Certifikácia a audity v Centrálnom dátovom archíve

Centrálny dátový archív
Univerzitná knižnica v Bratislave
Mgr. Katarína Tomková

28. 11. 2018

cda.kultury.sk

www.opis.culture.gov.sk

OPIS je spolufinancovaný z ERDF

Centrálny dátový archív

OPIS je spolufinancovaný z ERDF

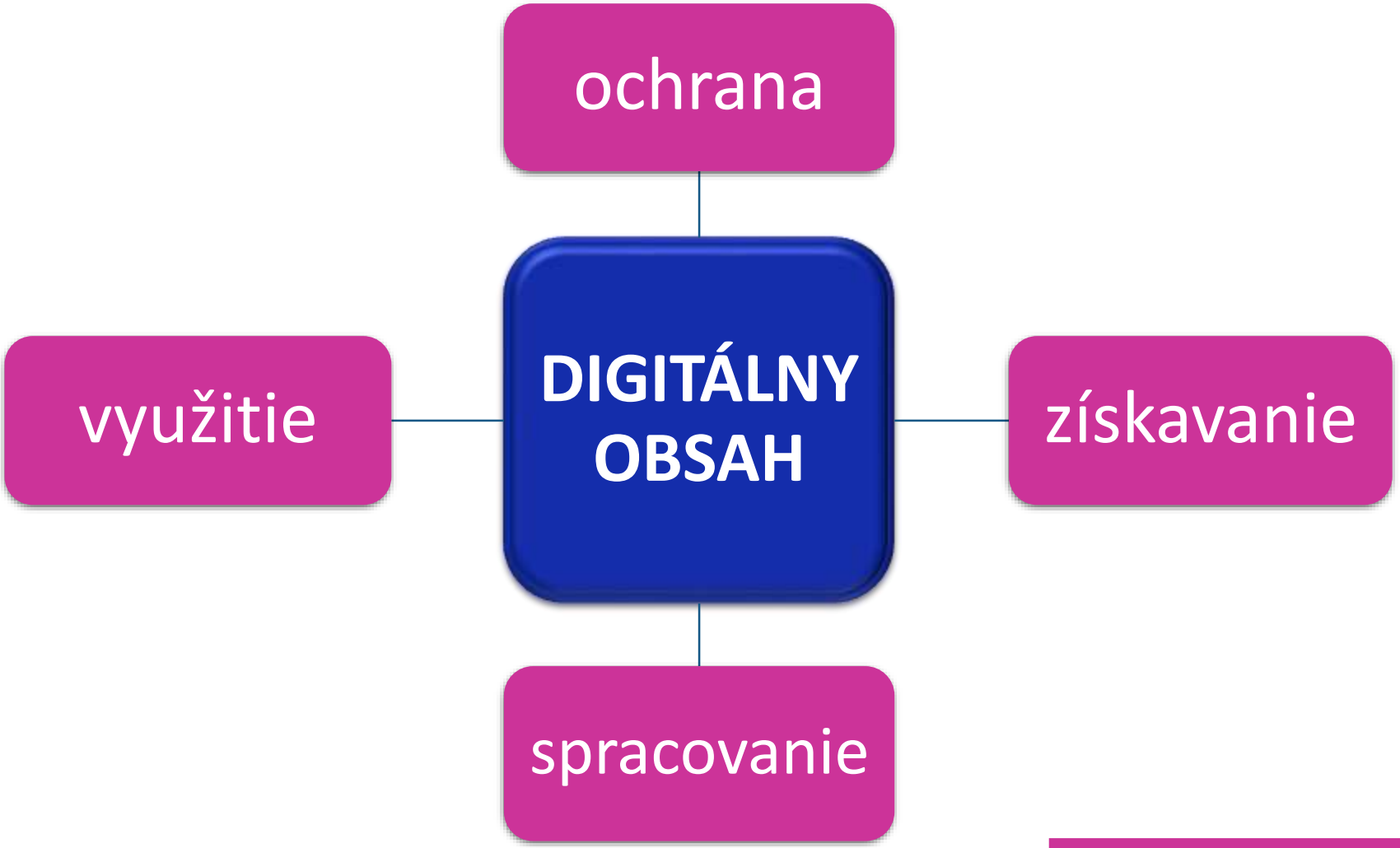
Projekt Ministerstva kultúry SR

Operačný program Informatizácia spoločnosti

LTP riešenie pre kultúrne dedičstvo na Slovensku

OPIS je spolufinancovaný z ERDF

www.opis.culture.gov.sk


ochrana
využitie
DIGITÁLNY OBSAH
získavanie
spracovanie

13.03.2012	• ERDF zmluva
31.05.2012	• realizácia zmluvy
09.07.2012	• technológia lokality B
26.09.2012	• prvý vklad
30.06.2014	• technológia lokality A
27.11.2014	• certifikácia SMIB ISO/IEC 27001:2013
31.12. 2014	• ukončenie projektu
01.01.2015 ~ 31.12.2019	• doba udržateľnosti

