MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

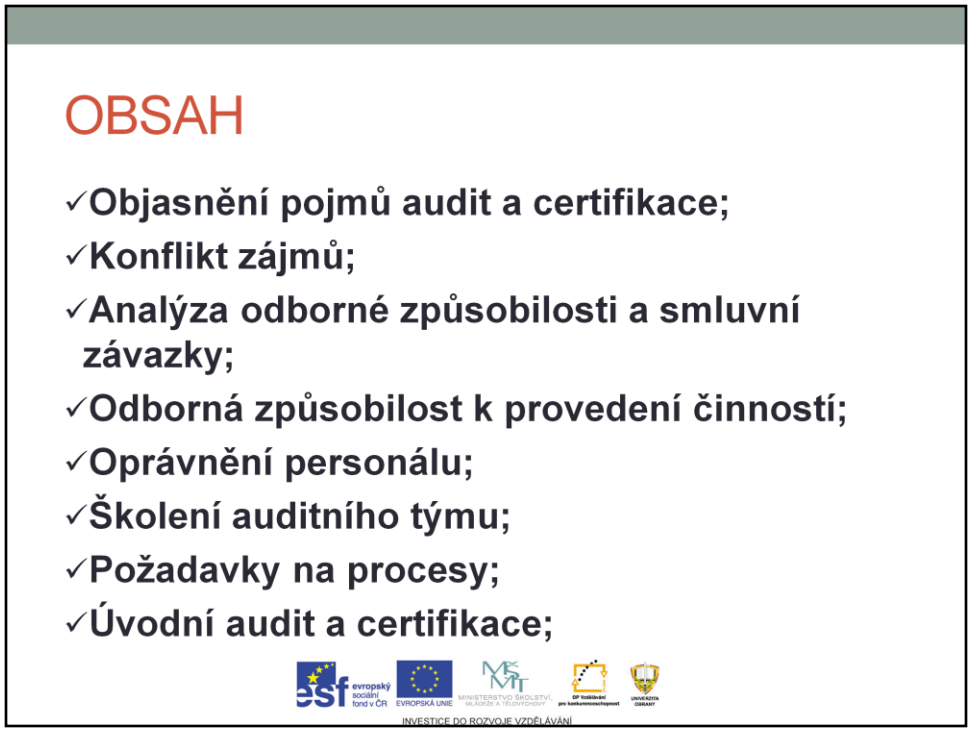
TÉMA Č. 1
POŽADAVKY NA ORGÁNY PROVÁDĚJÍCÍ AUDIT A CERTIFIKACI SYSTÉMŮ ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

pplk. Ing. Radek DUBEC, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra celoživotního vzdělávání
E-mail.: radek.dubec@unob.cz

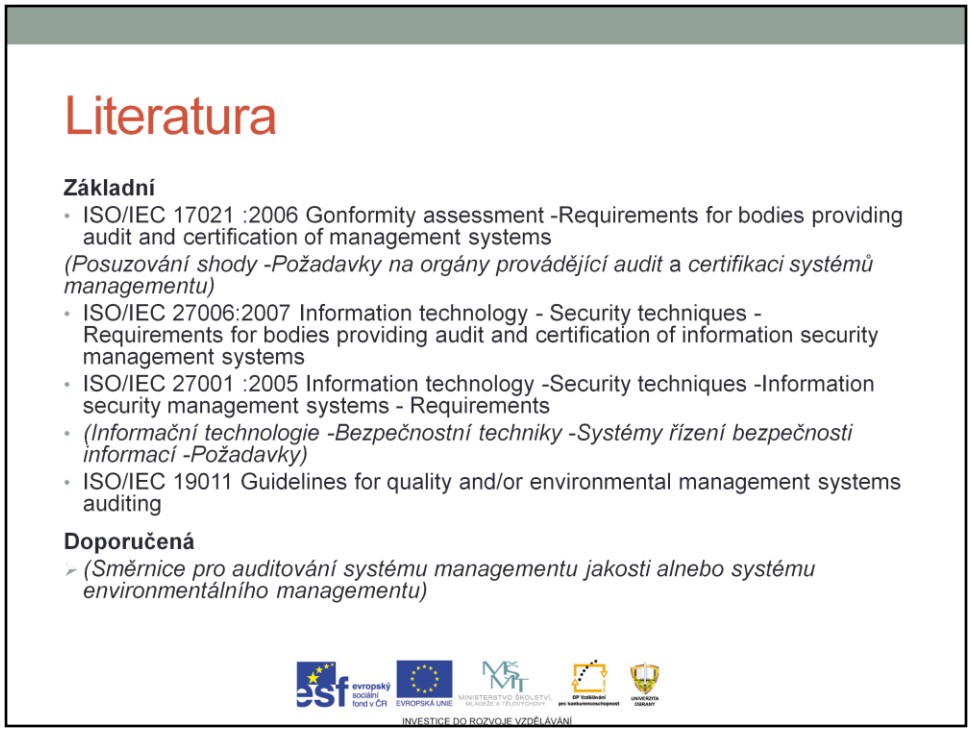
Operační program Vzdělávání pro konkurenceschopnost
Projekt: ***Vzdělávání pro bezpečnostní systém státu***
(reg. č.: CZ.1.01/2.2.00/15.0070)

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Dnešní téma se vztahuje k problematice požadavků na orgány provádějící audit a certifikaci systémů řízení. bezpečnosti informací



V rámci tohoto tématu se budeme zabývat následujícími oblastmi– viz snímek.



Pro studium této problematiky mezi základní literaturu patří norma ISO/IEC 17021 :2006 Gonformity assessment -Requirements for bodies providing audit and certification of management systems *(Posuzování shody -Požadavky na orgány provádějící audit* a *certifikaci systémů managementu) a norma* ISO/IEC 27006:2007 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

Další neméně významnou publikací je monografie GRASSEOVÁ, M., DUBEC, R., ŘEHÁK, D. Analýza podniku v rukou manažera. 1. vydání. Brno: Computer Press, 2010, 325 s. ISBN 978-80-251-2621-9.(Strana 139-175), popisující obecné přístupy k řízení rizik a základní postupy pro zavedení tohoto nástroje do organizace.

