Verification 4 Systems Ltd.

Certifikace digitálních repositářů
ISO 16363

Obsah

- Přestavení Verification 4 Systems Ltd.
- Standard ISO 16363
- Prolnutí s ostatními standardy
- Požadavky a průběh certifikace

Představení V4S

Mateřská společnost

Verification 4 Systems Ltd.

- Sídlo: 2 Tintagel Close, Rushden, Northants NN10 0QN, United Kingdom
- ID: 6998348

Pobočka v ČR

Verification 4 Systems Ltd., Czech Republic branch, organizační složka

- Sídlo: Kosmova 665/10, Ostrava 70200, Czech Republic
- IČ: 29393311

Profil

Služby ve třech základních oblastech:

- Certifikace systémů managementu
  - primární zaměření na ISMS, IT procesy, QMS
- Audity (interní, SW, penetrační testování, ochrana dat)
- Školení v oblasti systémů řízení, ITIL, ISMS a další

Auditoři:

- Disponujeme 15+ auditory s mezinárodními certifikacemi, např.:

  CISA, IRCA, RABQSA, IQNET, BSA-QA, VDA QMC a další
- Požadavky PTAB

Standardy a služby

- ISO 9001 - Quality Management Systems (QMS)
- ISO 20000-1 - IT Service Management (ITSM/ITIL)
- ISO 27001 - Information Security Management System (ISMS)
- ISO 16363 – Trustworthy digital repositories (TDR)
- ISO 15489 – Information & Records Management (Správa informací a záznamů IRMS)
- ISO 22301 - Business Continuity Management (BCM)
- ISO 21500 - Quality Management Systems – Project Management (PM)
- ISO 14001 - Environmental Management Systems (EMS)
- ISO 16949 - Quality Management Systems: Automotive industry
- ISO 18001 - Occupational Health & Safety Advisory Systems (OHSAS)
- SA 8000 - Social Accountability Standard (CSR)
- ISO 13485 - Quality Management Systems – Medical Devices

Digitální repositáře a Standard ISO 16363

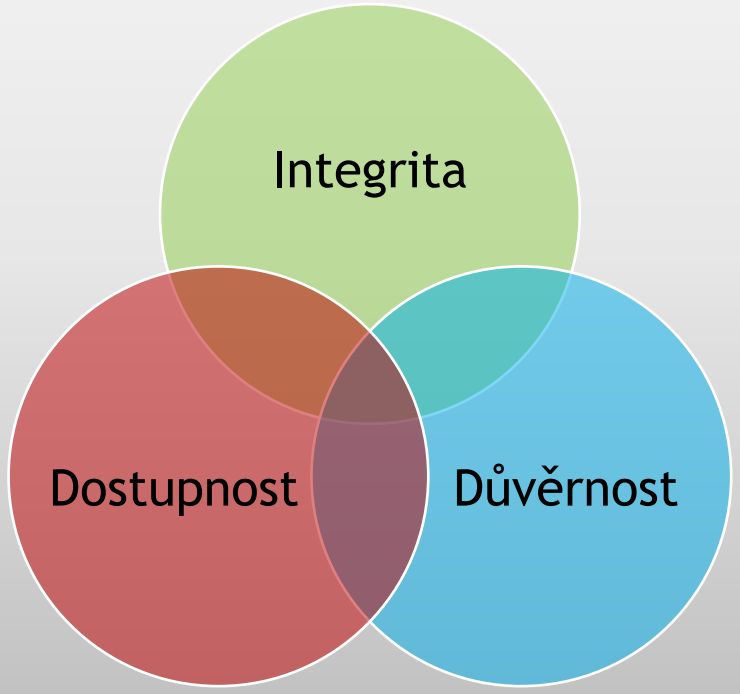
ISO 16363 je mezinárodní norma zaměřená na zajištění důvěryhodnosti digitálních repozitářů.

