# ZPRÁVA Z AUDITU / AUDIT REPORT

ČSN EN ISO 9001:2009 ČSN ISO/IEC 27001:2006

|  |  |  |
| --- | --- | --- |
| Dozor  (Routinesurveilance audit) | X | X |

Joint-audit with:

Organizace:

(Organization):

Adresa:

(Address):

Rozsah certifikace:

(scope of certificate):

NACE:

Číslo certifikátu:

(Numberofcetificate):

Pořadí dozorového auditu:

(Sequenceofsurveillance audit):

TERMÍN AUDITU:

(Term of audit):

**TÝM AUDITORŮ (Audit team):**

**Vedoucí auditor**: **2. auditor**:

(Leadauditor) (2nd auditor)

**Technický expert:** **Auditor v přípravě**:

(Technical expert) Auditor in training

**Vrcholové vedení (Top management):**

**Představitel managementu ISMS:**

(management representative ISMS)

**Počet zaměstnanců:**

(numbers of employees)

Identifikace organizace, na kterou se vztahuje Prověřeno/plánováno v rámci auditu (Checked/planned

Certifikace (ústředí a pobočky)/ obec: during the audit)

(identificationof the organisation´sall Cert.audit 1. Cert.audit

Premisesrelated to the certification/city) stupeň 2.stupeň 1.dozor 2.dozor

(cert.audit 1st (cert.audit (1stroutine (2nd rou.

Level) 2ndlevel) audit) audit)

X X X/X X

**Místo organizace, kde byl prováděn audit, včetně dočasných pracovišť**

(the premises, where the audit has been done):

**Místa pracovišť, kde jsou umístěny další části organizace včetně dočasných pracovišť**

(Anotherorganization´spremises):

Doba strávená na auditu (celkem) / Timespent on audit (overal): XX hodin / hours

Z toho čas strávený (timespent)

* Přezkoumáváním dokumentace (reviewofdocumentation) XX hodin / hours
* Posouzením provedení analýzy rizik XX hodin / hours

(assessmentof the risk analysis)

* Vypracování zprávy z auditu (preparationof audit report) XX hodin / hours

Plán auditu upřesňuje cíle auditu, předmět auditu (např. lokality, organizační jednotky, činnosti, procesy), kritéria auditu (normativní dokument systému managementu, procesy), případně použitou metodologii auditu.

# VYHODNOCENÍ AUDITU / EVALUATION OF AUDIT

**Komentář k systému managementu**: (Commentary on quality management systém)

**Při dozorovém auditu byly prověřeny změny v systému** (Duringroutine audit the followingchanges in systém werefollowedup):

**Personál (Staff):**

Organizace (Organization):

Prohlášení o aplikovatelnosti (StatementofApplicability):

Prohlášení o aplikovatelnosti je zpracováno ve formě příloh Manuální řízení. Poslední vydání je z 30.3.2011

Postupy, procesy (Procedures, processes):

Od posledního audity beze změn

Postupy, procesy, zjišťované pomocí externích zdrojů (Procedures, outsourcedprocesses)

Společnost nevyužívá externí zdroje pro žádný z procesů, které mají vliv na shodu produktu.

Komunikace s třetími stranami (Communicationwith the thirdparties) (orgány veřejné správy, zájmové skupiny, externí subjekty…):

Způsob komunikace s třetími stranami je definováno v SM2 Organizační a pracovní rád.

Dokumentace (Documentation):

Od posledního auditu beze změn.

Závažné incidenty (Consequentialincidents):

Závažné incidenty od posledního auditu nebyly identifikovány

**Při dozorovém auditu byly prověřeny** (Duringroutine audit the followingitemswerefollowed up):

**Preventivní opatření a opatření k nápravě (realizace opatření k nápravě a vypořádání neshod na základě zjištění z předchozího auditu).** (Corrective and preventiveactionsbasen on the findingsfrom the foregoing audit):

V předchozím auditu nebyly zjištěny žádné nedostatky

**Stížnosti zákazníků** (Customercomplataints):

Nebyly zjištěny ani zaznamenány žádné stížnosti zákazníků.

**Správnost používání certifikačních značky CQS a IQNet**(Corretness of using of certification mark CQS and IQNet):

xxx nevyužívá certifikační značky CQS a IQNet.

**Zhodnocení systému management z hlediska uplatňování PCDA:** (Assassmentof the management systém withrespectofapplicationof PCDA)

**Plánování systému managementu a cílů kvality:** (Quality management systém planning and qualityobjectives)

Procesy společnosti jsou plánovány. Ve společnosti je vyhlášena integrovaná politika, které je pravidelně ročně přezkoumávána. Pravidelná analýza a vyhodnocení rizik ISMS. Analýza rizik reaguje na aktuální stav v organizaci a jsou identifikována nová rizika. Počet identifikovaných rizik v roce 2013 je 40 a jsou ošetřena stanovenými plány zvládání rizik.

**Provádění – procesy:** (Do - processes)

Ve společnosti jsou vypracovány směrnice a metodické pokyny. Všechny činnosti jsou realizovány na základě schválených plánů.

