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.	(4) The data repository has an explicit mission in the area of digital archiving and promulgates it.

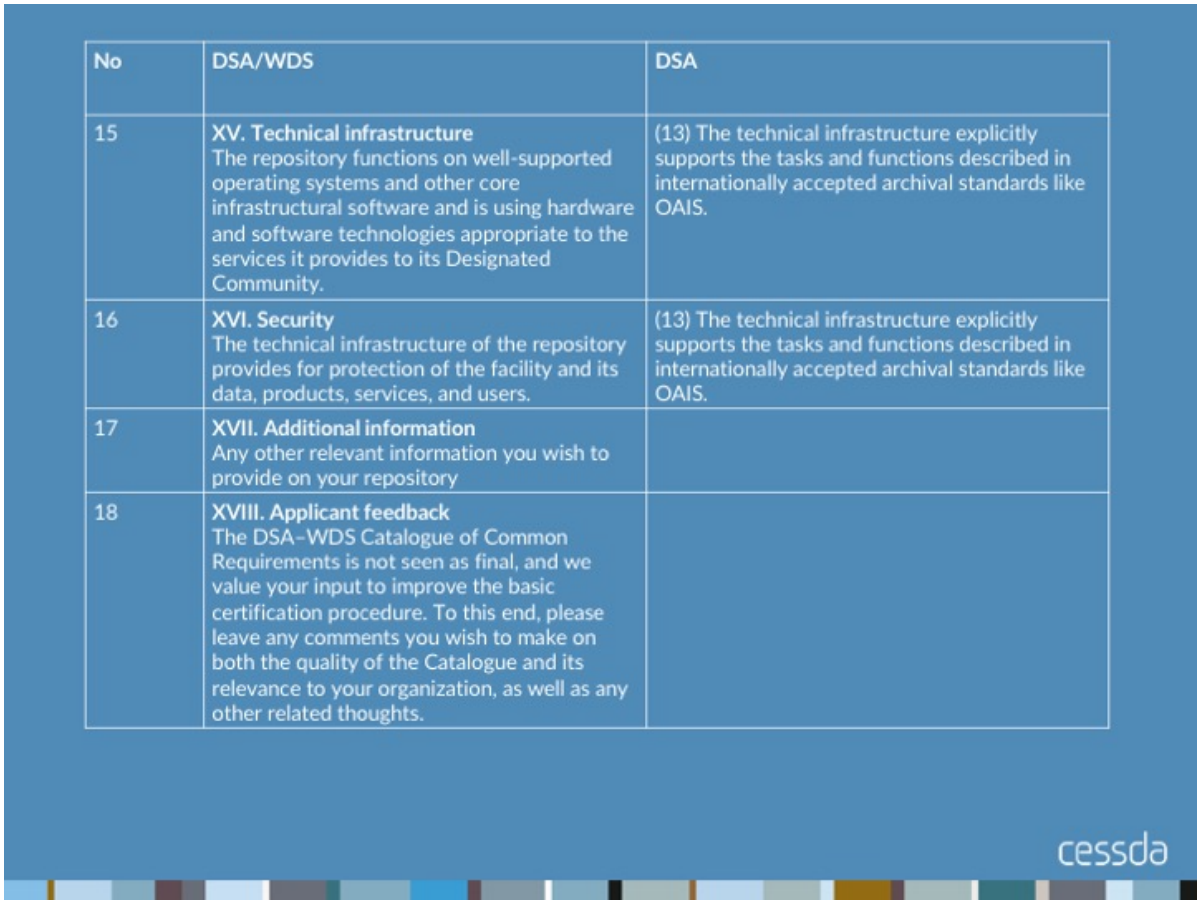
No	DSA/WDS	DSA
4	**IV. Confidentiality/Ethics** The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.	(5) The data repository uses due diligence to ensure compliance with legal regulations and contracts, including, when applicable, regulations governing the protection of human subjects. (15) The data consumer conforms to and agrees with any codes of conduct that are generally accepted in higher education and scientific research for the exchange and proper use of knowledge and information.
5	**V. Organizational infrastructure** The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.	~(4) The data repository has an explicit mission in the area of digital archiving and promulgates it. ~(8) Archiving takes place according to explicit workflows across the data life cycle.
6	**VI. Expert guidance** The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).	(5) The data repository uses due diligence to ensure compliance with legal regulations and contracts, including, when applicable, regulations governing the protection of human subjects. (13) The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS.
7	**VII. Data integrity and authenticity** The repository guarantees the integrity and authenticity of the data.	(11) The data repository ensures the integrity of the digital objects and the metadata. (12) The data repository ensures the authenticity of the digital objects and the metadata.



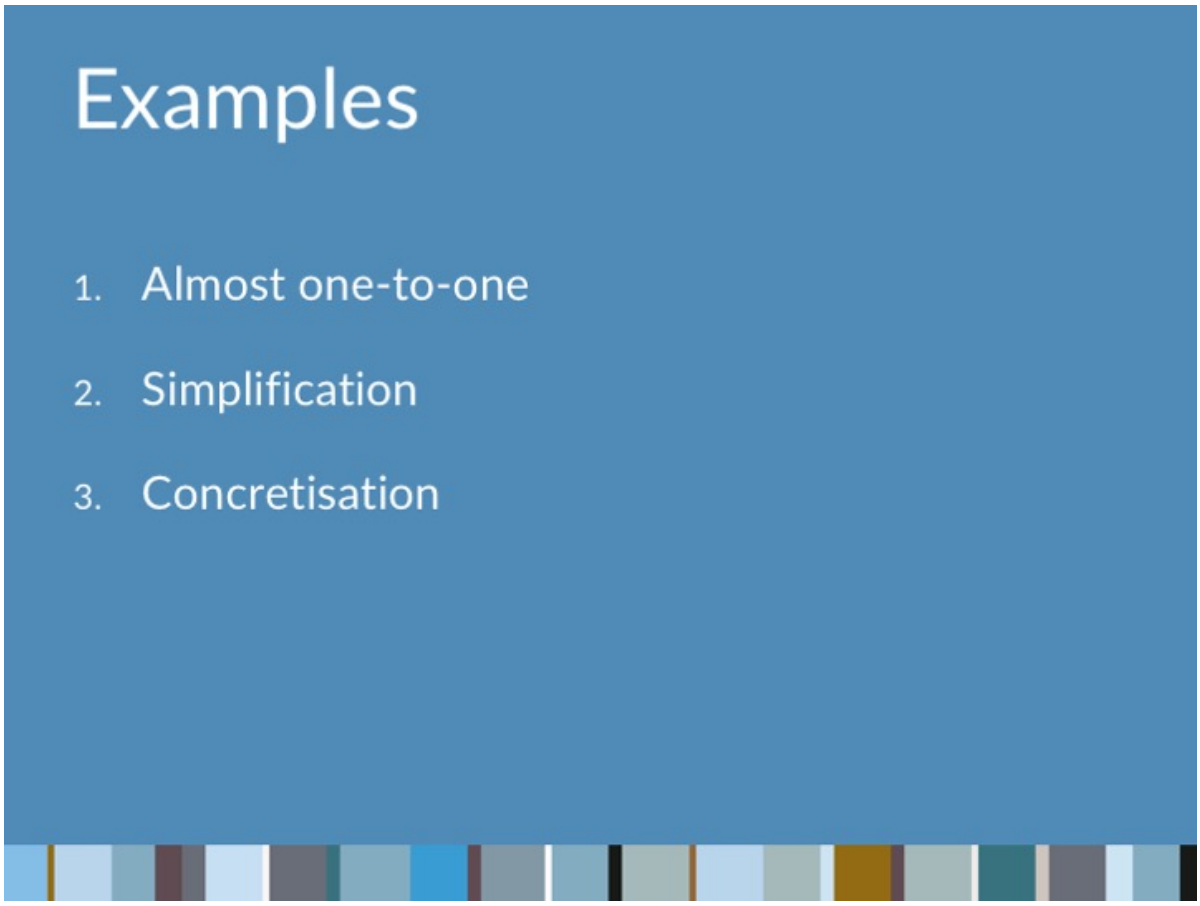
No	DSA/WDS	DSA
8	**VIII. Appraisal** The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.	~(2) The data producer provides the research data in formats recommended by the data repository. ~(3) The data producer provides the research data together with the metadata requested by the data repository. ~(6) The data repository applies documented processes and procedures for managing data storage. ~(8) Archiving takes place according to explicit workflows across the data life cycle.
9	**IX. Documented storage procedures** The repository applies documented processes and procedures in managing archival storage of the data.	(6) The data repository applies documented processes and procedures for managing data storage.
10	**X. Preservation plan** The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.	(1) The data producer deposits the research data in a data repository with sufficient information for others to assess the scientific and scholarly quality of the research data and compliance with disciplinary and ethical norms. (5) The data repository uses due diligence to ensure compliance with legal regulations and contracts, including, when applicable, regulations governing the protection of human subjects.

