INFORMACE PRO ŽADATELE / DRŽITELE CERTIFIKÁTŮ

Systém managementu bezpečnosti informací – ISMS

ISO/IEC 27001:2022

ÚVOD

Vážení zákazníci,

chceme-li uspět na náročných světových, evropských i českých trzích v době neustále rostoucí konkurence, musíme si být vědomi, že tento proces vyžaduje trvalé zvyšování a prokazování kvality výrobků, kvality služeb i znalostí Vašich pracovníků, při současné minimalizaci negativních dopadů do životního prostředí a omezování veškerých druhů rizik.
Získat důvěru vašich stávajících i potencionálních zákazníků vám pomůže certifikát prokazující způsobilost Vaší organizace i Vašich pracovníků. V celém světě, Evropě i v naší republice neustále roste počet organizací a pracovníků, kteří absolvovali proces certifikace podle různých mezinárodních standardů. Naše zkušenosti aplikované u rozšiřujícího se počtu klientů, nás přesvědčují o tom, že certifikace je dobrou investicí do budoucnosti. Proto se při realizaci našich certifikačních služeb, řídíme zásadou: ***„Vysoká odbornost – objektivnost – za přijatelnou cenu – při maximální efektivnosti“.***

Naším cílem je dosáhnout maximálních pozitivních efektů pro Vaši organizaci, zvýšit prestiž Vaší organizace v pohledu Vašich zákazníků externích, ale i interních a usnadnit komunikaci s orgány státní správy či kontrolních nebo inspekčních orgánů. Smyslem auditu pro nás je v komunikaci se zákazníkem vyhledávat potenciály ke zlepšení efektivnosti firemních procesů s využitím přenosu zkušeností z jiných firem, nikoliv vyhledávání chyb a neshod v dokumentaci systému.

Služby certifikačního orgánu jsou poskytovány s cílem dosažení jejich špičkové evropské úrovně, a to jak po stránce odborné, tak i organizační a v souladu se světovým trendem poskytovat klientovi nejenom vlastní konstatování o shodě, či neshodě, ale rovněž přidanou hodnotu ve formě konstatování silných a slabých stránek a potenciálů pro zlepšení.

Certifikační orgán pro certifikaci systémů managementu č. 3027 CERT-ACO, s.r.o. Kladno je akreditován k certifikaci systémů managementu národním akreditačním orgánem, tj. Českým institutem pro akreditaci, o.p.s. (dále jen ČIA). Disponuje vysoce kvalifikovanými auditory a experty. Auditoři jsou držiteli českých i evropských akreditovaných personálních certifikátů. Úzce spolupracujeme při certifikaci systémů managementu s jinými nadnárodními mezinárodními certifikačními orgány.

Certifikáty vydávané certifikačním orgánem CERT-ACO, s.r.o. prokazují, že systém managementu je zaveden, dokumentován, používán a udržován v souladu s příslušnou normou. Platnost certifikátů je stanovena na ***3 roky*** po úspěšném absolvování (re) certifikačního auditu. V průběhu platnosti certifikátu jsou každý rok plánovány dozorové (kontrolní) roční audity.

Certifikáty jsou vystavovány v rámci platné akreditace, proto mají mezinárodní platnost a plnohodnotnost v souladu s uzavřenými multilaterálními dohodami o uznávání certifikátů (MLA) uzavřenými na úrovni Evropy (EA - European Organisation for Accreditation) i na úrovni celosvětové (IAF - International Accreditation Forum).

Předkládáme Vám základní informace o procesu certifikace systémů managementu, v tomto případě ***systému managementu kvality ISMS***. Pokud se rozhodnete pro certifikaci u našeho certifikačního orgánu, přeji Vám mnoho úspěchů a věřím, že získaný certifikát bude základním podkladem pro zlepšení všech činností ve Vaší organizaci, pro zvýšení konkurenceschopnosti a ekonomického profitu, a že bude základem na cestě k trvalé úspěšnosti „Excellence".

Účelem tohoto dokumentu je v souladu s požadavky na akreditovaný certifikační orgán podle normy ISO/IEC 17021-1 tj. poskytnout podrobný popis prvotní certifikace a návazných činností, včetně žádosti, úvodních auditů, dozorových auditů a procesů udělení a udržování certifikace, rozšíření nebo omezení rozsahu certifikace, obnovení, pozastavení nebo obnovení platnosti nebo odnětí certifikace; sdělit normativní požadavky na certifikaci; dokumentovat popis práv a povinnosti certifikovaných klientů, včetně požadavků na odkazování na certifikaci při komunikaci jakéhokoli druhu; informovat o postupech vyřizování stížností a odvolání.

1 KONTAKT

Název: CERT – ACO, s.r.o.
Adresa: Huťská 229
CZ - 272 01 Kladno
Tel.: + 420 702 163 520
E-mail: ondekova@cert-aco.cz
Web site: http://www.cert-aco.cz

2 ZÁKLADNÍ INFORMACE – CERTIFIKACE ISMS

Norma určená k posuzování shody (certifikační norma):
ISO/IEC 27001 - Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

2.1 VŠEOBECNÁ PRÁVA A POVINNOSTI ŽADATELŮ O CERTIFIKACI / CERTIFIKOVANÝCH ORGANIZACÍ

Povinnosti:

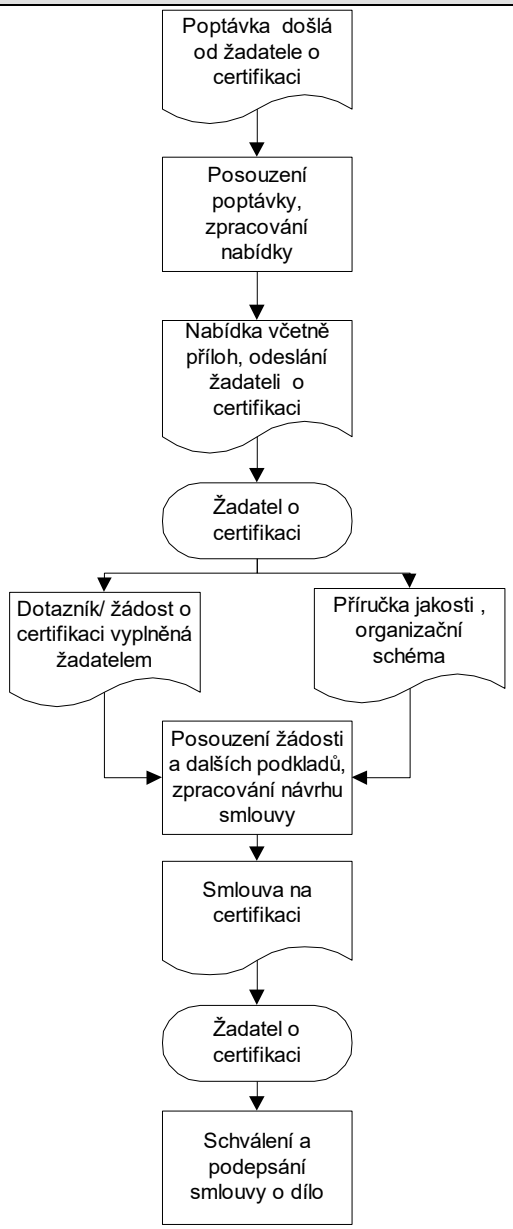
- řádně pověřeným zástupcem žadatele oficiálně na formuláři *„dotazník / žádost o certifikaci“* požádat o provedení certifikace
- přesně definovat rozsah certifikace (provozovny, organizační jednotky, procesy, výrobky)