- Jednotné požadavky pro digitální uložiště k zajištění důvěryhodnosti
- V rámci repozitáře se počítá s tím, že informace v něm budou uloženy velmi dlouho
- Musí být zaručena dlouhodobá použitelnost a přístupnost informací/dat uživatelům

Digitální repositáře a Standard ISO 16363

Dlouhodobá použitelnost informací

- Využívá se principů ISO 27001
- Zajištění dostupnosti, důvěrnosti a integrity aktiv
- ISO 27001 je podmínkou pro fungování ISO 16363
- Před implementací TDR je vhodné splnit podmínky fungování systému dle ISO/IEC 27001

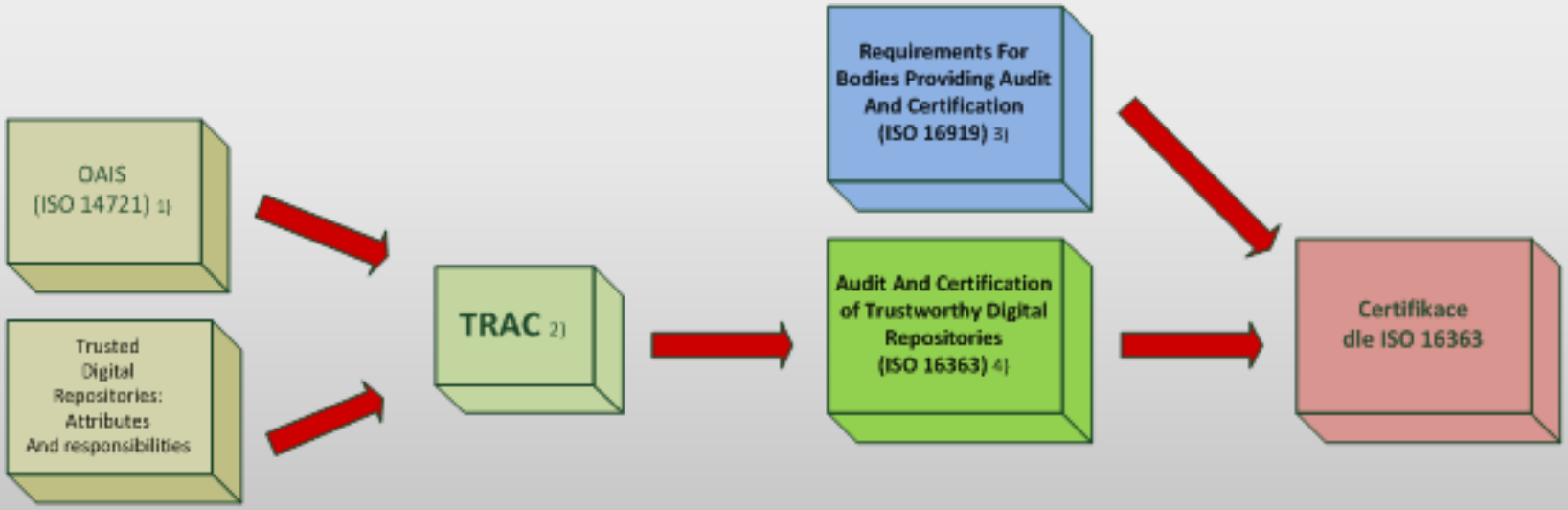


Standard ISO 16363

Původ standardu

- Norma ISO 16363 byla vydána na začátku roku 2012
- vychází z Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist z roku 2007.
- Vytvořena sdružením The Primary Trustworthy Digital Repository Authorisation Body (PTAB).
- Jednotné požadavky pro zajištění důvěry digitálních repositářů

Cesta k ISO 16363



Požadavky ISO 16363

požadavky jsou uvedeny v mezinárodní normě ISO 16363:2011 a rozepsány do jednotlivých kapitol:

- Organizační infrastuktura – důraz na vlastnosti prostředí (organizace)
- Management digitálních objektů – zajištěno vlastnostmi LTP, ale i vnitřními normami
- Infrastruktura a řízení rizik