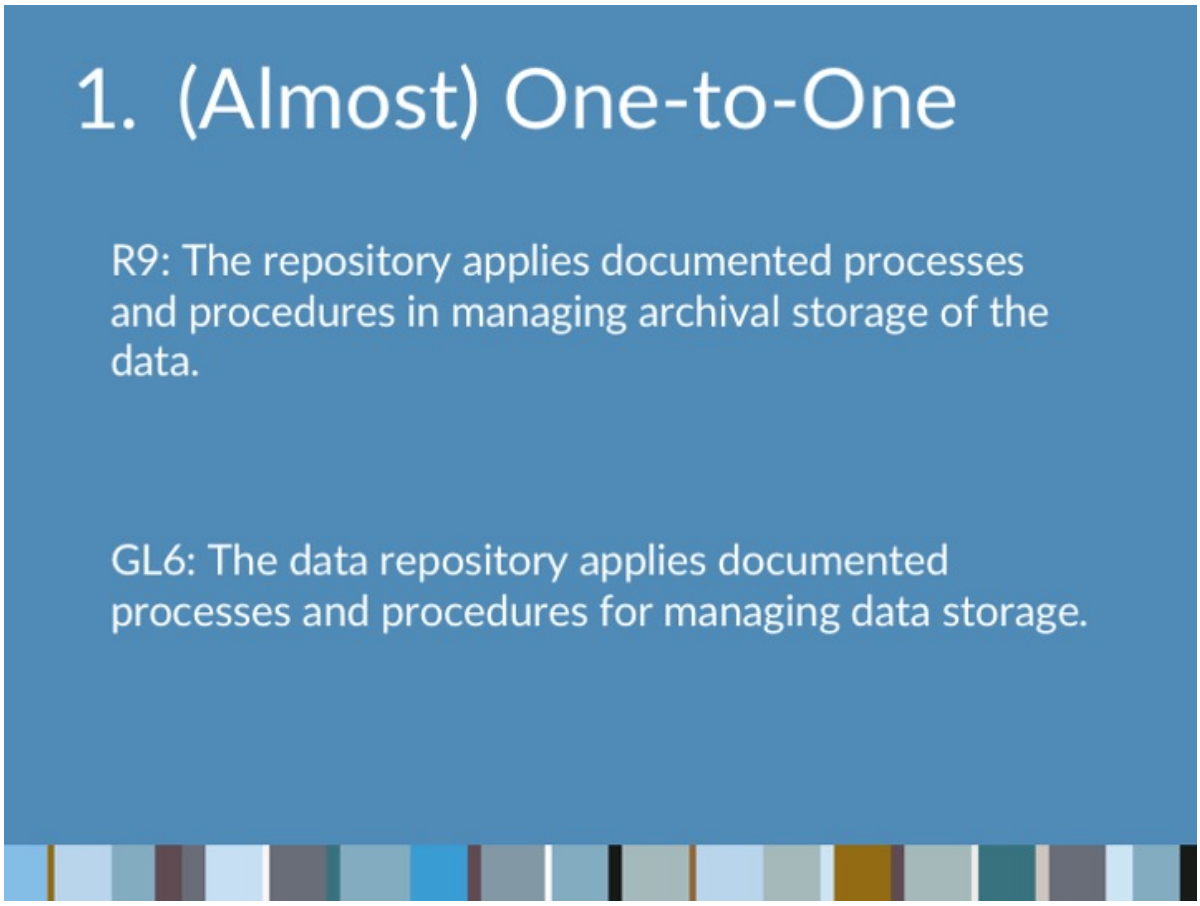


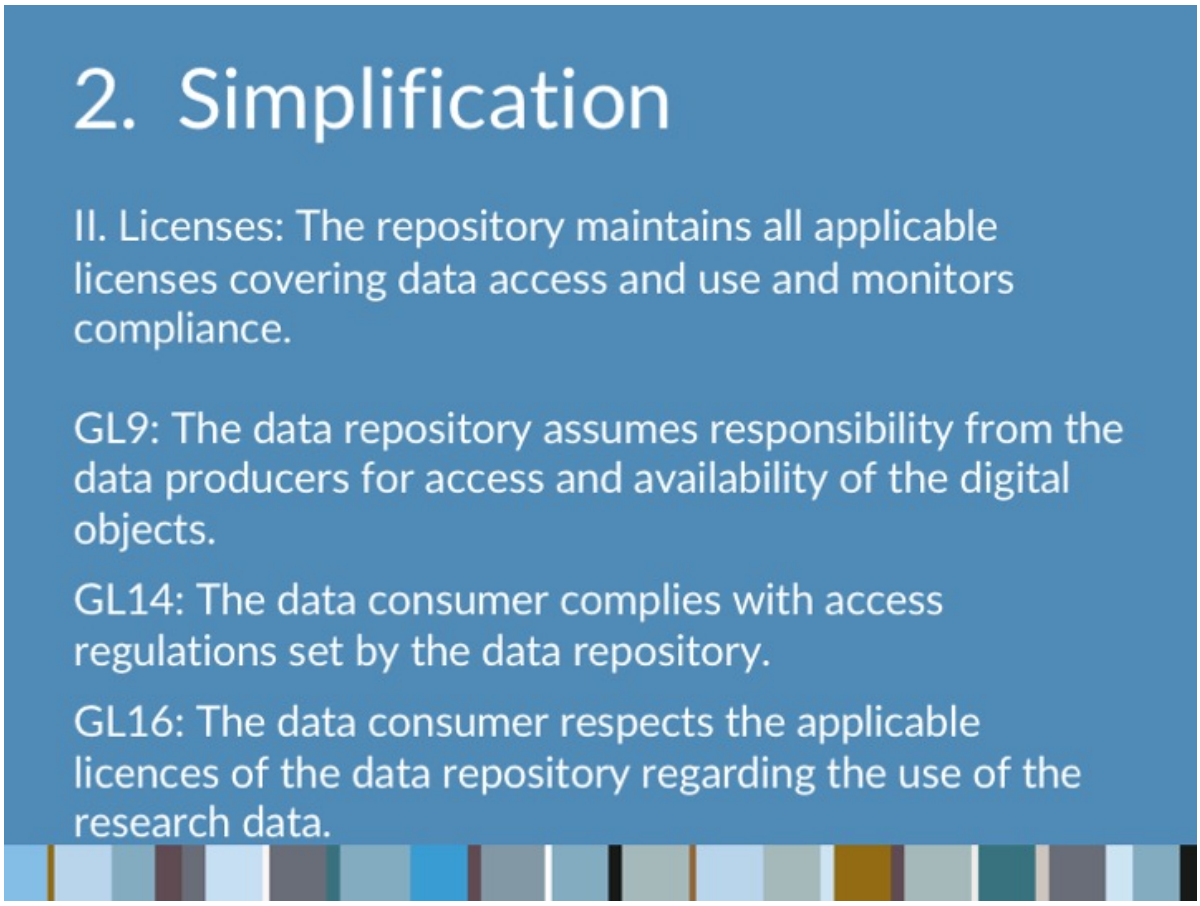
No	DSA/WDS	DSA
11	**XI. Data quality** The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.	(1) The data producer deposits the research data in a data repository with sufficient information for others to assess the scientific and scholarly quality of the research data and compliance with disciplinary and ethical norms. (3) The data producer provides the data together with the metadata requested by the data repository. (10) The data repository enables the users to utilize the research data and refer to them.
12	**XII. Workflows** Archiving takes place according to defined workflows from ingest to dissemination.	(8) Archiving takes place according to explicit workflows across the data life cycle.
13	**XIII. Data discovery and identification** The repository enables users to discover the data and refer to them in a persistent way through proper citation.	(10) The data repository enables the users to utilize the research data and refer to them.
14	**XIV. Data reuse** The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.	(7) The data repository has a plan for long-term preservation of its digital assets. (10) The data repository enables the users to utilize the research data and refer to them.