- poskytnout všeobecné údaje o žadateli (název, adresa, organizační struktura, zdroje)
- poskytnout informace o systému bezpečnosti dat (popis systému, norem a jiných normativních dokumentů, kterých se v jednotlivých případech využívá)
- poskytnout a udržovat aktuální výtisk příručky bezpečnosti dat, vytvořit postup pro zajištění toho, aby informace poskytnuté certifikačnímu orgánu byly udržovány v aktuálním stavu
- zavázat se k vyhovění požadavkům na certifikaci a přístup auditorů k informacím, které slouží k posouzení shody systému bezpečnosti dat s požadavky normy
- předložit všechny informace nezbytné k hodnocení
- vést záznamy a evidenci všech stížností a opatření k nápravě vztahujících se k systému bezpečnosti dat a předkládat je při kontrolním auditu.

2.2 Práva:

- být seznámen s podmínkami pro udělení certifikace (postupem posuzování a certifikace)
- být seznámen s podmínkami dozoru a opakované certifikace
- být seznámen s finančními podmínkami certifikace
- být informován o složení skupiny auditorů a vznášet proti nim námitky
- být seznámen s pravidly používání certifikátů a certifikační značky
- zachování důvěrnosti informací o žadateli na všech úrovních certifikačního orgánu
- podat odvolání proti rozhodnutí certifikačního orgánu
- informovat zákazníky a dodavatele o všech nebo dílčích informacích o certifikaci
- užívat certifikát a certifikační značku
- uvést v dotazníku/žádosti jazyk, ve kterém bude veden audit, není-li specifikována jednací řeč, je jí jazyk český.

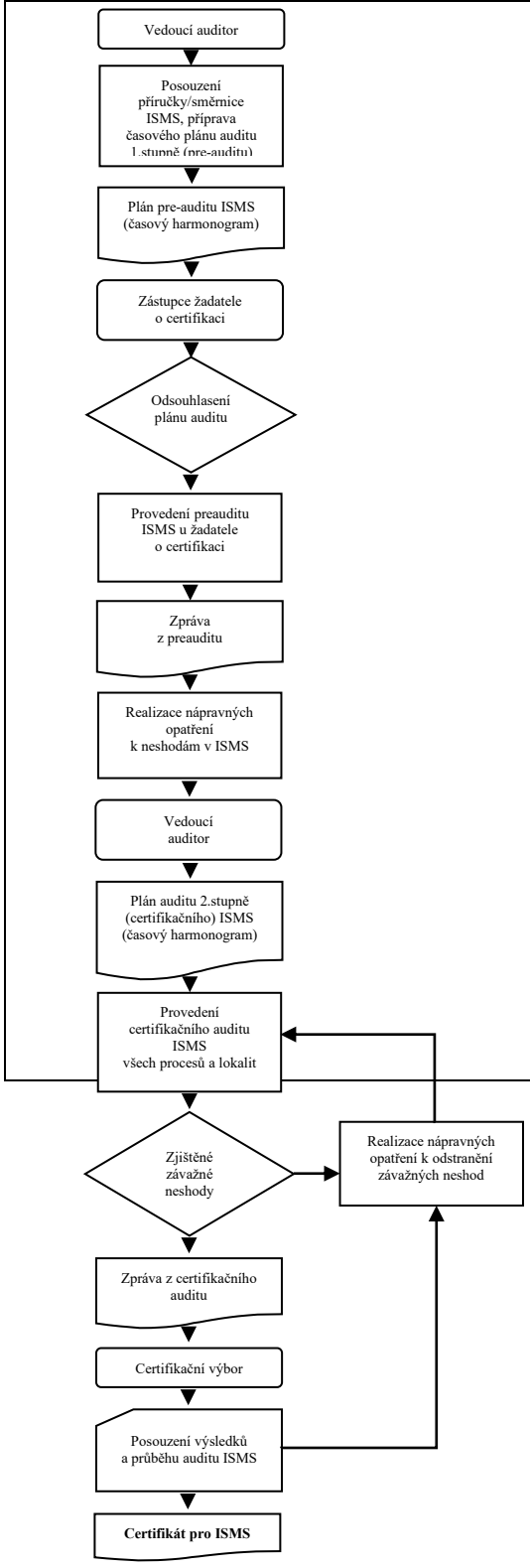
3. POSTUP OBJEDNÁNÍ CERTIFIKACE, UZAVŘENÍ SMLOUVY O DÍLO

Flowchart	*Komentář*
	Poptávka musí obsahovat alespoň základní informace o žadateli (počet lokalit, počet zaměstnanců, obor a procesy pro které je systém bezpečnosti dat implementován, předpokládaný termín certifikace) Poptávka je posouzena, zda obsahuje veškeré potřebné informace nutné k vypracování nabídky. V případě potvrzení způsobilosti je zpracována nabídka. Nabídka vždy obsahuje předpokládaný rozsah auditů, cenu, platební podmínky, postup certifikace. Nedílnou součástí jsou přílohy „Informace pro žadatele o certifikát“ a „Žádost o certifikaci / dotazník“. Žadatel o certifikaci v případě akceptování podmínek uvedených v nabídce vyplní „Žádost o certifikaci / dotazník“, kde detailněji specifikuje rozsah certifikovaného systému. K posouzení, zda uvedené údaje jsou pravdivé a úplné slouží nezbytné přílohy tj. příručka bezpečnosti dat (specifikující organizační strukturu, procesy a jejich vztahy, odpovědnosti). „Žádost o certifikaci/ dotazník“ je certifikačním orgánem považován za závaznou objednávku. Údaje uvedené v „Žádosti o certifikaci/ dotazníku“ jsou posouzeny z pohledu jejich shody s poptávkou a je vypracován návrh smlouvy o dílo na certifikaci. Tento návrh je odeslán žadateli o certifikaci (podle požadavků – nebo e-mailem). V případě akceptování podmínek ve smlouvě o dílo, tuto schválí a podepíší statutární zástupci obou stran. Certifikačním orgánem je určen auditorský tým, který bude posuzování (audit) systému provádět. Vedoucí auditor kontaktuje představitele vedení pro systém bezpečnosti dat žadatele a společně plánují harmonogram následných činností.