ZÁKLADNÍ POJMY

certifikát *(certificate)*

certifikát vydaný certifikačním orgánem v souladu s podmínkami jeho akreditace a nesoucí schválený symbol nebo sdělení

certifikační orgán *(certification body)*

třetí strana, která hodnotí a certifikuje ISMS klientské organizace s ohledem na publikované ISMS normy a další dokumentaci požadovanou pro certifikovaný systém

certifikační dokument *(certification document)*

dokument označující, že ISMS klientské organizace vyhovuje předepsaným normám a další dokumentaci vyžadované pro certifikovaný systém

značka *(mark)*

právně registrovaná ochranná známka nebo jinak chráněný symbol, který je vydaný akreditačním nebo certifi- kačním orgánem a označuje, že byla demonstrována

adekvátní důvěra v systémy řízené lidmi, nebo že příslušné produkty nebo osoby jsou v souladu s požadavky konkrétní normy

organizace *(organization)*

společnost, podnik, firma, závod, úřad nebo instituce nebo jejich část či kombinace, ať už zapsané v obchodním rejstříku či nikoliv, veřejné nebo soukromé, které mají své vlastní funkce a správu a jsou schopné aplikovat principy bezpečnosti informací

Konflikt zájmů

Certifikační orgán může vykonávat následující služby bez toho, aby byly považovány za poradenství nebo aby se dostal do potenciálního konfliktu zájmů:

- a) certifikaci, včetně informačních schůzek, plánování schůzek, přezkoumání dokumentace, audit (nejedná-li se o interní audit ISMS nebo interní bezpečnostní revize) a opětovné posouzení identifikovaných neshod;

Konflikt zájmů

- b) pořádání přednáškové nebo školicí činnosti a účast v roli lektora za předpokladu, že v případech, kdy se kurzy týkají řízení bezpečnosti informací, systémů řízení nebo auditu, by se měl certifikační orgán omezit na poskytování obecně dostupných informací a doporučení, tj. neměl by poskytovat informace ve větším rozsahu, než jak je uvedeno v bodě c) níže;
- c) zpřístupnit nebo na vyžádání zveřejnit svoji vlastní interpretaci jednotlivých požadavků norem, podle kterých provádí certifikaci;

Konflikt zájmů

- d) činnosti předcházející auditu výhradně zaměřené na určení připravenosti organizace k certifikačnímu auditu. Nicméně takovéto činnosti by neměly mít za následek poskytnutí doporučení nebo rady, která by porušovala požadavky této kapitoly. Certifikační orgán by měl být schopen doložit, že činnosti spojené s před certifikačním auditem nejsou brány jako odůvodnění případného zkrácení certifikačního auditu;
- e) provádět zákaznické a jiné audity v souladu s normami nebo předpisy mimo rozsah jejich akreditace;

Konflikt zájmů

- f) nabídnout přidanou hodnotu během návštěv certifikačního a dohledového auditu, například identifikováním příležitostí ke zlepšení tak, jak se projeví během auditu, ale bez toho, aby nabízela konkrétní řešení.
- Certifikační orgán musí být nezávislý na orgánu nebo orgánech (včetně všech zainteresovaných jednotlivců), které provádějí interní audity ISMS v zákazníkově organizaci v rozsahu, který je předmětem certifikace ISMS.

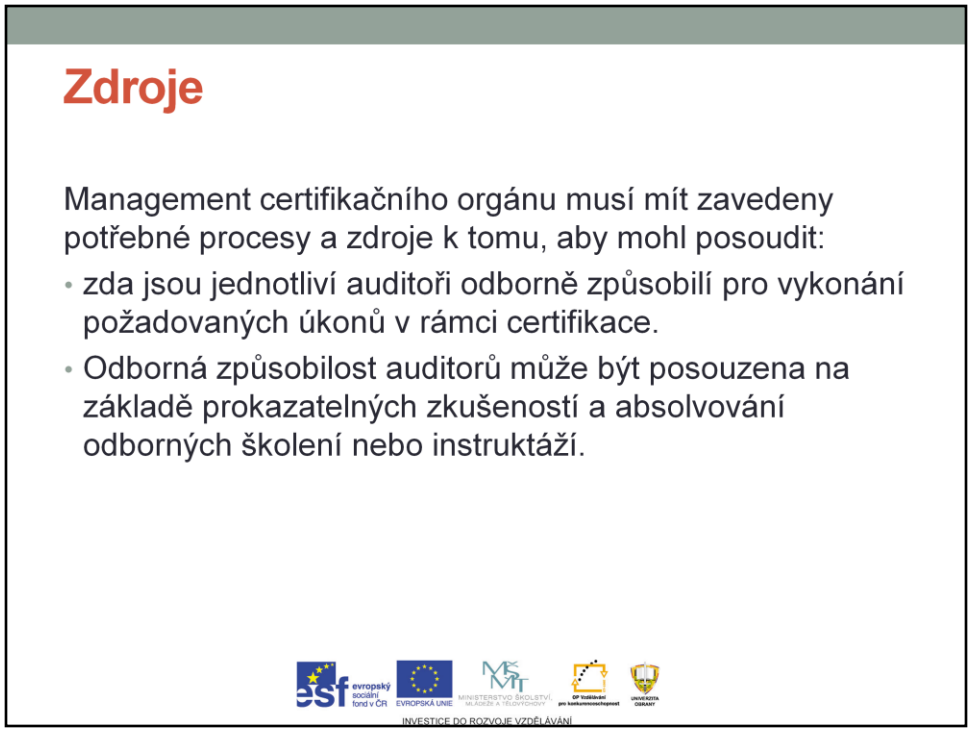
Analýza odborné způsobilosti a smluvní závazky

Certifikační orgán musí zajistit, že má odpovídající vývoj znalostí, technologií a legislativy v oblastech relevantních k ISMS organizace, kterou hodnotí.

- Certifikační orgán musí mít efektivní systém pro analýzu odborných způsobilostí, které potřebuje mít k dispozici v oblasti řízení bezpečnosti informací a to s ohledem na všechny technické oblasti, v nichž působí.
- Vůči svým klientům musí být certifikační orgán schopen doložit, že provedl analýzu odborné způsobilosti (tj. posouzení požadovaných znalostí podle identifikovaných potřeb) podle požadavků každé relevantní oblasti dříve, než na sebe převezme smluvní závazky. Na základě výsledků této analýzy musí certifikační orgán ve spolupráci s klientem provést revizi smlouvy. Certifikační orgán musí být zejména schopen demonstrovat, že má odbornou způsobilost k provedení následujících činností:

Odborná způsobilost k provedení činností:

- a) porozumění oblastem činností organizace klienta a souvisejících rizik vyplývajících z činností;
- b) určení potřebných odborných způsobilostí ve vztahu k identifikovaným činnostem a hrozbám působícím na informační aktiva a ve vztahu k zranitelnostem a dopadům na organizaci klienta;
- c) potvrdit dostupnost požadovaných odborných způsobilostí.



Certifikační orgán musí být schopen efektivně komunikovat se všemi organizacemi, kterým poskytuje své služby.