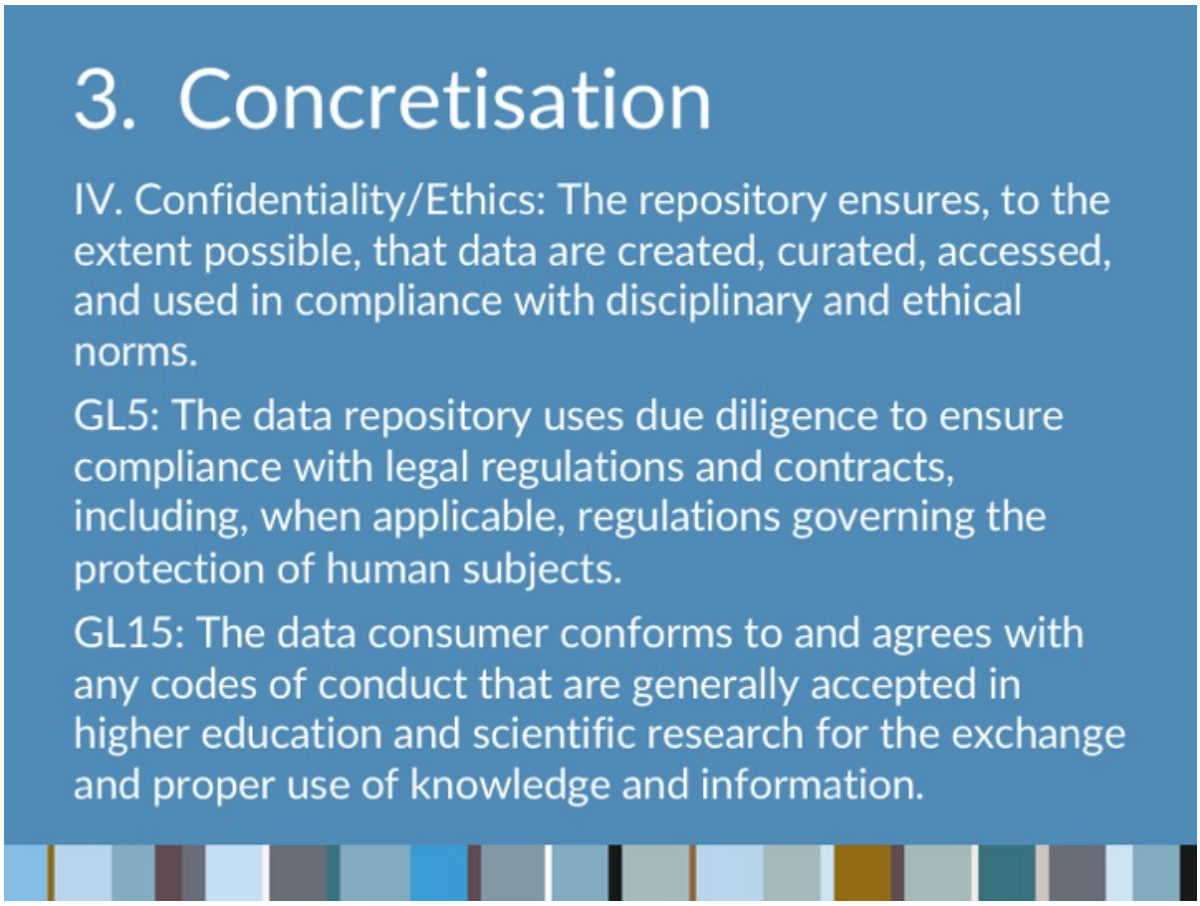


No	DSA/WDS	DSA
15	**XV. Technical infrastructure** The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.	(13) The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS.
16	**XVI. Security** The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.	(13) The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS.
17	**XVII. Additional information** Any other relevant information you wish to provide on your repository	
18	**XVIII. Applicant feedback** The DSA–WDS Catalogue of Common Requirements is not seen as final, and we value your input to improve the basic certification procedure. To this end, please leave any comments you wish to make on both the quality of the Catalogue and its relevance to your organization, as well as any other related thoughts.	


Examples
1. Almost one-to-one
2. Simplification
3. Concretisation


1. (Almost) One-to-One
R9: The repository applies documented processes and procedures in managing archival storage of the data.
GL6: The data repository applies documented processes and procedures for managing data storage.


2. Simplification
II. Licenses: The repository maintains all applicable licenses covering data access and use and monitors compliance.
GL9: The data repository assumes responsibility from the data producers for access and availability of the digital objects.
GL14: The data consumer complies with access regulations set by the data repository.
GL16: The data consumer respects the applicable licences of the data repository regarding the use of the research data.


3. Concretisation
IV. Confidentiality/Ethics: The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.
GL5: The data repository uses due diligence to ensure compliance with legal regulations and contracts, including, when applicable, regulations governing the protection of human subjects.
GL15: The data consumer conforms to and agrees with any codes of conduct that are generally accepted in higher education and scientific research for the exchange and proper use of knowledge and information.

Summary

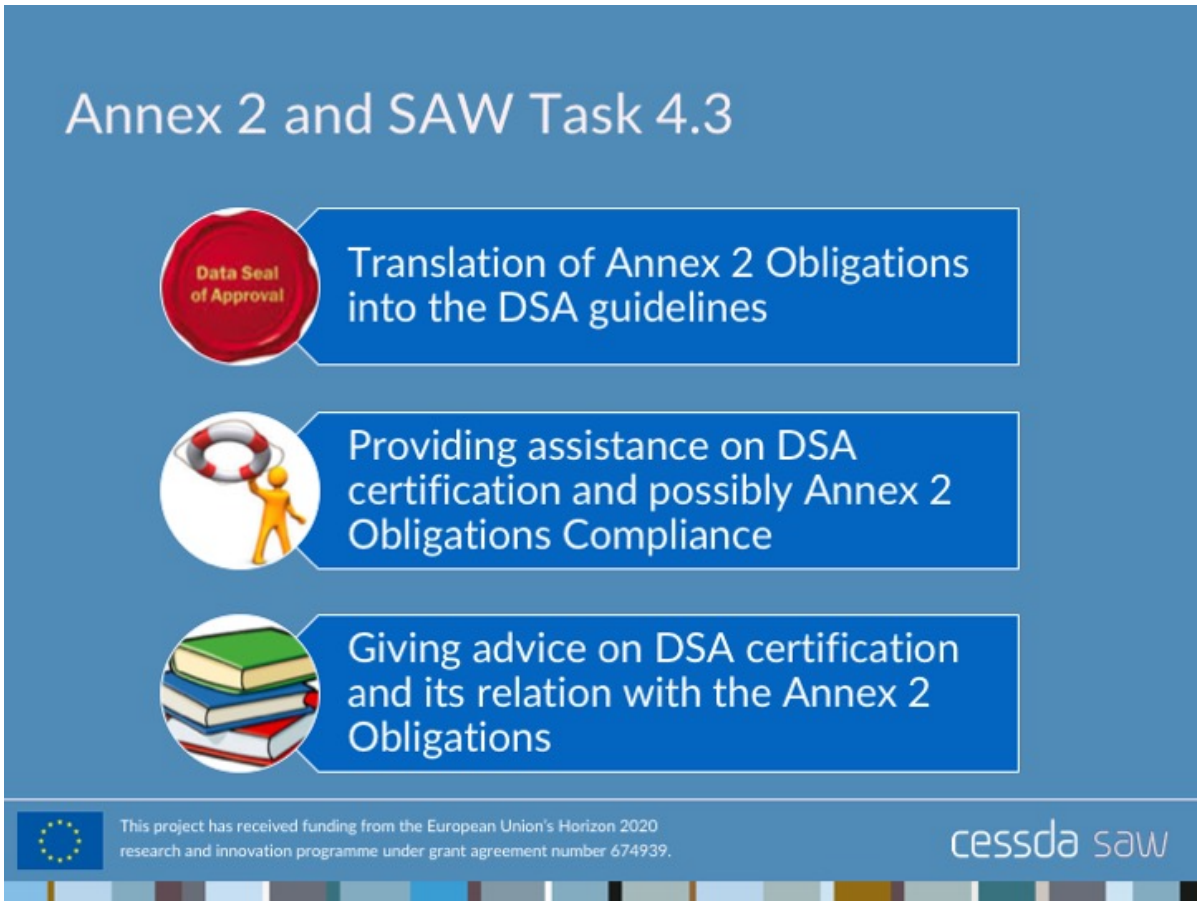
- No change of contents
- New structure:
  - Like the standards within the framework
  - Easier to go through
- Stronger emphasis on documented procedures and plans
- Clear labeling of the requirements

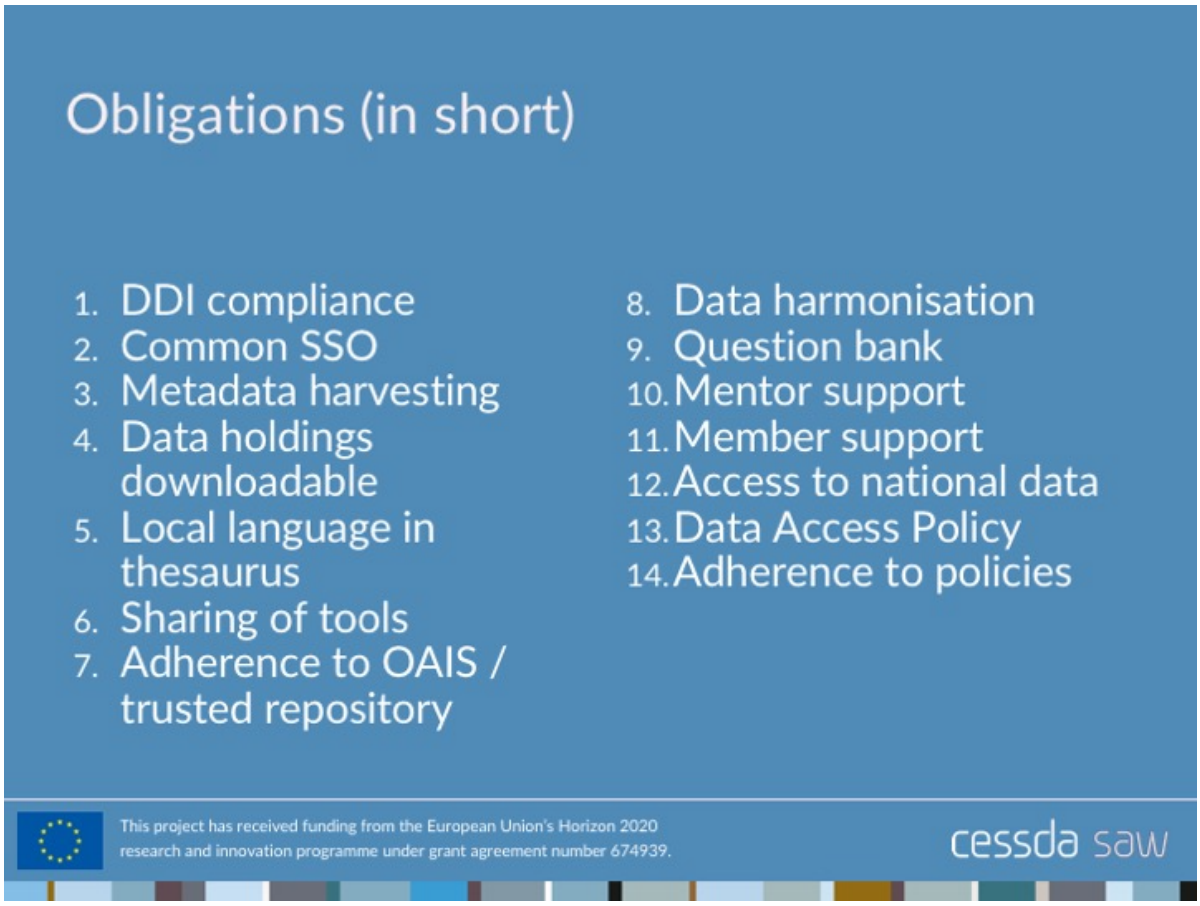
cessda saw

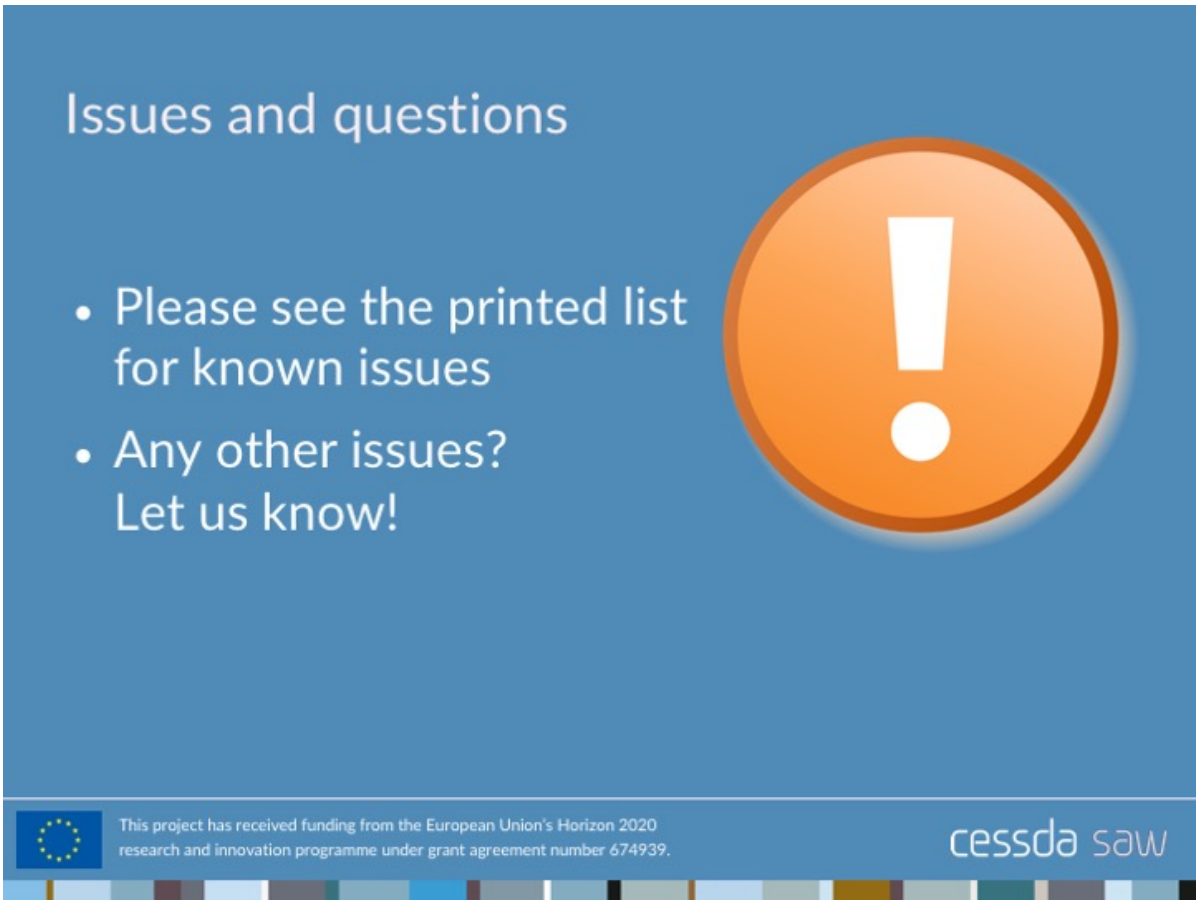
Annex 2 Obligations

Workshop 1
The Hague
16.-17.6.2016

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 674939.


Annex 2 and SAW Task 4.3
Data Seal of Approval
Translation of Annex 2 Obligations into the DSA guidelines
Providing assistance on DSA certification and possibly Annex 2 Obligations Compliance
Giving advice on DSA certification and its relation with the Annex 2 Obligations
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 674939.
cessda saw


Obligations (in short)
1. DDI compliance
2. Common SSO
3. Metadata harvesting
4. Data holdings downloadable
5. Local language in thesaurus
6. Sharing of tools
7. Adherence to OAIS / trusted repository
8. Data harmonisation
9. Question bank
10. Mentor support
11. Member support
12. Access to national data
13. Data Access Policy
14. Adherence to policies
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 674939.
cessda saw


Issues and questions
• Please see the printed list for known issues
• Any other issues? Let us know!
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 674939.
cessda saw

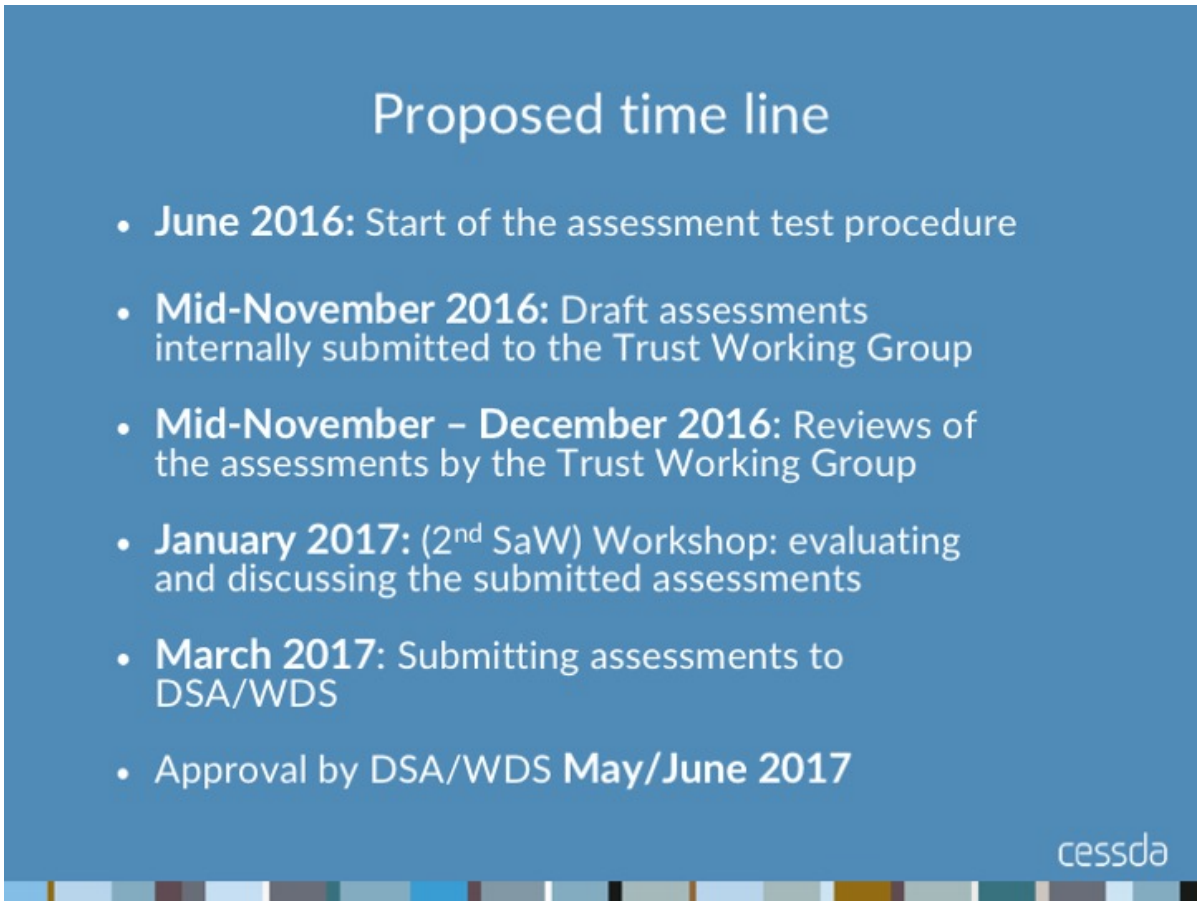

cessda
—thanks for your attention!
website: www.cessda.net / twitter: @CESSDA_Data

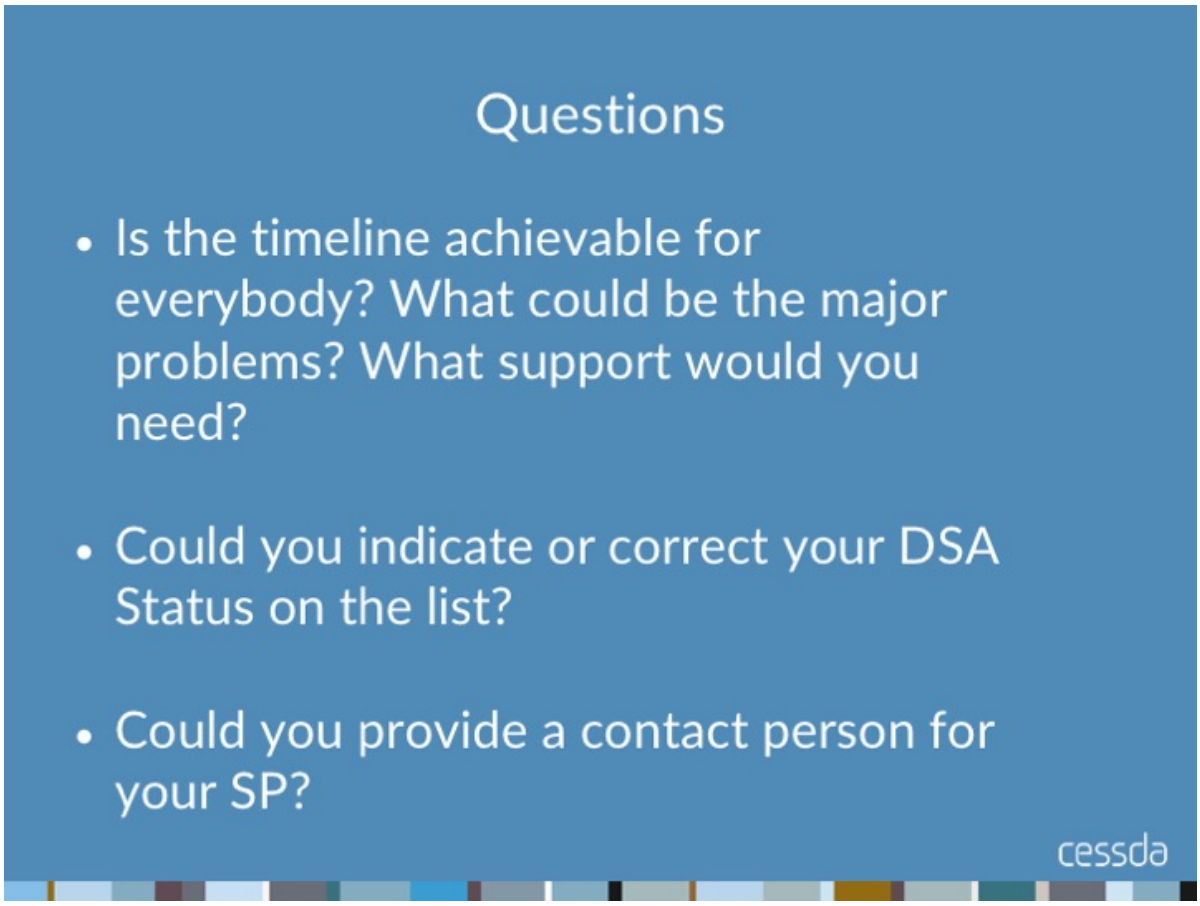
CESSDA Trust and Certification

Trust Session 1:
Questions from the participants, questions to the participants

CESSDA SAW Workshop
The Hague, 16-17 June 2016

cessda


Proposed time line
June 2016: Start of the assessment test procedure
Mid-November 2016: Draft assessments internally submitted to the Trust Working Group
Mid-November – December 2016: Reviews of the assessments by the Trust Working Group
January 2017: (2nd SaW) Workshop: evaluating and discussing the submitted assessments
March 2017: Submitting assessments to DSA/WDS
Approval by DSA/WDS May/June 2017
cessda


Questions
• Is the timeline achievable for everybody? What could be the major problems? What support would you need?
• Could you indicate or correct your DSA Status on the list?
• Could you provide a contact person for your SP?
cessda


cessda
—in your circle of trust.
website: www.cessda.net / twitter:
@CESSDA_Data

CESSDA Trust and Certification

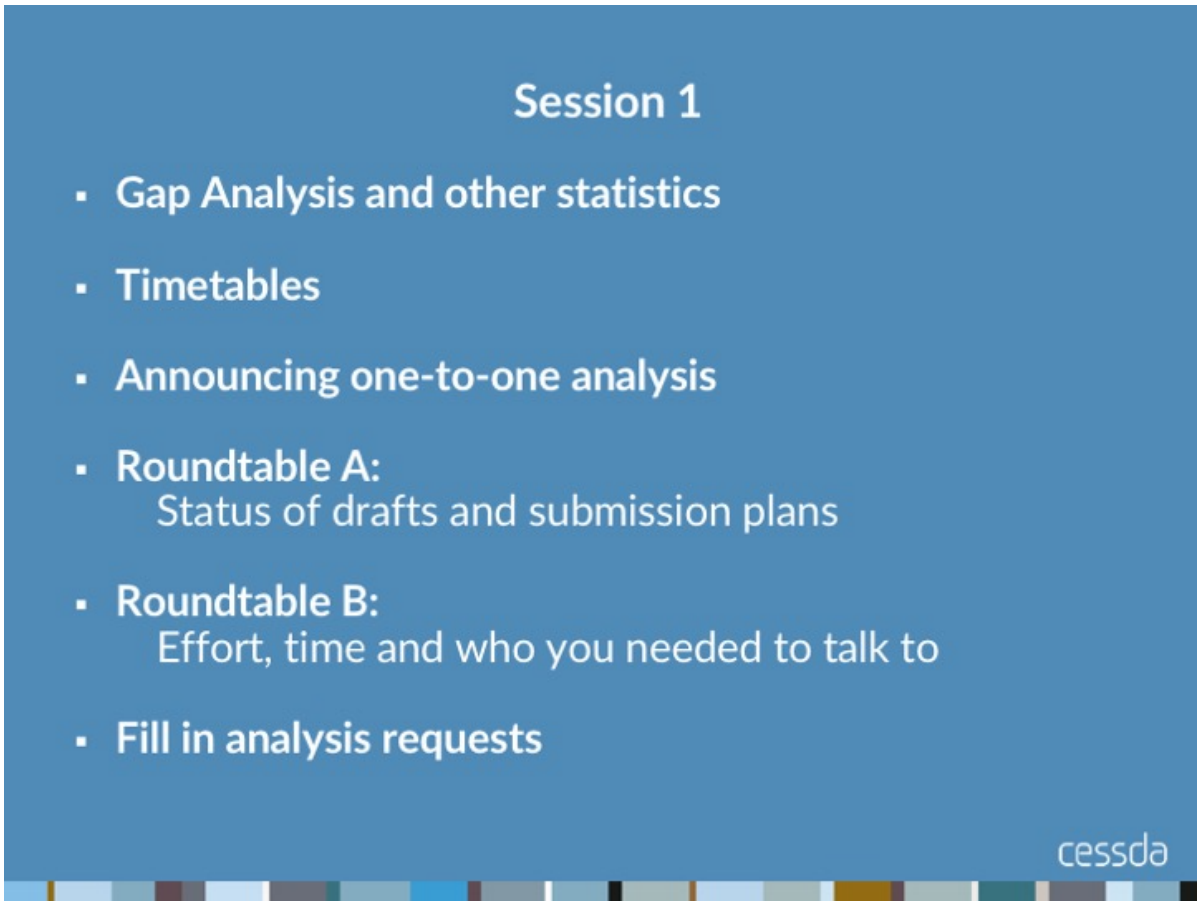
Introduction Session 1

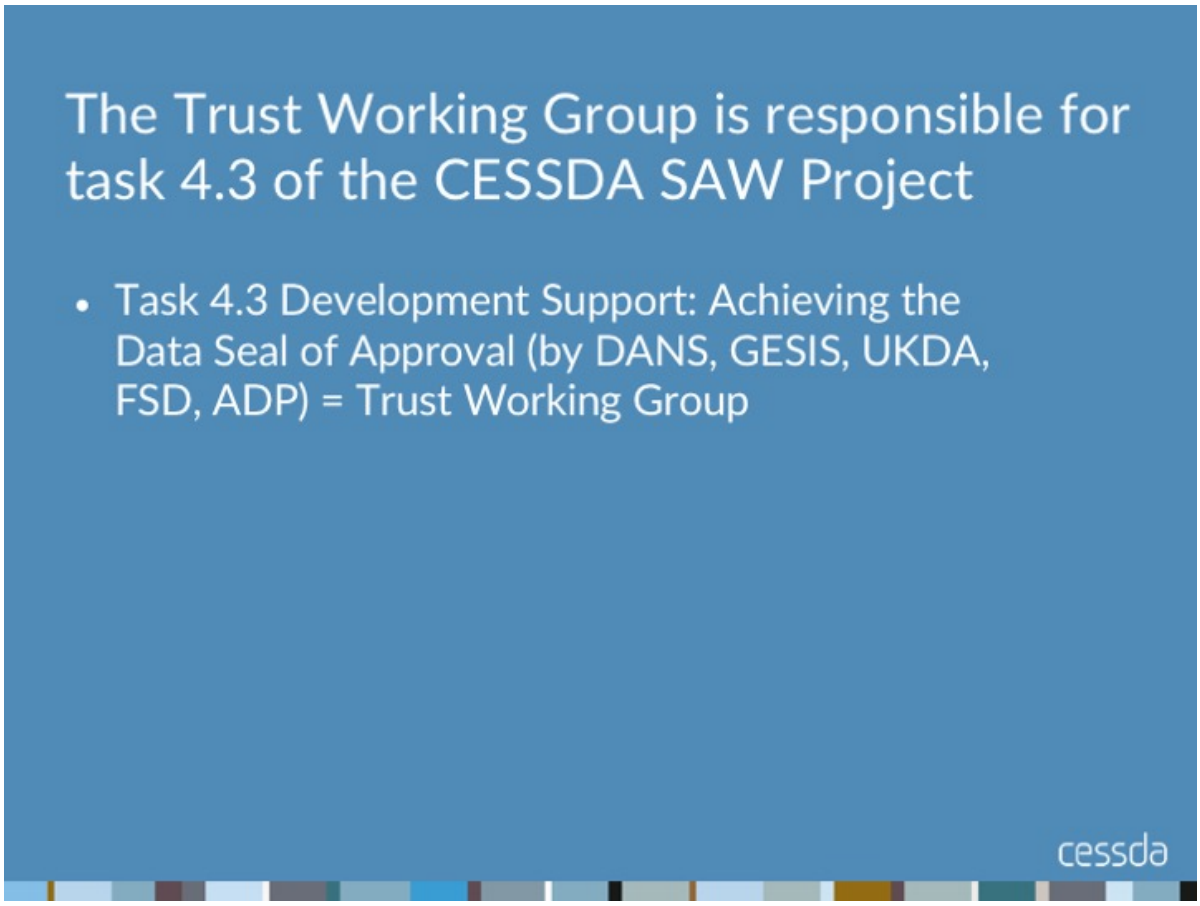
CESSDA SAW Workshop
Zagreb, 1-2 March 2017

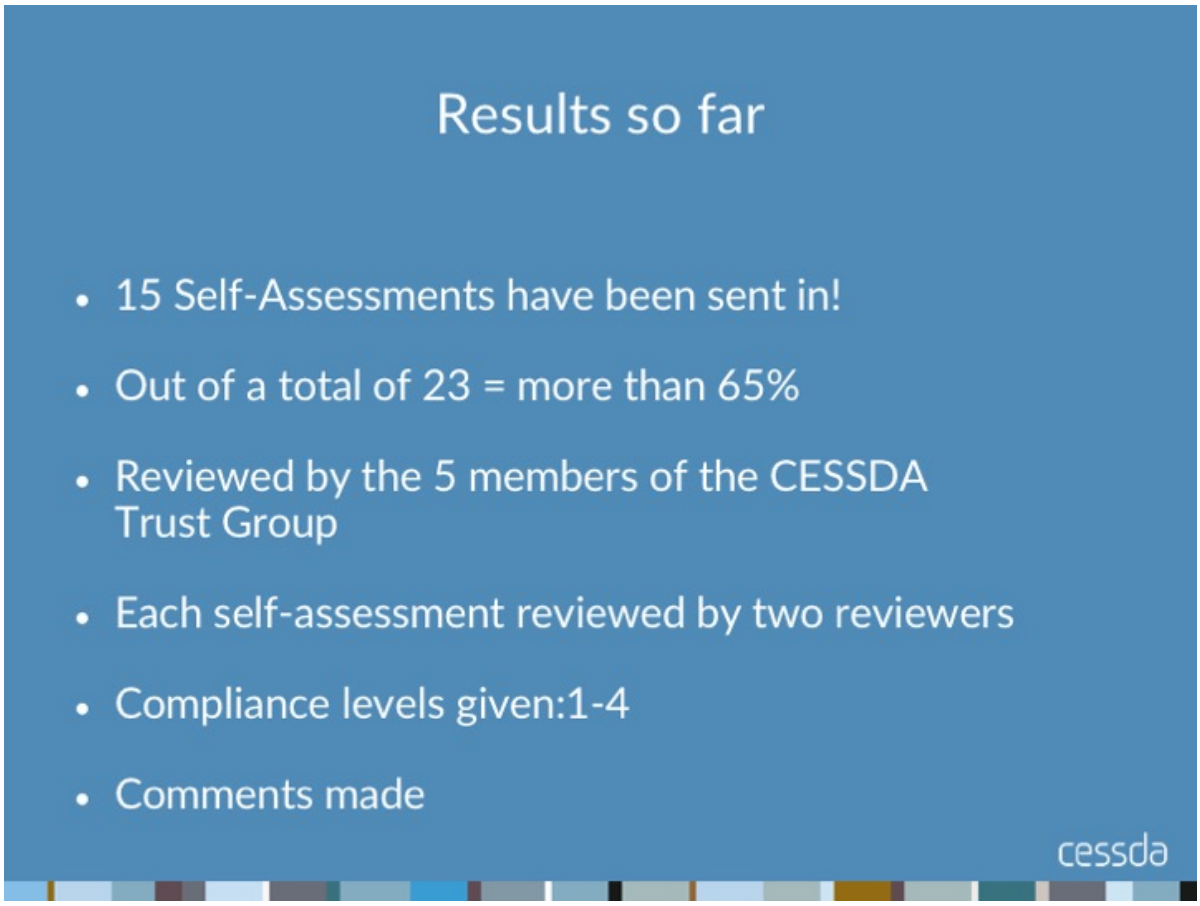
Heiko Tjalsma
Policy advisor DANS
Chairman Trust Working Group