3.1 PODMÍNKY PRO ZAHÁJENÍ CERTIFIKAČNÍHO PROCESU

- Organizace přiměřeně zdokumentovala systém managementu bezpečnosti dat (ISMS) v příručce nebo v souboru dokumentace minimálně v rozsahu požadovaném v prvku 4.3 normy pro systém managementu bezpečnosti dat
- Organizace stanovila rozsah a hranice implementovaného ISMS v dokumentu „Rozsah realizovatelnosti“.
- Stanovila a vyhlásila politiku ISMS.
- Provedla analýzu rizik v oblasti bezpečnosti dat a nastavila management rizik.
- Organizace identifikovala a ocenila svá informační aktiva
- Organizace formulovala plán zvládání rizik, vymezila odpovídající řídící činnosti, priority a odpovědnosti pro ISMS.
- Organizace identifikovala možné hrozby těmto aktivům a nastavila opatření k eliminaci těchto hrozeb,
- Organizace provedla interní audity všech lokalit, procesů a realizovala účinná nápravná opatření k odstranění neshod.
- Organizace provedla monitorování a úplné přezkoumání systému bezpečnosti dat vedením (management review).

3.2 SCHÉMA POSTUPU POSUZOVÁNÍ A CERTIFIKACE

Flowchart	*Komentář*
	Vedoucí auditor prostuduje žadatelem předloženou příručku resp. dokumentaci popisující systém, popř. si může vyžádat návaznou dokumentaci popisující vybrané postupy systému bezpečnosti dat. Vedoucí auditor vypracuje návrh plánu auditu 1.stupně (pre-audit), který obsahuje termín, časový harmonogram, posuzované lokality, posuzované organizační jednotky, posuzované procesy a cíle auditu. Žadatel o certifikaci s časovým předstihem dostává plán auditu 1.stupně (pre-auditu) k odsouhlasení, v případě jeho akceptování jej potvrzený předává vedoucímu auditorovi. V případě potřeby upravit plán auditu je tento vedoucím auditorem přizpůsoben v rámci časových možností. Audit 1.stupně (pre-audit) probíhá ve formě interview s odpovědnými osobami za jednotlivé části systému a procesy. Auditor je povinen posoudit veškerou dokumentaci a záznamy tak, aby bylo prokázáno splnění cíle auditu 1.stupně (pre-auditu), který je uveden níže v textu.

	Veškerá zjištění jsou auditorem zaznamenána ve zprávě z auditu, která je předána zástupci posuzované společnosti. Zpráva obsahuje závěry, zda je možno přistoupit k auditu 2.stupně (certifikačnímu) a v jakém termínu. Jestliže při auditu 1.stupně (pre-auditu) nejsou konstatována zjištění, která by potenciálně znamenala „neshody“ je možno audit 2.stupně (certifikační) provést do 2 týdnů po auditu 1.stupně (pre-auditu). V případě zjištěných “potenciálních neshod“ a konstatování nepřipravenosti, musí společnost přijmout nápravná opatření k jejich účinnému odstranění a proces pokračuje opakovaně auditem 1.stupně. Maximální doba na odstranění neshod jsou 3 měsíce. Vedoucí auditor vypracuje návrh plánu auditu 2.stupně (certifikačního), který obsahuje termín, časový harmonogram, posuzované lokality, posuzované organizační jednotky, posuzované procesy a cíle auditu. Plán odsouhlasí zástupce posuzované společnosti. Certifikační audit probíhá ve formě interview, testování, vizuální inspekce s odpovědnými osobami za jednotlivé části systému a procesy. Auditor je povinen posoudit stupeň implementace systému tak, aby byl prokázán cíl auditu, který je uveden níže v textu. V případě zjištěných “neshod“ jsou tyto zaznamenány ve formě „protokolu neshod“, v němž musí společnost přijmout nápravná opatření k jejich účinnému odstranění. Účinnost přijatých opatření je doložena vedoucímu auditorovi. Maximální doba na odstranění neshod jsou 3 měsíce. Veškerá zjištění jsou auditorem zaznamenána ve zprávě z auditu, která je předána zástupci posuzované společnosti. Zpráva obsahuje závěry, zda je možno potvrdit shodu s kriteriální normou pro systém managementu bezpečnosti dat. Zpráva též stanovuje termín a rozsah kontrolního auditu. Nedílnou součástí je odsouhlasený text certifikátu. Vedoucí auditor předkládá podklady certifikačnímu výboru, který s konečnou platností rozhoduje o vystavení certifikátu.

	Certifikát resp. certifikáty ve zvolených jazykových mutacích jsou slavnostně předány zástupci certifikované společnosti. Platnost certifikátů je omezena na 3 roky.