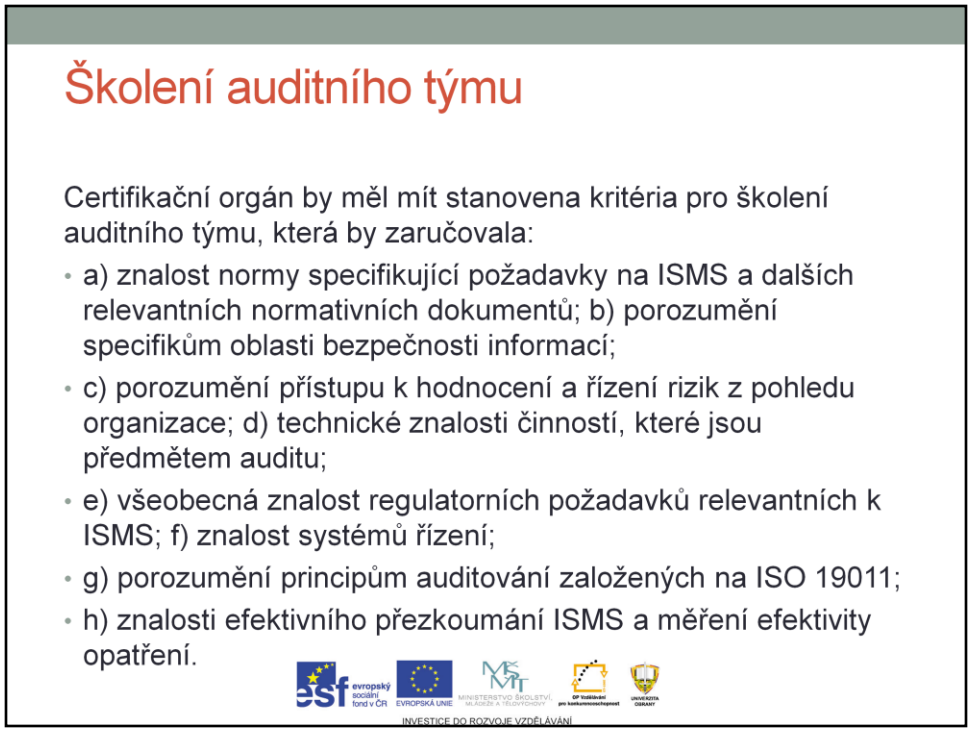
Management certifikačního orgánu musí mít zavedeny potřebné procesy a zdroje k tomu, aby mohl posoudit:

zda jsou jednotliví auditoři odborně způsobilí pro vykonání požadovaných úkonů v rámci certifikace.

Odborná způsobilost auditorů může být posouzena na základě prokazatelných zkušeností a absolvování odborných školení nebo instruktáží.

Oprávnění personálu

- Oprávnění personálu certifikačního orgánu Certifikační orgán by měl mít osoby oprávněné k:
- a) výběru a ověření odborné způsobilosti auditorů ISMS vybraných do auditních týmů konkrétního auditu;
- b) instruování auditorů ISMS a zajištění potřebného odborného školení;
- c) rozhodnutí o udělení, udržování, stažení, pozastavení, prodloužení nebo omezení certifikací;
- d) přípravě a vedení procesu odvolání a stížností.



Tyto požadavky na školení jsou aplikovatelné pro všechny členy auditního týmu s výjimkou bodu d), který může

být mezi členy auditního týmu rozdělen.

Při výběru auditního týmu, který má být jmenován pro konkrétní certifikační audit, musí certifikační orgán zajistit odpovídající znalosti pro všechny vytyčené úkoly. Tým by měl:

a) mít odpovídající technické znalosti o specifických činnostech v rozsahu certifikovaného ISMS a tam, kde je to relevantní, o souvisejících postupech a jejich potenciálních rizicích pro bezpečnost informací (tuto funkci mohou plnit techničtí odborníci, kteří sami nejsou auditory);

b) mít odpovídající stupeň znalostí organizace klienta k spolehlivému provedení certifikačního auditu ISMS .: a zvládnutí všech aspektů bezpečnosti informací souvisejících činností, produktů a služeb;

c) mít odpovídající znalosti regulatorních požadavků aplikovatelných na ISMS organizace.

Auditní tým může být v případě potřeby doplněn o technické experty, kteří mají odpovídající znalosti o technologiích, které jsou součástí auditu. Je důležité si uvědomit, že tito experti nemohou nahradit auditory ISMS, mohou však auditorovi poskytnout odbornou radu v technických otázkách týkajících se auditovaného systému řízení. Certifikační orgán musí mít postupy pro:

a) výběr auditorů a technických expertů na základě jejich odborné způsobilosti, školení, kvalifikace a zkušeností;

b) hodnocení auditorů a technických expertů během certifikačních auditů a pro následné monitorování jejich výkonnosti. Při výběru auditního týmu, který má být jmenován pro konkrétní certifikační audit, musí certifikační orgán zajistit odpovídající znalosti pro všechny vytyčené úkoly.

Tým by měl:

a) mít odpovídající technické znalosti o specifických činnostech v rozsahu certifikovaného ISMS a tam, kde je to relevantní, o souvisejících postupech a jejich potenciálních rizicích pro bezpečnost informací (tuto funkci mohou plnit techničtí odborníci, kteří sami nejsou auditory);

b) mít odpovídající stupeň znalostí organizace klienta k spolehlivému provedení certifikačního auditu ISMS .: a zvládnutí všech aspektů bezpečnosti informací souvisejících činností, produktů a služeb;

c) mít odpovídající znalosti regulatorních požadavků aplikovatelných na ISMS organizace.

Auditní tým může být v případě potřeby doplněn o technické experty, kteří mají

odpovídající znalosti o technologiích, které jsou součástí auditu. Je důležité si uvědomit, že tito experti nemohou nahradit auditory ISMS, mohou však auditorovi poskytnout odbornou radu v technických otázkách týkajících se auditovaného systému řízení. Certifikační orgán musí mít postupy pro:

a) výběr auditorů a technických expertů na základě jejich odborné způsobilosti, školení, kvalifikace a zkušeností;

b) hodnocení auditorů a technických expertů během certifikačních auditů a pro následné monitorování jejich výkonnosti.

Požadovaná úroveň vzdělání, pracovních zkušeností, absolvovaná školení auditorů a zkušenosti z auditů ISMS

Následující kritéria se musí vztahovat na každého auditora v ISMS auditním týmu. Auditor musí mít: a) ukončené středoškolské vzdělání;

b) nejméně čtyři roky pracovních zkušeností v oblasti informačních technologií, z toho nejméně dva roky v roli

nebo funkci související s bezpečností informací;

c) úspěšně ukončené pětidenní školení, které svým rozsahem pokrývá audity ISMS a vedení auditů, je pova- žováno za přiměřené;

d) zkušenosti z celého procesu hodnocení bezpečnosti informací dříve než převezme odpovědnost za provedení auditu v roli auditora. Zkušenosti by měl auditor získat účastí na minimálně čtyřech certifikačních auditech v délce trvání minimálně 20 dní, včetně přezkoumání dokumentace a analýzy rizik, hodnotících a auditních zpráv;

e) současné znalosti v daném oboru;

f) schopnost podívat se na komplexní operace ze širší perspektivy a porozumět rolím jednotlivých oddělení ve větších organizacích;

g) aktuální znalosti a kvalifikaci v oblasti bezpečnosti informací a auditu a tyto znalosti udržovat v rámci konti- nuálního profesního rozvoje.

Techničtí experti musí splňovat kritéria uvedená v bodech a), b), e) a f).

Vedoucí auditních týmů musí splňovat, kromě požadavků uvedených ve výše uvedených bodech, i následující požadavky, které musí být demonstrovány v rámci auditů pod dohledem:

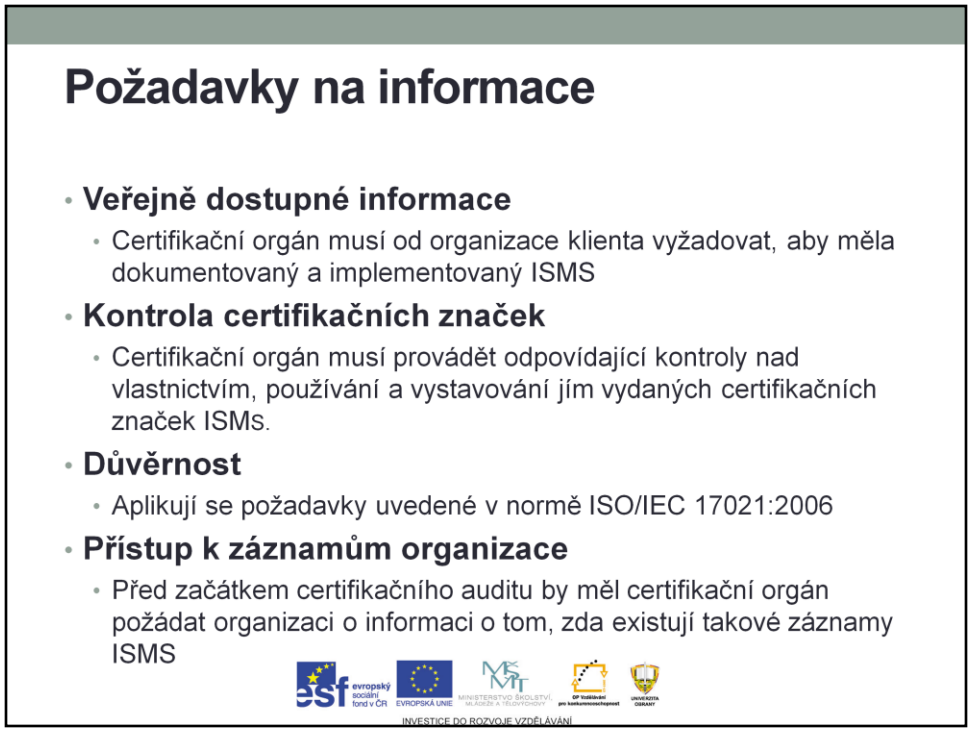
a) mít znalosti a vlastnosti potřebné k řízení certifikačního auditu;

b) mít jako auditor za sebou minimálně tři kompletní audity ISMS;

c) úspěšně demonstrovat schopnosti efektivní komunikace jak ústní, tak i písemné.

Použití externích auditorů a technických expertů

Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 7.3.



Požadavky na informace

Veřejně dostupné informace

Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 8.1, doplněné o následující specifické požadavky a doporučení ISMS.

Postupy pro udělení, udržováni, prodloužení, omezení, pozastavení nebo odebrání certifikace

Certifikační orgán musí od organizace klienta vyžadovat, aby měla dokumentovaný a implementovaný ISMS

v souladu s požadavky ISO/IEC 27001 a další relevantní dokumentaci požadovanou pro certifikaci. Certifikační orgán musí mít dokumentované postupy pro:

a) úvodní certifikační audit ISMS organizace v souladu s ustanoveními ISO 19011, ISO/IEC 17021 a další relevantní dokumentací;

b) periodický, dohledový a recertifikační audit ISMS organizace v souladu s ISO 19011 a ISO/IEC 17021 na trvající shodu s relevantními požadavky a pro verifikaci toho, že organizace realizuje kroky pro nápravu všech zjištěných neshod.

Certifikačni dokumenty

Aplikují se požadavky uvedené v normě ISO/IEC 17021:2006, v 8.2, doplněné o následující specifické požadavky a doporučení ISMS.

Certifikační dokumenty ISMS

Certifikační orgán musí dodat každé organizaci, jejíž ISMS certifikoval, certifikační dokumenty, tj. listinu nebo certifikát, podepsaný osobou, které byla tato odpovědnost přidělena. Certifikát musí identifikovat rozsah udělené certifikace, pro jakou část organizace a pro jaké systémy byla certifikace udělena, a normu podle které je ISMS certifikován, tedy ISO/IEC 27001. Jako další by měl certifikát obsahovat odkaz na verzi prohlášení o aplikovatelnosti.

Seznam certifikovaných zákazníků

Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 8.3.

8.4 Odkazování se na certifikaci a používání značek

Aplikují se požadavky uvedené v normě ISO/IEC 17021:2006, v 8.4 doplněné o následující specifické požadavky a doporučení ISMS.

Kontrola certifikačních značek

Certifikační orgán musí provádět odpovídající kontroly nad vlastnictvím, používání a vystavování jím vydaných certifikačních značek ISMS. Pokud certifikační orgán udělí

práva k používání certifikační značky, označující certifikaci ISMS, měl by zajistit, že organizace tuto značku používá pouze v mezích písemně udělené autorizace. Certifikační orgán nesmí organizaci udělit oprávnění používat certifikační značku na označení produktu nebo jakýmkoliv jiným způsobem, který by mohl být interpretovaný jako označení shody produktu s požadavky normy.

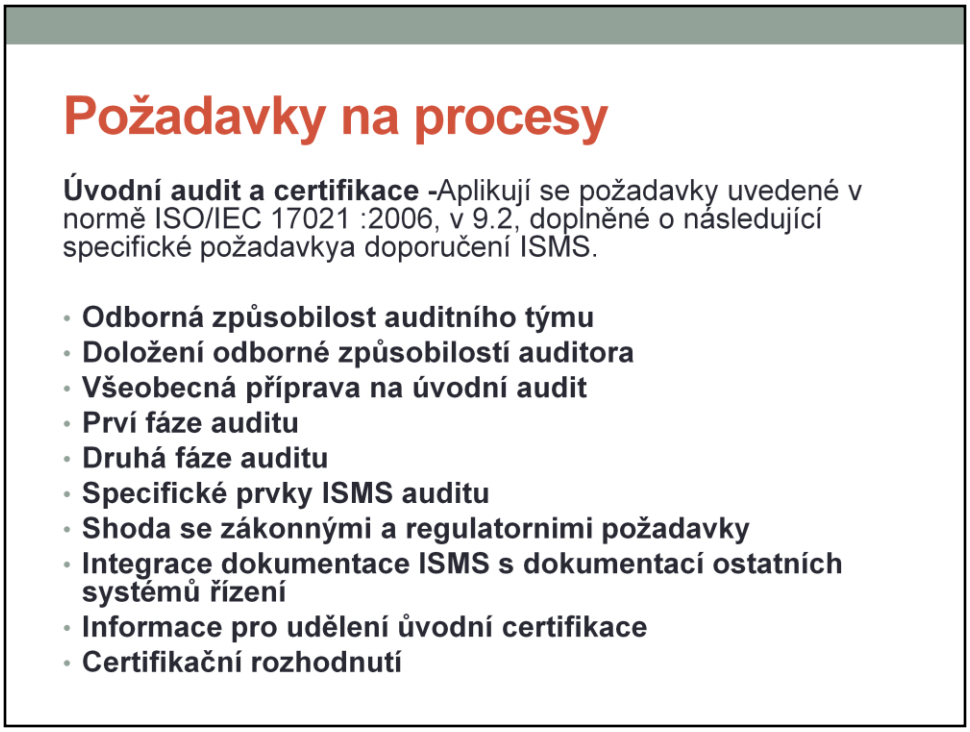
Důvěrnost

Aplikují se požadavky uvedené v normě ISO/IEC 17021:2006, v 8.5, doplněné o následující specifické požadavky a doporučení ISMS.

Přístup k záznamům organizace

Před začátkem certifikačního auditu by měl certifikační orgán požádat organizaci o informaci o tom, zda existují takové záznamy ISMS, které nemohou být zpřístupněné pro přezkoumání auditním týmem z toho důvodu, že obsahují důvěrné nebo citlivé informace. Certifikační orgán musí stanovit, zda bude možné provést odpoví- dající audit ISMS při absenci těchto záznamů. Pokud certifikační orgán usoudí, že není možné provést audit ISMS bez toho, aby přezkoumal identifikované důvěrné nebo citlivé záznamy, doporučí organizaci, aby certifikační audit proběhl teprve poté, co budou provedena opatření pro získání odpovídajícího přístupu.

8.6 Výměna informaci mezi certifikačnim orgánem a jeho zákazníky Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 8.6.



Úvodní audit a certifikace

Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 9.2, doplněné o následující specifické požadavkya doporučení ISMS.

- **Odborná způsobilost auditního týmu**

Kromě požadavků uvedených jsou pro certifikační hodnocení aplikovatelné také následující požadavky. V rámci dohledových činností se aplikují jen ty požadavky, které jsou relevantní pro plánovaný rozsah prací.

Následující požadavky se týkají auditního týmu jako celku:

a) V každé z následujících oblastí musí aspoň jeden člen auditního týmu naplňovat kritéria certifikačního orgánu tak, aby mohl za danou oblast v rámci týmu převzít odpovědnost:

1) schopnost řídit auditní tým,

2) znalost systémů řízení a procesů aplikovatelných na ISMS,

3) znalost legislativních a regulatorních požadavků v oblasti bezpečnosti informací,

4) schopnost identifikace hrozeb a trendů incidentů souvisejících s bezpečností informací,

5) schopnost identifikace zranitelností organizace a určení pravděpodobnosti jejich zneužití, možných dopadů a způsobů jejich omezení a kontroly,

6) znalost opatření ISMS a jejich implementace,

7) znalost způsobů přezkoumání efektivnosti a měření účinnosti zavedených opatření,

8) znalost relevantních norem ISMS, nejlepších praktik daného odvětví, bezpečnostních politik a postupů, 9) znalost postupů pro zvládání bezpečnostních incidentů a řízení kontinuity činností,

10) povědomí o hmotných a nehmotných informačních aktivech a postupech analýzy dopadů, 11) znalost současných technologií, u kterých je potřeba se zaměřit na bezpečnost,

12) znalost procesů a způsobů řízení rizik.

b) Auditní tým musí být schopný propojit jakékoliv náznaky možných bezpečnostních incidentů, identifikovaných

v rámci ISMS organizace, na jednotlivé prvky ISMS.

c) Auditní tým musí mít odpovídající pracovní i praktické zkušenosti s aplikací výše uvedených požadavků (samozřejmě to neznamená, že každý auditor musí mít znalosti a zkušenosti ze všech oblastí informační bezpečnosti, ale jako celek musí mít auditní tým dostatek znalostí a zkušeností tak, aby byly pokryty poža- davky auditovaného ISMS).

Auditní tým může sestávat z jedné osoby pod podmínkou, že tato osoba splňuje všechna kritéria uvedené v 9.2.1.a).

- **Doložení odborné způsobilostí auditora**

Auditoři musí být schopni doložit své zkušenosti a znalost výše uvedených kritérií, například: a) získáním uznávané ISMS kvalifikace; b) získáním auditorské registrace;

c) absolvováním schváleného školení ISMS;

d) doložením záznamů o kontinuálním profesním rozvoji;

e) absolvováním reálného auditu ISMS za účasti dohlížejících zkušených auditorů.

- **Všeobecná příprava na úvodní audit**

Cerrifikační orgán musí po organizaci požadovat, aby provedla všechny nezbytné přípravy pro provedení cer1ifi- kačního auditu, včetně přípravy dokumentace a zajištění přístupu ke všem oblastem, záznamům (včetně interních auditních zpráva zprávo nezávislých přezkoumáních bezpečnosti informací) a personálu za účelem cer1ifikační auditu, certifikačního auditu a řešení stížností.

Minimálně následující informace musí být klientem poskytnuty předtím, než je zahájen certifikační audit na místě:

a) celková informace o ISMS a činnostech, které zahrnuje;

b) kopie požadované dokumentace ISMS, podle 4.3.1 normy ISO/IEC 27001 :2005 a tam kde je to vyžadováno

kopie ostatní relevantní dokumentace.

- **Úvodní certifikační audit**

Prví fáze auditu

V této fázi auditu musí certifikační orgán obdržet dokumentaci popisující návrh ISMS, v rozsahu požadovaném v 4.3.1 normy ISO/IEC 27001.

Cílem první fáze auditu je poskytnout vstupy pro zaměření a naplánování druhé fáze auditu porozuměním, jak ISMS funguje v kontextu cílů organizace a politiky ISMS a jaká je celková připravenost organizace na certifikační audit.

První fáze auditu zahrnuje, ale neměla být omezena na přezkoumání dokumentace. Certifikační orgán se musí s organizací klienta dohodnout na tom, kdy a kde se přezkoumání dokumentace uskuteční. V každém případě musí být přezkoumání dokumentace dokončeno před zahájením druhé fáze auditu.

Výsledky první fáze auditu musí být shrnuty v auditní zprávě. Certifikační orgán musí přezkoumat auditní zprávu z první fáze auditu předtím, než je učiněno rozhodnutí přejít k druhé fázi auditu a je sestaven vhodný auditní tým, sestávající z jedinců požadované odborné způsobilosti.

Certifikační orgán musí uvědomit organizaci klienta o dodatečných požadavcích na informace a záznamy, které mohou být vyžádány k detailnímu přezkoumání v rámci druhé fáze auditu.

Druhá fáze auditu

Druhá fáze auditu se vždy koná se v prostorách organizace klienta. Na základě nálezů zdokumento- vaných vauditní zprávě z první fáze připraví cer1ifikační orgán návrh plánu pro druhou fázi auditu. Cíle druhé fáze auditu jsou:

a) potvrdit, že je organizace klienta v souladu s vlastní politikou, stanovenými cíly a postupy;

b) potvrdit, že ISMS organizace vyhovuje všem požadavkům normy ISO/IEC 27001 a dosahuje cílů stanovených v politice ISMS.

Pro naplnění těchto cíl u musí být audit organizace zaměřen na:

a) hodnocení rizik bezpečnosti informací a na to, že hodnocení dávají porovnatelné a opakovatelné výsledky; b) požadavky na dokumentaci uvedené

v 4.3.1 normy ISO/IEC 27001 :2005;

c) výběr cílů opatření a jednotlivých opatření v závislosti na procesech hodnocení a zvládání rizik;

d) přezkoumání efektivnosti ISMS a měření efektivnosti bezpečnostních opatření, hlášení a přezkoumávání stavu oproti stanoveným cílům ISMS;

e) interní audity ISMS a přezkoumání vedením organizace; f) odpovědnost vedení za bezpečnostní politiku;

g) soulad mezi vybranými a implementovanými opatřeními, prohlášením o aplikovatelnosti, výsledky procesů hodnocení a zvládání rizik, politikou a cíli ISMS;

h) implementaci opatření (viz Příloha D), S ohledem na měření jejich efektivnosti (viz bod d) výše) S cílem určit zda jsou opatření implementována a zda jsou účinná pro dosahování stanovených cílů;

i) ověření toho, že jsou programy, procesy, postupy, záznamy, interní audity a přezkoumání efektivnosti ISMS dohádatelné v záznamech o rozhodnutích učiněných vedením a v souladu s cíli a politikou ISMS.

- **Specifické prvky ISMS auditu**

Role certifikačního orgánu je v určení toho, zda mají organizace klientů zaveden konzistentní přístup pro identifikaci, posouzení a vyhodnocení hrozeb, zranitelností a dopadů na aktiva organizace. Certifikační orgán musí:

a) požadovat, aby organizace demonstrovala, že provedená analýza hrozeb je relevantní a dostačující prostředí organizace;

POZNÁMKA Organizace je odpovědná za definici kritérií, podle kterých jsou identifikována významná bezpečnostní rizika a za vytvoření postupů jejich identifikace.

b) ustanovit zda postupy pro identifikaci, posouzení a vyhodnocení hrozeb působících na aktiva, zranitelností vůči těmto hrozbám a dopadů jsou konzistentní s politikou a cíli organizace.

Certifikační orgán musí také určit, zda postupy použité pro analýzu důležitosti (významu) jsou ověřené a řádně implementované. Pokud jsou hrozby, zranitelnosti nebo dopady vyhodnoceny jako významné musí být zvládány v rámci ISMS.

- **Shoda se zákonnými a regulatornimi požadavky**

Za určení a dodržování shody se zákonnými a regulatorními požadavky je odpovědná organizace klienta. Certifikační orgán se pouze omezí na to, aby zkontroloval a ověřil,

že ISMS v tomto ohledu řádně funguje. Certifikační orgán musí ověřit, že organizace má nastaven systém řízení tak, aby naplňovala zákonné a regulatorní požadavky s ohledem na identifikovaná rizika bezpečnosti informací a možné dopady.

- **Integrace dokumentace ISMS s dokumentací ostatních systémů řízení**

Organizace klienta může sloučit dokumentaci ISMS s dokumentací dalších systémů řízení jako je systém řízení kvality, systém bezpečnosti a ochrany zdraví při práci,

Certifikační orgán může nabídnout pouze certifikaci ISMS, případně může nabídnout i certifikaci ISMS spojenou s certifikací dalších systémů řízení.

Audit ISMS může být spojen s audity dalších systémů řízení. Takové spojení auditů je možné provést, pokud lze doložit, že audit splňuje veškeré požadavky pro certifikaci ISMS. Všechny požadavky důležité pro audit ISMS, musí být součástí auditní zprávy a ve zprávě snadno identifikovatelné. Kvalita auditu ISMS nesmí být nepříznivě ovlivněna spojením s dalšími audity.

POZNÁMKA ISO 19011 poskytuje doporučení pro provedení kombinovaných auditů systémů řízení.

- **Informace pro udělení úvodní certifikace**

Jako podklad pro objektivní rozhodnutí o udělení certifikace, musí certifikační orgán vyžadovat přehledné auditní zprávy, na základě kterých je možné učinit konečné rozhodnutí.

Auditní tým předává certifikačnímu orgánu zprávy z jednotlivých fází certifikačního auditu. Kromě základních informací by auditní zprávy měly minimálně obsahovat informace požadované v IS 9.1.6.

- **Certifikační rozhodnutí**

Entita certifikačního orgánu, může se jednat i o jednotlivce, která učiní rozhodnutí o udělení/odebrání certifikace, by měla mít dostatečnou úroveň znalostí a zkušeností ve všech oblastech tak, aby mohla zodpovědně vyhodnotit průběh auditu a doporučení předaná auditním týmem.

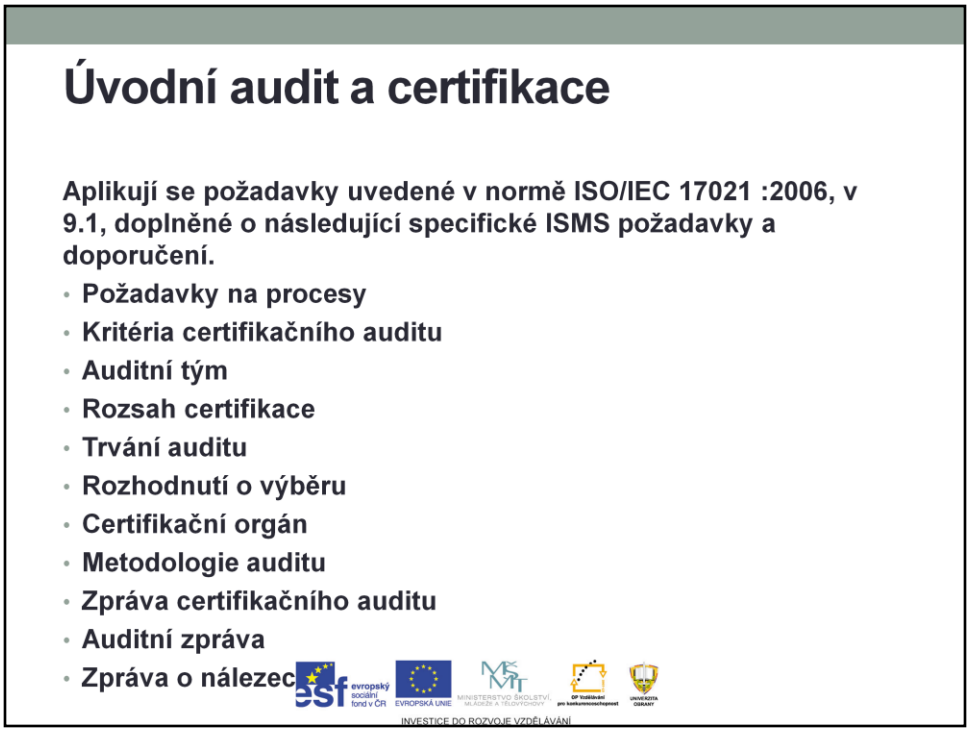
Rozhodnutí o udělení certifikace musí být přijato na základě informací shromážděných v průběhu certifikačního procesu a jakýkoliv dalších relevantních informací. Rozhodnutí o udělení certifikace nesmí být učiněno těmi, kteří se účastnili auditu. Rozhodnutí musí být založeno na zjištěních a doporučeních auditního týmu, která jsou obsažena v auditní zprávě (viz IS 9.1.6) a na dalších relevantních informacích dostupných certifikačnímu orgánu.

Entita, která činí rozhodnutí o udělení certifikace, by normálně neměla zvrátit

negativní doporučení ze strany auditního týmu. Pokud však přesto takováto situace nastane, musí certifikační orgán podrobně zdokumentovat a odůvodnit své rozhodnutí.

Norma ISO/IEC 17021 neuvádí konkrétní periodu, v jaké by měly být prováděny interní audity ISMS nebo přezkoumání ISMS vedením. Certifikační orgán však může tuto periodu stanovit. Bez ohledu na to zda certifikační orgán tuto periodu stanovil, musí zavést metriky pro měření efektivnosti prováděných interních auditů ISMS a přezkoumání ISMS vedením.

Certifikace nesmí být organizaci udělena do té doby, než organizace doloží, že má zavedeny postupy pro provádění interních auditů ISMS a pro přezkoumání ISMS vedením organizace, a že jsou tyto postupy účinné a budou nadále udržované.



Požadavky na procesy

- **Obecné požadavky**

Aplikují se požadavky uvedené v normě ISO/IEC 17021 :2006, v 9.1, doplněné o následující specifické ISMS požadavky a doporučení.

Kritéria certifikačního auditu

Kritéria, vůči kterým je prováděn audit ISMS klienta, musí být ta, která jsou uvedena v normě ISO/IEC 27001 a ostatních dokumentech požadovaných pro certifikaci a relevantních k vykonávaným činnostem. V případě, že je požadováno vysvětlení, pokud se týče aplikace těchto dokumentů na specifický certifikační program, musí být toto vysvětlení podáno příslušnou nestrannou komisí nebo osobami, které mají nezbytné technické znalosti a zveřejněno certifikačním orgánem.

Politiky a postupy

Dokumentace certifikačního orgánu musí zahrnovat politiku a postupy pro implementaci certifikačního procesu, včetně kontrol použití a aplikace dokumentace použité během certifikace ISMS a kontrol postupů auditu a certifikace.

Auditní tým

Auditní tým musí být formálně ustanoven a vybaven odpovídajícími pracovními dokumenty. Plán a datum auditu musí být s organizací klienta předem dohodnut. Pověření, které je dáno auditnímu týmu, musí být jasně definováno a sděleno organizaci klienta a vyžaduje od auditního týmu, aby prozkoumal strukturu, politiky a postupy organizace a potvrdil, že splňují všechny relevantní požadavky dané rozsahem certifikace, a že implementované postupy zaručují důvěru v ISMS organizace.

- **Rozsah certifikace**

Auditní tým musí provést audit ISMS organizace oproti všem certifikačním požadavkům platným ve stanoveném rozsahu. Certifikační orgán musí zajistit, že jsou rozsah a hranice ISMS organizace jasně definovány s ohledem na povahu činností, na specifika organizace, její polohu, aktiva a technologie. Certifikační orgán musí potvrdit, že v rozsahu certifikovaného ISMS organizace klienta splňuje požadavky v 1.2 normy ISO/IEC 27001 :2005.

Certifikační orgán musí zajistit, že proces hodnocení a zvládání rizik v prostředí organizace pokrývá aktivity a jejich hranice tak, jak požaduje norma ISO/IEC 27001. Certifikační orgán musí potvrdit, že se tak děje v souladu s definovaným rozsahem ISMS organizace a že je to promítnuto do prohlášení o aplikovatelnosti.

Certifikační orgán musí zajistit, že rozhraní na služby nebo činnosti, které nejsou zcela v rozsahu ISMS, jsou předmětem posouzení v průběhu certifikace a jsou zahrnuté do hodnocení rizik bezpečnosti informací organizace. Příkladem takovéto situace je

sdílení vybavení (tj. IT systémů, databází a telekomunikačních systémů) s dalšími organizacemi.

- **Trvání auditu**

Certifikační orgán musí poskytnout auditorům dostatečný čas k provedení všech činností vážících se k úvodnímu, dohledovému nebo recertifikačnímu auditu. Vyhrazený čas by měl stanoven na základě následujících faktorů:

a) rozsahu ISMS (například počtu používaných informačních systémů, počtu zaměstnanců);

b) komplexnosti ISMS (například kritičnosti informačních systémů, rizikovosti ISMS);

c) typu vykonávaných činností v rozsahu ISMS;

d) rozsahu a různorodosti technologií použitých při implementaci různých součástí ISMS jako jsou implementovaná opatření, dokumentace a/nebo kontrola procesů, nápravná/preventivní opatření, apod.);

e) počtu pracovišť;

f) již demonstrovaném fungování ISMS;

g) rozsahu outsourcingu a ujednání o využití služeb třetích stran v rámci ISMS;

h) aplikovatelných norem a předpisů, které jsou relevantní pro rozsah certifikace.

Certifikační orgán musí být připraven odůvodnit nebo ospravedlnit množství času potřebného k provedení úvodního, dohledového nebo recertifikačního auditu.

- **Rozhodnutí o výběru**

Rozhodnutí o výběru vzorových pracovišť je v případě certifikace ISMS složitější než

stejné rozhodnutí u certifikací systémů řízení kvality. V případě, že má organizace klienta více pracovišť splňujících kritéria uvedená níže v bodech a) až c), může certifikační orgán rozhodnout o provedení auditu na reprezentativním vzorku pracovišť:

a) všechna pracoviště organizace klienta operují pod stejným ISMS, který je centrálně spravovaný a auditovaný a je předmětem přezkoumání vedením;

b) všechna pracoviště organizace klienta jsou zahrnuta do programu interního auditu ISMS;

c) všechna pracoviště organizace klienta jsou zahrnuta do programu přezkoumání vedením.

