Popis certifikačního postupu BCMS, ISMS, SMS

BCMS – Systém řízení kontinuity činností organizace; ISO 22301
ISMS – Systém řízení bezpečnosti informací; ISO 27001
SMS – Řízení a zajištění kvality; ISO 2000-1

TÜV NORD CERT Odvětvové normy / Sector-Specific-Standards (3S)

Certifikační postup systému managementu (BCMS, ISMS, SMS) sestává z přípravy nabídky a smlouvy, přípravy auditu, provedení auditu 1. stupně a vyhodnocení systémové dokumentace, provedení auditu 2. stupně, vydání certifikátu a kontrolních auditů/recertifikace.

V případě potřeby může být certifikační postup pro systémy řízení (BCMS, ISMS, SMS) doplněn o hodnocení „odvětvových norem“ / "sector-specific-standards" (3S).

Ze skupiny norem ISO 27001 se jedná např. o:

- ISO27010 Systém řízení bezpečnosti informací pro komunikaci uvnitř organizace a uvnitř sektoru
- ISO27011 Doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů na základě ISO/IEC 27002
- ISO27015 Systém řízení bezpečnosti informací pro finanční sektor
- ISO27017 Soubor postupů pro opatření bezpečnosti informací pro cloudové služby na základě ISO/IEC 27002
- ISO27018 Soubor postupů na ochranu osobně identifikovatelných informací (personal identifiable information – PII) ve veřejných cloudech vystupujících jako zpracovatelé PII
- ISO27019 Systém řízení bezpečnosti informací pro energetické řídicí systémy na základě ISO/IEC 27002
- ISO27799 Systém řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27000

Nebo německý zákon o inteligentním měření spotřeby (smart metering) “Smart Meter Operation law” / Messstellenbetriebsgesetz (MStBG):
- TR03109 Správa brány inteligentního měření spotřeby (Smart Meter Gateway Administration)

Některé odvětvové normy / „Sector-Specific-Standards“ (3S) společnosti TN CERT mají vlastní akreditaci nebo se nachází v akreditačním řízení, např.
- BNetzA § 11 Abs.1aEnWG / Specifické požadavky na provozovatele energetických sítí
- IEC 62443-2-1 – Bezpečnost informací / Kybernetická bezpečnost – Požadavky na systém řízení bezpečnosti informací IACS
- IEC 62443-2-4 – Bezpečnost informací / Kybernetická bezpečnost – Požadavky na dodavatele bezpečnostních řešení IACS
- IEC 62443-3-2 – Bezpečnost informací / Kybernetická bezpečnost – Hodnocení bezpečnostních rizik a návrh systému

Některé odvětvové normy / "Sector-Specific-Standards" společnosti TÜV NORD CERT jsou navrženy pro „kritické infrastruktury“ ("critical infrastructures"), např.:
- TN CERT odvětvová norma / Sector-Specific-Standard (3S) Energetika
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Vodohospodářství
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Potravinářství
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Informační technologie a telekomunikace
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Zdravotnictví
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Finanční služby a pojišťovnictví
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Doprava a provoz
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Státní správa
- TN CERT odvětvová norma / Sector-Specific--Standard (3S) Média a kultura

Všechny odvětvové normy / "Sector-Specific-Standards" (3S) společnosti TÜV NORD CERT dodržují právní požadavky, požadavky německého práva pro „Spolkový úřad pro bezpečnost informací" ("Bundesamt für Sicherheit in der Informationstechnik (BSIG) - § 8a ff."). V případě potřeby jsou poskytnuty doplňující informace.

Seznam odvětvových norem / "Sector-Specific-Standards"(3S) bude průběžně aktualizován. Další odvětvové normy / "Sector-Specific-Standards" (3S) budou poskytnuty na vyžádání.

Auditoři jsou nominováni certifikačním místem TÜV NORD CERT GmbH dle jejich kvalifikace a oprávnění pro dané odvětví (scope).

1. Certifikační postup

1.1 Příprava auditu

Po uzavření smlouvy auditor provede na základě dotazníku k certifikaci a kalkulačního listu přípravu k auditu a prodiskutuje a domluví s auditovanou organizací další postup.

Pokud v organizaci nastanou zvláštní okolnosti, které vyžadují zachování dodatečné bezpečnosti nebo důvěrnosti, musí být podepsána dodatečná dohoda o zachování důvěrnosti.
Zákazník musí předem informovat certifikační místo o přítomnosti důvěrných nebo vysoce citlivých dokumentů, které nemohou být zpřístupněny auditorům. Certifikační místo musí před zahájením auditu určit, zda je možné systém managementu adekvátně zauditovat i bez těchto záznamů. Pakliže dojde certifikační místo k závěru, že není možné adekvátně zauditovat systém managementu bez přezkoumání těchto důvěrných nebo citlivých záznamů, sdělí zákazníkovi, že certifikační audit bude moci proběhnout pouze v případě, že budou tyto záznamy zpřístupněny.

V rámci přípravy na kontrolní a recertifikační audit se auditované organizace zavazují informovat certifikační místo o podstatných změnách v organizační struktuře nebo v procesech organizace.

1.2 Audit 1. stupně

Audit 1. stupně se provádí, aby

- byla získána a přezkoumána zákazníkova dokumentace systému managementu dle normy,
- se bylo možné zaměřit se na plánování auditu 2. stupně
- byla zajištěna připravenost společnosti pro audit 2. stupně (na základě porozumění systému managementu v kontextu politiky a cílů společnosti).

Zákazník provede všechna nutná opatření k provedení certifikačního auditu, včetně možnosti přezkoumání dokumentace a přístupu do všech oblastí, ke všem záznamům (včetně zpráv z interních auditů a přezkoumání dokumentace) a zaměstnancům, kterých se týká certifikační, recertifikační audit a vyřizování stížností. Zákazník dodá veškerou potřebnou dokumentaci k auditu v jejich aktuální platné verzi nejpozději 4 týdny před auditem.

Audit 1. stupně obsahuje, ale není omezen na přezkoumání dokumentace. Certifikační místo se dohodne se zákazníkem, kdy a kde přezkoumání dokumentace proběhne.

Aktuální řídicí dokumentace je posouzena a obsahuje:

BCMS – ISO 22301	ISMS - ISO 27001	SMS - ISO 20000-1
• BCMS politika a cíle	• ISMS politiky a cíle	• SMS politiky a cíle
• Rozsah BCMS	• Oblast použitelnosti / rozsah ISMS	• Oblast použitelnosti / rozsah SMS
• Postup(y) BCMS	• Postup(y) a činnosti ISMS	• Plán managementu služeb
• Analýza dopadů na podnikání (BIA) • Posuzování rizik (Risk assessment)	• Prohlášení o použitelnosti	• Dokumentované dohody o úrovních služeb (SLA)
• Strategie kontinuity podnikání	• Libovolné relevantní dokumenty / záznamy vztahující se k normě, podle které je prováděn audit	• Dokumentované procesy a postupy požadované normou
• Struktura reakce na incident • Plány kontinuity podnikání / Plán řízení incidentu • Záznamy o využití BCMS	• Management rizik, který zahrnuje ○ Popis metodiky hodnocení rizik ○ Zprávu hodnocení rizik ○ Plán ošetření rizik	• Záznamy požadované normou

V případě posuzování odvětvových norem / "Sector-Specific-Standards" (3S) zákazník vyplní standardní dotazník pro příslušnou normu před provedením auditu 1. stupně. Formulář dotazníku obdrží zákazník předem.

Organizace obdrží písemnou zprávu o výsledcích 1. stupně, včetně posouzení řídící dokumentace a má tím pádem možnost odstranit veškeré neshody před 2. stupněm auditu. Je také možné v této době předat vyjádření k otázkám, které nejsou zcela jasné.

Pokud byly během 1. stupně auditu identifikovány neshody, organizace je musí odstranit před provedením 2. stupně.

Pokud nakonec nelze konstatovat, že je zákazník na audit 2. stupně připraven, dochází po auditu 1. stupně k přerušení certifikačního procesu.

Za koordinaci činností spojených s auditem 1. stupně, příp. za vzájemnou komunikaci a spolupráci zúčastněných auditorů, je zodpovědný vedoucí auditor.

1.3 Certifikační audit (audit 2. stupně)

Audit probíhá v souladu s plánem auditu, který byl se zákazníkem odsouhlasen před zahájením auditu. Zákazník má právo odmítnout nominované auditory. Zákazník prokazuje použití a účinnost procesů, které byly popsány a stanoveny během auditu.
Audit začíná úvodním rozhovorem, při němž dochází k představení účastníků auditu. Je probrán průběh auditu. V rámci auditu v organizaci auditoři přezkoumávají a vyhodnocují účinnost zavedeného systému managementu.

Během auditu zákazník umožní týmu auditorů nahlédnout do záznamů, které se vztahují k rozsahu auditu a také umožní přístup do příslušných oddělení podniku.

Během auditu jsou mimo jiné prozkoumávány následující údaje:

- Dokumenty, které slouží jako základ pro posuzování
- Důkazy toho, že přípravy na přezkoumání vedením a interní audity byly provedeny, jsou efektivní a budou dodržovány
- Efektivita systému řízení v oblastech rozsahu auditu
- Správné používání certifikátu/certifikační značky (pokud je to relevantní)
- Námitky k systému managementu
- Účinnost nápravných opatření s ohledem na neshody z předcházejícího auditu (pokud je to relevantní).

Zákazník je povinen zaznamenat veškeré námitky vůči systému managementu a jejich nápravě a předložit je během auditu.
Během závěrečného rozhovoru jsou zákazníkovi oznámeny výsledky auditu a zaznamenané neshody. Neshody jsou požadavky, které nebyly splněny a u kterých má zákazník zahájit příslušná nápravná opatření a tato opatření ověřit. Musí být předložen odpovídající důkaz.

Neshody mohou vést k předložení nové/zrevidované dokumentace/postupů a/nebo k re-auditu.
Vedoucí auditor rozhodne o rozsahu re-auditu, během kterého jsou auditovány pouze aspekty, které se vztahují k neshodám (procesy, postupy, oblasti organizace).
Po zavedení všech nápravných opatření a odstranění všech neshod a jejich podepsání je navržena zpráva z auditu.

1.4 Vydání certifikátu

Certifikát je vydán po provedení kontroly a uvolnění certifikačního postupu certifikačním místem. Osoba, která dokumentaci kontroluje a uvolňuje, nesmí být účastníkem auditu.

Certifikát může být vydán pouze v případě, že auditní tým neshody přijal a verifikoval.

Certifikáty mají tříletou platnost.

2. Kontrolní audit

Během kontrolního auditu jsou prověřeny následující body:

- Účinnost systému managementu v rámci celé společnosti prostřednictvím menšího náhodného výběru
- Správné používání certifikátu/certifikační značky
- Námitky vůči systému managementu
- Účinnost nápravných opatření s ohledem na neshody z předcházejícího auditu (pokud je to relevantní).

Během závěrečného rozhovoru jsou zákazníkovi oznámeny výsledky auditu, včetně všech zaznamenaných neshod.

Po provedení kontrolního auditu zákazník obdrží zprávu.

Kontrolní audity musejí být provedeny jednou ročně během období platnosti certifikátu (3 roky).
Při stanovení data / audit relevantního data pro kontrolní audit rozlišujeme mezi novými zákazníky (počáteční certifikace od 1. ledna 2008) a stávajícími zákazníky (počáteční certifikace před 1. lednem 2008).

Nový zákazník:

- Audit relevantní datum pro roční kontrolní audit, který následuje po certifikačním auditu, nesmí být stanoven později než 12 měsíců od posledního dne 2. stupně auditu.

Stávající zákazník:

- Audit relevantní datum pro roční kontrolní audit je datum platnosti certifikátu k 1. lednu 2008 (den a měsíc) minus 1 měsíc.

Nový a stávající zákazník:

- Audit relevantní datum řídí všechny následující audity (kontrolní a recertifikační audity).
- Každý kontrolní audit, včetně ověření, přijetí a verifikace opatření k nápravě neshod, zpracování zprávy z auditu a uvolnění certifikačním místem, musí být uzavřen nejpozději do dvou (2) měsíců po audit relevantním datu.
- V rámci ročního dozoru může být dozorový audit proveden nejdříve tři (3) měsíce před audit relevantním datem.

Povolená tolerance při provádění ročních kontrolních auditů:
audit relevantní datum -3/+ 0 měsíců.

3. Recertifikační audit

Recertifikační audity musí být, včetně přezkoumání opatření k nápravě neshod, uzavřeny před uplynutím platnosti certifikátu.
Při recertifikačním auditu je provedeno přezkoumání dokumentace systému managementu organizace a audit na místě, přičemž je třeba zohlednit výsledky předchozího(-ích) kontrolního(-ích) auditu(-ů) certifikačního cyklu. Jsou auditovány všechny požadavky normy.
Okolnosti recertifikačního auditu mohou vyžadovat audit 1. stupně, pokud se vyskytnou významné změny v systému managementu nebo v souvislosti s činností organizace (např. legislativní změny).

Metodika auditu při recertifikačním auditu odpovídá metodice auditu 2. stupně.

4.1 Rozšiřovací audit

Má-li být rozšířen obor platnosti stávajícího certifikátu, může se tak stát při rozšiřovacím auditu. Provedení rozšiřovacího auditu může následovat v rámci kontrolního, recertifikačního auditu nebo ve zvlášť stanoveném termínu.

Doba platnosti certifikátu se tímto nemění. Výjimky musí být písemně odůvodněny.

5. Převzetí certifikátu jiných certifikačních míst

Všeobecně platí, že mohou být přebírány pouze certifikáty akreditovaných certifikačních míst. K organizacím s certifikáty, které byly vydány neakreditovanými certifikačními místy, je přistupováno jako k novým zákazníkům.

Kompetentní osoba přebírajícího certifikačního místa musí provést "Pre-Transfer-Review“, které se skládá zpravidla z prohlédnutí důležitých dokumentů a návštěvy u zákazníka.

Pozastavené certifikáty nebo takové certifikáty, u kterých hrozí riziko pozastavení, nesmí být přebírány. Otevřené odchylky by měly být, je-li to možné, vyjasněny původním certifikačním místem ještě před převzetím certifikace. V opačném případě musí být projednány během auditu.

Program dalšího kontrolního auditu se řídí podle předchozího programu platného do převzetí certifikátu.

6. Certifikace organizace s více místy

Bude-li certifikována organizace, která provozuje více míst, je nutné auditovat rovněž tato místa. Certifikace organizace s více výrobními místy/pobočkami/místy atd. s podobným profilem činností nebo pod jednotným systémem managementu může být provedena za použití postupu namátkového výběru.

7. Řízení neshod

Pro každou neshodu musí organizace provést analýzu příčin a zavést příslušná opatření k nápravě. Organizace je povinna, v závislosti na závažnosti neshod, informovat auditorský tým během 90-ti dnů buď o stanovených opatřeních k nápravě a plánovaných termínech jejich zavedení, nebo o zavedení opatření k nápravě. Nebude-li tato lhůta dodržena, nebude audit považován za úspěšný, tj. audit nebyl vykonán. Žádný certifikát nemůže být vydán, příp. stávající certifikát je stažen.