3.3 Cíle auditu 1.stupně (pre-auditu):

Získat informace, potřebné pro naplánování certifikačního auditu. Seznámit se s ISMS (systém managementu bezpečnosti dat) ve vztahu k všem popsaným informačním aktivům i s možností jejich selhání a zejména s připraveností na audit, že přezkoumá, do jaké míry:

- ISMS zahrnuje odpovídající postup pro zajištění bezpečnosti dat služeb, výrobků a činností dle ISO/IEC 27001.
- je ISMS koncipován tak, aby dosáhl cílů politiky bezpečnosti dat a informací organizace
- způsob zavedení ISMS opravňuje přikročit k certifikačnímu auditu
- interní audit odpovídá požadavkům normy, specifikující požadavky na ISMS
- přezkoumat dokumentaci a informace, které je třeba získat před certifikačním auditem

Dokumentace při preauditu musí přinést následující informace:

- seznam křížových odkazů na příslušné požadavky norem, specifikující požadavky na ISMS
- popis organizace a postupů, hodnocení rizik bezpečnosti informací
- popis prostředků, zabezpečující neustálé zlepšování
- programy a zprávy z interních auditů a přezkoumání vedením organizace

Další důležité informace – záznamy posuzované při preauditu:

- záznamy prokazující splnění požadavků kladených na systém bezpečnosti dat
- podrobnosti o interně zjištěných neshodách, včetně podrobností o odpovídajících nápravných a preventivních opatřeních, která byla přijata během posledních 12 měsíců (nebo od počátku zavedení ISMS min. 3 měsíce)
- záznamy o přezkoumání vedením
- hodnocení a zvládání rizik, akceptaci zbytkových rizik, prohlášení o aplikovatelnosti
- odpovědnost vedení za bezpečnostní politiku
- záznamy o jakýchkoliv sděleních (stížnostech) týkajících se ISMS a o všech opatřeních přijatých na základě těchto sdělení

Cíl auditu 2.stupně (certifikačního):

- Přezkoumat odstranění neshod zjištěných při preauditu a účinnost přijatých opatření.
- Přezkoumat, zda ISMS aplikuje odpovídající postupy pro zajištění bezpečnosti dat a informací, ve vztahu ke všem zákazníkům na praktických ukázkách realizovaných zakázek.

- Přezkoumat odpovědnost vedení za bezpečnostní politiku organizace
- Přezkoumat, zda ISMS je nastaven tak, že jsou naplňovány zákonné a regulatorní požadavky s ohledem na identifikovatelná rizika bezpečnosti informací.
- Přezkoumání, zda ISMS dosahuje cílů a cílových hodnot bezpečnostní politiky organizace a způsob zavedení ISMS opravňuje vystavit certifikát.
- Prokázat, že jsou efektivně využívány prostředky, zabezpečující neustálé zlepšování.
- Přezkoumat, že programy a zprávy z interních auditů prokazují účinnost při hledání a odstraňování neshod v ISMS.
- Přezkoumat podrobnosti o interně zjištěných neshodách, včetně podrobností o odpovídajících nápravných a preventivních opatřeních, která byla přijata během posledních 12 měsíců (nebo od počátku zavedení ISMS min. 3 měsíce).
- Přezkoumat záznamy o přezkoumání vedením.
- Přezkoumat záznamy o jakýchkoliv sděleních (stížnostech) týkajících se ISMS a o všech opatřeních přijatých na základě těchto sdělení.
- Přezkoumat do jaké míry jsou procesy efektivní, zdali je dosahováno neustálého zlepšování spokojenosti zákazníků
- Přezkoumat soulad mezi vybranými a implementovanými opatřeními, prohlášení o aplikovatelnosti, výsledky procesů, hodnocení a zvládání rizik, politikou a cíli ISMS
- Přezkoumat, že programy, procesy, postupy, záznamy, interní audity a přezkoumání efektivnosti ISMS jsou dohledatelné v záznamech o rozhodnutích učiněných vedením a v souladu s cíli a politikou ISMS
- Přezkoumat, že provedená analýza hrozeb je relevantní a dostačující prostředí organizace a hrozby působící na aktiva jsou identifikovány posouzeny a hodnoceny a jejich dopady jsou konsistentní s politikou a cíli organizace

Certifikační orgán poskytuje přiměřené časové období, nejdéle však 3 měsíce, během kterého musí organizace prokázat, že odstranila zjištěné nedostatky při certifikačním auditu, v opačném případě navrhuje ředitel certifikačního orgánu neudělit certifikát. Podmínky pro udělení certifikátu jsou uvedeny dále.

3.4 DOZOR NAD CERTIFIKOVANÝMI ORGANIZACEMI

Všeobecně:
Pravidelný dozor nad certifikovanou organizací se provádí minimálně 1x ročně formou kontrolního (dohledového) auditu, v případě, že dojde v systému bezpečnosti dat certifikované organizace ke změnám, které vyžadují kontrolu, lze vyvolat i mimořádný kontrolní audit. Certifikační orgán si vyhrazuje právo upravit četnost dozorů podle posouzení stavu systému managementu bezpečnosti dat.

Cíl kontrolního auditu (pravidelného dozoru):

- Přezkoumat, že schválený ISMS je řádně provozován a případné změny v organizaci jsou do ISMS implementovány a
- Přezkoumat, zda ISMS je efektivní a dosahuje cílů a cílových hodnot politiky bezpečnosti dat organizace a způsob zavedení ISMS opravňuje potvrdit platnost certifikátu.
- Přezkoumat fungování postupů, jimiž je vedení informováno o všech porušeních v ISMS.
- Přezkoumat pokrok plánovaných činností zaměřených na zlepšování fungování systému.
- Přezkoumat, že závěry z interních auditů jsou sledovány a prokazují účinnost při hledání a odstraňování neshod v systému.

- Přezkoumat záznamy o jakýchkoliv sděleních (stížnostech, odvoláních a sporech) týkajících se ISMS a o všech opatřeních přijatých na základě těchto sdělení, především tam, kde je riziko, že organizace neplní požadavky na certifikaci. Musí se prokázat, že organizace přezkoumává své systémy a postupy a přijímá vhodná opatření k nápravě.

Program dohledového (kontrolního) auditu vždy obsahuje ověření:
- prvku 5 normy – Odpovědnost vedení – přezkoumání vedením
- prvku 8 normy – Zlepšování, opatření k nápravě a prevenci
- prvku 4.3 - Změny dokumentovaného systému
- prvku 6 - Interní audity bezpečnosti dat z pohledu zabezpečení:
  - efektivnosti systému bezpečnosti dat z hlediska dosahování cílů organizace
  - informovanosti vedení o případech nefunkčnosti postupů
  - trvalého zlepšování systému bezpečnosti dat
  - oblastí ve kterých dochází ke změnám činností a postupů
  - účinné interakce mezi procesy a prvky systému bezpečnosti dat
  - kontroly plnění závěrů interních auditů
  - účinnosti přijatých opatření k nápravě a prevenci
- ověření dalších náhodně vybraných prvků systému managementu bezpečnosti dat tak, aby v tříletém období platnosti certifikátu byly prověřeny všechny procesy/prvky systému
- vypořádání neshod z předchozího auditu ve formě ověření přijatých opatření
- kontrola změn v systému managementu bezpečnosti dat (ve všech oblastech)
- kontrola stížností zákazníků na systém managementu bezpečnosti dat a jejich účinné řešení
- dodržování pravidel používání certifikátů a certifikační značky

Certifikační orgán poskytuje přiměřené časové období, nejdéle však 3 měsíce, během kterého musí certifikovaná organizace prokázat, že odstranila zjištěné nedostatky při kontrolním auditu, v opačném případě navrhuje ředitel certifikačního orgánu odejmutí certifikátů. Podmínky pro potvrzení platnosti certifikátu jsou uvedeny dále.