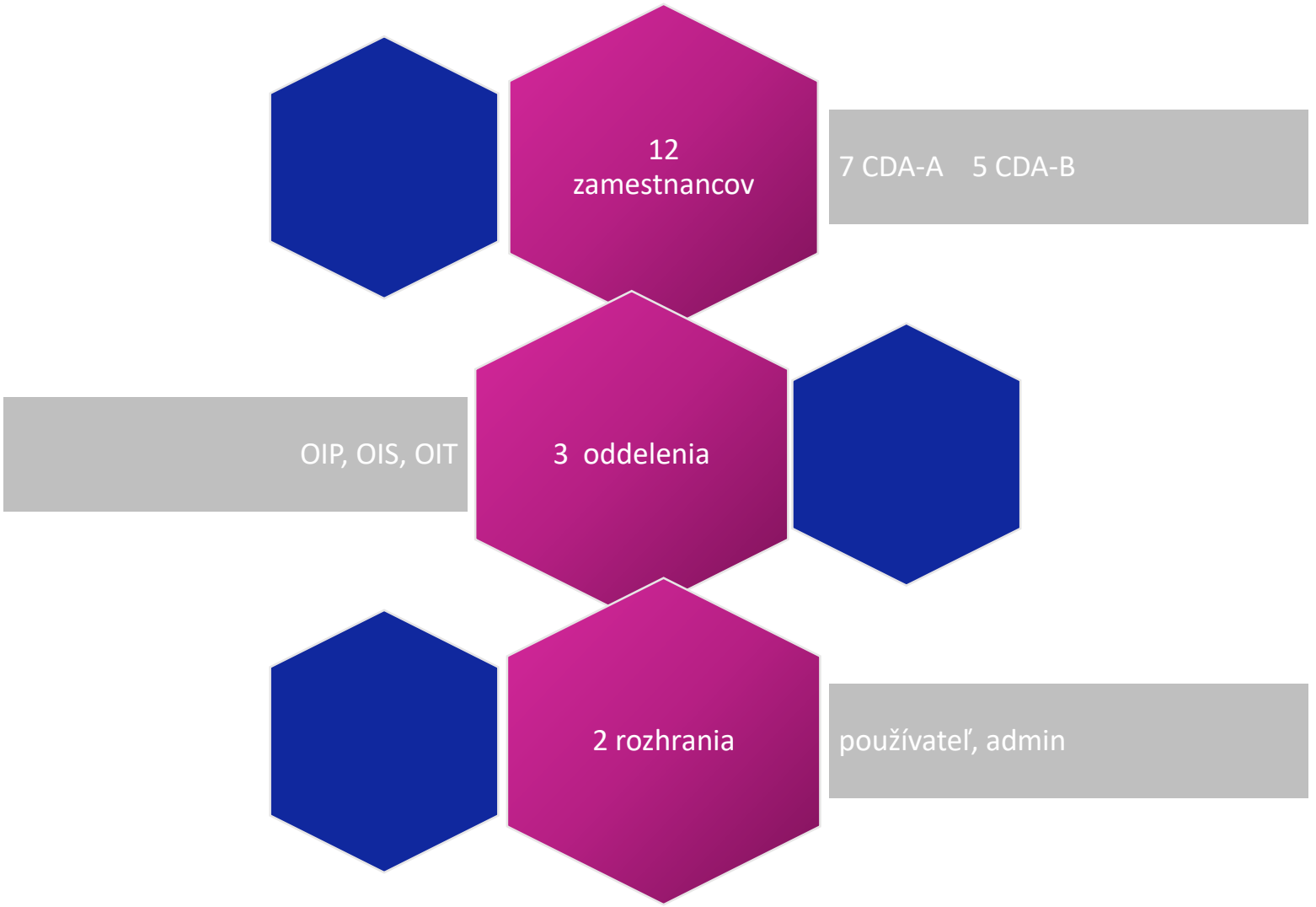
LOKALITY

- CDA-A
  - Dátové centrum
  - UKB
- CDA-B
  - Dátové centrum
  - SNK Martin
- CDA-C
  - trezor
  - UKB

OPIS je spolufinancovaný z ERDF


Total SIP
• 1 727 095
Total TB
• 4 360,8175
Kapacita:
25
PetaByte

Slovenská národná knižnica	•243 849 SIP	84 TB
Slovenský národný archív	•1 265 253 SIP	771 TB
Slovenská národná galéria	•10 184 SIP	14 TB
Pamiatkový úrad SR	•196 SIP	6 TB
Slovenský filmový ústav	•1 110 SIP	664 TB
Múzeum Slovenského národného povstania	•154 882 SIP	2 740 TB
Štátny geologický ústav Dionýza Štúra	•16 560 SIP	1 TB
Vojenský historický ústav	•20 783 SIP	0,3 TB
Slovenská knižnica pre nevidiacich Mateja Hrebendu v Levoči	•3 862 SIP	15 TB
Odbor digitalizácie UKB	•2 324 SIP	59 TB
Depozit digitálnych prameňov UKB	•4 895 SIP	0,5 TB
Štátna vedecká knižnica v Prešove	•0 SIP	0 TB
Národné osvetové centrum	•0 SIP	0 TB
Slovenský ľudový umelecký kolektív	•0 SIP	0 TB
Kancelária Ústavného súdu SR	•0 SIP	0 TB
Trnavský samosprávny kraj	•0 SIP	0 TB
Nitriansky samosprávny kraj	•0 SIP	0 TB



OPIS je spolufinancovaný z ERDF

dáta

vytvorenie balíčka

logistika (online/offline)

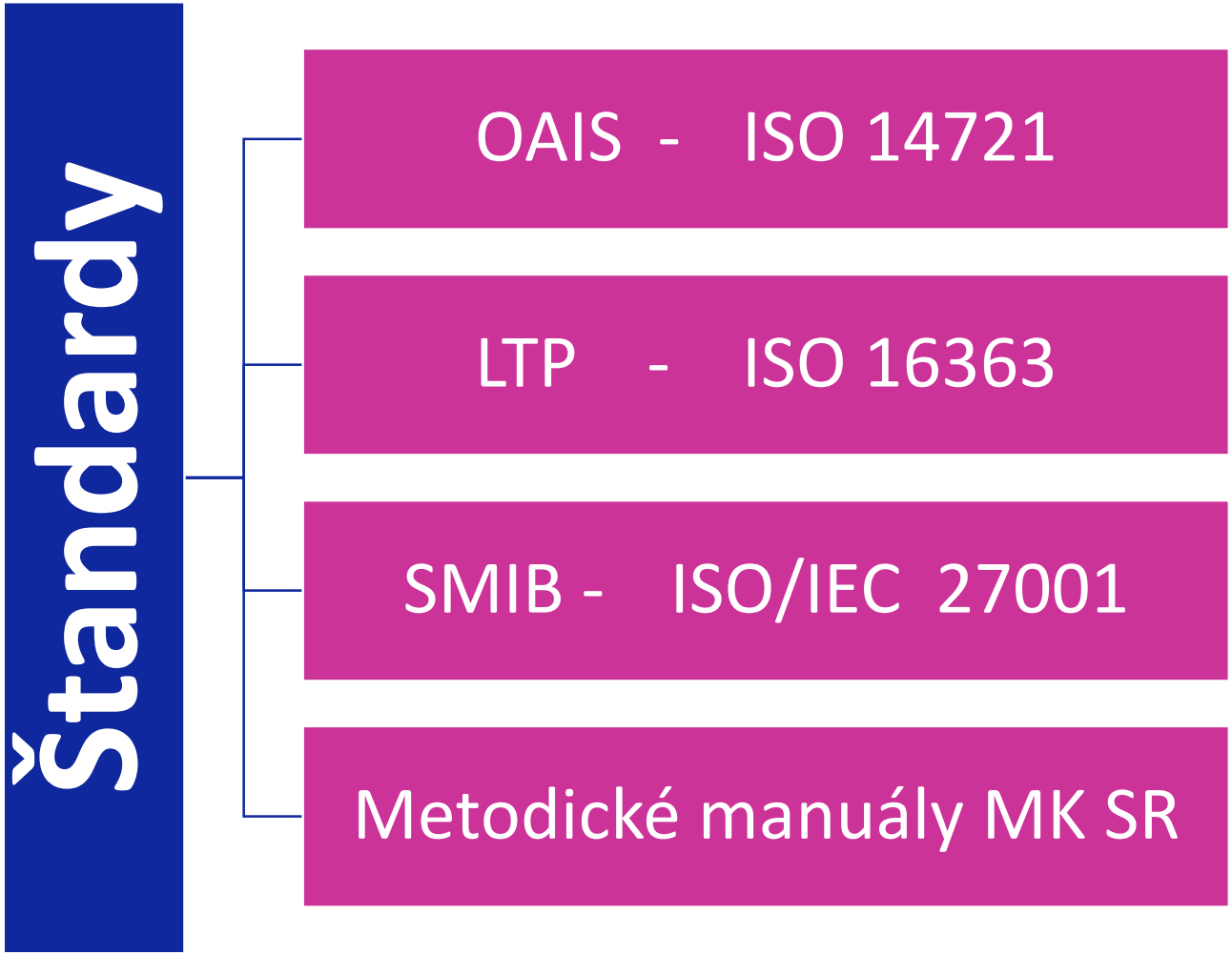
kontrola

uloženie

vytvorenie kópií

OPIS je spolufinancovaný z ERDF

www.opis.culture.gov.sk


Štandardy
OAIS - ISO 14721
LTP - ISO 16363
SMIB - ISO/IEC 27001
Metodické manuály MK SR

Certifikácia ISO 16363

(Space data and information transfer systems - Audit and certification of trustworthy digital repositories)

- certifikácia digitálnych repozitárov
- 2013 – preklad ISO normy do slovenčiny
- 2013 – začlenenie do systému slovenských technických noriem
- 2014 – interný audit Moravskou knižnicou

OPIS je spolufinancovaný z ERDF

www.opis.culture.gov.sk

Certifikácia ISO 27001

(SMIB systém manažérstva informačnej bezpečnosti)

- 2014 certifikačný audit
- 2015 dozorný audit
- 2016 dozorný audit
- 2017 recertifikačný audit

OPIS je spolufinancovaný z ERDF

Certifikácia ISO 27001

(SMIB systém manažérstva informačnej bezpečnosti)

dokumentácia	školenia	interný audit
plán obnovy	riziká	bezpečnostné incidenty
postupy	riadenie prístupov	aktíva

OPIS je spolufinancovaný z ERDF

Certifikácia ISO 27001

(SMIB systém manažérstva informačnej bezpečnosti)