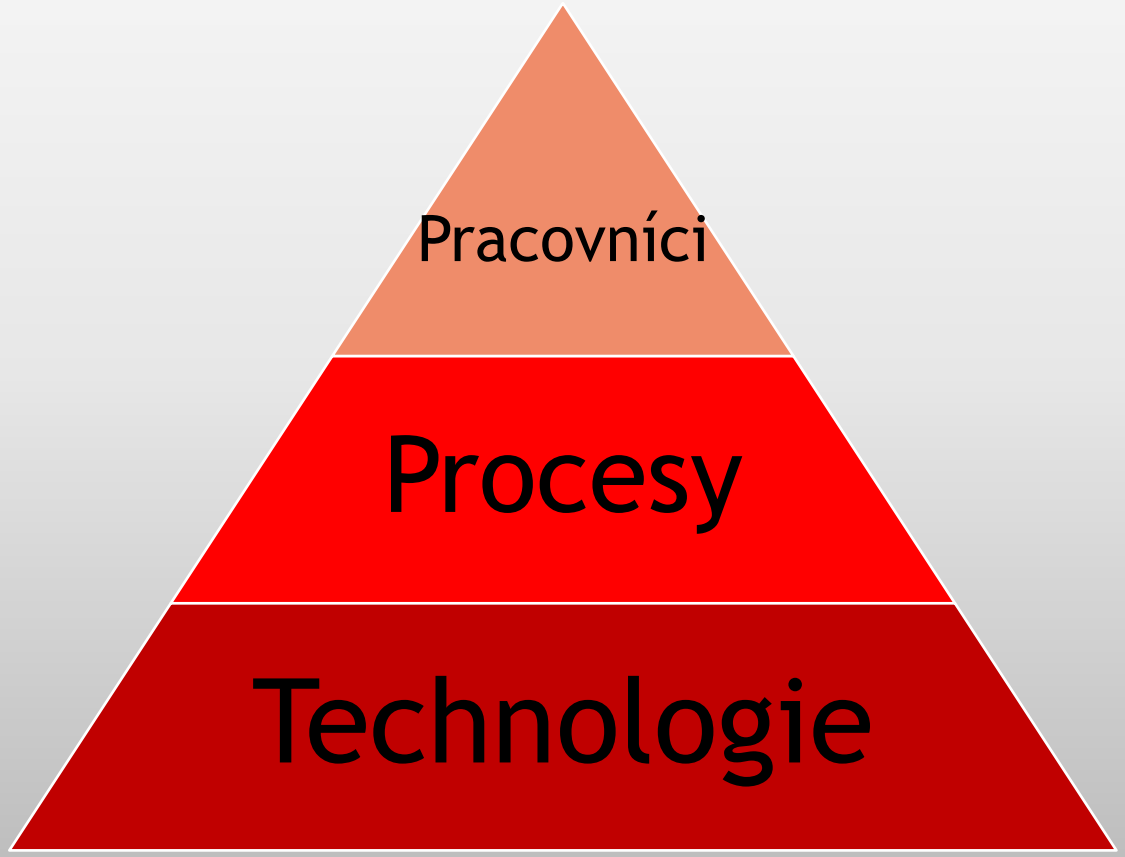
V jednotlivých kapitolách jsou vedeny požadavky tak, aby bylo krom požadavku podáno vysvětlení a návrh jak tento požadavek uplatnit.