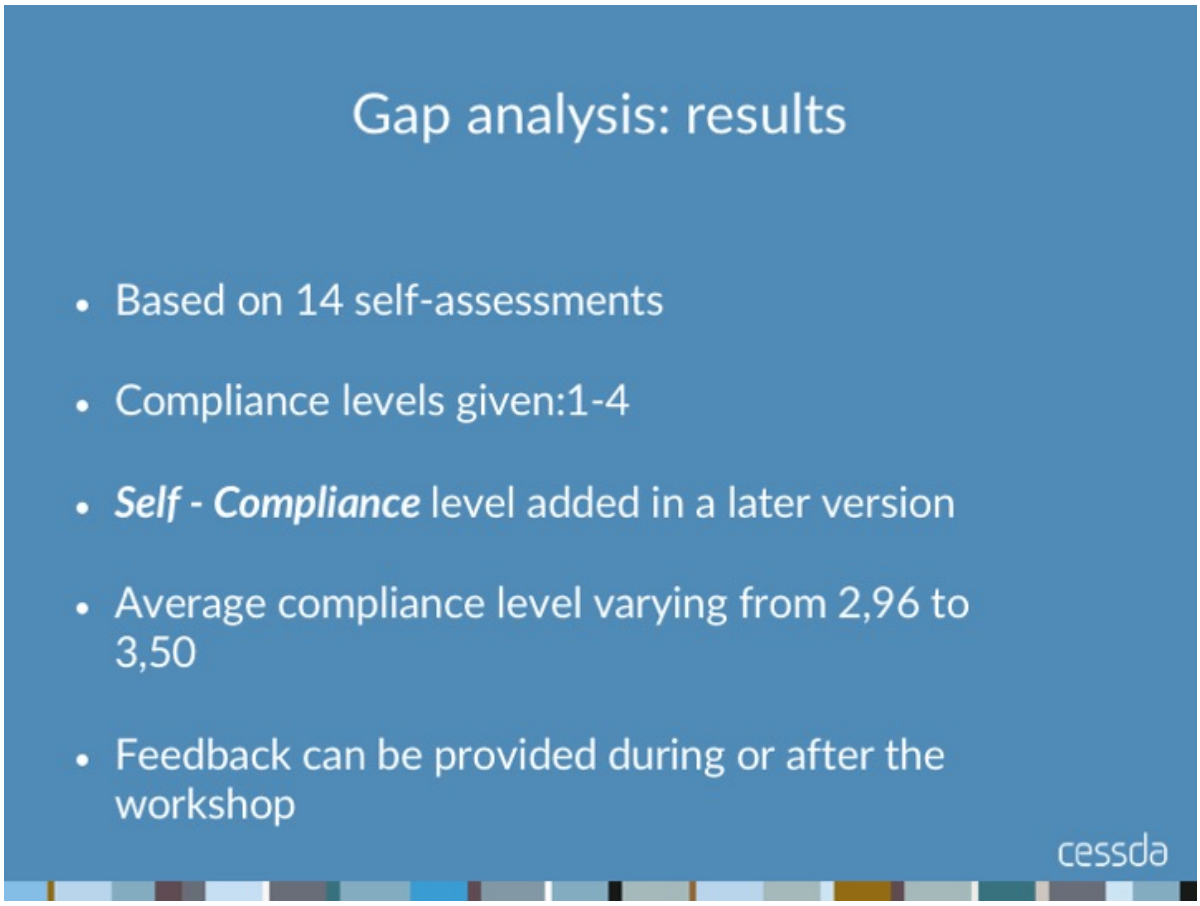
cessda

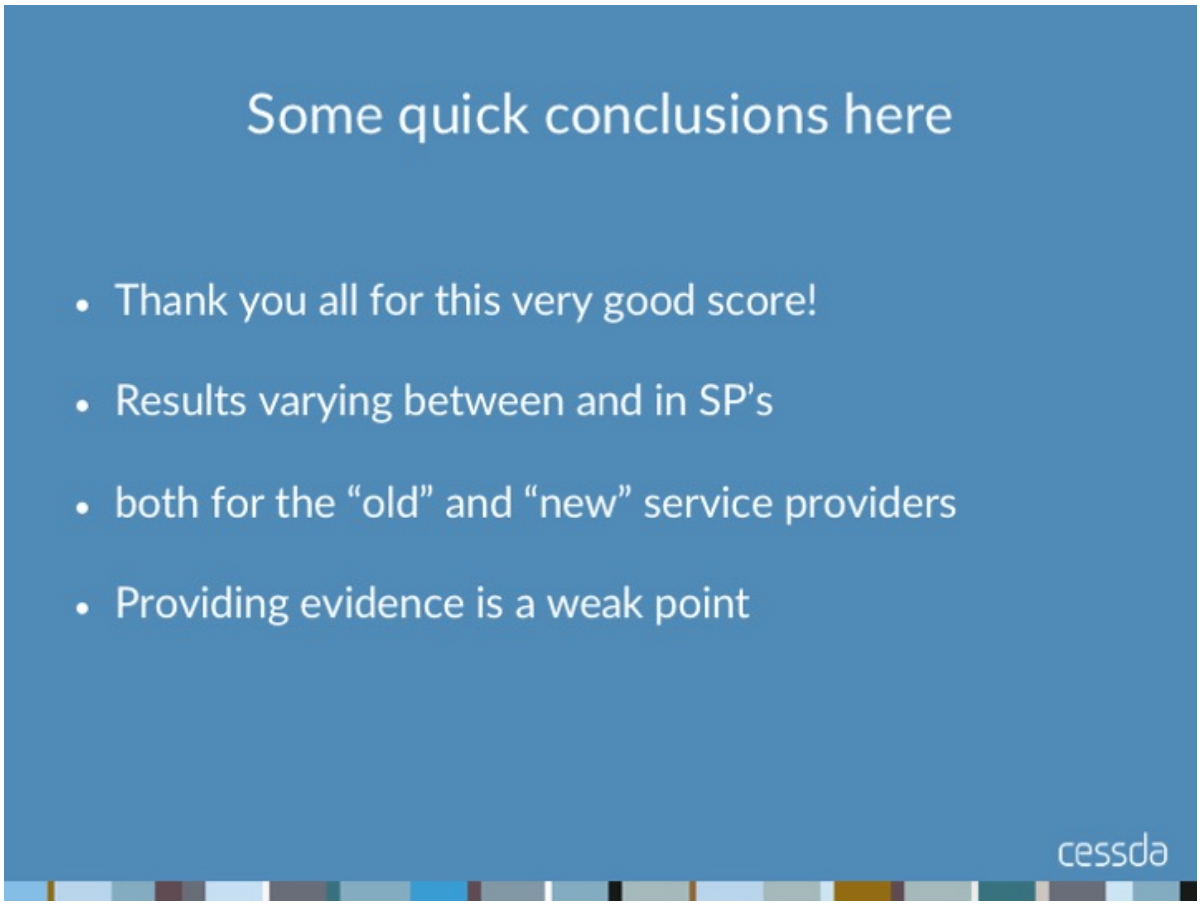

Three sessions on Trust in the workshop
• Wednesday 11.00 – 12.30 Session 1: Gap Analysis, Time table, Round tables on status and efforts
• Wednesday 14.00 – 15.30 Parallel Session 2: Requirements and comments, Round table on successes and challenges
• Thursday 9.00 – 10.30 Parallel Session 3: Ideal Evidence: start with 5 biggest challenges
cessda

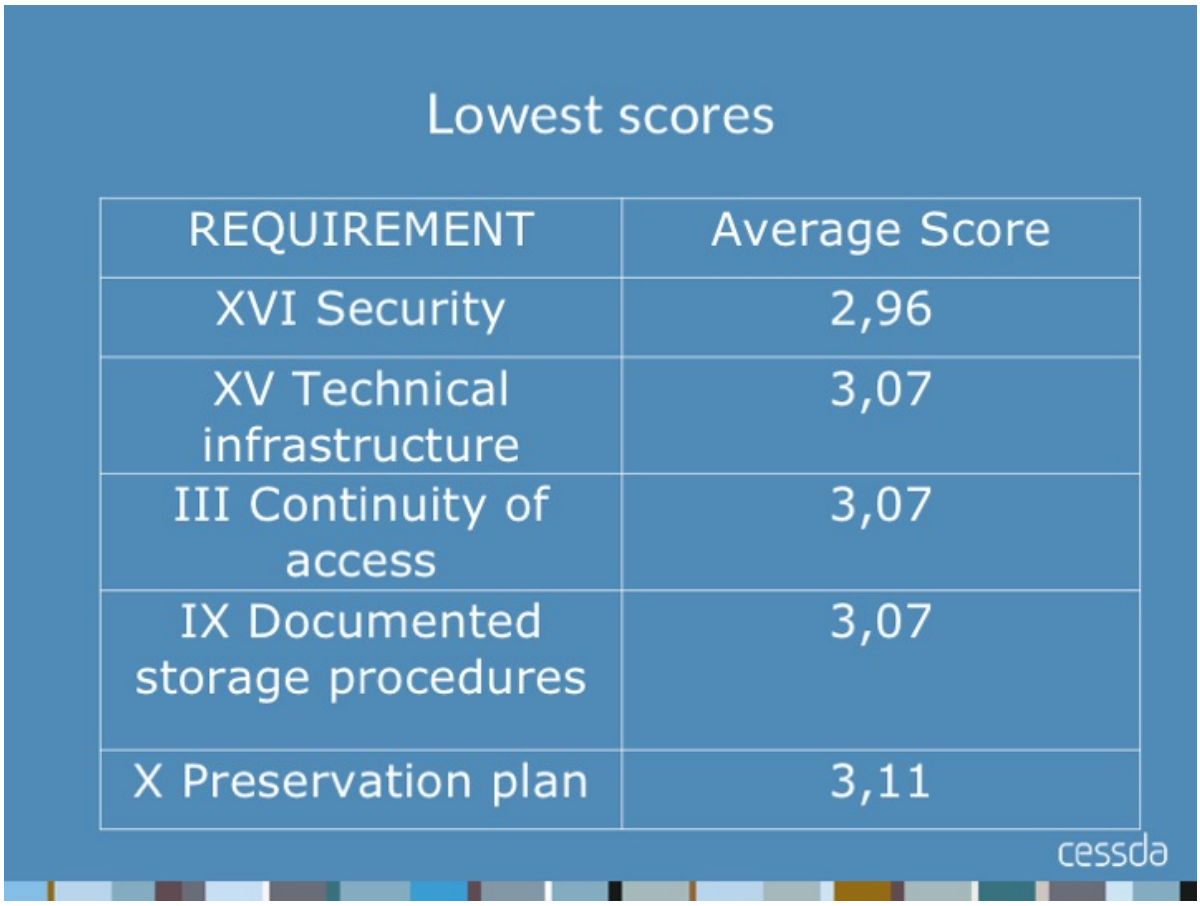

Session 1
Gap Analysis and other statistics
Timetables
Announcing one-to-one analysis
Roundtable A:
Status of drafts and submission plans
Roundtable B:
Effort, time and who you needed to talk to
Fill in analysis requests
cessda


The Trust Working Group is responsible for task 4.3 of the CESSDA SAW Project
• Task 4.3 Development Support: Achieving the Data Seal of Approval (by DANS, GESIS, UKDA, FSD, ADP) = Trust Working Group
cessda


Results so far
• 15 Self-Assessments have been sent in!
• Out of a total of 23 = more than 65%
• Reviewed by the 5 members of the CESSDA Trust Group
• Each self-assessment reviewed by two reviewers
• Compliance levels given:1-4
• Comments made
cessda

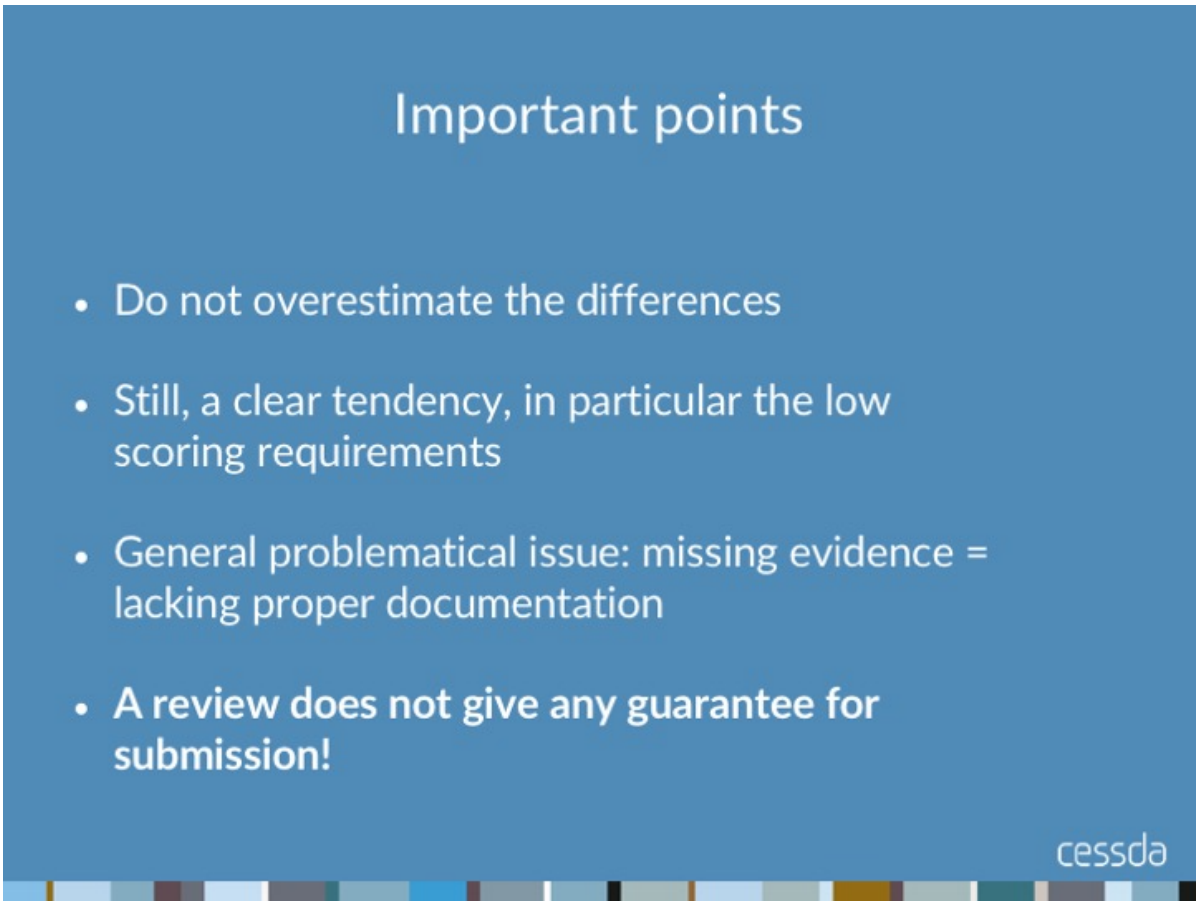

Gap analysis: results
Based on 14 self-assessments
Compliance levels given:1-4
Self - Compliance level added in a later version
Average compliance level varying from 2,96 to 3,50
Feedback can be provided during or after the workshop
cessda