13.-14.11.2018 - interný audit

12.12.2018 - dozorný audit

Certifikácia Data Seal of Approval

3 kroky

- sebahodnotenie cez online DSA web tool
- preskúmanie expertmi
- udelenie pečate DSA

platnosť 2 roky

Štruktúra

- 3 sekcie
- 16 požiadaviek
- + 2 ďalšie kritériá

Úrovne súladu (0 - neaplikovateľné -> 4 - plne implementované)

OPIS je spolufinancovaný z ERDF

www.opis.culture.gov.sk

Certifikácia Data Seal of Approval

A. Organizačná infraštruktúra

- úloha / rozsah
- licencie
- kontinuita prístupu
- dôvernosť / etika
- organizačná infraštruktúra
- odborné poradenstvo

B. Správa digitálnych objektov

- integrita a pravosť údajov
- posúdenie
- dokumentované postupy skladovania
- plán uchovávania
- kvalita údajov
- pracovné postupy
- zisťovanie a identifikácia údajov
- opätovné použitie údajov

C. Technológia

- technická infraštruktúra
- bezpečnosť

D. Dodatočné

- ďalšie informácie
- spätná väzba žiadateľa

OPIS je spolufinancovaný z ERDF

www.opis.culture.gov.sk

Certifikácia Core Trust Seal

- 2017 – príprava dokumentácie
- 2018 – zmena názvu na Core Trust Seal
- 2018 – zavedený poplatok 1 000 EUR
- 2018 – sebahodnotenie cez online DSA web tool
- 2018 – zaplatenie poplatku
- ...a teraz čakáme na vyjadrenie expertov

OPIS je spolufinancovaný z ERDF

ICSU
WORLD DATA SYSTEM

Core Trustworthy Data Repositories Requirements

Background & General Guidance

The Core Trustworthy Data Repositories Requirements are intended to reflect the characteristics of trustworthy repositories. As such, all Requirements are mandatory and are equally weighted, standalone items. Although some overlap is unavoidable, duplication of evidence sought among Requirements has been keep to a minimum where possible. The choices contained in checklists (e.g., repository type and curation level) are not considered to be comprehensive, and additional space is provided in all cases for the applicant to add 'other' (missing) options. This and any comments given may then be used to refine such lists in the future.

Each Requirement in the Catalogue is accompanied by guidance text to assist applicants in providing sufficient evidence that their repositories meet the Requirement, outlining the types of information that a reviewer will expect in order to perform an objective assessment. Furthermore, the applicant must indicate a compliance level for each of the Requirements:

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

Compliance levels provide a useful part of the self-assessment process, but all applicants will be judged against statements supported by appropriate evidence; not against self-assessed compliance levels. In this regard, if the applicant believes a Requirement is not applicable, the reason for this must be documented in detail. Note also that compliance levels 1 and 2 can be valid for internal self-assessments, while certification may be granted if some guidelines are considered to be at level 3—in the implementation phase—since the Requirements include an assumption of a repository's continuous improvement.

Reponses must be in English. Although attempts will be made to match reviewers to applicants in terms of language and discipline, this is not always possible. If evidence is in another language, an English summary must be provided in the self-assessment.

Because core certification does not involve a site visit, the Requirements should be supported by links to public evidence. Nevertheless, it is understood that for reasons such as security, it may not always possible to include all information on an organization's website, and provisions are made within the certification process for repositories who want sensitive parts of their evidence to remain confidential.

Repositories are required to be reassessed every three years. It is recognized that while basic systems and capabilities evolve continuously according to technology and user needs, they may not undergo major changes in this timeframe. However, the Trustworthy Repository ISO standard (ISO 16363) has a five-year review cycle, and a shorter period is considered necessary for a core trust standard to allow for possible modifications and corrections. Hence, an organization with well-managed records and business processes should reasonably expect to be able to submit an application with only minimal revisions after three years, unless the Requirements themselves have been updated within the intervening period.

Glossary of Terms

Please refer to the Core Trustworthy Data Repositories Requirements Glossary: https://goo.gl/rQK5RN.

Organizational Infrastructure

I. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:

Response

Guidance:
Repositories take responsibility for stewardship of digital objects, and to ensure that materials are held in the appropriate environment for appropriate periods of time. Depositors and users must be clear that preservation of, and continued access to, the data is an explicit role of the repository.

For this Requirement, please describe:

- Your organization's mission in preserving and providing access to data, and include links to explicit statements of this mission.
- The level of approval within the organization that such a mission statement has received (e.g., approved public statement, roles mandated by funders, policy statement signed off by governing board).

II. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:

Response

Guidance:
Repositories must maintain all applicable licenses covering data access and use, communicate about them with users, and monitor compliance. This Requirement relates to the access regulations and applicable licenses set by the data repository itself, as well as any codes of conduct that are generally accepted in the relevant sector for the exchange and proper use of knowledge and information. Reviewers will be seeking evidence that the repository has sufficient controls in place according to the access criteria of their data holdings, as well as evidence that any relevant licences or processes are well managed.

For this Requirement, please describe:

- License agreements in use.
- Conditions of use (distribution, intended use, protection of sensitive data, etc.).
- Documentation on measures in the case of noncompliance with conditions of access and use.

Note that if all data holdings are completely public and without conditions imposed on users—such as attribution requirements or agreement to make secondary analysis openly available—then it can simply be stated.

This Requirement must be read in conjunction with R4 (Confidentiality/Ethics) to the extent that ethical and privacy provisions impact on the licenses. Assurance that deposit licences provide sufficient rights for the repository to maintain, preserve, and offer access to data is covered under R10 (Preservation Plan).

Please refer to the Core Trustworthy Data Repositories Requirements Glossary: https://goo.gl/rQK5RN.

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type. Select all relevant types from:

☐ Domain or subject-based repository ☐ Institutional repository ☑ National repository system; including governmental
☐ Publication repository ☑ Library/Museum/Archives ☐ Research project repository ☐ Other (Please describe below)

Brief Description of Repository

The Central Data Archive (CDA) is the long-term preservation (LTP) repository for cultural heritage in Slovakia.
In 2011, the University Library in Bratislava was charged with setting up a powerful infrastructure for the long-term preservation of digitized cultural heritage across „the national memory" institutions. The CDA project is realised in the framework of the Operational Programme Informatisation of Society (OPIS), prevailingly financed by the European Regional Development Fund (ERDF).
Upon the priority axis "Development and renewal of the national infrastructure of repository institutions" is realised a set of specific digitisation projects: Digital Museum, Digital Gallery, Digital Library and Digital Archive, Digital Audio Vision and Digital

Brief Description of the Repository's Designated Community.

- DP08: Digital Fund of the Industrial Property Office (Industrial Property Office)
- DP09: The most important historical and artistic monuments of PSK (Trnava Regional Office)

The membership of the designated community is based on a written contract between CDA and the data producers/owners: The Agreement of entrustment of content for long-term preservation. The CDA staff provides for the designated community all necessary support and communication both via the repository website [cda.kultury.sk] and the helpdesk.

Level of Curation Performed. Select all relevant types from:

☐ A. Content distributed as deposited ☐ B. Basic curation – e.g. brief checking; addition of basic metadata or documentation
☐ C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation
☐ D. Data-level curation – as in C above; but with additional editing of deposited data for accuracy

Comments

Outsource Partners. If applicable, please list them.

• Any global cluster or network organization that the repository belongs to.

ORGANIZATIONAL INFRASTRUCTURE

I. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:
No value

Response:

Guidance:

Repositories take responsibility for stewardship of digital objects, and to ensure that materials are held in the appropriate environment for appropriate periods of time. Depositors and users must be clear that preservation of, and continued access to, the data is an explicit role of the repository.

For this Requirement, please describe:

• Your organization's mission in preserving and providing access to data, and include links to explicit statements of this mission.

• The level of approval within the organization that such a mission statement has received (e.g., approved public statement, roles mandated by funders, policy statement signed off by governing board).

II. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:
No value

Response:

---

taken to counter the threats to the repository and its Designated Community. This should be an ongoing process.

For this Requirement, please describe:

• Procedures and arrangements in place to provide swift recovery or backup of essential services in the event of an outage.

• Your IT security system, disaster plan, and business continuity plan; employees with roles related to security (e.g., security officers); and any risk analysis tools (e.g., DRAMBORA) you use.

This Requirement describes some of the aspects generally covered by others—for example, R12 (Workflows)—and is supplementary to R9 (Documented storage procedures).

APPLICANT FEEDBACK

Comments/feedback

These requirements are not seen as final, and we value your input to improve the core 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.

Response:

Thank you very much for completing the application form for CoreTrustSeal Data Repository certification. If you have any additional comments or documents that you would like to share with the CoreTrustSeal Board/Secretariat or the Reviewers, please add them below.

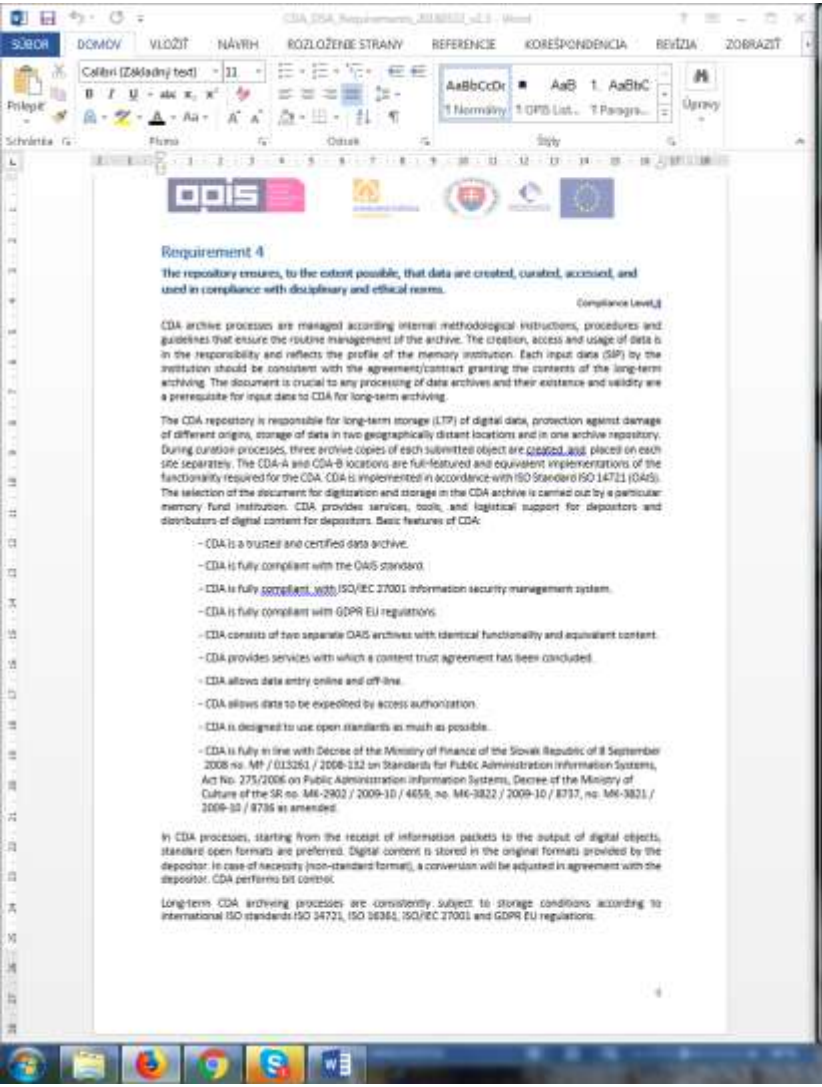
Comment

Attachment File

Prehľadávať... Nie je zvolený súbor.