3.5 OPAKOVANÉ POSUZOVÁNÍ – OPAKOVACÍ AUDIT

Všeobecně:
Platnost certifikátů je 3 roky. Po uplynutí této doby je proveden opakovací audit, za účelem ověření, že systém managementu bezpečnosti dat je trvale řádně zaveden a udržován v celém komplexu požadavků normy.

Cíl opakovacího auditu (recertifikace):

- Ověřit účinnou interakci mezi všemi prvky systému a prokázat závazek udržovat efektivnost systému ISMS.
- Přezkoumat odstranění neshod zjištěných při předchozích auditech a účinnost přijatých opatření.
- Přezkoumání, zda ISMS aplikuje odpovídající postupy pro zajištění bezpečnosti dat služeb, výrobků a činností, ve vztahu ke všem zákazníkům na praktických ukázkách realizovaných zakázek.
- Přezkoumání, zda je ISMS efektivní a dosahuje cílů a cílových hodnot politiky bezpečnosti dat organizace a způsob zavedení ISMS opravňuje vystavit certifikát i z pohledu změn činností.
- Prokázat, že jsou efektivně využívány prostředky, zabezpečující neustálé zlepšování.
- Přezkoumat, že programy a zprávy z interních auditů prokazují účinnost při hledání a odstraňování neshod v systému.

- Přezkoumat podrobnosti o interně zjištěných neshodách, včetně podrobností o odpovídajících nápravných a preventivních opatřeních, která byla přijata během posledních 12 měsíců.
- Přezkoumat záznamy o přezkoumání vedením.
- Přezkoumat záznamy o jakýchkoliv sděleních (stížnostech) týkajících se ISMS a o všech opatřeních přijatých na základě těchto sdělení.
- Přezkoumat do jaké míry jsou procesy efektivní, zdali je dosahováno neustálého zlepšování spokojenosti zákazníků

Program opakovacího auditu:
Program opakovacího auditu vždy obsahuje všechny prvky a procesy systému bezpečnosti dat ve vybraných lokalitách. Kritéria a podmínky pro certifikát jsou shodné s úvodním posuzováním a certifikací včetně termínů pro odstranění neshod. Též činnosti spojené s prověřením dokumentace ISMS jsou provedeny v rámci opakovaného posuzování – opakovacího auditu nikoliv samostatně.

4. PODMÍNKY PRO UDĚLENÍ CERTIFIKÁTU/ POTVRZENÍ PLATNOSTI CERTIFIKÁTU

Dokumentace: Systém managementu bezpečnosti dat musí být popsán vyváženým souborem dokumentace, zastřešenou Příručkou (směrnicí) bezpečnosti dat – I. vrstva, která popisuje způsob řešení všech procesů a prvků systému bezpečnosti dat se zahrnutím požadavků na procesy svařování a související procesy.
Rozsah a hranice ISMS, hodnocení a zvládání rizik, politika ISMS, prohlášení o aplikovatelnosti,
Příručku (směrnici) bezpečnosti dat a vybranou dokumentaci II. vrstvy (požadovanou normou ISO/IEC 27001 je žadatel povinen předložit do 14 dnů před zahájením auditu.

Kritéria (ne)udělení certifikátu: Tým auditorů na základě objektivních zjištění v průběhu auditu o závažnosti případných nedostatků v těchto úrovních:

systémová neshoda:

- prověřovaný systém bezpečnosti dat nebo jeho podstatná část zásadně odporuje požadavkům kriteriálních norem
- chybí část systému, která je podle specifických podmínek prověřované organizace nezbytná pro správnou funkci systému bezpečnosti dat
- existuje velké množství závažných neshod

neshoda:

- nedokonalé zavedení některého požadavku (článku) normy (nedokonalá dokumentace a/nebo nedokonalá implementace)
- neshoda, která by mohla vést k selhání systému bezpečnosti dat nebo ke ztrátě schopnosti zajistit řízené postupy a výrobky
- větší počet drobných neshod u jednoho z požadavků kriteriální normy, jež může pravděpodobně vést k selhání systému

drobná neshoda

- je odchylka od formulace normy, nebo dílčí nedodržení postupu systému, u kterých zkušenost a posouzení ukazují, že nepovede k selhání systému bezpečnosti dat ani schopnosti zajistit řízené postupy a výrobky

Podmínkou pro udělení certifikátu je neexistence systémových neshod a odstranění závažných neshod.

Systémová neshoda:
při zjištění je auditor povinen okamžitě přerušit audit a informovat vedení prověřované společnosti. Skutečnosti jsou protokolovány ve zprávě z auditu a formou *„Protokolů neshod“*. Po odstranění je nutno provést audit znovu, v celém rozsahu formou následného auditu.

Závažná neshoda:
při zjištění je auditor povinen informovat v průběhu závěrečného jednání s vedením prověřované společnosti. Skutečnosti jsou protokolovány ve zprávě z auditu a formou *„Protokolů neshod“.* S žadatelem auditor dohodne termín opatření a postup jejich ověření tj. předložením objektivních důkazů o realizaci nápravných opatření nebo následným auditem prvku normy, kde neshoda zjištěna. Termínem pro odstranění závažných neshod jsou 3 měsíce, při jeho nedodržení je nutno provést audit znovu, v celém rozsahu formou následného auditu.

Drobná neshoda:
při zjištění je auditor povinen je uvést do zprávy z auditu, prověřovaná organizace je povinna je odstranit do doby dozorového (kontrolního) auditu. V případě, že nejsou řešeny, mohou se stát závažnou neshodou.

