Projekt ISO/IEC 27001

Nabídka konzultačních služeb pro:

CzechGlobe, Ústav výzkumu globální změny AV ČR, v. v. i.

Dne 17.5.2022

Vypracoval:

[redacted]

Obchodní ředitel

[redacted]

Obsah

Úvod

CzechGlobe, Ústav výzkumu globální změny AV ČR, v.v.i. (dále pouze “CzechGlobe”) je organizací, jejíž činnost je zaměřená na výzkum Globální změny z pohledu ekologických věd, a jejího dopadu na atmosféru, ekologii, zemědělství, energetiku, a další oblasti s celospolečenským přesahem. Významně spolupracuje s mezinárodní vědeckou a odbornou komunitou a její činnost má uplatnění i v komerční sféře v oblasti např. predikcí vývoje, počasí či přímo v oblasti národní energetiky.

Požadavky centra excelence CzechGlobe na přípravu projektu bezpečnosti dat a informací dle ISO/IEC 27001:2013 vychází jak z potřeby zvýšit prestiž organizace pro své partnery v lokálním i mezinárodním měřítku a ujistit je o systematickém přístupu k této problematice, tak začlenit i tuto oblast do již existujícího systému integrovaného managementu dle ISO 9001:2008.

Jedná se z praktického hlediska především o výzkumná a projektová data, data třetích stran podléhající licenčnímu užití, a data poskytovaná dále soukromým či státním subjektům.

CzechGlobe požádal společnost Redwoods s.r.o. (dále pouze “Redwoods”) o předložení nabídky konzultačních služeb k implementaci řízení bezpečnosti informací dle ISO/IEC 27001 za účelem splnění požadavků certifikačního auditu.

Společnost Redwoods vypracovala vstupní analýzu pro identifikaci důležitých okruhů a oblastí na které bude potřeba se v rámci projektu zaměřit.

Manažerské shrnutí

Záměrné a cílené řízení rizik je jedním ze základních pilířů úspěšné manažerské koncepce každé organizace. Schopnost predikovat hrozby a předcházet bezpečnostním incidentům je v moderní informační éře důležité především z hlediska zajištění kontinuity chodu organizace, souladu s předpisy a regulacemi a zajištění důvěry třetích stran v to, že se organizace dokáže kvalifikovaně postarat o data, která s nimi další subjekt, partner či zákazník sdílel.

CzechGlobe může mít před sebou určitá bezpečnostní rizika, avšak ta skýtají také příležitosti k tomu celou oblast bezpečnosti řešit koncepčně a stát se tak vzorovou, oficiálně certifikovanou organizací. Vzhledem ke specifickému zacílení výzkumu jsou požadavky na bezpečnost rozhodně na místě.

Certifikace

Prioritu certifikací doporučujeme následovně:

1. ISO/IEC 27001
2. Zvážit zapojení ISO/IEC 20000 do systému integrovaného managementu

Jiné certifikace doporučujeme řešit až v momentě, kdy bude o ně požádáno ze strany třetích stran, spolupracujících s CzechGlobe.

Projektový plán a cenová nabídka

Projektový plán – certifikace ISO/IEC 27001

Trvání a odhad náročnosti

Odhadované trvání a náročnost projektu implementace ISO/IEC 27001 jsou následující:

- Časový rámec
  - 7–11 měsíců od zahájení projektu
- Interní prostředky
  - 0.5 FTE (úvazku, Full Time Employee) Bezpečnostní Manažer – pro přípravu, nasazení a údržbu (vzhledem k velikosti CzechGlobe může jít o sdílenou roli, nesmí ale docházet ke konfliktu zájmů)
  - 0.5–1 FTE pro implementaci a údržbu bezpečnostních opatření (rozpuštěno do celého týmu)
- Externí prostředky
  - 19 MD (člověkodnů, mandays) externího dodavatele bezpečnostního poradenství a konzultačních služeb (v tabulce červeně)
  - 4 MD externího auditora v prvním roce + 3 MD v každém následujícím roce (v tabulce modře)

Návrh rozsahu (Scope)

Stejný jako pro stávající certifikace ISO 9001 a 14001; 1 fyzická lokalita (Brno), cca 100 zaměstnanců.

Infrastruktura, informační systémy, software a hardware vlastněn CzechGlobe.

Návrh projektu (Work Breakdown Structure, WBS)

Fáze	Deliverables	Odhad interních prostředků (MD)	Odhad externích prostředků (MD)	Odhad trvání (týdny)
Analýza	Rozsah ISMS	1	0	0

	Vybrání dodavatele pro audit a certifikaci			
Inventář aktiv, analýza rizik a Business Impact Assessment	Datový inventář Registr rizik Kritické procesy a podklady pro řízení kontinuity	20	5	4
Gap analýza – opatření ISO/IEC 27001	Rozdíl aktuálního stavu od požadavků ISO/IEC 27001	5	1	2
Příprava dokumentace	• Politika bezpečnosti informací[1] • Matice klasifikace aktiv[2] • Inventář aktiv[3] • Politika bezpečného vývoje (Secure Development Lifecycle, SDLC)[4] • Framework bezpečnostních opatření (popsaný například v Politice operační bezpečnosti, fyzické bezpečnosti, bezpečnosti ve vztazích s dodavateli)[5] • Plány kontinuity podnikání a obnovy po haváriích (Disaster Recovery)[6] • Seznam aplikovatelných právních požadavků[7] • Prohlášení o Aplikovatelnosti[8] Podpůrné dokumenty • Plán zvládání krizí[9]	15	5	4