Comments

Save as Draft | Request Feedback | Submit for Review | Cancel



Requirement 4

The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

Compliance Level:3

CDA archive processes are managed according internal methodological instructions, procedures and guidelines that ensure the routine management of the archive. The creation, access and usage of data is in the responsibility and reflects the profile of the memory institution. Each input data (SIP) by the institution should be consistent with the agreement/contract granting the contents of the long-term archiving. The document is crucial to any processing of data archives and their existence and validity are a prerequisite for input data to CDA for long-term archiving.

The CDA repository is responsible for long-term storage (LTP) of digital data, protection against damage of different origins, storage of data in two geographically distant locations and in one archive repository. During curation processes, three archive copies of each submitted object are created and placed on each site separately. The CDA-A and CDA-B locations are full-featured and equivalent implementations of the functionality required for the CDA. CDA is implemented in accordance with ISO Standard ISO 14721 (OAIS). The selection of the document for digitization and storage in the CDA archive is carried out by a particular memory fund institution. CDA provides services, tools, and logistical support for depositors and distributors of digital content for depositors. Basic features of CDA:

- CDA is a trusted and certified data archive.
- CDA is fully compliant with the OAIS standard.
- CDA is fully compliant with ISO/IEC 27001 information security management system.
- CDA is fully compliant with GDPR EU regulations.
- CDA consists of two separate OAIS archives with identical functionality and equivalent content.
- CDA provides services with which a content trust agreement has been concluded.
- CDA allows data entry online and off-line.
- CDA allows data to be expedited by access authorization.
- CDA is designed to use open standards as much as possible.
- CDA is fully in line with Decree of the Ministry of Finance of the Slovak Republic of 8 September 2008 no. MF / 013261 / 2008-132 on Standards for Public Administration Information Systems, Act No. 275/2006 on Public Administration Information Systems, Decree of the Ministry of Culture of the SR no. MK-2902 / 2009-10 / 4659, no. MK-3822 / 2009-10 / 8737, no. MK-3821 / 2009-10 / 8736 as amended.

In CDA processes, starting from the receipt of information packets to the output of digital objects, standard open formats are preferred. Digital content is stored in the original formats provided by the depositor. In case of necessity (non-standard format), a conversion will be adjusted in agreement with the depositor. CDA performs bit control.

Long-term CDA archiving processes are consistently subject to storage conditions according to international ISO standards ISO 14721, ISO 16363, ISO/IEC 27001 and GDPR EU regulations.

infrastructure) and R19 (Security) in that it covers full business continuity of the preservation and access functions.

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.

Compliance Level:

No value

Response:

Guidance:

Adherence to ethical norms is critical to responsible science. Disclosure risk—for example, the risk that an individual who participated in a survey can be identified or that the precise location of an endangered species can be pinpointed—is a concern that many repositories must address. Evidence sought is concerned with not only having good practices for data with disclosure risks, but also the necessity to maintain the trust of those agreeing to have personal/sensitive data stored in the repository.

For this Requirement, responses should include evidence related to the following questions:

- How does the repository comply with applicable disciplinary norms?
- Does the repository request confirmation that data collection or creation was carried out in accordance with legal and ethical criteria prevailing in the data producer's geographical location or discipline (e.g., Ethical Review Committee/Institutional Review Board or Data Protection legislation)?
- Are special procedures applied to manage data with disclosure risk?
- Are data with disclosure risk stored appropriately to limit access?
- Are data with disclosure risk distributed under appropriate conditions?
- Are procedures in place to review disclosure risk in data, and to take the necessary steps to either anonymize files or to provide access in a secure way?
- Are staff trained in the management of data with disclosure risk?
- Are there measures in place if conditions are not complied with?
- Does the repository provide guidance in the responsible use of disclosive, or potentially disclosive data?

Evidence for this Requirement should be in alignment with provisions for the procedures stated in R12 (Workflows) and for any licenses in R2 (Licences).

cda.kultury.sk

Ďakujem Vám za pozornosť!

Centrálny dátový archív
Univerzitná knižnica v Bratislave
Mgr. Katarína Tomková

katarina.tomkova@ulib.sk

www.opis.culture.gov.sk

OPIS je spolufinancovaný z ERDF