4.1 PODMÍNKY PRO UŽITÍ CERTIFIKAČNÍ ZNAČKY A CERTIFIKÁTŮ

- Grafická značka je certifikačním znakem CERT-ACO, s.r.o. Kladno. Značku je možné používat v barvě černé.
- Značku CERT-ACO Kladno lze používat jen na dopisních hlavičkových papírech a na podobných dokumentech u služeb poskytovaných v oborech a oblastech činnosti, v té době spadajících pod platný certifikát a po schválení ředitelem CERT-ACO Kladno. Značka nesmí být používána na obalech a výrobcích.
- Umístění značky na dokumentech musí vždy být takové, aby nápis „CERT-ACO“ byl vždy čitelný v horizontální rovině a aby značka nezasahovala do jiné textové části a ani nepřekrývala jiný tisk. Značka má být používána ve spojení s grafickým znakem objednatele a stejně výrazně.
- Předloha značky s číslem certifikátu je zapůjčena společně s příslušným certifikátem. Certifikovaná organizace může kopírovat certifikát (i ve zvětšeném nebo zmenšeném měřítku za předpokladu, že zůstane čitelný v celém původním rozsahu).
- Certifikáty zůstávají majetkem certifikačního orgánu po celou dobu platnosti tj. 3 roky. Za nesprávné použití nebo zneužití certifikátu je považováno přímá vazba na výrobek a tvrzení o jeho zkoušení shody. Za falešné tvrzení je považováno též u certifikované organizace tvrzení, že systém bezpečnosti dat zabezpečuje činnosti spojené s návrhem (vývojem) není–li to uvedeno přímo v textu certifikátu.
- Za zneužití certifikátu se považuje jeho použití v době po uplynutí platnosti resp. v době pozastavení jeho platnosti. V případě zjištění nepovoleného použití je případ projednán a ředitel uplatní vůči certifikované organizaci nápravná opatření tj. zveřejnění opravy.
- Poplatky za užití certifikační značky a za jeden originál certifikátu ve 3 (slovy třech) jazykových mutacích jsou zahrnuty v ceně certifikace.

Certifikační značka pro systém managementu bezpečnosti dat:

5. PODMÍNKY VÝBĚRU MÍST PRO POSUZOVÁNÍ

Má-li organizace více pracovišť, kde všechna operují pod stejným ISMS, který centrálně spravovaný a auditovaný a je předmětem přezkoumání vedením, všechna tato pracoviště jsou zahrnuta do programu interních auditu ISMS a všechna jsou zahrnuta do programu přezkoumání vedením může certifikační orgán rozhodnout o provedení auditu na reprezentativním vzorku pracovišť. Při výběru vzorku pracovišť postupuje certifikační orgán podle IS 9.1.4 normy ISO/IEC 27006

Definice a vymezení pojmů:

a) Místo organizace
Je definováno jako veškeré pozemky, na nichž jsou prováděny činnosti řízené organizací v daném místě včetně skladování surovin, polotovarů, vedlejších produktů, výrobků i odpadů a veškerá zařízení a infrastruktura spojená s těmito činnostmi, bez ohledu na to, zda je s daným místem spojena pevně či nikoliv.
V rámci posuzování ISMS organizace je prověřována místo v plné šíři uvedené definice.

b) Dočasné místo
Jsou např. staveniště, která jsou zahrnuta do ISMS organizace která je řídí, ať již jsou umístěna kdekoliv. V rámci posuzování ISMS organizace je prověřováno místo umístění vedení organizace (to které činnosti v dočasném místě řídí) a minimálně 1. dočasné místo. Výběr dočasného místa pro prvotní posuzování provede vedoucí auditor při 1.stupni auditu náhodným výběrem. Pro kontrolní a opakované posuzování provede výběr místa vedoucí auditor v rámci činností plánování harmonogramu auditu.

c) Místo poskytování služby
Kde není umístění organizace rozhodující je certifikace vztahována k místu umístění vedení včetně jejích činností a k procesu poskytování služby. V rámci posuzování ISMS organizace je prověřováno místo umístění vedení organizace (to které činnosti v dočasném místě řídí) a minimálně 1.místo poskytování služby. Výběr místa poskytování služby provede vedoucí auditor při 1.stupni auditu náhodným výběrem. Pro kontrolní a opakované posuzování provede výběr místa vedoucí auditor v rámci činností plánování harmonogramu auditu.

d) Organizace umístěná na více místech (pobočky)
Činnosti organizace zahrnuté do jediného ISMS jsou prováděny v různých geografických lokalitách.

Varianta č.1–V rámci posuzování ISMS organizace je prověřováno místo umístění vedení organizace (to které činnosti v pobočce řídí) a činnosti v dané pobočce. Výsledkem je certifikát zahrnující pouze činnosti v daném místě (pobočce).

Varianta č.2 - Jestliže organizace vznese požadavek na certifikaci ISMS pod jehož působnost spadá činnost podobných míst spadajících pod jediný ISMS a má být vystaven certifikát zahrnující všechna tato místa. Ředitel pro certifikaci s vedoucím auditorem provede předběžný výběr (potvrdí vedoucí auditor po preauditu – 1.stupni) representativních míst pro posuzování, při splnění podmínek:
- místa splňují a uplatňují jednotný ISMS, který je centrálně řízen, prověřován a podroben přezkoumání vedením
- ve všech místech byl proveden interní audit podle stanovených postupů a opatření byla uplatněna na všech místech

výběr representativních míst a jejich počtu je proveden dle faktorů:
- výsledky interních auditů jednotlivých míst a auditu ústředí (vedení)
- výsledky přezkoumání vedením
- vyzrálost systému ISMS
- dostupné informace o organizaci
- velikosti míst, složitosti míst a složitosti ISMS
- směnnosti provozů, rozmístění pracovníků v jednotlivých místech

- rozdíly v postupech a prováděných činnostech
- opakovatelnost užívaných postupů
- rozdílným právním a jiným předpisům
- zprávy a názory od zainteresovaných stran

Minimální celkový počet prověřených míst – representativních vzorků je:

Počáteční posuzování	počet míst je druhá odmocnina počtu míst (včetně ústředí) zaokrouhlena na vyšší celé místo. ½ míst určuje selektivně ředitel pro certifikaci podle výše uvedených zásad a ½ míst náhodným výběrem vedoucí auditor.
Dozorová návštěva	počet míst je druhá odmocnina počtu míst (včetně ústředí) násobeno koeficientem 0,6 a zaokrouhleno na vyšší celé místo. ½ míst určuje selektivně ředitel pro certifikaci podle výše uvedených zásad a ½ míst náhodným výběrem vedoucí auditor, při respektování požadavku, aby v době platnosti certifikátu nejdéle však v periodě 5 let byla prověřena všechna místa.
Opakované posuzování	počet míst je druhá odmocnina počtu míst (včetně ústředí) zaokrouhlena na vyšší celé místo. V případě, že se systém managementu jakost osvědčil, velikost vzorku může být snížena faktorem 0,8. ½ míst určuje selektivně ředitel pro certifikaci podle výše uvedených zásad a ½ míst náhodným výběrem vedoucí auditor.

Poznámka: V případě zjištěné neshody v sídle vedení nebo na některém z vybraných míst zahrnutých do certifikace ISMS se opatření k nápravě musí uplatnit na všech místech spadajících pod působnost certifikátu a do doby prokázání realizace opatření nelze certifikát udělit. Není přípustné aby organizace „problematické místo“ dodatečně vyloučila z rozsahu působnosti.

Preaudit (audit 1.stupně) je zaměřen na činnosti ústředí (vedení), aby se certifikační orgán ujistil, že pro všechna místa platí jediný ISMS a že organizace je řízena vedením na všech operativních stupních.

5.1 ORIENTAČNÍ DOBY (ROZSAHY) POSUZOVÁNÍ

Certifikační orgán uvede do návrhu smlouvy na certifikaci, s přihlédnutím k výše citovaným podmínkám počtu vybraných míst a podle níže uvedené tabulky (slouží jako vodítko), dobu potřebnou k prověření systému organizace. Doba k provedení počáteční prověrky je vyčíslena pomocí počtu pracovníků x den.
Tato doba zahrnuje činnosti spojené s prověřováním systému podle normy ISO/IEC 27001 a zahrnuje preaudit (první stupeň auditu-prověrku dokumentů), certifikační audit (druhý stupeň auditu – prověrku činností), ale nezahrnuje čas strávený na cestě do místa klienta resp. mezi prověřovanými oblastmi klienta.

Trvání auditu
Certifikační orgán při stanovování doby trvání auditu vychází z IS 9.1.3 normy ISO/IEC 27006 a čas je stanoven s přihlédnutím k:

a) rozsahu ISM
b) komplexnosti ISMS
c) typu vykonávaných činností v rozsahu ISMS

d) rozsahu a různorodosti technologií použitých při implementací různých součástí ISMS
e) počtu pracovišť
f) již demonstrovaného výkonu ISMS
g) rozsahu outsourcingu a ujednání o využití služeb třetích stran
h) aplikovatelnosti norem a předpisů, které jsou relevantní pro rozsah certifikace

V případě, že se pro certifikaci stanoví s přihlédnutím k jmenovaným důvodům o trvání kratším, než uvádí tabulka, musí v dotazníku/ žádosti organizace uvést důvody:

- žádné/nízké riziko produktu/procesů
- dřívější znalost organizace (např. certifikace organizace podle jiné normy stejným certifikačním orgánem)
- připravenost zákazníka k certifikaci (např. certifikován jinou třetí stranou)
- procesy zahrnují jedinou hlavní činnost (např. pouze službu)
- vyzrálost zavedeného systému managementu
- vysoké procento pracovníků provádějících stejné jednoduché činnosti / úkoly

V případě, že se stanoví s přihlédnutím k jmenovaným důvodům o trvání delším, než uvádí tabulka, musí v dotazníku/ žádosti organizace uvést důvody:

- komplikovaná logistika zahrnující více než jednu budovu nebo místo, kde organizace provádí činnosti
- zaměstnanci (personál) mluvící více než jedním jazykem a je nutno využívat služeb tlumočníka
- velký počet regulatorních požadavků
- ISMS pokrývá vysoce komplexní procesy nebo relativně velký počet samostatných činností
- procesy využívají kombinace HW, SW, procesů a služeb
- činnosti, které vyžadují návštěvu dočasných poboček k ověření činností na stálých pracovištích, jejichž systém řízení je předmětem certifikace

Rozhodnutí o snížení/ zvýšení rozsahu trvání auditu může učinit též vedoucí auditor na základě zjištění a výsledků auditu předcházejícího stupně. Tato zjištění musí uvést ve zprávě z auditu a o jejich akceptování rozhoduje ředitel pro certifikaci a zástupce certifikované organizace.

Prvotní posuzování (predaudit a certifikační audit, tj. audit 1. a 2. stupně dohromady).
Z uvedených rozsahů musí auditor strávit posuzováním na místě organizace minimálně 70 %, kdy hodnoty jsou uvedeny pro 8 hodinový pracovní den. Nepřipouští se snižovat počty auditorodnů tím, že program obsahuje více hodin na jeden pracovní den.

5.2 Příloha B. 8.3 dle normy ISO/IEC 27006

Počet zaměstnanců	*Čas strávený auditory při počátečním auditu*
1-10	5
11-25	7
26-45	8,5
46-65	10
66-85	11
86-125	12
126-175	13
176-275	14
276-425	15
426-625	16,5
626-875	17,5
876-1175	18,5
1176-1550	19,5
1551-2025	21

2026-2675	22
2676-3450	23
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27
8501-10700	28
>10700	Atd.

Pozn. hodnoty uvedené v tabulce mají být použity pro každé místo, které spadá pod působnost certifikovaného systému.

Dozorový audit (kontrolní audit) – platí, že hodnoty uvedené v tabulce minimálně tvoří 1/3.
Opakované posuzování (opakovací audit) – platí, že hodnoty uvedené v tabulce tvoří minimálně 2/3.

Počty zaměstnanců
V tabulce je uvažováno počet zaměstnanců včetně nestálých (sezonních, dočasných, subdodavatelsky zabezpečovaných) zaměstnanců. Pracovníci na částečný úvazek musí být započteni pomocí ekvivalentu pracovníků s plným úvazkem.

6 PŘEVOD AKREDITOVANÉ CERTIFIKACE

6.1 Všeobecně

Držitelé platného certifikátu systému managementu vydaného jiným certifikačním orgánem (akreditovaným signatářem MLA IAF) mohou zažádat o převod tohoto certifikátu na certifikační orgán CERT-ACO.

6.2 Rozhodnutí o možnosti zahájení procesu převodu certifikátu

Převod certifikace je definován jako uznání existujícího platného certifikátu systému managementu uděleného jedním akreditovaným certifikačním orgánem jiným akreditovaným certifikačním orgánem za účelem vydání jeho vlastního certifikátu.

Na základě žádosti (písemné či ústní) obdrží žadatel o převod akreditované certifikace od certifikačního orgánu formulář žádosti převod certifikace, kterou vyplní a zašle na adresu certifikačního orgánu. Na základě vyplněné žádosti rozhodne ředitel certifikačního orgánu o možnosti převedení certifikátu. Pokud rozhodne záporně, je žadateli zasláno vysvětlení a návrh dalšího možného řešení, tj. žadatel je posuzován jako nový žadatel bez certifikace.

Podmínky pro převod:

- stávající převáděný certifikát musí být vydán v rámci platného akreditačního oprávnění a musí být platný (nelze po ukončení platnosti nebo v době jeho pozastavení)
- neexistují žádné nevyřešené neshody či potenciální problémy identifikované původním certifikačním orgánem

Následně obdrží žadatel nabídku a následně návrh smlouvy, po jejímž podepsání následuje příprava převodu certifikátu. Převod certifikátu probíhá buď formou:

a) přezkoumání dokumentace a/nebo
b) auditem na místě (tj. v případě, že rozhodnutí o převodu certifikace nebylo možno spolehlivě provést na základě předložených dokumentů) s minimálním rozsahem 0,5 auditodne na místě.

6.3 Převod certifikátu – přezkoumání

Auditor se při přezkoumání dokumentace, resp. při auditu na místě zaměří na:

a) ověření rozsahu certifikace,
b) prověření důvodu pro uskutečnění převodu,
c) posouzení zpráv z posledního certifikačního, resp. recertifikačního auditu a po něm následujících dozorových auditů, včetně z nich vyplývajících neshod (pokud nejsou tyto dokumenty k dispozici, pak je s žadatelem zacházeno jako s novým klientem),
d) obdržené stížnosti a přijatá opatření,
e) ověření, zda nebyla subjektu pozastavena nebo zda mu nehrozí pozastavení platnosti certifikátu (takováto certifikace nemůže být převedena),
f) na kontrolu nápravných opatření stanovených v rámci odstranění neshod, které doposud neprověřil vydávající certifikační orgán,
g) jakékoliv současné závazky organizace vůči regulačním orgánům, co se týče dodržování zákonů,
h) stupeň věrohodnosti prováděných interních auditů,
i) přezkoumávání systému managementu,
j) ostatní oblasti, přichází-li to v úvahu.

6.4 Rozhodnutí o převodu certifikace

O výsledku přezkoumání zpracuje zprávu včetně přiložení dostupných podkladů, kterou předkládá CeV, který rozhodne o převodu certifikace nebo o tom, že bude s žadatelem zacházeno jako s novým klientem.

V případě, že se převod certifikace bude realizovat, je žadateli vystaven certifikát s datem rozhodnutí certifikačního orgánu, a to s konečnou dobou platnosti totožnou s původním certifikátem. Program pokračujícího dozoru má vychází z předchozího certifikačního režimu/cyklu, pokud převod nebyl realizován v rámci recertifikačního auditu CERT-ACO. Pak program dozorů vychází z nového certifikačního režimu/cyklu.

7.0 POZASTAVENÍ A ODNĚTÍ CERTIFIKÁTU

7.1 Politika

Certifikační orgán systematicky zajišťuje důvěryhodnost vydávaných certifikátů. To znamená, že zainteresované strany (např. zákazníci certifikovaných organizací, orgány státní správy, obchodní partneři) mohou mít důvěru v to, že certifikovaný systém managementu objektivně odpovídá požadavkům příslušného certifikačního kritéria (normy). V případě, že certifikovaný subjekt nesplňuje požadavky příslušné normy či porušuje závazky z certifikace pro něj plynoucí, uplatňuje certifikační orgán nástroje jako jsou pozastavení certifikátu, odnětí certifikátu či omezení rozsahu certifikátu.

7.2 Všeobecně

Při pozastavení je certifikace systému managementu klienta dočasně neplatná. Pozastavení platnosti certifikátu znamená pro organizaci zákaz aktivně uvádět, vystavovat nebo propagovat certifikaci svého systému managementu udělenou certifikačním orgánem. Při pozastavení zůstává certifikát v držení organizace.

Při odnětí je certifikace systému managementu klienta trvale neplatná. Odnětí certifikátu znamená pro organizaci zákaz aktivně uvádět, vystavovat nebo propagovat certifikaci svého systému managementu. Organizace je povinna vrátit certifikačnímu orgánu certifikát, případně certifikační značku. Odnětí následuje obvykle po pozastavení, jestliže organizace včas neučinila nápravu a nepředložila důkazy o opatřeních k nápravě zjištěných nedostatků.

7.3 Kritéria pro pozastavení certifikace

Certifikační orgán pozastaví certifikaci v případech, kdy:

- certifikovaný systém managementu klienta trvale nebo vážně selhává při plnění certifikačních požadavků, včetně požadavků na efektivitu systému managementu;
- certifikovaný klient nedovolí provedení dozorových auditů nebo recertifikačních auditů v požadované četnosti a termínech;
- provedení změn uvnitř organizace certifikovaného klienta, které změnily podmínky, za kterých byl certifikát vydán;
- nesprávné použití či zneužití certifikátu a certifikační značky;
- nesplnění finančních podmínek smlouvy;
- certifikovaný klient dobrovolně požádal o pozastavení.

Certifikační orgán je povinen učinit informaci o stavu pozastavení certifikace veřejně dostupnou. Certifikační orgán poskytne přiměřený čas, obvykle do 3 měsíců (ve výjimečných případech na žádost organizace po schválení ředitelem certifikačního orgánu 6 měsíců) během kterého musí certifikovaná organizace prokázat, že odstranila zjištěné nedostatky.

Certifikační orgán obnoví platnost pozastavené certifikace, pokud byly vyřešeny problémy, které k pozastavení vedly. Pokud v době stanovené certifikačním orgánem nedojde k vyřešení problémů, které vedly k pozastavení, pak tato skutečnost musí vést k odnětí nebo k omezení předmětu certifikace.

7.4 Kritéria pro odnětí certifikace

Certifikační orgán musí odejmout certifikaci v případech, kdy:

- nebyla ve stanoveném termínu realizována opatření k odstranění příčiny, pro kterou byl certifikát pozastaven;
- nebyl proveden dozorový, resp. recertifikační audit ani v odloženém termínu;
- došlo k vydání nového certifikátu (například při změně rozsahu);
- na základě žádosti certifikované organizace.

Certifikační orgán je povinen učinit informaci o stavu odnětí certifikace veřejně dostupnou.

Integrované/kombinované certifikace: jestliže se pozastavení nebo odnětí bude týkat jedné normy systému managementu certifikační orgán prověřuje, zda jsou či nejsou rovněž dotčeny další normy systémů managementu a certifikát(y).