cessda eric
Consortium of European
Social Science Data Archives

SciDataCon 2018: The Digital Frontiers of Global Science, 5 - 8 November 2018, Gaborone (Botswana)
Session: *Improving Data Repository Trustworthiness*

TECHNICAL AND SECURITY ASPECTS of the CoreTrustSeal Application

Past work of the **CESSDA Trust Working Group*** has identified that technical and security infrastructure elements are a challenge for repositories undertaking self-assessments against the CoreTrustSeal perhaps because staff undertaking self-assessments are usually from the curation rather than the technical side of the organisation. The CoreTrustSeal addresses the issues of technical and security infrastructure through *Requirements 15* and *16*, however, technology and security aspects come into the picture throughout the 16 requirements.

0. BACKGROUND/CONTEXT

- *Definition of the designated community (their technical expertise implies type of data formats).*
- *Outsourcing (technical interoperability, SLAs, certificates)*

ORGANIZATIONAL INFRASTRUCTURE

I. Mission/Scope

- *Should cover people, processes, technology.*

II. Licenses

- *Types of access, e.g. based on data sensitivity (Authentication/Authorization. Safe room environments in place?)*

III. Continuity of Access

- *Business continuity of preservation and access functions (Question of technical handover).*

IV. Confidentiality/Ethics

- *Data with disclosure risk (Appropriate storage? Importance of documented procedures!).*

V. Organizational Infrastructure

- *Sufficient technical resources?*
- *Skilled and competent technical staff? Their ongoing training?*

VI. Expert Guidance

- *Access to objective technical expert advice beyond own skilled staff? How is keeping up with new technologies ensured?*

DIGITAL OBJECT MANAGEMENT

VII. Data Integrity and Authenticity

- *What data and metadata management system is in use? Who has access?*

VIII. Appraisal

- *Question of dealing with data deposited in non-preferred formats: Do you transform formats? With what software? How do you document changes to files and how do you preserve their significant properties?*

IX. Documented Storage Procedures

- *Documented processes and procedures, including levels of security, risk management techniques, checks of data files etc.*
- *How is the deterioration of storage media handled?*

X. Preservation Plan

- *Ensure that changes to data technology and user requirements are handled in a stable and timely manner.*

XI. Data Quality

- *Question of assessing big or complex data.*
- *Quality checks of documentation and metadata.*

XII. Workflows

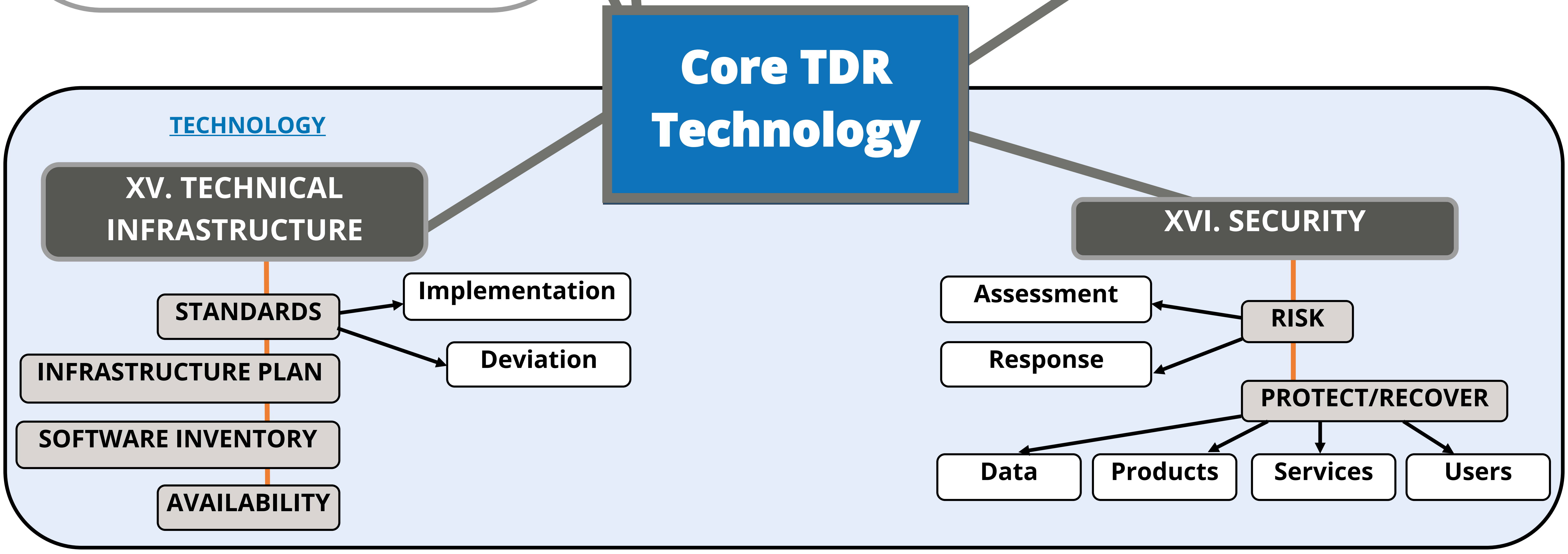
- *Levels of security at each step of the workflow + technical workflows.*

XIII. Data Discovery and Identification

- *Give advice on technical solutions to enhance usability.*
- *Technical aspects of data discovery and identification for man and machine.*
- *Extended searchability of the catalogue (elastic) + metadata harvesting.*

XIV. Data Reuse

- *Designated community uses technology that implies data formats for access.*


Core TDR Technology

TECHNOLOGY

XV. TECHNICAL INFRASTRUCTURE
STANDARDS
Implementation
Deviation
INFRASTRUCTURE PLAN
SOFTWARE INVENTORY
AVAILABILITY

XVI. SECURITY
RISK
Assessment
Response
PROTECT/RECOVER
Data
Products
Services
Users

* **CESSDA ERIC** provides large-scale, integrated and sustainable data services to the social sciences. Its key principle is that Service Providers must be trusted by each other and by their stakeholders. The **CESSDA Trust Working Group** supports this goal through supporting SP's towards certification against the CoreTrustSeal.

Authors: Maja DOLINAR (ADP), Birger JERLEHAG (SND), Hervé L'HOURS (UKDS),
Mari KLEEMOLA (FSD), Illona VON STEIN (DANS), Jonas RECKER (GESIS)
Contact: maja.dolinar@fdv.uni-lj.si