Some quick conclusions here
• Thank you all for this very good score!
• Results varying between and in SP's
• both for the "old" and "new" service providers
• Providing evidence is a weak point
cessda


Lowest scores
REQUIREMENT
Average Score
XVI Security
2,96
XV Technical infrastructure
3,07
III Continuity of access
3,07
IX Documented storage procedures
3,07
X Preservation plan
3,11
cessda

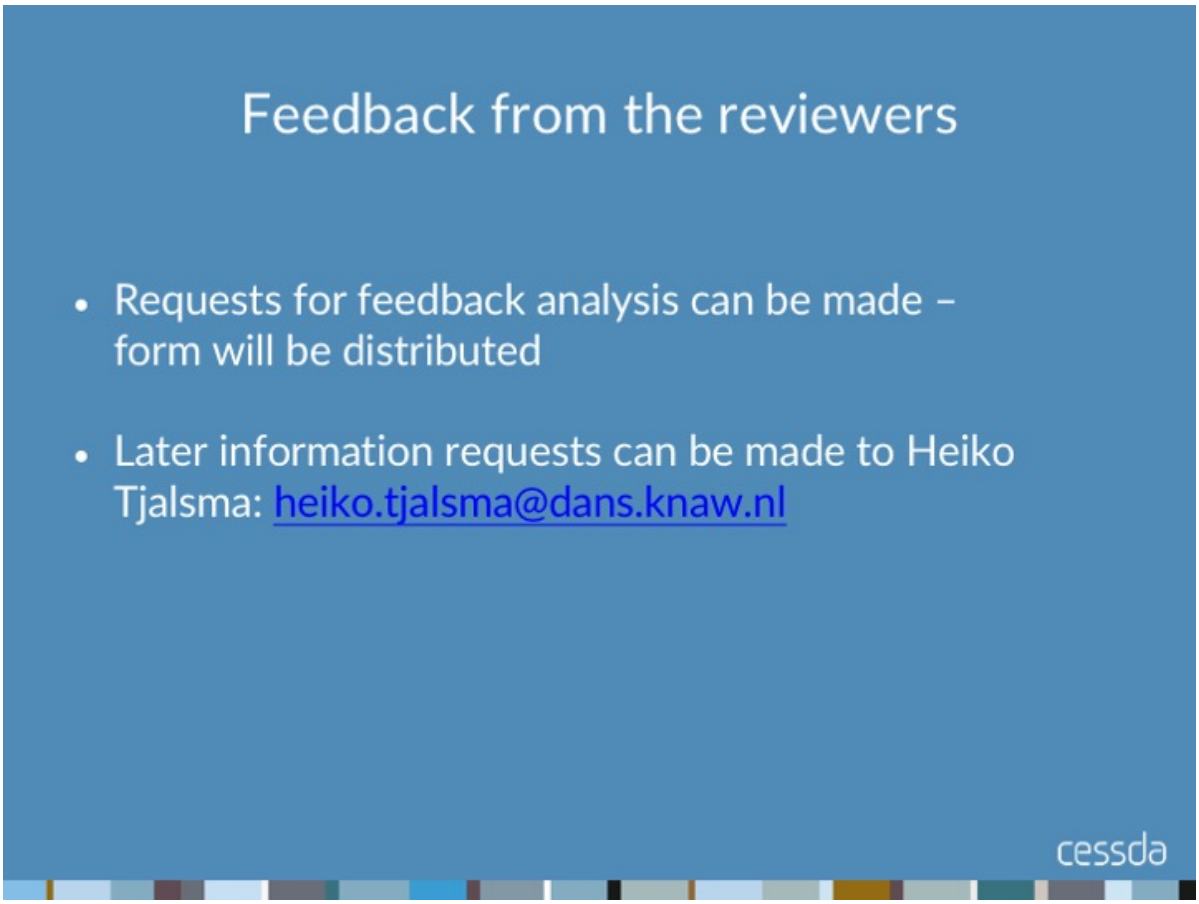

Lowest scores
XV. Technical infrastructure
• The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.
XVI. Security
• The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.
•III. Continuity of access
• The repository has a continuity plan to ensure ongoing access to and preservation of its holding
IX. Documented storage procedures
• The repository applies documented processes and procedures in managing archival storage of the data.
X. Preservation plan
• The repository assumes responsibility for longterm preservation and manages this function in a planned and documented way.
cessda

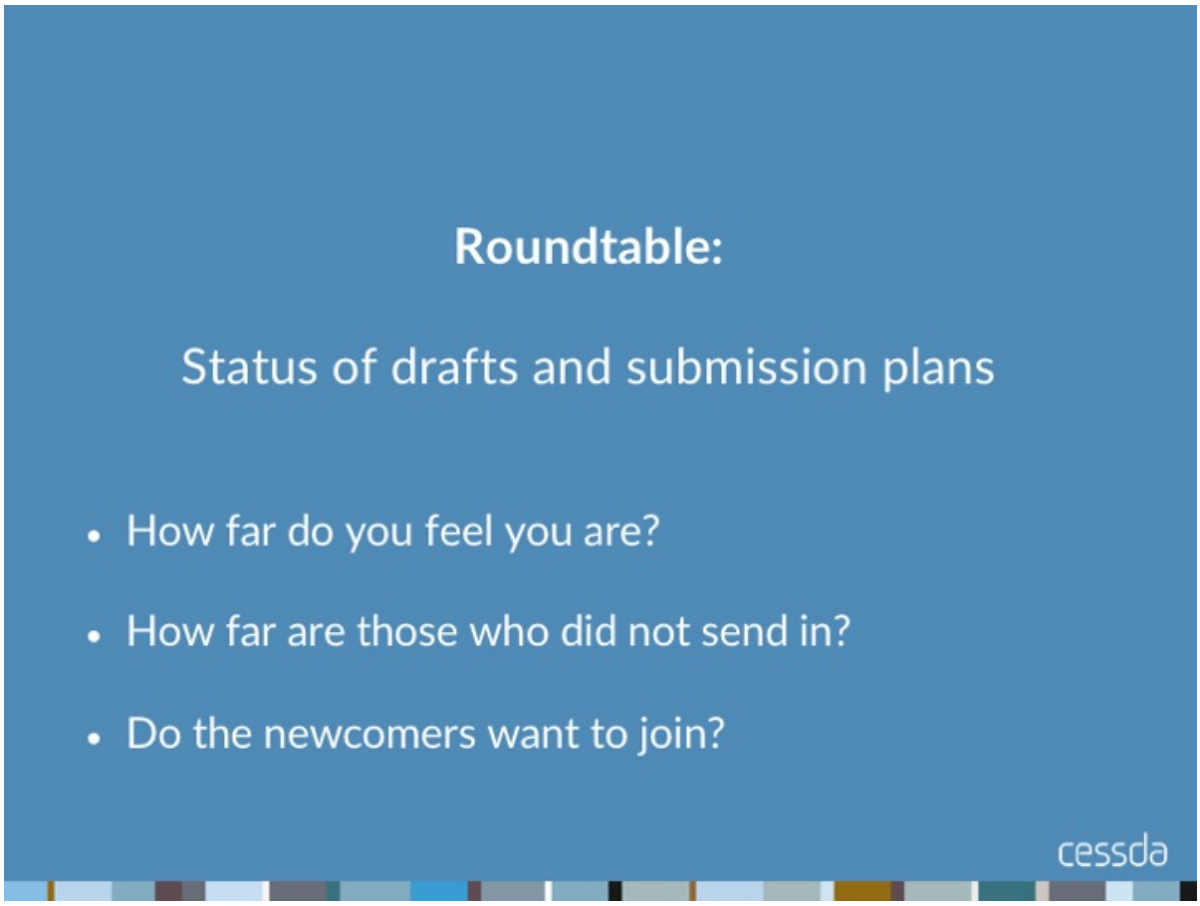

Highest scores
REQUIREMENT
Average Score
I Mission / Scope
3,50
XIV Data reuse
3,50
VI Expert guidance
3,48
IV Confidentiality / Ethics
3,46
cessda


Important points
• Do not overestimate the differences
• Still, a clear tendency, in particular the low scoring requirements
• General problematical issue: missing evidence = lacking proper documentation
• A review does not give any guarantee for submission!
cessda


• Time Schedule
Dates in 2017
Activity
13 January
Draft assessments internally submitted to the Trust Working Group
January – February
Review draft assesments
1-2 March
2nd SaW Workshop: evaluating and discussing the submitted assessments
March
Submitting assessments to DSA/WDS
June
Initial responses (accept or reject) from DSA/WDS
June - September
Re-submitting assessments
September
Final approval by DSA/WDS
October
End of SaW project
cessda


Vital date:
• March
• Submitting assessments to DSA/WDS
• September:
• Certification achieved
• If not:
• Explanation in Final Report
cessda


Feedback from the reviewers
• Requests for feedback analysis can be made – form will be distributed
• Later information requests can be made to Heiko Tjalsma: heiko.tjalsma@dans.knaw.nl
cessda


Roundtable:
Status of drafts and submission plans
• How far do you feel you are?
• How far are those who did not send in?
• Do the newcomers want to join?
cessda


cessda
—in your circle of trust.
website: www.cessda.net / twitter:
@CESSDA_Data