- **Certifikační orgán**

Certifikační orgán, který chce provést audit na reprezentativním vzorku pracovišť, musí mít zavedeny postupy zajišťující následující:

a) Během úvodního přezkoumání smlouvy musí být v maximální možné míře identifikovány rozdíly mezi jednotlivými pracovišti tak, aby mohl být vybrán vhodný reprezentativní I/zorek.

b) Při výběru reprezentativního počtu pracovišť bylo bráno v úvahu následující:

1. výsledky interních auditů centrály a jednotlivých pracovišť,
2. výsledky přezkoumání vedením;
3. rozdíly ve velikostech jednotlivých pracovišť;
4. rozdíly v činnostech jednotlivých pracovišť;

5. složitosti ISMS;
6. složitosti informačních systémů na jednotlivých pracovištích;
7. rozdíly v pracovních postupech;
8. rozdíly v prováděných činnostech;
9. potenciální interakce s kritickými informačními systémy nebo s informačními systémy zpracovávajícími citlivé informace;
10. jakékoliv odlišnosti od zákonných požadavků.

c) Reprezentativní vzorek je vybrán ze všech pracovišť v rozsahu ISMS organizace; tento výběr by měl být

založen na kritickém posouzení, které odráží jak faktory uvedené v bodě b), tak i jiné náhodné elementy.

d) Každé pracoviště v rozsahu ISMS, které podléhá významným rizikům je předmětem auditu certifikačním orgánem dříve, než je udělena certifikace.

e) Dohledový program byl navržen S ohledem na výše uvedené požadavky a pokrývá všechna pracoviště organizace nebo ta, která spadají do rozsahu certifikovaného ISMS a jsou tedy zahrnuta do certifikace.

f) V případě, že je zjištěna neshoda, a to bud' v centrále anebo na některém pracovišti, jsou přijata nápravná opatření v centrále a všech pracovištích z daného vzorku.

Audit popsaný v IS 9.1.5 musí zahrnovat činnosti v centrále organizace tak, aby byl zajištěn jeden ISMS aplikovatelný pravšechna pracoviště a dodává centrální

správní na operační úrovni. Audit musí adresovat všechny výše zmíněné body.

- **Metodologie auditu**

Certifikační orgán musí mít postupy, které zajistí, aby organizace klienta byla schopna demonstrovat, že má naplánovány interní audity ISMS, a že plán i postupy jsou funkční a jejich funkčnost může být předvedena.

Postupy certifikačního orgánu by neměly předem předpokládat konkrétní způsob implementace ISMS nebo konkrétní formát pro dokumentaci a záznamy. Certifikační postupy se musí zaměřit na prokázání toho, že ISMS organizace splňuje požadavky normy ISO/IEC 27001 a požadavky politik a cílů organizace.

Plán auditu by měl identifikovat auditní techniky využívající síťových služeb, které bude vhodné během auditu využít.

POZNÁMKA Auditní techníky využívající síťových služeb mohou například zahrnovat telekonference, web meetingy, inter- aktivní internetové komunikace a vzdálený přístup k dokumentaci a/nebo procesům ISMS. Tyto techniky by se měly zaměřit na zvýšení efektivnosti a účínnosti auditu a měly by podporovat integritu audítního procesu.

- **Zpráva certifikačního auditu**

Certifikační orgán si může vytvořit vlastní postupy pro podávání zprávo výsledcích auditu tak, aby vyhovovaly jeho potřebám, minimálně však musí být zajištěno následující:

a) předtím než auditní tým ukončí posuzování na místě a opustí prostory organizace, setká se s vedením organizace a poskytne mu následující:

1) písemnou nebo ústní informaci o shodě ISMS organizace s

konkrétními požadavky na certifikaci,

2) příležitost k dotazům ohledně auditních nálezů;

b) auditní tým předá certifikačnímu orgánu auditní zprávu, která obsahuje výsledky zkoumání shody ISMS organizace s požadavky na certifikaci.

Auditní zpráva

Auditní zpráva by měla obsahovat následující informace:

a) záznam z auditu včetně závěrů z přezkoumání dokumentace;

b) záznam z certifikačního auditu o tom, že organizace provedla analýzu informačních rizik;

c) celkovou délku auditu, včetně detailní specifikace času stráveného na přezkoumání dokumentace,

posouzení provedené analýzy rizik, při auditu na místě a vypracování auditní zprávy;

d) šetření, která byla během auditu provedena, odůvodnění pro jejich výběr a použitá metodologie.

- **Zpráva o nálezech auditu**

Zpráva o nálezech auditu předaná certifikačnímu orgánu musí obsahovat dostatečnou úroveň detailu tak, aby podpořila rozhodování o udělení certifikace, zejména pak:

a) oblasti pokryté auditem (tj. certifikační požadavky a pracoviště, která byla předmětem auditu), včetně významných auditních záznamů a použité metodologie (viz IS 9.1.5);

b) učiněná pozorování a to jak pozitivní (například pozoruhodné úsilí), tak i negativní (tj. potencionální neshody);

c) podrobnosti o všech identifikovaných neshodách, podpořené objektivními důkazy, včetně odkazů na konkrétní požadavky normy ISO/IEC 27001 nebo na požadavky dalších relevantních dokumentů potřebných pro udělení certifikace;

d) vyjádření o shodě ISMS organizace s certifikačními požadavky, včetně přesné identifikace zjištěných neshod, odkazu na verzi prohlášení o aplikovatelnosti a tam, kde to je vhodné, srovnání s výsledky předchozích certifikačních auditů.

Vyplněné dotazníky, kontrolní seznamy, pozorování, záznamy nebo poznámky auditora mohou tvořit nedílnou část auditní zprávy. Jestliže jsou tyto metody použity, musí být jejich výstupy předloženy certifikačnímu orgánu pro podporu rozhodnutí o udělení certifikace. Informace o hodnocených vzorových pracovištích by měla být zahrnuta do auditní zprávy nebo jiné dokumentace z certifikace.

Auditní zpráva

Auditní zpráva musí posoudit přiměřenost interní organizace a osvojených postupů tak, aby dávaly dostatečnou důvěru v provozovaný ISMS.

Kromě požadavků uvedených v ISO/IEC 17021 :2006, v 9.1.10, by auditní zpráva měla pokrývat:

-stupeň důvěry, která může být vložena na interní audity ISMS a přezkoumání vedením organizace;

-přehled nejdůležitějších pozorování, pozitivních i negativních, týkajících se implementace a efektivnosti

ISMS;

-doporučení auditního týmu o udělení/neudělení certifikace ISMS, včetně informací zdůvodňujících toto doporučení.

ZÁVĚR

Po prostudování uvedené přednášky a doporučené literatury budou studenti chápat:

- ✓Objasnění pojmů audit a certifikace;
- ✓Konflikt zájmů ;
- ✓Analýza odborné způsobilosti a smluvní závazky;
- ✓Odborná způsobilost k provedení činností;
- ✓Oprávnění personálu;
- ✓Školení auditního týmu;
- ✓Požadavky na procesy;
- ✓Úvodní audit a certifikace;

Dotazy?

pplk. Ing. Radek Dubec, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra celoživotního vzdělávání
E-mail.: radek.dubec@unob.cz

Dotazy?