**Kontrola – analýza dat:** (Check – analysisof data)

Přezkoumání v celém rozsahu probíhá jednou ročně. Z těchto přezkoumání jsou identifikovány podněty pro zlepšení na následující období. Interní audit je zajišťován vlastním týmem a v požadovaném rozsahu. Interní audit slouží jako nástroj pro ověření funkčnosti zavedeného systému.

**Akce – zlepšování:** (Act - improvments)

Proces kontinuálního zlepšování a řešení preventivních opatření je stanoveno v příslušné dokumentaci. Postupy jsou v praxi aplikovány a probíhají v souladu se stanovenou metodikou. Pravidelně se provádí vyhodnocení evidovaných nedostatků, neshod, událostí a incidentů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Norma a článek/proces**  (Standard and article/process) | | **Silné stránky/Důkazy o plnění**  (Pošerfull points/Evidences of fulfilment) | **Příležitosti pro zlepšení**  (Opportunities for improvement) |
| 4. 2. 1 ISMS | Politika, cíle, programy | Politika je integrovaná se systémem QMS. Politika i cíle jsou pravidelně přezkoumávány a aktualizovány. Jejich plnění je rovněž kontrolováno. | Oblast bezpečnosti informací nemá stanoven celkový směr řízení v souladu s bezpečnostní politikou |
| 4. 2. 2 ISMS | Zavedení systému, aktualizace hodnocení rizik, identifikace | Pravidelné vyhodnocení rizik ISMS včetně sledování vývoje ratingu rizik. Klasifikace významnosti a finančního dopadu rizika. |  |
| 4. 3 ISMS | Požadavky na dokumentaci | Pravidelná aktualizace dokumentace s ohledem na současné potřeby systému řízení. | Dokumentace aktualizovat častěji |
| 5 ISMS | Odpovědnost vedení | Aplikace systémových přístupů. Systém BI má dostatečnou podporu vedení. |  |
| 6 ISMS | Interní audity ISMS | Interní audity probíhají v přiměřeném rozsahu. Výstupy přináší podněty ke zlepšení. |  |
| 7 ISMS | Přezkoumání ISMS vedením organizace | Přezkoumání vedením probíhá integrovaně. Rozsah přezkoumání je odpovídající. | Periodu přezkoumání vedením upravit tak, aby probíhalo vždy po uzavření hospodářského roku. |
| 8 ISMS | Zlepšování ISMS | Systém zaveden a je funkční opakovaná analýza a vyhodnocení rizik identifikace nových rizik v org |  |
| A 5 | Bezpečnostní politika | Závazek vedení definován v politice a také manuálu řízení. |  |
| A 6 | Organizace bezpečnosti informací | Odpovědnost rozdělena | Zavedení fungujícího systému pravidelného zálohování dat včetně určení odpovědnosti za zálohování dat. |
| A 7 | Řízení aktiv | Stávající postupy vyhovující. |  |
| A 8 | Bezpečnost lidských zdrojů | Pravidelná školení zaměstnanců k požadavkům na systém řízení bezpečnosti informací. |  |
| A 9 | Fyzická bezpečnost a bezpečnost prostředí | Systém řízení přístupu do prostor společnosti na velmi dobré úrovni. Prezentovány záznamy o pravidelné údržbě zařízení. |  |
| A 10 | Řízení komunikací a řízení provozu | Dokumentované postupy přístupné na firemním portále. Přehledně vedené záznamy. |  |
| A 11 | Řízení přístupu | Záznamy o přezkoumání přístupových práv provádí administrátor. Vytvořen skript pro extrakci oprávnění do excelovské tabulky. |  |
| A 12 | Akvizice, vývoj a údržba informačních systémů | Základní pravidla jsou stanovena v Manuálu řízení. |  |
| A 13 | Zvládání bezpečnostních incidentů | Incidenty a události jsou evidovány v excelu. | Pravidelné aktualizace tabulek určené auditorům. |
| A 14 | Řízení kontinuity činnosti organizace | Dokumentace na postačující úrovni, testování plánů kontinuity zdokumentováno včetně screenshotů a problémů. |  |
| A 15 | Soulad s požadavky | Relevantní legislativa |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ISO/IEC 27001** | A | B | C | D | E | **Vyhodnocení** |
| **4. 1 Všeobecné požadavky** (General requirements |  | X |  |  |  | Vyhovuje |
| **4. 2 Ustavení a řízení ISMS** (Establishing and managing ISMS) |  | X |  |  |  | Vyhovuje |
| **4. 3 Požadavky na dokumentaci** (Documentation manrequirements) |  | X |  |  |  | Vyhovuje |
| **5. Odpovědnost vedení** (Management responsibility) |  | X |  |  |  | Vyhovuje |
| **6. Interní audity ISMS** (Internal ISMS audits) |  | X |  |  |  | Vyhovuje |
| **7. Přezkoumání ISMS vedením organizace** (Management review) |  | X |  |  |  | Vyhovuje |
| **8. Zlepšování ISMS** (ISMS improvement) |  | X |  |  |  | Vyhovuje |
| **A5. Bezpečnostní politika** (Security policy) |  | X |  |  |  | Vyhovuje |
| **A6. Organizace bezpečnosti infomrací** (Organization of information security) |  | X |  |  |  | Vyhovuje |
| **A7. Řízení aktiv** (Asset management) |  | X |  |  |  | Vyhovuje |
| **A8. Bezpečnost lidských zdrojů** (Human resources security) |  | X |  |  |  | Vyhovuje |
| **A9. Fyzická bezpečnost a bezpečnost prostředí** (Physical and environmental security) |  | X |  |  |  | Vyhovuje |
| **A10. Řízení komunikací a řízení provozu** (Communications and operations management) |  | X |  |  |  | Vyhovuje |
| **A11. Řízení přístupu** (Access control) |  | X |  |  |  | Vyhovuje |
| **A12. Akvizice, vývoj a údržba infromačních systémů** (Information systems aquisition, development and maintenance) |  | X |  |  |  | Vyhovuje |
| **A13. Zvládání bezpečnostních incidentů** (Information security incident management) |  | X |  |  |  | Vyhovuje |
| **A14. Řízení kontinuity činností organizace** (Business continuity management) |  | X |  |  |  | Vyhovuje |
| **A15. Soulad s požadavky** (Compliance) |  | X |  |  |  | Vyhovuje |