Požadavek → Vysvětlení → Návrh uplatnění požadavku

Princip fungování

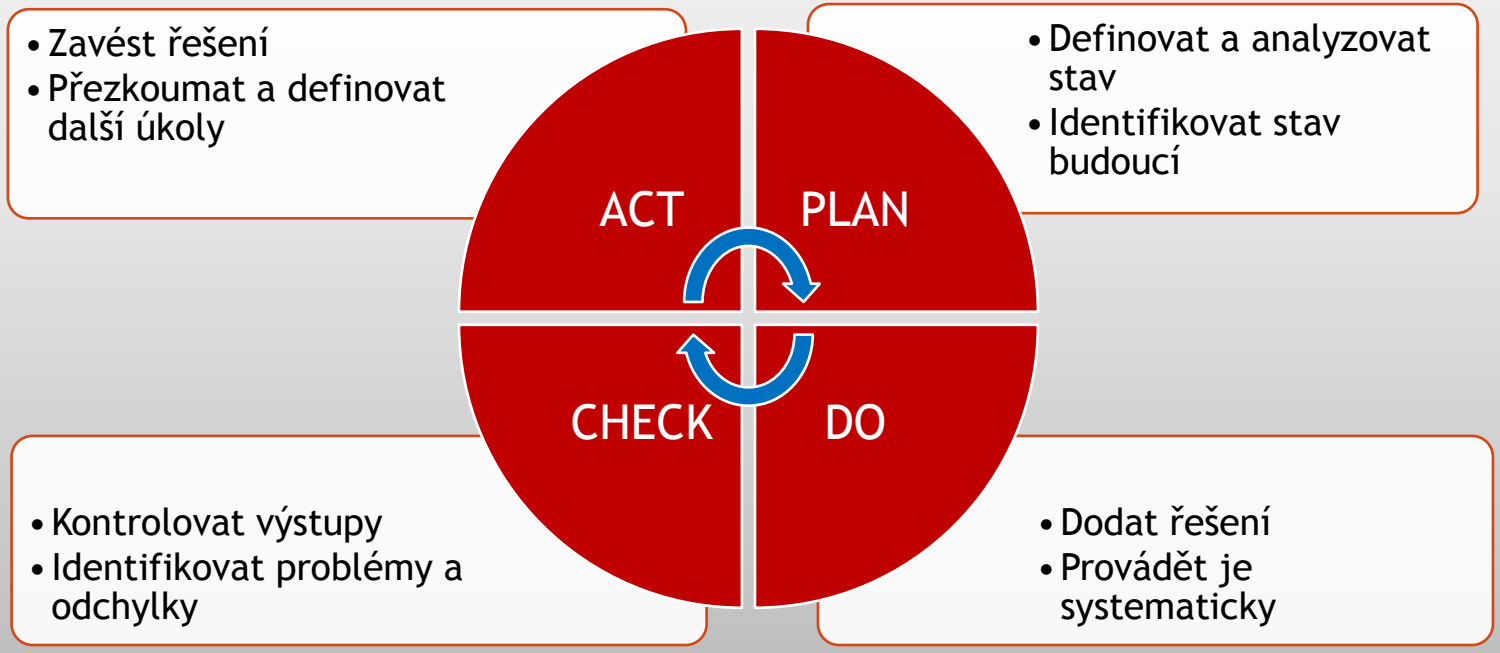
Zajištění fungování:

- Propojenost technologické a lidské stránky systému
- Nastavené komunikační cesty
- Nastavené procesy – IT best practices



Princip fungování

Důležité informace pro fungování a zlepšování z PDCA cyklu:



Přínosy certifikace ISO 16363

- Certifikace slouží jako důkaz o schopnostech depozitáře plnit podmínky na důvěryhodné digitální uložiště
- Implementací a následnou certifikací dle ISO 16363 dávám důkaz o schopnostech uchovávat data dle mezinárodních standardů a v souladu s legislativou EU
- Pro splnění podmínek ISO 16363 je nezbytné splnit nejdříve podmínky pro všeobecnou bezpečnost, nejlépe dle ISO 27001

Kdo provádí certifikaci

- Certifikace ISO 16363 provádí nezávislý certifikační orgán, tedy je to certifikace třetí stranou
- CO splňuje požadavky ISO 16919
- Auditoři provádějící tyto audity jsou akreditování a školení s pomocí sdružení The Primary Trustworthy Digital Repository Authorisation Body (PTAB).
- Auditoři splňují kvalifikační kritéria dle dokumentu „RED BOOK"

