Systém managementu bezpečnosti informací (ISMS) podle ISO/IEC 27001:2005

Praha – květen 2008

Volba jistoty.
Více hodnoty.

Informace - Bezpečnost informací

Informace jsou aktiva, která mají pro organizaci hodnotu.

Informace mohou existovat v různých podobách - vytištěny, nebo napsány na papíře, uloženy v elektronické podobě, posílány, zachyceny na film nebo vyřčeny při konverzaci).




Bezpečnost informací je charakterizována jako zachování:

Důvěrnosti – vlastnost zajišťující nepřístupnost informace nebo odkrytí neoprávněnými jednotlivci, skupinami nebo procesy,

Integrity – vlastnost zabezpečující správnost a úplnosti aktiv,

Dostupnosti – vlastnost zajišťující přístup a použití oprávněným skupinám na vyžádání.

Zdroj: ČSN ISO/IEC 27001

Normy v oblasti systémů managementu bezpečnosti informací

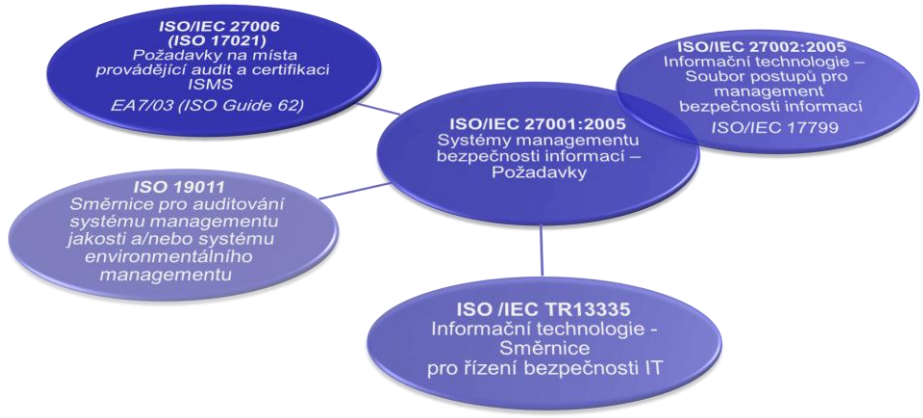
Czech

ISO 27000	–	ISMS, Základy a slovník
ISO 27001	–	ISMS, Požadavky
ISO 27002	–	ISMS, Soubor postupů (předchozí ISO 17799)
ISO 27003	–	ISMS, Metriky a měření
ISO 27004	–	ISMS, Návod pro implementaci
ISO 27005	–	ISMS, Management rizik (předchozí BS7799-3)
ISO 27006	–	ISMS, Požadavky na místa provádějící audit a certifikaci ISMS
ISO 27007..9	–	ISMS, další oblasti, včetně kompetencí ISMS auditorů

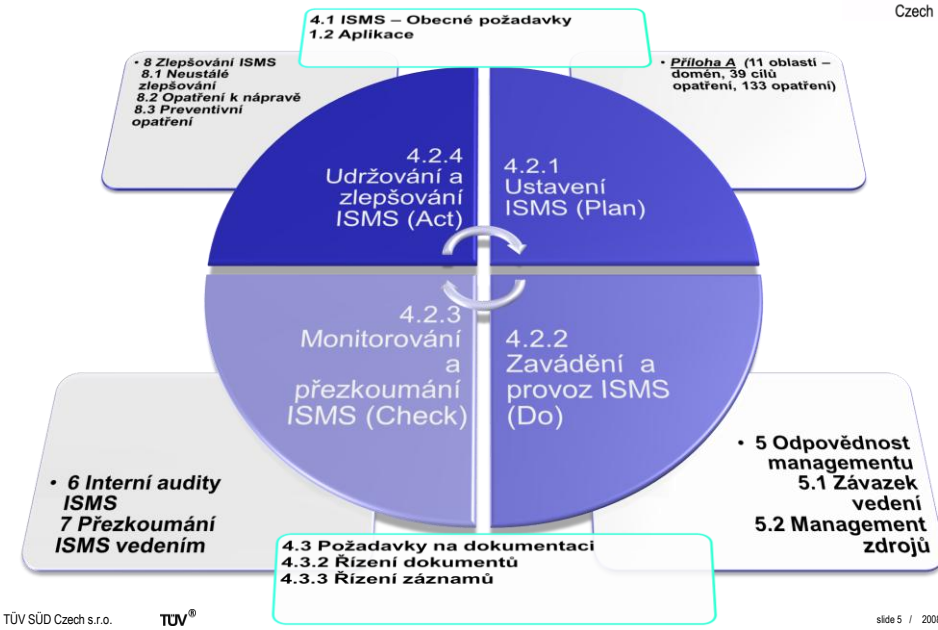
Vydané normy

Vztahy mezi normami pro oblast ISMS

Czech



Struktura normy ISO/IEC 27001:2005



ISO/IEC 27002:2005 – příloha A ISO/IEC 27001:2005

4 – Hodnocení a zvládání rizik				
5 – Bezpečnostní politika informací				
6 – Organizace bezpečnosti informací				
7 – Klasifikace a řízení aktiv				
8 – Bezpečnost lidských zdrojů	9 – Fyzická bezpečnost a bezpečnost prostředí	10 - Řízení komunikací a provozu	11 – Řízení přístupu	12 – Pořízení, vývoj a údržba informačních systémů
13 – Správa incidentů bezpečnosti informací				
14 - Řízení kontinuity činností				
15 – Soulad s požadavky				

Proces certifikace

Czech

Cíl: Získat certifikát vydaný certifikační společností akreditované podle pravidel akreditační společnosti

- Platnost certifikátu – 3 roky
- Certifikační audity – audit 1. a 2. stupně
- Dozorové audity – roční, tolerance -3/+0 měsíce závislé na datu certifikačního auditu
- Po 3 letech probíhají recertifikační audity
- Pokud je potřebné změnit, rozšířit obor platnosti certifikace, je vhodné toto provést během plánovaných auditů.


TGA - Trägergemeinschaft für Akkreditierung - German Association for Accreditation GmbH

Deutschen AkkreditierungsRat

Accreditation

Informace → Příprava auditu → Certifikační audit – stupeň 1 → Certifikační audit – stupeň 2 → Dozorové audity → Recertifikační audit → Dozorové audity

Proces certifikace - INFORMACE

Czech

Cíl: Získat informace, které jsou dostatečné pro zpracování nabídky a/nebo vypracování časového harmonogramu certifikace a vlastního průběhu auditu 1.stupně a 2.stupně

- Údaje o zákazníkovi (kontaktní údaje)
- Analýza komplexnosti a specifik prověřovaných oblastí:
  počet zaměstnanců, externích pracovníků, počet sítí, uživatelů, serverů, klientů, vliv legislativních požadavků, specifikace sektorů auditované společnosti
- Možné, kombinované audity
- Dohoda o rozsahu ISMS
- NDA, pokud je potřebná

Informace → Příprava auditu → Certifikační audit – stupeň 1 → Certifikační audit – stupeň 2 → Dozorové audity → Recertifikační audit → Dozorové audity

Proces certifikace – PŘÍPRAVA AUDITU

Cíl: podle potřeb zákazníka může být vyjasněny všechny požadavky certifikace, např. provedení předauditu

- Předběžné prověření dokumentace ISMS
- Setkání k vyjasnění potřeb zákazníka
- Předaudit
- Workshop k rozsahu ISMS
- Analýza stavu pro specifické legislativní sektory
- jakákoliv kombinace výše uvedených činností

Proces certifikace – STUPEŇ 1

Cíl: Zaměřit se na plánování a pochopení ISMS v kontextu politiky a cílů ISMS organizace zákazníka, především na stav připravenosti na audit 2. stupně a souhlas pro další aktivity auditu na místě

Audit dokumentace ISMS:

- politika a cíle ISMS, rozsah ISMS, postupy pro podporu ISMS,
- popis metodologie hodnocení rizik, zpráva o hodnocení rizik,
- plán zvládání rizik, záznamy vyžadované normou,
- prohlášení o aplikovatelnosti.
- Audit vybraných procesů a pracovišť

Výstup:

- zpráva o prověření dokumentace

Proces certifikace – STUPEŇ 2

Czech

Cíl: Ověřit, že organizace dodržuje své vlastní postupy, zásady, politiky a cíle. Ověřit, že ISMS je ve shodě se všemi požadavky ISO27001 a jsou dosahovány všechny cíle opatření v organizaci.

Audit na místě je zaměřen na:

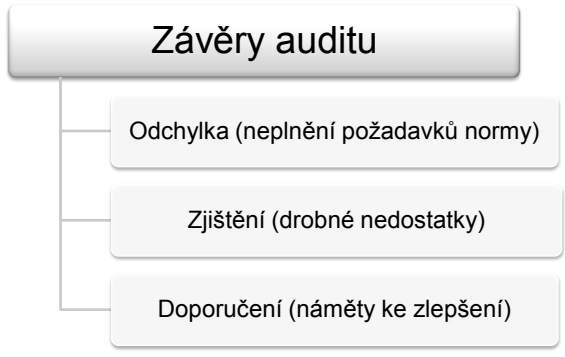
- hodnocení rizik souvisejících s bezpečností informací,
- předloženou dokumentaci z 1.stupně a její implementaci,
- výběr cílů opatření a implementaci opatření založený hodnocení rizik,
- efektivnost ISMS prostřednictvím auditů, přezkoumání vedením,
- monitorovaných procesů, postupů, stanovených odpovědností.

Výstupy:

- Plán auditu (před auditem na místě)
- Zpráva z auditu
- zprávy o odchylce(kách), odstranění do 3 měsíců
- Certifikát(y)

Certifikace dle ISO/IEC 27001:2005 – HODNOCENÍ A ZÁVĚRY AUDITU

Czech



Proces certifikace – DOZOR NAD CERTIFIKACÍ

Cíl: Ověření, že certifikovaný ISMS je udržován, zda jsou posuzovány potřeby změn a jsou prováděny změny. Dále je ověřována shoda s certifikačními požadavky.

Dozorové audity standardně zahrnují:

- prověření udržování ISMS (provádění interních auditů, přezkoumání vedením, opatření k nápravě a preventivní opatření
- komunikaci s externími stranami a dokumenty požadované certifikací změny v ISMS
- vybrané prvky ISO 27001
- další vybrané oblasti, pokud je to vhodné

Výstupy:

- Plán auditu
- zpráva z auditu
- Zprávy o odchylce(kách), pokud se vyskytnou
- změny certifikátů

Roman Prášek
Auditor

TÜV SÜD Czech s.r.o.
CZ – 142 21 Praha 4

Tel: +420 725 707 296
E-mail: roman.prasek@tuv-sud.cz
www.tuv-sud.cz

Volba jistoty.
Více hodnoty.