Univerzita Hradec Králové
Fakulta informatiky a managementu

Posudek oponenta diplomové práce

Jméno studenta: Bc. Ondřej Škeřík

Název práce: Systém řízení bezpečnosti informací prostřednictvím normy ČSN/EN ISO/IEC 27001

Autor posudku: Ing. Luboš Mercl

Cíl práce: Cílem práce je provést analýzu a posouzení specifických podmínek informační bezpečnosti v odlišných typech organizací s ohledem na související legislativní požadavky a požadavky normy ČSN/EN ISO/IEC 27001. Dále bude v práci pojednáno o vztazích normy ČSN/EN ISO/IEC 27001 a platné legislativy, zejména zákona 181/2014 Sb. o kybernetické bezpečnosti a souvisejících prováděcích právních předpisů (vyhláška o kybernetické bezpečnosti, vyhláška o stanovení významných informačních systémů a jejich určujících kritériích). V praktické části autor ukáže některé z důležitých dokumentů normy ČSN/EN ISO/IEC 27001 na třech modelových organizacích různého typu a zhodnotí rozdíly při zavádění normy mezi různé typy organizací. Součástí této části bude také získávání informací pomocí průzkumu dotazníkovou formou.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)			
	A	**C**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐
Vymezení cíle a jeho naplnění	☒	☒	☐	☐
Zpracování teoretických aspektů tématu	☒	☒	☐	☐
Zpracování praktických aspektů tématu	☐	☒	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☒	☐	☐
Hloubka a správnost provedené analýzy	☒	☒	☐	☐
Práce s literaturou	☐	☒	☐	☐
Logická stavba a členění práce	☐	☒	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐
Formální úprava a náležitosti práce	☐	☒	☐	☐
Vlastní přínos studenta	☒	☒	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☒	☒	☐	☐

Dílčí připomínky a náměty:

Práce několik nedostatků ve formátování a stylistiky textu. Například nadpisy na koncích stránek, spojky na koncích řádků, apod. Pro příklad stranu 22 a kapitolu 2.6.1. by bylo dobré zpracovat jinak, především s ohledem na kapitoly 2.6.2 a 2.6.3. V textu je dále také několik překlepů a chyb.
Praktická část práce není až tak rozsáhlá, jak by mohla být, nicméně to je důsledkem faktu, že oblast norem a jejich problematika je spíše popisnou oblastí.
Kapitolu 4, kde je největší praktická část práce, by bylo vhodné posunout blíže k závěru práce, protože kapitoly 5 a 6 jsou spíše teoretické a popisné.
Vzhledem k množství čerpaného textu z jiných zdrojů a počtů cizích zdrojů by autor měl používat více citování a uvádění zdroje informací.

Celkové posouzení práce a zdůvodnění výsledné známky:

Diplomová práce se zabývá především aplikací normy ČSN/EN ISO/IEC 27001 a jejích souvislostí a rámcově představuje problematiku informační bezpečnosti a její řízení.
Teoretická část práce je věnována především popisu bezpečnostních mechanismů a standard a nejdůležitějším pojmů. U této části práce bohužel chybí u některých částí textu citace a nejsou uvedeny zdroje informací.
V praktické části práce autor provedl především aplikaci poznatků, které vyplývají z certifikace na základě normy ČSN/EN ISO/IEC 27001 a souvisejících bezpečnostních požadavků. Tuto aplikaci provedl na tři fiktivní společnosti a vytvořil potřebné dokumenty, které k práci přiložil.
Autor dále provedl dotazníkové šetření, kde získal 11 odpovědí od respondentů. Toto šetření by bylo dobré doplnit do práce i grafy a vzhledem k počtu odpovědí i zpracovat do přílohy práce jednotlivé dotazníky a jednotlivé odpovědi tak uvést i v kontextu jednotlivého subjektu.
Část práce je dále věnována popisu a principu zákonu o kybernetické bezpečnosti.
Celkově práce působí jako dobrý odrazový můstek pro zabývání se informační bezpečností a zaváděním norem, které ovšem je pro možnou implementaci nutné nastudovat.

Otázky k obhajobě:

Co určuje rozsah zabezpečení a investované prostředky do bezpečnosti informací?
Lze s ohledem na počet organizací v šetření, které data poskytly, považovat tento průzkum za reprezentativní a vypovídající?
Jaké automatické mechanismy jsou používány v oblasti zabezpečení dat a informací?
V kapitole 4.3.1 uvádíte postup implementace normy ISO 27001 po krocích, které doporučuje společnost MANA Consulting s.r.o. S tímto postupem se plně ztotožňujete a schvalujete ho nebo byste tento postup dle Vašeho uvážení upravil?

Práci doporučuji k obhajobě.

Navržená výsledná známka: C - velmi dobře

V Hradci Králové**, dne 13. května 2016**

podpis