Příbuzné standardy

Normy, které souvisí s ISO 16363, sdílejí principy a doplňují se:

- Normy řady ISO 9000 – systém managementu kvality v organizacích
- Normy ISO 17799 a ISO 27001 – systémy informační bezpečnosti v organizacích
- Norma ISO 14721 (OIAS)– popisuje požadavky na systém pro archivaci informací

Předpoklady certifikace ISO 16363

- Funkční systém řízení bezpečnosti informací dle ISO 27001 (systémový požadavek)

✓ Zavedený

✓ Certifikovaný (doporučení)

✓ Min. 1 rok fungování (doporučení)

- Splnění požadavků ISO 16363

✓ Splněné prvky (požadavků) normy

✓ Fungující systém TDR

✓ Self-audit celého systému (ISMS+TDR)

Standard ISO/IEC 27001

- definuje požadavky ISMS, především pak řízení bezpečnosti a důvěry informací pro zaměstnance, procesy
- zaměření na organizační, technologické, personální a systémové
- je plně slučitelný s již zavedenými systémy managementu

Přínosy ISMS

- zvládání rizik spojených s hrozbami, které jsou identifikovány v procesech a okolním prostředí společnosti
- systémový přístup k managementu rizik, neustálé zlepšování
- prokázání důvěryhodnosti vůči externím partnerům

Požadavky ISO 27001

- Identifikace aktiv
- Identifikace rizik
- Plán řízení rizik
- Snižování hodnoty rizik
- Interní audity ISMS
- Zlepšování systému

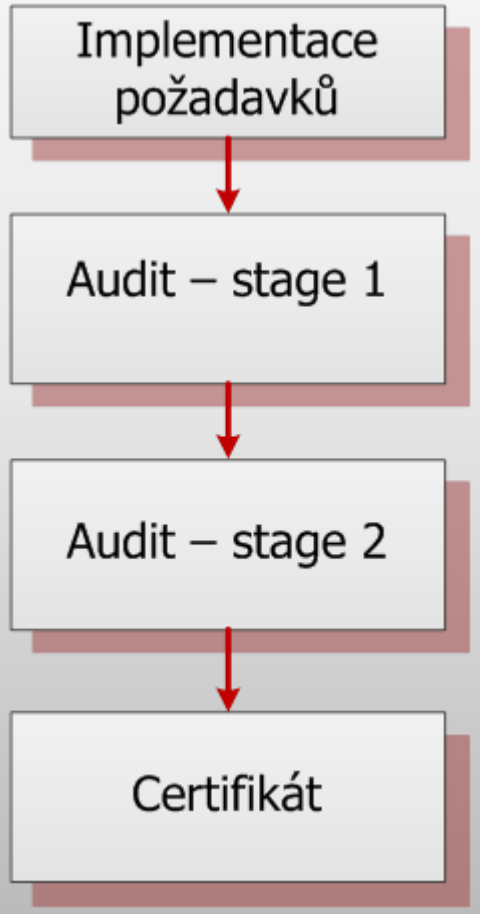
Symbioza ISO 27001 + ISO 16363

- ISMS jako podklad pro implementaci ISO 16363
- ISMS dle ISO 27001 připraví prostředí z hlediska splnění minimálních požadavků na bezpečnost informací
- ISO 16363 dále upřesňuje a zpřísňuje ty oblasti ochrany a ukládání dat, které jsou nezbytné pro TDR
- Při implemetaci ISO 16363 budou již známy hrozby na daný systém repozitáře (informace z implementovaného systému ISMS)
- Bezpečnost dat a fungování repozitáře na vyšší úrovni při certifikaci **ISO 27001 a následně ISO 16363**

Průběh certifikace - audit

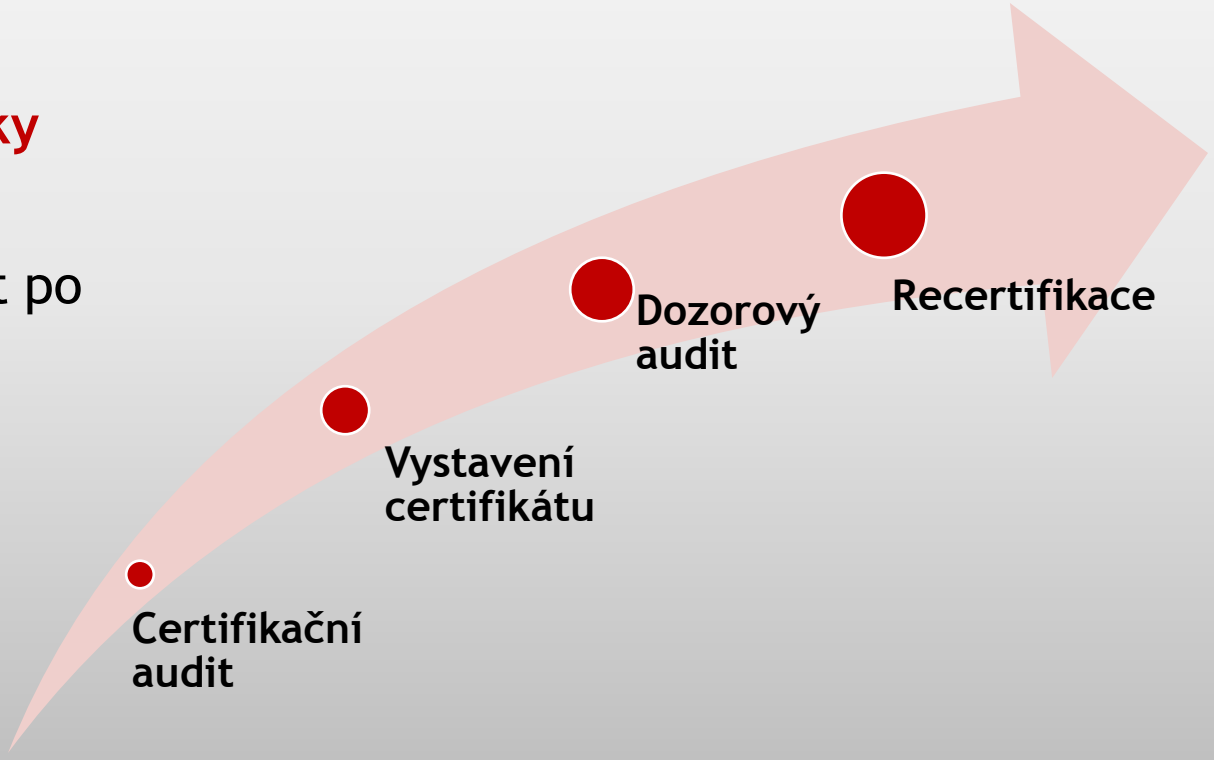
Dvoustupňový audit

- **Stage 1** auditu je počáteční stanovení rozsahu auditu. Je založena na vlastním interním auditu, případně s krátkou úvodní návštěvy auditorů.
- **Stage 2** auditu zahrnuje návštěvu auditorského týmu a kontrola všech požadavků normy ve větší detailnosti.



Udržování certifikace

- Certifikáty s platností **3 roky**
- dozorový audit po 18 měsících
- Po vypršení platnosti – **recertifikace**



Současný stav a směr

- Probíhají první audity TDR
- Digitální repozitáře implementují požadavky dle ISO 16363
- Provádění Self-auditů s pomocí nezávislých organizací
- Zavádění systému TDR min. 1 rok před auditem/ certifikací

Jak začít?

- Norma ISO 16363:2011
- Self audit formulář
- Určení metrik a zdrojů systému
- Posouzení integrace systému
- Aplikace opatření k požadavkům normy
- Self-audit dle ISO 16363
- Zlepšení systému a příprava k nezávislému auditu