[1] Interní směrnice, která definuje systém řízení bezpečnosti informací, role a odpovědnosti, metodiku řízení rizik a další
[2] Dokument, definující klasifikaci informačních aktiv dle jejich citlivosti
[3] Databáze, klasifikující informační aktiva dle jejich citlivosti
[4] Interní směrnice, definující pravidla bezpečného vývoje aplikací
[5] Dle potřeby, interní směrnice uvádějící nasazená bezpečnostná opatření dle jejich kategorií (fyzická, operativní, atd.)
[6] Interní směrnice a plány kontinuity a obnovy po výpadku, zahrnující scénáře ohrožující funkčnost CzechGlobe jako organizace
[7] Seznam všech relevantních právních požadavků pro bezpečnost dat; pro CzechGlobe jsou to zejména pravidla ochrany osobních údajů
[8] Tabulka s přehledem všech požadavků ISO/IEC 27001 a jejich aplikovatelnost a implementace v rámci CzechGlobe
[9] Interní směrnice, definující role, odpovědnosti a pravidla v případě vyhlášení krize v rámci CzechGlobe

	• Plán zvládání incidentů[10] • Plán interních auditů[11] • Životní cyklus vývoje aplikací[12] • Politika osobních zařízení pro práci[13] • Politika pro kryptografické algoritmy[14]			
Nastavení procesů	Dle potřeby na základě dokumentace a chybějících bodů Gap analýzy: • Všechny bezpečnostní procesy z politik výše • Řízení vztahů s dodavateli • Proces vývoje • Release process (produkty a integrace) • Řízení změn • Řízení konfigurací • Interní audit	30-60	4	4-12
Nasazení opatření	Administrativní, fyzická a technická opatření; alespoň: • Inventář aktiv a jejich vlastnictví • Řízení přístupových oprávnění (autentizace, hardening, řízení privilegovaných oprávnění) • Monitorování, logování & upozornění • Bezpečnostní požadavky ve smlouvách • Bezpečný transfer dat s třetími stranami • Bezpečná destrukce dat • Bezpečnostní testování • Řízení zranitelností	60-120	4	8-16

[10] Interní směrnice, definující role, odpovědnosti a pravidla kolem zvládání bezpečnostních incidentů (typu výpadek systémů, únik dat atp.)
[11] Plán interních bezpečnostních auditů a revizí stavu bezpečnosti
[12] Podpůrný dokument, definující procesy ve vývoji aplikací (např. Agilní vývoj, waterfall)
[13] Taky politika Bring Your Own Device, BYOD - interní směrnice, definující pravidla použití osobních zařízení pro pracovní účely
[14] Interní směrnice, definující pravidla použití kryptografických algoritmů pro ochranu dat v rámci nasazených bezpečnostních opatření a v rámci vyvíjených aplikací

	• Bezpečnostní školení pro uživatele, vlastníky dat, auditory a IT			
Pre-Audit	Zpráva Pre-Auditu a nálezy Implementovány doporučení	5	1	4
Audit a certifikace	Certifikát	7	3	2
Údržba systému řízení bezpečnosti informací (ISMS)	Záznamy a logy Evidence o prozkoumáních bezpečnosti, KPI, funkčnost ISMS Reporty z auditů Evidence o kompetenci lidí	100-150 ročně[15]	0	N/A
Údržba certifikace	Re-Audit report Obnovený certifikát	6 ročně	3 ročně	2

Odhady náročnosti jsou postaveny na zkušenosti s obdobnými firmami (30-300 zaměstnanců, ČR) a na chybějících částech, identifikovaných v průběhu úvodního workshopu.

Cenová nabídka konzultačních služeb Redwoods

Typ služby	Jednotka	Počet	Celková cena
Odborné konzultace	MD	19	247.000,-*

*Ceny jsou uvedeny bez DPH, cena neobsahuje služby Auditu a certifikace

Odborným garantem projektu je:

[redacted] Senior Lead Implementer

Proč Redwoods s.r.o.

Jsme profesionálové v oblasti informační bezpečnosti.

Pomáháme organizacím a firmám vyhovět náročným požadavkům jejich zákazníků v oblasti procesní, datové a produktové bezpečnosti.
Postupujeme nejen podle standardů ISO/IEC 27001 ale především i best practices, které jsme nasbírali za více než 10 let působení v technologických společnostech zabývajících se IT bezpečností.

Za tým Redwoods:

[redacted]

jednatel, obchodní ředitel

[15] Rozpuštěno do celého týmu, koordinováno manažerem bezpečnosti