**Závěry z dozorového auditu** (Conclusion of surveillance audit):

**Neshody v systému** (Nonconformities of systém):

Nebyly zjištěny.

**Nedostatky (nutno odstranit do příštího dozorového auditu)** (Minor nonconformities (necessary to remove before the next routine audit):

Nebyly zjištěny.

**Příležitosti pro zlepšování** (Opportunities for improvement):

1. Periodu přezkoumíní vedením upravit tak, aby přezkoumání probíhalo vždy po uzavření hospodářského roku.

**Termín příštího auditu** (Term of next audit):

**Měsíc / rok**

**VYHODNOCENÍ CERTIFIKAČNÍM ORGÁNEM**

CERTIFICATION BODY EVALUATION

Výsledek je vyznačen zaškrtnutím příslušné kolonky (The result is given by ticking the appropriate box).

|  |  |  |  |
| --- | --- | --- | --- |
| **STUPEŇ KRITIKY**  DEGREE OF CRITISM | | **DOPORUČOVANÉ OPATŘENÍ**  RECOMMENDED ACTION | **27001** |
| **1** | Žádné systémové ani závažné neshody, omezený počet nedostatků.  *No major criticisms, limited number of minor ones.* | Shoda systému managementu kvality s požadavky normy.  *The system conforms to the standard.*  **Zachovat certifikát – kontrola nedostatků při příštím dozorovém auditu.**  ***Certificate continues. Realisation will be checked during surveillance audit.*** | X |
| **2** | Omezený počet závažných neshod, případně větší počet nedostatků.  *A larger number of minor criticisms and or major ones.* | Shoda systému managementu kvality s požadavky normy není ohrožena. Shodu lze dosáhnout.  *The conformity has not been jeopardized.*  **Zachovat certifikát po provedení opatření k nápravě – kontrola neshod při příštím dozorovém auditu.**  ***Corrective actions to the criticisms must be submitted. Implementation will be checked during surveillance audit.*** |  |
| **3** | Omezený počet systémových neshod, případně větší množství závažných neshod a nedostatků, ale není ohrožen soulad s normou.  *A larger number of minor criticisms and or major but not vital criticism.* | Organizace musí provést rozsáhlejší opatření k nápravě.  *Organization must organize large corrective actions.*  **Zachovat certifikát po provedení a kontrole opatření k nápravě – kontrola neshod formou následného auditu.**  ***The certificate will be maintained after the corrective action are proved to be fulfilled during follow-up audit.*** |  |
| **4** | Neshody takové povahy, že soulad s normou je ohrožen.  *Critisms of vital nature.* | Organizace není způsobilá, požaduje se opakovaný audit a proškolení.  *Organization is not copable the longer, training and implementation period necessary.*  **Odejmout certifikát.**  ***Certification withdraw*.** |  |

**Změna certifikátu** (Changesofcertificate): Ano (Yes) Ne (No)

|  |  |  |
| --- | --- | --- |
| Změna rozsahu cerifikace (Changeofscopeofcertificate) |  | X |
|  |  | |
| Změna adresy (Changeofaddress) |  | X |
|  |  | |
| Změna poboček (Changeofpremises) |  | X |
|  |  | |
| Jiný důvod (Otherreason): |  | X |
| Např. změna prohlášení o aplikovatelnosti ze dne . . . . . . | | |

**Závěr (Conclusion):**

Tým auditorů konstatuje **shodu – ~~neshodu~~** systému managementu bezpečnosti informací s požadavky uvedené normy ISO/IEC 27001

The audit team statesthat he ISMS **is (~~not~~)** in compliancewith ISO/IEC 27001.

Datum: xx. xx. 20xx Vypracoval: xxxxxx

Date: Elaborated: