Implementace systému řízení bezpečnosti informací podle ISO 27001:2022

Bc. Ondřej Martinec

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondřej Martinec**
Osobní číslo:	**A22367**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní management**
Forma studia:	**Prezenční**
Téma práce:	**Implementace systému řízení bezpečnosti informací podle ISO 27001:2022**
Téma práce anglicky:	**Implementation of an information security management system according to ISO 27001:202**

Zásady pro vypracování

1. Vypracujte literární rešerši na téma ISMS.
2. Proveďte komparaci normy ČSN EN ISO/IEC 2700X:2013 se stávající verzí normy ČSN EN ISO/IEC 2700X:2022.
3. Zpracujte analýzu současného stavu ISMS v podniku.
4. Navrhněte implementační proces pro přechod na aktualizovanou verzi.
5. Vytvořte jednoduchý nástroj pro usnadnění celého procesu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ČSN EN ISO/IEC 27002:2022 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
2. ČSN EN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
3. ČSN EN ISO/IEC 27001:2022 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky
4. ČSN EN ISO/IEC 27001:2013 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky
5. JAŠEK, Roman a David MALANÍK, Bezpečnost informačních systémů. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978-80-7454-312-8.
6. SEDLÁK, Petr a Martin KONEČNÝ. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
7. SEDLÁK, Petr a KONEČNÝ, Martin. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.
8. ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 9788073807375.

Vedoucí diplomové práce: **Ing. Lukáš Králík, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **20. listopadu 2023**
Termín odevzdání diplomové práce: **28. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 1. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 27.5.2024

Ondřej Martinec, v.r.
podpis studenta

ABSTRAKT

Diplomová práce má za cíl porovnat aktualizovanou verzi normy ISO/IEC 27000:2022 s verzí normy ISO/IEC 2700X:2013. Dalším z hlavních cílů je zavádění systému řízení bezpečnosti informací (ISMS) ve výrobních podnicích. Je zde vytvořena metodika pro zavedení ISMS na základě materiálů od Národního úřadu pro kybernetickou a informační bezpečnost, odborné literatury, norem ISO/IEC 2700X a dalších velmi blízkých zákonů, norem a směrnic jako je např. evropská směrnice NIS2. Tato metodika bude příhodná pro auditorské účely.

Klíčová slova: ISMS, kybernetická bezpečnost, PDCA, ISO 27001, ISO 27002

ABSTRACT

The aim of the thesis is to compare the updated version of ISO/IEC 27000:2022 with the version of ISO/IEC 2700X:2013. Another main objective is the implementation of an information security management system (ISMS) in manufacturing companies. A methodology for implementing an ISMS is developed based on materials from the National Cyber and Information Security Authority, literature, ISO/IEC 2700X standards and other very close laws, standards and guidelines such as the NIS2 directive. This methodology will be convenient for auditing purposes.

Keywords: ISMS, cyber security, PDCA, ISO 27001, ISO 27002

S upřímnou vděčností bych rád poděkoval všem, kteří mi pomohli s touto diplomovou prací. Zvláštní poděkování patří panu Mgr. Tomášovi Kuželovi, DiS. za jeho postřehy a připomínky a také mému vedoucímu diplomové práce Ing. Lukášovi Králíkovi, Ph.D. za jeho cenné vedení, rady a podporu. Při vypracovávání této práce pro mě ale největší roli hrála má rodina a za to jsem jim opravdu vděčný.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Informační bezpečnostní management systém (ISMS) představuje klíčový nástroj pro ochranu citlivých informací a zajištění kontinuity podnikových procesů. Zavedení ISMS umožňuje podnikům efektivně řídit a minimalizovat rizika spojená s únikem dat, kybernetickými útoky a dalšími bezpečnostními hrozbami.

Norma ISO 27001 je mezinárodní standard, který poskytuje specifické požadavky na zavedení, udržování a neustálé zlepšování ISMS. Organizace, které se rozhodnou implementovat ISO 27001, získávají nejen strukturovaný přístup k řízení informační bezpečnosti, ale také vyšší důvěru svých zákazníků a obchodních partnerů. Tento standard klade důraz na systematické řízení rizik a pravidelné provádění auditů, které zajišťují, že všechny procesy odpovídají nejnovějším bezpečnostním požadavkům. [15]

ISO/IEC 27002 je doplňkovou normou, která poskytuje doporučení a nejlepší praktiky pro implementaci bezpečnostních kontrol. Tato norma slouží jako návod, jak konkrétně aplikovat požadavky ISO 27001, a pomáhá organizacím identifikovat vhodné bezpečnostní opatření a kontroly pro různé oblasti jejich činnosti. [16]

Zavedení ISMS v podniku přináší mnoho výhod. Kromě ochrany citlivých dat a zajištění souladu s legislativními požadavky, jako je zákon o kybernetické bezpečnosti, přispívá ISMS k celkovému zlepšení firemní kultury a zvýšení povědomí zaměstnanců o důležitosti informační bezpečnosti. Pravidelné audity a kontinuální zlepšování ISMS pak umožňují organizacím pružně reagovat na nové hrozby a udržovat vysokou úroveň bezpečnosti. [4]

V dnešním digitálním světě je ochrana informací a kybernetická bezpečnost zásadní pro úspěch a dlouhodobou udržitelnost podnikání. Implementace ISMS podle normy ISO 27001 a využití doporučení ISO/IEC 27002 představuje účinný způsob, jak toho dosáhnout.

Jelikož byla aktualizovaná norma ISO/IEC 27002 vydána v roce 2022, neuběhla ještě dostatečně dlouhá doba pro to, aby se firmy mohli, přizpůsobit novému standardu. Jelikož se nyní revidovaná verze týká také více subjektů v ČR, je to aktuální téma pro mnoho firem a podniků. Protože ISO/IEC 27001:2013 končí platnost dne 31. 10. 2025, tak od 1. 11. 2025 budou certifikáty dle ISO/IEC 27001:2013 neplatné. Proto je přínosné, se na certifikaci důkladně připravit. V této práci je, pro již zmíněné důvody pro přechod na novou verzi

normy, vytvořen program, který může usnadnit přípravu na získání certifikace. Dále zde jsou pomocné kapitoly a soubory, které mohou opět usnadnit celý proces kontroly podniku.

Implementace ISMS má nejen technický, ale i právní a organizační rozměr. V České republice je zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) klíčovým právním předpisem, který stanovuje povinnosti pro subjekty veřejné správy i vybrané soukromé podniky. Tento zákon klade důraz na prevenci a ochranu před kybernetickými hrozbami, což je plně v souladu s principy ISO 27001 a 27002. V souladu s tímto zákonem jsou podniky povinny zavést adekvátní opatření pro ochranu svých informačních systémů a dat. Integrace požadavků tohoto zákona s normami ISO přináší synergické efekty, které posilují celkovou bezpečnost podniku.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

Pro ponoření se do problematiky této práce je důležité, aby se čtenář seznámil se základními, důležitými a často zmiňovanými pojmy. Také se v této kapitole poukáže na historii anebo naopak na vývoj v oblasti bezpečnosti informací.

1.1 Základní pojmy

Entita – Její smysl může mít fyzický nebo logický původ. Jedná se o prvek který je relevantní pro funkční smysl domény, která má rozpoznatelně zřetelnou existenci.

Data – Jedná se o „surovou“ formu jakéhokoliv výstupu, který není nikterak zformulován nebo upraven.

Informace – Zde se může jednat už o zpracovanou, upravenou nebo systematickou formu získaných dat. Může být považována jako abstraktní entita která snižuje neurčitost znalostí. V informatice je tvořena informace kódovanými daty a to například v analogové, nebo digitální podobě. [1]

Citlivá informace – Jde o informaci, u které je potřeba se chránit před neoprávněným přístupem, nedostupností, pozměněním, publikování neoprávněným jednotlivcům nebo skupinám. V případě úniku této informace může dojít nežádoucí újmě. Jedná se zejména o ztrátu financí, reputaci, morálku, bezpečnost apod.

Přenos informací – Jedná se o změnu umístění informace jinému, dalšímu zdrojovému činiteli. V informatice se tento přenos označuje jako digitální komunikace.

Bezpečnost informací – Určena k ochraně informací jakéhokoliv typu, které jsou pro daný subjekt citlivé, nebo důležité. Níže jsou definovány základní pilíře bezpečnosti informací:

1) **Dostupnost (availability)** – Vlastnost, která zaručuje jednotlivci, entitě nebo procesu přístup k informaci v požadovaný okamžik;
2) **důvěrnost (confidentiality)** - Zajištění, že informace je dostupná pouze autorizovaným / pověřeným jednotlivcům, entitám nebo procesům;
3) **integrita (integrity)** – Garantování správnosti a úplnosti informace.

Další pilíře, které je důležité chránit a kontrolovat pro dodržení bezpečnosti informací:

1) **autenticita (authenticity)** - Vlastnost, která zajišťuje, že informace pochází od osoby, entity nebo systému, za kterou se vydává. Ověřuje pravost a původ informace;
2) **odpovědnost (responsibility)** - Schopnost přiřadit zodpovědnost za danou informaci nebo akci konkrétní osobě, entitě nebo systému;
3) **nepopíratelnost (undeniability)** - Charakteristika znemožňující popřít autorství nebo provedení akce s danou informací. Jedná se o upevnění nezpochybnitelnosti informace;
4) **spolehlivost (reliability)** – Atribut, který zaručuje, že informace je přesná, důvěryhodná a konzistentní. Zajišťuje, že se na informace lze spolehnout.

Aktivum – Jako aktivum je považováno vše, co má pro subjekt určitou hodnotu. Pokud je určitý prvek nebo vlastnost jakkoliv ohrožen hrozbou a může tak klesnou hodnota daného prvku nebo vlastnosti, můžeme to považovat jako aktivum. Aktiva se dělí na: [3]

1) hmotná aktiva – Peníze, elektronická zařízení, nemovitost, výrobní materiály;
2) nehmotná aktiva – Kód programu, informace, know-how, kvalifikace zaměstnanců.

Hrozba – Jedná se o událost, která může ohrozit hodnotu aktiva. Zneužívá zranitelnosti a může tak následně vytvořit určité riziko.

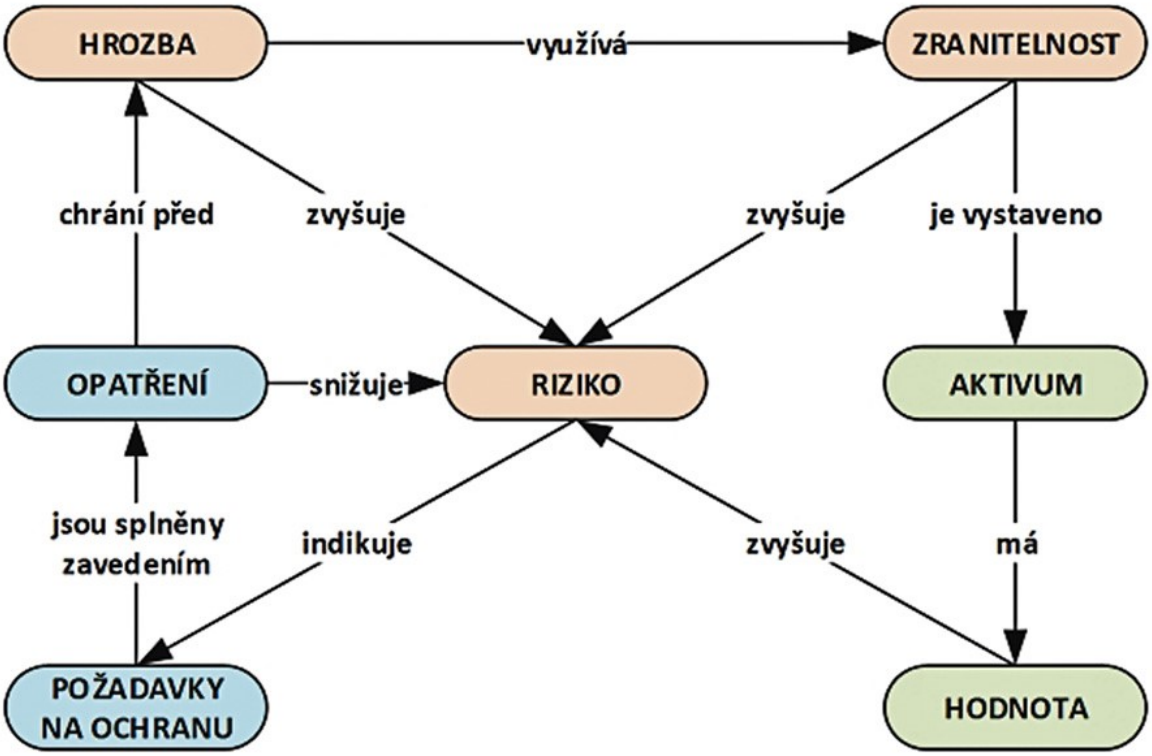
Zranitelnost – Slabé místo aktiva, které může být zneužito k znehodnocení aktiva. Může tak jít o negativní vlastnost v softwaru, hardwaru nebo v konfiguraci systému.

Opatření - Opatření jsou kroky, které přispívají k ochraně systému před hrozbami. Může se jednat o technická opatření, jako je instalace bezpečnostního softwaru, nebo o organizační opatření, jako je školení uživatelů o bezpečnosti.

Riziko – Je určitá míra pravděpodobnost, že daná hrozba zneužije zranitelnosti a stane se realitou. Riziko se obvykle vyjadřuje jako součin pravděpodobnosti a dopadu hrozby.

Dopad - Dopad je míra škody, která by byla způsobena, pokud by se hrozba stala realitou. Dopad se obvykle vyjadřuje jako finanční ztráta, ale může se jednat i o jiné typy škod, jako je ztráta dat nebo narušení provozu.

Pro lepší pochopení vztahů zmíněných v této kapitole je zde přiložen obrázek, který zobrazuje schéma vztahů aktiv, zranitelností, hrozeb, opatření a vlivu na rizika.



Obrázek 1. Přehledové schéma k řízení rizik [17]

1.2 Základní názvosloví

IS (Information system) – Informační systém: Celek který zajišťuje systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací a dat. [1]

IT (Information technology) – Informační technologie: Soubor nástrojů, zařízení a procesů, které slouží k práci s informacemi a daty. Zahrnuje hardware (počítače, servery, síťové komponenty), software (operační systémy, aplikace, databáze) a také lidské zdroje (programátoři, správci IT, analytici). [1]

ISMS (Information Security Management System) – Systém řízení informační bezpečnosti: Soubor pravidel, procesů a kontrol, které slouží k ochraně informací a dat před neoprávněným přístupem, použitím, zneužitím, ztrátou, poškozením nebo zničením. ISMS pomáhá organizaci identifikovat, posoudit a řídit rizika informační bezpečnosti. [1]

ICT (Information and Communication Technology) – Informační a komunikační technologie: Souhrnný název pro technologie, které slouží k práci s informacemi a daty a k jejich sdílení mezi lidmi a systémy. [1]

1.3 Historický vývoj informační bezpečnosti

Historie informační bezpečnosti sahá do počátků vývoje elektronických počítačů. První koncepty informační bezpečnosti se objevily během druhé světové války, kdy bylo nutné chránit citlivé informace před nepřátelskými silami.

1.3.1 Klíčové milníky v historii informační bezpečnosti

Tato kapitola se zaměřuje na klíčové milníky v historii informační bezpečnosti, které formovaly současné postupy a technologie a které jsou základem pro pochopení dnešních bezpečnostních výzev. [20,23]

40. léta 20 stol.: Během druhé světové války byly vyvinuty první šifrovací techniky a metody pro ochranu citlivých informací. Tato doba je často považována za začátek moderní informační bezpečnosti.

Obrázek 2. Šifrovací stroj Enigma [22]

70. léta 20 stol.: Výzkumný projekt ARPANET, předchůdce dnešního internetu, přinesl první vážné obavy o kybernetickou bezpečnost. Byly vyvinuty základní bezpečnostní protokoly a metody, které měly chránit data přenášená po síti.

80. léta 20 stol.: Bezpečnost se začala posouvat od čistě vojenského využití k širšímu komerčnímu využití. Zaměření se rozšířilo z ochrany důvěrnosti na zahrnutí integrity a dostupnosti dat. V této době se začaly objevovat první počítačové viry a malware.

90. léta 20 stol. Rozmach internetu vedl k nárůstu kybernetických hrozeb a nutnosti vyvinout sofistikovanější bezpečnostní opatření. Byly vyvinuty první firewally a antivirové programy.

Počátky 21. stol.: Kybernetická bezpečnost se stala klíčovou součástí informační bezpečnosti s rozvojem nových technologií a rostoucími hrozbami. Vznikly nové standardy a regulace, jako například GDPR v Evropské unii. V počátku 21. století začaly vlády přísněji trestat hacking, což zahrnovalo delší tresty odnětí svobody a vysoké pokuty. To byl značný rozdíl oproti 80. létům, kdy hackeři dostávali mírné tresty, jako jsou napomenutí nebo podmínečné odnětí svobody. S růstem internetu rostla i informační bezpečnost, ale také se šířily viry, které mohly zasáhnout celé organizace, města, státy.

První dekáda 20. stol.: Éra velkých úniků dat kdy technologický pokrok usnadnil hackingu získat mnohem větší moc, což vedlo k několika významným únikům dat.

1) Snowden & NSA, 2013: Edward Snowden, bývalý zaměstnanec CIA, který napomohl k úniku utajovaných informací o sledování veřejnosti vládou;
2) Yahoo, 2013-2014: Hackeři získali přístup k účtům všech tří miliard uživatelů Yahoo. Společnost byla pokutována 35 miliony dolarů a prodejní cena Yahoo klesla o 350 milionů dolarů;
3) WannaCry, 2017: První "ransomworm" zasáhl počítače s Windows a požadoval výkupné v bitcoinech. Během jednoho dne infikoval přes 230 000 počítačů ve 150 zemích. [23]

1.4 Audit a certifikace

Audit a certifikace jsou klíčové procesy pro ověření shody organizace s normami. Audit zahrnuje posouzení a ověření systémů řízení, zatímco certifikace poskytuje formální uznání, že organizace splňuje specifikované požadavky, což zvyšuje důvěryhodnost a zajišťuje bezpečnost informací.

Audit: Jedná se o systematický, nezávislý a dokumentovaný proces shromažďování a hodnocení důkazů s cílem posoudit míru plnění stanovených kritérií.

Typy auditů:

1) Interní audit (audit první stranou): Provádí sama organizace nebo externí dodavatel v jejím zájmu.
2) Audit druhou stranou: Provádí externí organizace, která má s auditovanou organizací určitý vztah (např. na základě smluvních podmínek).
3) Audit třetí stranou (certifikační audit): Nezávislý externí audit, který slouží nejčastěji jako podklad pro certifikaci. [4]

Certifikace: Potvrzení shody systému řízení s požadavky norem. Certifikace poskytuje důvěryhodný doklad o shodě s těmito normami, tím zajišťuje kvalitu, bezpečnost, spolehlivost nebo jiná specifická kritéria.

Obrázek 3. Příklad certifikátu pro normu ISO/IEC 27001:2013 [20]

Akreditace: Jedná se o potvrzení nezávislosti, objektivity a odborné způsobilosti subjektu pro provádění certifikačních činností. Akreditaci uděluje národní akreditační orgán (v ČR Český institut pro akreditaci, ČIA).

1.5 ISO a IEC

V oblasti standardizace hrají klíčovou roli dvě mezinárodní organizace a to: Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC). Obě organizace se zaměřují na podporu a rozvoj standardizačních aktivit v globálním měřítku, čímž usnadňují mezinárodní obchod a spolupráci v technických oblastech. [4]

1.5.1 ISO (International Organization for Standardization)

Cílem ISO je prosazovat standardizaci a s ní související aktivity na celosvětové úrovni. Název ISO není akronymem, ale odvozením z řeckého slova „isos", které znamená „rovný" nebo „stejný". To odráží snahu ISO o harmonizaci norem a standardů na mezinárodní úrovni. [4]

1.5.2 IEC (International Electrotechnical Commission)

IEC je mezinárodní organizace zaměřená na tvorbu a vydávání norem v oblasti elektrotechniky, elektroniky a souvisejících oborů (např. elektřina, magnetismus, elektromagnetismus, elektroakustika, multimédia, telekomunikace, výroba a distribuce energie, terminologie, měření, návrh a bezpečnost). [4]

1.5.3 České technické normy (ČSN)

Systém českých technických norem (ČSN) se skládá z norem převzatých z mezinárodních a evropských standardizačních organizací a z původních norem vyvinutých na základě národních potřeb.

1) Přejímané normy: ČSN EN (evropské normy), ČSN IEC (normy IEC), ČSN ISO (normy ISO), ČSN ETS (normy Evropského telekomunikačního standardizačního institutu) a další;
2) původní normy: Tyto normy vznikají v reakci na specifické potřeby České republiky a slouží k zachování funkčnosti a relevance fondu ČSN. [4]

1.6 Obecné informace o ISO 27001

ISO/IEC 27001 je uznávaný mezinárodní standard pro správu bezpečnosti informací. Zaměřuje se na vytvoření, zavedení, údržbu a kontinuální zlepšování systému řízení bezpečnosti informací (ISMS), který zahrnuje soubor politik, postupů, procesů a systémů na řízení rizik spojených s informacemi v organizaci [25].

Primárním cílem ISO/IEC 27001 je zajistit ochranu informačních aktiv organizací před ztrátou, krádeží, poškozením či jiným zneužitím. Tento standard poskytuje strukturovaný přístup k řízení citlivých dat, včetně informací o zákaznících, finančních údajů, duševního vlastnictví a dalších důležitých informací. Implementace tohoto standardu pomáhá organizacím identifikovat a řídit rizika, zlepšovat jejich kybernetickou odolnost a zajistit dodržování právních a regulačních předpisů.

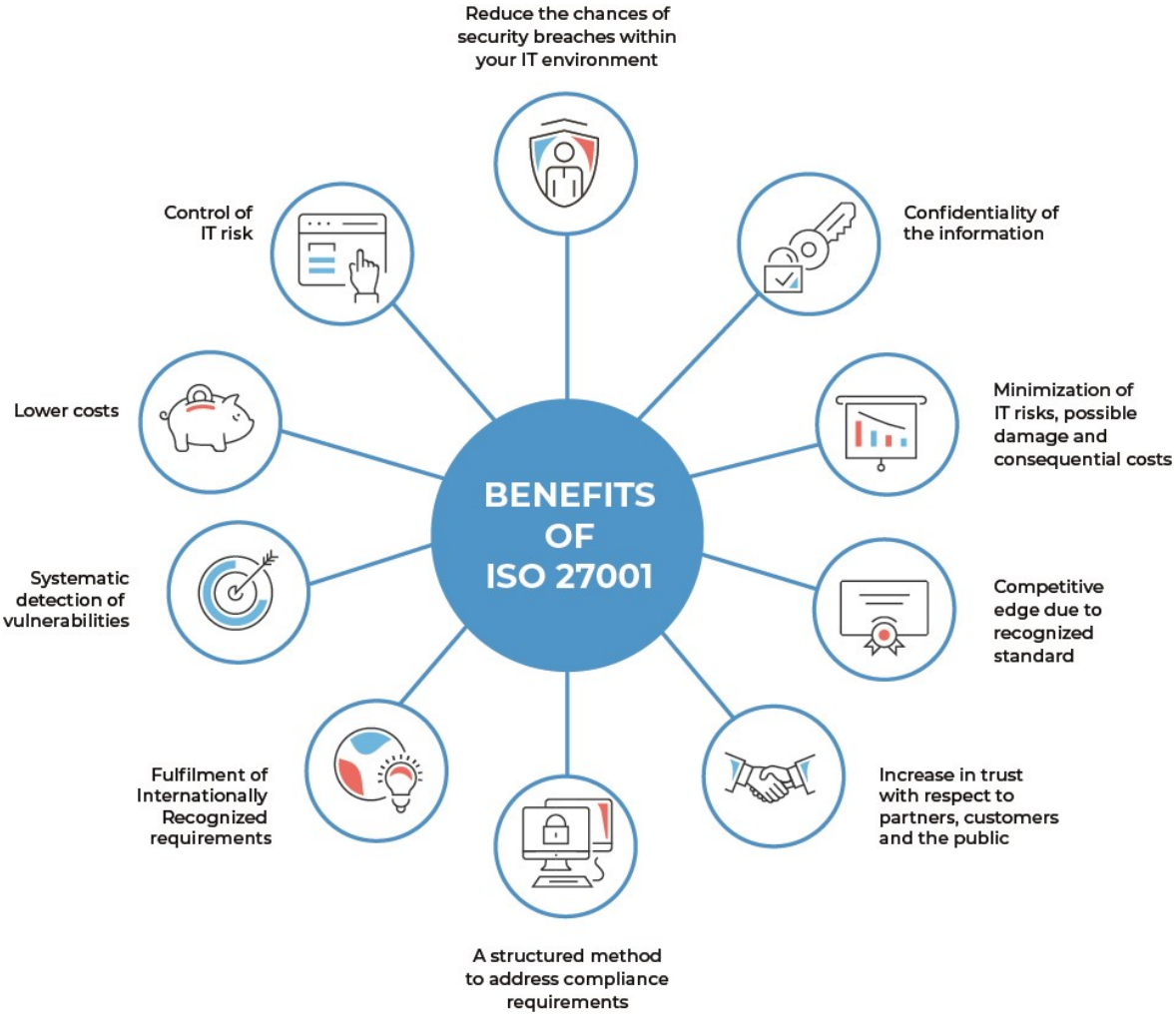
ISO/IEC 27001 stanovuje konkrétní požadavky, které organizace musí splnit pro certifikaci. Tyto požadavky zahrnují:

1) Zřízení ISMS: Organizace musí určit rozsah ISMS a vytvořit politiku bezpečnosti informací;
2) posouzení rizik: Organizace musí identifikovat a vyhodnotit rizika spojená s informacemi, aby určila potřebná opatření;
3) řízení rizik: Organizace musí zavést kontrolní opatření ke zvládnutí nebo snížení rizik;
4) monitorování a přezkoumání: Organizace musí pravidelně sledovat a přezkoumávat ISMS, aby zajistila jeho účinnost a neustálé zlepšování. [26]

Aby byla udělena certifikace podle ISO/IEC 27001 musí proběhnout posouzení nezávislým certifikačním orgánem, který ověřuje, zda organizace splňuje požadavky tohoto standardu. Úspěšná certifikace zvyšuje důvěryhodnost organizace a prokazuje její závazek k ochraně informací. Mnohé organizace používají ISO/IEC 27001 nejen k ochraně svých dat, ale také ke získání konkurenční výhody, protože certifikace často preferují zákazníci a obchodní partneři, obzvláště nadnárodní organizace, jako je například NATO.

Implementace ISO/IEC 27001 zahrnuje různé aspekty bezpečnosti informací, včetně technických, fyzických a organizačních opatření. To zahrnuje ochranu před kybernetickými útoky, fyzickou bezpečnost datových center, školení zaměstnanců a další opatření nezbytná pro zajištění komplexní ochrany informací.

Celkově ISO/IEC 27001 představuje zásadní nástroj pro každou organizaci, která chce systematicky chránit své informace a řídit s nimi spojená rizika. Poskytuje jasný rámec a metodologii pro řízení bezpečnosti informací a je klíčovým prvkem pro efektivní ochranu dat v moderním digitálním prostředí [26].



Obrázek 4. Výhody zavedení normy ISO 27001

1.6.1 Historický vývoj normy

Počátek 90. let: Britské ministerstvo obchodu a průmyslu (DTI) požádalo komerční centrum pro bezpečnost počítačů (CCSC) o vytvoření kritérií pro hodnocení bezpečnosti IT produktů, což vedlo ke vzniku ITSEC.

CCSC bylo také pověřeno vytvořením kodexu nejlepších postupů pro informační bezpečnost, což vyústilo v dokument známý jako DISC PD003. Práce na DISC PD003 pokračovala a rozdělila se do dvou hlavních oblastí: BS7799-1 a BS7799-2.

Konec 90. let: Dokument BS7799-1 byl rozčleněn do 10 sekcí, z nichž každá popisovala sérii kontrol a kontrolních cílů. Tento dokument položil základy pro standard ISO 27002.

Mezitím BS7799-2 vytvořil formální standard pro rozvoj systému řízení informační bezpečnosti (ISMS). Tento dokument byl poprvé publikován Britským institutem pro standardizaci (BSI) v roce 1998 a později se vyvinul v ISO 27001. V prosinci roku 2000 přijala Mezinárodní organizace pro standardizaci (ISO) BS7799-1 jako základ pro vytvoření standardu ISO/IEC 17799.

Duben 2001: ISO/IEC uspořádala v setkání v Oslu, kde diskutovala o zásadních revizích ISO 17799, a práce na nové verzi standardu pokračovaly od roku 2001 do roku 2004. Nová verze ISO 17799 byla schválena a potvrzena v dubnu 2005 ve Vídni a publikována v červnu 2005. Mezitím, v říjnu 2005, byla BS7799-2 formálně přijata jako ISO 27001.

Od té doby došlo k několika aktualizacím: v roce 2007 byl ISO 17799 přejmenován na ISO 27002. V roce 2017 byla publikována verze standardu ISO/IEC 27001:2013, která zahrnovala drobné změny ve formulacích a formátování. [24]

Říjen 2022: V Norma ISO/IEC 27001 byla v roce 2022 aktualizována a vydána jako ISO/IEC 27001:2022, což je její aktuální verze.

1.6.2 Proces certifikace ISO/IEC 27001

Proces certifikace podle ISO/IEC 27001 zahrnuje několik kroků, včetně předběžného auditu, ověření dokumentace ISMS, hodnocení účinnosti, pravidelných monitorovacích auditů a recertifikace každé tři roky. Tento proces zajišťuje, že organizace splňuje přísné požadavky na řízení bezpečnosti informací a neustále zlepšuje svůj systém řízení rizik. Obrázek č. 5 popisuje proces certifikace podle ISO/IEC 27001, který zahrnuje několik klíčových kroků:

1) Preliminary audit (předběžný audit):

   kontrola dokumentace, která ověřuje úplnost a shodu se standardy;

2) certification audit (certifikační audit):

   a. stage 1 (fáze 1): Ověření dokumentace ISMS,

   b. stage 2 (fáze 2): Potvrzení účinnosti ISMS;

3) report (Zpráva):

   dokumentace auditu včetně hodnocení systému řízení;

4) certification (certifikace):

   důkaz úspěšné certifikace s maximální platností 3 roky;

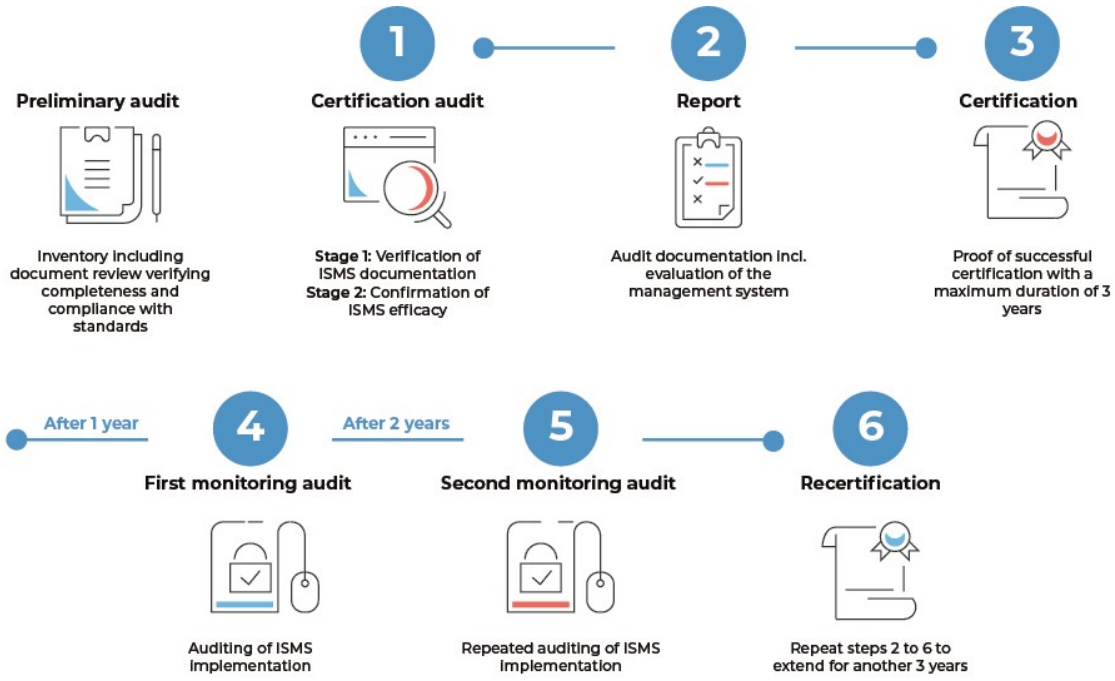
5) first monitoring audit (první monitorovací audit):

   první kontrola implementace ISMS po jednom roce;

6) second monitoring audit (druhý monitorovací audit):

   opakovaný audit implementace ISMS po dvou letech;

7) recertification (recertifikace).



Obrázek 5. Proces certifikace a recertifikace

Pro získání recertifikace na další 3 roky je potřeba provádět opakování kroků 2 až 6. Tento proces je navržen tak, aby zajistil, že organizace neustále splňuje požadavky ISO/IEC 27001 a udržuje vysokou úroveň bezpečnosti informací.

1.7 Metodiky a standardy pro řízení bezpečnosti informací

V oblasti informační bezpečnosti se dnes nejčastěji používají metodiky a standardy ISO 27001, ISO 27002, COBIT a ITIL. Každá z nich přistupuje k problematice z jiného úhlu pohledu. Mohou se používat samostatně, ale i v kombinaci. [4]

Kombinace těchto metodik umožňuje komplexní a efektivní přístup k řízení informační bezpečnosti. Metodika COBIT s hierarchickým přístupem „shora dolů" umožňuje systematické zavádění kontrolních mechanismů a pokrytí všech identifikovaných rizik. Díky tomu je implementace systému řízení bezpečnosti informací (ISMS) snazší a plynulejší. Integrace ISMS s existujícími systémy pro správu služeb dle metodiky ITIL dále usnadňuje začlenění bezpečnostních aspektů do celkového fungování organizace.

Výše uvedené metodiky a standardy hrají klíčovou roli při zajišťování komplexní ochrany informačních aktiv organizace. Jejich správná implementace a propojení umožňuje efektivní řízení rizik, dodržování regulačních požadavků a budování důvěryhodného image organizace. [4]

1.7.1 Synergie metodik COBIT, ITIL a ISO 27002

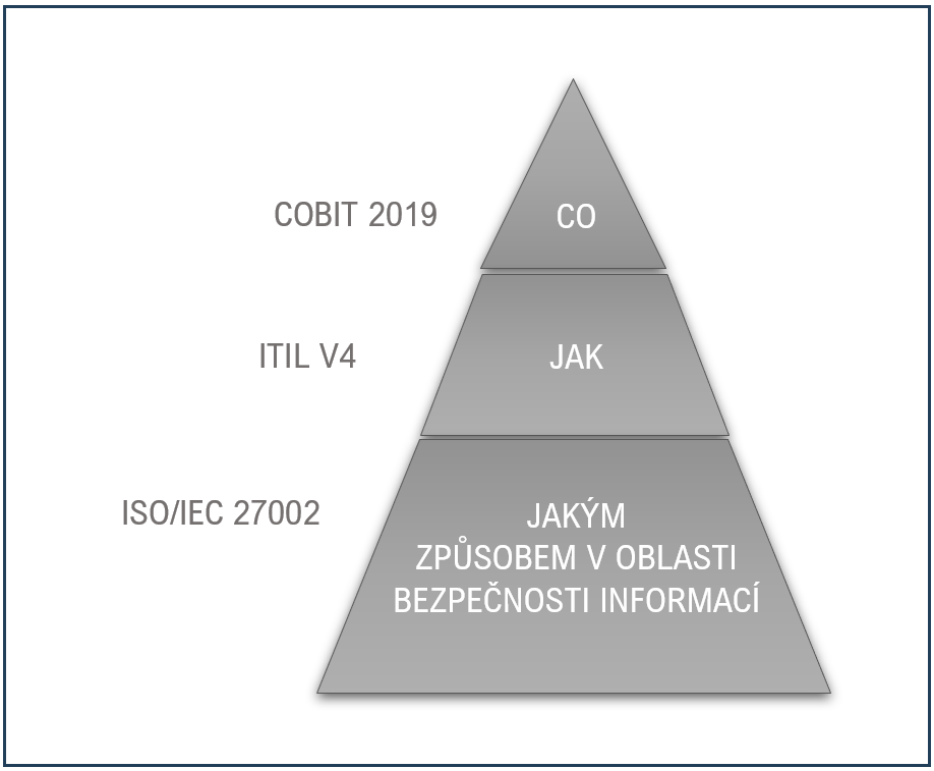
Pro dosažení komplexní správy informační bezpečnosti je vhodné synergicky kombinovat tři klíčové metodiky: COBIT, ITIL a ISO 27002. [6]

COBIT (Control Objectives for Information and Related Technologies) poskytuje rámec pro sladění obchodních cílů s cíli informačních a komunikačních technologií (ICT). Definuje role a odpovědnosti jednotlivých aktérů v rámci organizace a umožňuje efektivní řízení ICT procesů s cílem maximalizovat jejich přínos pro organizaci. [6]

ITIL (Information Technology Infrastructure Library) se zaměřuje na detailní procesy řízení IT s cílem optimalizovat zdroje a vytvářet hodnotu pro zákazníky. Poskytuje osvědčené postupy pro implementaci a správu IT služeb a pomáhá tak organizacím dosahovat jejich cílů efektivněji s nižšími náklady.

ISO 27002 (Information technology — Security techniques — Information security controls) stanovuje cíle a opatření pro řízení bezpečnosti informací. Poskytuje soubor osvědčených praktik pro ochranu informačních aktiv organizace před kybernetickými hrozbami a zajišťuje tak soulad s legislativními požadavky.

Kombinace těchto metodik umožňuje organizacím komplexně a efektivně řídit své informační systémy a data. COBIT zajišťuje strategické propojení ICT s obchodními cíli, ITIL optimalizuje procesy řízení IT a ISO 27002 garantuje robustní ochranu informačních aktiv. Implementace synergického přístupu k těmto třem metodikám umožňuje organizacím dosahovat trvalé konkurenceschopnosti a budovat důvěru u svých zákazníků a partnerů. [6]



Obrázek 6. Porovnání COBIT, ITIL a ISO 27002

1.8 Definice ISMS

Systém řízení informační bezpečnosti (ISMS) představuje ucelený přístup k jejímu zajištění. ISMS není jen soubor pravidel, ale komplexní systém, který zahrnuje všechny aspekty správy informační bezpečnosti v rámci organizace.

Základem ISMS je cyklus PDCA (Demingův cyklus), rozdělený do čtyř fází:

1) **Ustanovení ISMS:** Definice rozsahu a určení odpovědností za informační bezpečnost;

2) **zavádění a provoz ISMS:** Implementace vybraných bezpečnostních opatření a jejich začlenění do fungování organizace;
3) **monitorování a přezkoumání ISMS:** Sledování efektivity zavedených opatření a hodnocení celého systému informační bezpečnosti;
4) **údržba a zlepšování ISMS:** Kontinuální identifikace slabých míst, jejich náprava a zefektivňování celého systému.

Hlavní body:

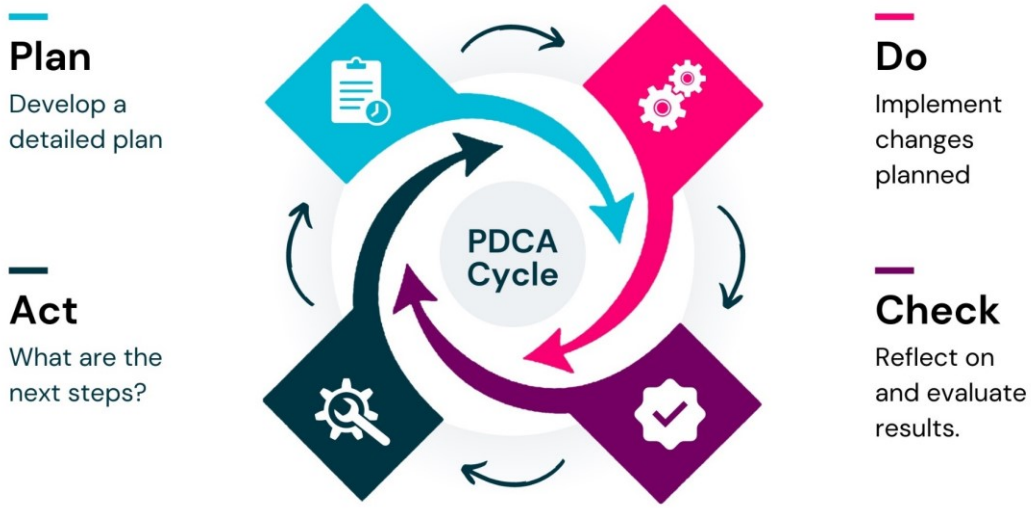
1) ISMS je komplexní systém pro správu informační bezpečnosti;
2) zahrnuje všechny aspekty informační bezpečnosti v rámci organizace;
3) je založen na cyklu PDCA a rozdělen do čtyř fází;
4) cílem ISMS je zajistit trvalou ochranu informačních aktiv organizace; [1]

1.9 PDCA

Jedná se o jednoduchý, ale efektivní nástroj. Cyklus PDCA je kontinuální proces, který se neustále opakuje. Díky němu je možné systematicky zlepšovat své produkty, služby, procesy, aplikace i data a dosahovat tak trvalého růstu a prosperity. [1]

Cyklus PDCA se skládá ze čtyř opakujících se kroků:

1) **Plánuj (Plan):** V první fázi je důležité jasně definovat, co má zlepšit. Stanoví se konkrétní cíle a ujasní se, jak se jich chce dosáhnout. V tomto kroku je klíčové důkladné plánování a analýza stávajícího stavu.
2) **dělej (Do):** Druhý krok spočívá v realizaci naplánovaných aktivit. Naplánované kroky, které byly stanoveny v první fázi cyklu se uvedou do praxe;
3) **kontroluj (Check):** Poté, co implementují změny, je důležité zhodnotit jejich efektivitu. Porovnají se dosažené výsledky s původními cíli a analyzuje se, zda se vám je podařilo naplnit. V této fázi se zaměřujeme na sběr dat a zpětné vazby;
4) **jednej (Act):** Na základě zjištění z fáze kontroly proveďte úpravy v plánu a v samotné realizaci. Pokud se vám podařilo dosáhnout cílů, implementujte provedené změny do praxe. V opačném případě je nutné plán upravit a proces opakovat.



Obrázek 7. Životní cyklus PDCA [10]

1.10 Zákon o kybernetické bezpečnosti

Zákon byl v roce 2014 schválen a v roce 2015 nabyla účinnosti novela zákona o kybernetické bezpečnosti (ZoKB) s cílem posílit ochranu informačních technologií a systémů v České republice. Hlavní důvody pro přijetí zákona zahrnoval nárůst kybernetických hrozeb, jako je kyberterorismus, a rostoucí závislost společnosti na informačních technologiích.

ZoKB definuje práva a povinnosti osob v oblasti kybernetické bezpečnosti a stanovuje pravomoci orgánů veřejné moci. Zákon dále zapracovává relevantní legislativu Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů. Zákon se nevztahuje na systémy nakládající s utajovanými informacemi.

Hlavním cílem ZoKB je stanovit rámec pro efektivní spolupráci mezi soukromým sektorem a veřejnou správou v oblasti kybernetické bezpečnosti. Zákon definuje oprávnění a povinnosti subjektů a má za cíl zvýšit odolnost kybernetického prostoru proti kybernetickým útokům. [3]

1.10.1 Základní pojmy dle ZoKB

ZoKB definuje klíčové pojmy v oblasti kybernetické bezpečnosti, které jsou nezbytné pro pochopení jeho obsahu a aplikace. Mezi nejdůležitější pojmy patří:

1) Kritická informační infrastruktura (KII): Prvky nebo systémy prvků KII v odvětví komunikací a informačních systémů (zákon č. 240/2000 Sb.), které jsou z hlediska kybernetické bezpečnosti kriticky důležité;
2) informační systém základní služby: Informační systém, na jehož fungování je závislé poskytování základní služby;
3) významný informační systém: Informační systém spravovaný orgánem veřejné moci, který není KII, ale jehož narušení by mohlo omezit nebo výrazně ohrozit fungování orgánu veřejné moci;
4) významná síť: Síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo přímé připojení ke KII;
5) základní služba: Služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na fungování společnosti v některém z odvětví uvedených v § 3 písm. i) ZoKB;
6) digitální služba: Služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která zahrnuje:
    a. On-line tržiště: Platforma umožňující spotřebitelům a prodávajícím uzavírat kupní smlouvy nebo smlouvy o poskytování služeb;
    b. Internetový vyhledávač: Nástroj pro vyhledávání informací na internetu na základě dotazu uživatele;
    c. Cloud computing: Služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti a výpočetním zdrojům, které je možné sdílet.

1.10.2 Nová směrnice - NIS2

Při aktuální fázi, kdy je směrnice připravována, by měla většina firem provést následující kroky, kterými by měla zjistit svůj aktuální stav k nové kybernetické směrnici. Níže jsou vypsány důležité informace o chystané směrnici: [18]

1) Nejprve je nutné zjistit, jestli konkrétní subjekt spadá mezi povinné subjekty. Doporučuje se provést předběžnou analýzu, aby se určilo, zda se NIS2 vztahuje na daný podnik. Pokud ano, poté se určí, do které kategorie spadá;

2) nová směrnice o kybernetické bezpečnosti může nabrat zpoždění oproti požadované lhůtě EU stanovené dne 17. října 2024, s očekávanou účinností od ledna 2025 nebo později;
3) směrnice vzniká z důvodu nutnosti implementace evropské bezpečnostní směrnice NIS2 a řeší mechanismus prověřování bezpečnosti dodavatelského řetězce;
4) směrnice NIS2 bude mít dopad na více než 6 000 firem oproti současným 400 organizacím, a také na 170 subjektů v oblastech telekomunikací, energetiky, veřejné správy a dopravy;
5) v rámci meziresortního připomínkového řízení bylo podáno 886 připomínek od 51 subjektů. Přibližně dvě třetiny připomínek byly akceptovány nebo částečně akceptovány, zbytek byl zamítnut kvůli potenciální nefunkčnosti navrhovaných úprav;
6) některé firmy vyjádřily obavy z ekonomických ztrát spojených se zákazem některých dodavatelů. Lhůty pro odstranění zařízení by měly odpovídat jejich odpisům;
7) při nezavedení hrozí podnikům pokuty až 10 milionů eur nebo 2 % ze světového obratu a postihy pro nejvyšší management. [18]

Nově budou mít firmy např. povinnost: [19]

1) Hodnocení a řízení rizik: Identifikace slabých stránek a rizik spojených s informačními systémy a daty je klíčová pro zavedení efektivního systému kybernetické bezpečnosti. Toho lze dosáhnout zavedením procesů pro hodnocení a analýzu rizik;
2) ochrana dat a informací: Implementace technických a organizačních opatření k zajištění důvěrnosti, integrity a dostupnosti dat a informací je nezbytná pro prevenci kybernetických útoků. Patří sem například šifrování dat, zálohování a implementace kontrol přístupu;
3) vzdělávání a povědomí: Zvyšování povědomí a vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti je klíčové pro minimalizaci lidského faktoru, který představuje významné riziko pro kybernetickou bezpečnost. Zaměstnanci by měli být obeznámeni s běžnými hrozbami, kybernetickými útoky a postupy pro hlášení podezřelých aktivit;

4) ochrana před útoky a reakce na incidenty: Implementace technických a organizačních opatření k detekci, prevenci a reakci na kybernetické útoky je nezbytná pro minimalizaci dopadů incidentů. Patří sem například firewally, systémy detekce narušení a plány pro reakci na incidenty;
5) obnova provozu: Zavedení procesů a plánů pro obnovu provozu a dat v případě kybernetického útoku nebo havárie je nezbytné pro minimalizaci downtime a dopadů na chod organizace. Plány obnovy by měly zahrnovat zálohování dat, testování procesů obnovy a komunikaci s relevantními stakeholders.

Těchto pět bodů je pouze skromný výčet z několika dalších povinností. Hospodářská komora ve svém dopise premiérovi České republiky uvedla, že dopady přicházejícího připravovaného kybernetického zákona do podnikatelské sféry mohou převýšit 65 miliard korun. [19]

1.11 Východiska směrnice NIS2 a ISO/IEC 27001:20222

Norma ISO/IEC 27001:2022 a směrnice NIS2 jsou navzájem propojeny, protože obě se zaměřují na zajištění vysoké úrovně bezpečnosti informací v organizacích, avšak každá s trochu odlišným přístupem.

1.11.1 NIS2 (Network and Information Systems Directive 2)

1) Regulace na úrovni EU: NIS2 je právně závazná směrnice v rámci Evropské unie, která klade důraz na zajištění kybernetické bezpečnosti kritických infrastruktur a základních služeb napříč členskými státy;
2) právní Požadavky: NIS2 stanovuje právní rámec a povinnosti pro provozovatele základních služeb a digitálních služeb, včetně povinnosti hlásit kybernetické incidenty a dodržovat minimální standardy bezpečnosti;
3) široký Dosah: Cílem NIS2 je zajistit vysokou úroveň kybernetické odolnosti v rámci celé EU, což zahrnuje nejen technické a organizační opatření, ale také koordinaci mezi státy a sdílení informací. [8]

1.11.2 ISO/IEC 27001:2022

1) Mezinárodní Standard: ISO/IEC 27001 je mezinárodně uznávaný standard pro systém řízení bezpečnosti informací (ISMS), který poskytuje rámec pro zavádění, udržování a neustálé zlepšování bezpečnostních procesů v organizacích;
2) procesní Přístup: Norma se zaměřuje na systematické řízení rizik a procesní přístup k bezpečnosti, zahrnující identifikaci, hodnocení a ošetření rizik souvisejících s informačními aktivy;
3) flexibilita: ISO/IEC 27001 je navržena tak, aby byla flexibilní a přizpůsobitelná různým typům organizací bez ohledu na jejich velikost nebo obor, což umožňuje přizpůsobení konkrétním potřebám a hrozbám. [9]

1.12 Ekonomický pohled na zavedení ISMS

Organizace má svobodu navrhnout a implementovat vlastní opatření pro zajištění informační bezpečnosti, ať už z interních zdrojů nebo s využitím externích poznatků. Při výběru a implementaci těchto opatření je důležité zvážit poměr mezi vynaloženými náklady a dosaženým přínosem pro organizaci.

Podrobnější pokyny pro posouzení ekonomické návratnosti investic do informační bezpečnosti a analýzu dopadů na chod organizace naleznete v normě ISO/IEC TR 27016:2014. Tato norma se zabývá problematikou rozhodování o investicích do systému řízení informační bezpečnosti (ISMS) a jejich ekonomickými důsledky v kontextu konkurenčních požadavků na zdroje. [4]

Klíčovým principem je najít rovnováhu mezi investicemi do preventivních opatření a potenciálními ztrátami v důsledku kybernetických incidentů. Výstupy z posouzení rizik by měly sloužit jako vodítko pro vedení organizace a pro prioritizaci kroků v oblasti řízení informačních rizik. Grafické znázornění problematiky je obsaženo v kapitole 4.6 normy ISO/IEC 27001:2013. [4]

Implementace efektivního systému řízení informační bezpečnosti přináší organizaci řadu ekonomických benefitů, které lze rozdělit do dvou kategorií:

1) Prevence negativních dopadů;
    a. Minimalizace negativních dopadů na obchodní cíle organizace;
    b. omezení finančních ztrát;

c. vyhnutí se nutnosti navyšovat kapitálové rezervy pro krytí neočekávaných událostí.

2) další benefity;

a. Možnost participace na projektech s vyšším stupněm rizika;

b. dodržování právních a regulačních požadavků;

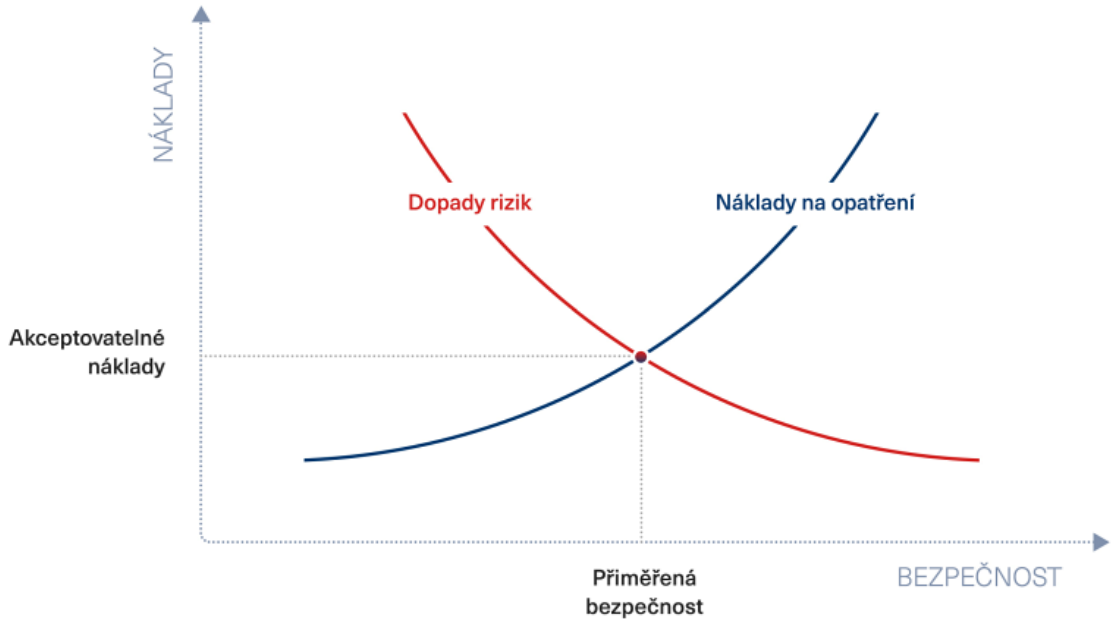
c. plnění očekávání zákazníků a komunity;

d. udržování důvěryhodné reputace organizace;

e. zajištění integrity a přesnosti účetnictví.

Rozsah a výše investic do zabezpečení informačního systému (IS) by měly odpovídat hodnotě chráněných aktiv a míře potenciálních rizik. Základní rámec pro toto hodnocení a alokaci zdrojů stanovuje bezpečnostní politika organizace. [4]

Na obrázku č. 9 jsou vyznačeny osy náklady a bezpečnost. Modře znázorněná křivka symbolizuje náklady na opatření, kdy pro vyšší bezpečnost, je zapotřebí vyšších nákladů na zabezpečení. Červená křivka zobrazuje, jak se s klesajícími výdaji na zabezpečení snižuje úroveň bezpečnosti.



Obrázek 8. Graf přiměřených nákladů na bezpečnost [12]

1.13 Klasifikace informací

Klasifikace informací je proces, který organizacím umožňuje seskupovat informační aktiva do relevantních kategorií podle úrovně jejich citlivosti a důležitosti. Tento proces je klíčový pro efektivní správu a ochranu informací. Klasifikace informací pomáhá určit, jaké bezpečnostní opatření je potřeba použít k ochraně různých typů dat, což je nezbytné pro dodržování právních a regulačních požadavků, stejně jako pro minimalizaci rizik spojených s únikem nebo ztrátou dat.

Proces klasifikace obvykle zahrnuje následující kroky: identifikaci všech informačních aktiv, určení vlastníků informací, hodnocení citlivosti a hodnoty těchto aktiv, přiřazení klasifikačních úrovní a zavedení odpovídajících kontrolních opatření. Klasifikace může být provedena na základě různých kritérií, včetně toho, kdo by měl mít přístup k informacím, jaké dopady by měla ztráta nebo zveřejnění informací, a jaké jsou zákonné požadavky na ochranu těchto dat. [28]

Klasifikace informací je často definována ve standardech, jako je ISO/IEC 27001 a ISO/IEC 27002. Klasifikace zajišťuje, že všechny citlivé informace jsou náležitě chráněny a spravovány [28].

V praxi se můžeme nejběžněji setkat s rozdělením do tří nebo čtyř kategorií. To je pro většinu firem zcela dostatečné. nejčastější a nejjednodušší formou klasifikace je rozdělování informací do následujících bodů 2,3 a 4. [13]

1) Důvěrné informace (confidential);
2) informace s omezeným přístupem (restricted);
3) interní informace (Internal use);
4) veřejné informace (Public).

Pro lepší přehled a bezpečnější práci s dokumenty nebo soubory se také dále používá podrobnější členění do více kategorií:

1) Veřejné informace (public)
2) interní informace (internal);
3) důvěrné informace (confidential);
    a. personálně důvěrné informace (personal confidential);

b. obchodně důvěrné informace (company confidential);

c. firemně důvěrné informace (business confidential).

Tabulka č. 1 popisuje úrovně důvěrnosti informací, jejich klasifikaci, stručný popis a požadovaná bezpečnostní opatření. Jedná se o tabulku zpracovanou od Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Tabulka 1. Vzorová pravidla ochrany úrovní aktiv (převzato a upraveno) [12]

Úroveň důvěrnosti	Klasifikace informací	Popis	Požadovaná bezpečnostní opatření
Nízká	Veřejné	Informace je veřejně přístupná nebo byla určena ke zveřejnění. Informace může být dále poskytována a šířena bez omezení.	Není vyžadována žádná ochrana.
Střední	Interní	Informace nejsou veřejně přístupné a tvoří know-how. Může být sdílena v rámci organizace a s partnery při zajištění důvěrnosti.	Využívány prostředky pro řízení přístupu.
Vysoká	Citlivé	Informace nejsou veřejně přístupné a vyžadují nadstandardní ochranu (např. obchodní tajemství, osobní údaje). Lze sdílet jen s určenými osobami se souhlasem původce.	Prostředky pro řízení a zaznamenávání přístupu, kryptografické prostředky.
Kritická	Diskrétní	Informace nejsou veřejně přístupné a vyžadují nadstandardní ochranu. Sdílení jen s určenými osobami.	Prostředky pro řízení a zaznamenávání přístupu, kryptografické prostředky.

Tabulka č.1 byla pro lepší přehlednost upravena. Obsahuje čtyři úrovně (Nízká, Střední, Vysoká, Kritická) a uvádí, jaké ochranné prostředky jsou vyžadovány pro zajištění důvěrnosti a bezpečnosti informací v každé kategorii.

II. PRAKTICKÁ ČÁST

2 KOMPARACE NORMY ISO/IEC 27002:2013 S NORMOU ISO/IEC 27002:2022

Pro práci s novou verzí normy je vhodné znát, jaké změny nastaly. Norma pro oblast informační bezpečnosti prošla v roce 2022 aktualizací, která reflektuje dynamický vývoj technologií, globalizaci a měnící se potřeby uživatelů i zúčastněných stran. I když se nejedná o rozsáhlou revizi, zavádí důležité úpravy, které zefektivňují procesy a posilují celkový systém řízení informační bezpečnosti (ISMS). Níže jsou zobrazeny původní a aktuální okruhy kontrol a také je zde popsán souhrn nově zavedené normy:

Tabulka 2. Okruh kontrol ISO 27002:2013 [6]

Označení	Okruh kontrol	Počet kontrol
A.5	Politiky informační bezpečnosti	2
A.6	Organizace informační bezpečnosti	7
A.7	Bezpečnost lidských zdrojů	6
A.8	Správa aktiv	6
A.9	Kontrola přístupu	14
A.10	Kryptografie	2
A.11	Fyzická a environmentální bezpečnost	15
A.12	Bezpečnost provozu	14
A.13	Komunikační bezpečnost	7
A.14	Akvizice, vývoj a údržba systémů	13
A.15	Vztahy se dodavateli	5
A.16	Řízení incidentů v oblasti informační bezpečnosti	7
A.17	Aspekty informační bezpečnosti řízení kontinuity podnikání	4
A.18	Dodržování	8

Původních **14** oddílů přílohy A se nyní zaměřuje na **4** následující témata:

Tabulka 3. Okruh kontrol ISO 27002:2022 [6]

Označení	Okruh kontrol	Počet kontrol
A.5	Organizační kontroly	37
A.6	Osobní kontroly	8
A.7	Fyzické kontroly	14
A.8	Technické kontroly	34

Příloha A standardu ISO/IEC 27001:2022 definuje kontroly, zatímco implementační příručka ISO/IEC 27002:2022 nabízí rozšířené metody jejich kategorizace. Ke každému opatření je přiřazeno pět atributů usnadňujících jejich zařazení. Tyto atributy umožňují filtrování, třídění a zobrazení opatření z různých organizačních perspektiv. Znázorněno v tabulce č. 4. [7]

Tabulka 4. Tabulka s atributy v příloze A.

Typ opatření	Vlastnosti informační bezpečnosti	Koncepty kybernetické bezpečnosti	Provozní schopnosti	Domény bezpečnosti

2.1 Souhrn hlavních změn

Norma ISO/IEC 27002/2022 byla podrobena nižšímu počtu kontrol z původních 114 na 93 kontrol. Nyní je tedy celkový počet o 21 kontrol menší. Na obrázku č. 10 je graficky znázorněno, jak se změnily kapitoly pro daná opatření.

Obrázek 9. Transformace ISO 27001:2013 na ISO 27001:2022 [11]

V aktualizaci normy ISO 27001:2022 došlo k několika významným změnám zaměřeným na zlepšení a zjednodušení řízení bezpečnosti informací. Jednou z hlavních změn bylo sloučení 57 kontrol do 25, což přispělo ke snížení celkového počtu kontrol. Tento krok zefektivnil strukturu a umožnil lepší správu těchto kontrolních opatření, aniž by došlo ke ztrátě jejich účinnosti nebo pokrytí požadavků.

Dále bylo zavedeno 11 nových kontrol, které reflektují aktuální bezpečnostní výzvy a technologické pokroky. Tyto nové kontroly zahrnují moderní aspekty, jako jsou ochrana proti kybernetickým útokům a zajištění bezpečnosti cloudových služeb.

Kromě toho byly tři kontroly odstraněny protože nebyly považovány za nezbytné v rámci současného bezpečnostního prostředí.

Aby byla norma srozumitelnější, bylo 23 kontrol přejmenováno. Tato změna usnadňuje pochopení a implementaci kontrolních opatření, čímž se zvyšuje jejich efektivnost při řízení bezpečnosti informací.

Tabulka 5. Souhrn hlavních změn

Změna ve skupině kontrol	Počet kontrol
Sloučené kontroly	57
Nové kontroly	11
Smazané kontroly	3
Kontroly beze změn	35
Přejmenované kontroly	23

Tabulka č. 5 porovnává změny v normě ISO/IEC 27001 a to konkrétně provázanost kontrolních opatření z předchozích kapitol do nových sloučených kapitol. Na levé straně tabulky jsou uvedeny nové sloučené kapitoly, kterých je celkem 25, zatímco na pravé straně jsou uvedeny původní kapitoly, těch bylo celkem 57. Každá kapitola obsahuje specifická opatření týkající se řízení bezpečnosti informací, která byla sloučena pro zjednodušení a efektivnější správu.

Tabulka také ukazuje, jak byly některé nové kapitoly vytvořeny z kombinace více původních kapitol. Například nová kapitola 5.9 "Evidence informací a dalších souvisejících aktivit" zahrnuje opatření z kapitol 8.1.1 a 8.1.2.

Tabulka 6. Sloučená opatření nové verze normy

Sloučená opatření (25)		**Předchozí opatření (57)**
Kapitola	**Název kapitoly**	**Předchozí kapitola**
5.1	Politiky pro informační bezpečnost	5.1.1 & 5.1.2
5.8	Informační bezpečnost v řízení projektů	6.1.5 & 14.1.1
5.9	Evidence informací a dalších souvisejících aktivit	8.1.1 & 8.1.2
5.10	Přípustné používání informací a dalších souvisejících aktivit	8.1.3 & 8.2.3
5.14	Předávání informací	13.2.1 & 13.2.2 & 13.2.3
5.15	Řízení přístupu	9.1.1 & 9.1.2
5.16	Vrácení aktiv	9.2.1 & 9.4.3
5.17	Autentizační informace	9.2.4 & 9.3.1 & 9.4.3
5.18	Přístupová práva	9.2.2 & 9.2.5 & 9.2.6
5.22	Monitorování, přezkoumávání a řízení změn dodavatelských služeb	15.2.1 & 15.2.2

5.29	Informační bezpečnost během narušení	17.1.1 & 17.1.2 & 17.1.3
5.31	Zákonné, statutární, regulatorní a smluvní požadavky	18.1.1 & 18.1.5
5.36	Dodržování politik, pravidel a norem pro informační bezpečnost	18.2.2 & 18.2.3
6.8	Podávání zpráv o událostech informační bezpečnosti	16.1.2 & 16.1.3
7.2	Fyzický vstup	11.1.2 & 11.1.6
7.10	Paměťová média	8.3.1 & 8.3.2 & 8.3.3 & 11.2.5
8.1	Koncová zařízení uživatele	6.2.1 & 11.2.8
8.8	Management technických zranitelností	12.6.1 & 18.2.3
8.15	Zaznamenávání formou logů	12.4.1 & 12.4.2 & 12.4.3
8.19	Instalace softwaru na provozních systémech	12.5.1 & 12.6.2
8.24	Používání kryptografie	10.1.1 & 10.1.2 & 18.1.5
8.26	Požadavky na bezpečnost aplikací	14.1.2 & 14.1.3
8.29	Testování bezpečnosti při vývoji a akceptaci	14.2.8 & 14.2.9
8.31	Oddělení prostředí vývoje, testování a produkce	12.1.4 & 14.2.6
8.32	Management změn	12.1.2 & 14.2.2 & 14.2.3 & 14.2.4

V tabulce č. 6 jsou uvedeny nové kapitoly, které byly zavedeny v aktualizované normě ISO/IEC 27001. Každá kapitola se zaměřuje na specifické aspekty řízení bezpečnosti informací.

Tabulka 7. Nově přidané kontroly do ISO 27001:2022

Kapitola	Název nové kapitoly
5.7	Zpravodajství o hrozbách
5.23	Informační bezpečnost při používání cloudových služeb
5.30	Připravenost ICT na zajištění kontinuity činnosti organizace
7.4	Monitorování fyzické bezpečnosti
8.9	Management konfigurace
8.10	Vymazání informací
8.11	Maskování dat
8.12	Prevence úniku dat
8.16	Monitorovací činnosti
8.23	Filtrování webových stránek
8.28	Bezpečné programování

3 ANALÝZU SOUČASNÉHO STAVU ISMS V PODNIKU

Pro kontrolu využitelnosti vytvořeného programu pro tuto diplomovou práci, tedy programu pro komparaci norem ISO/IEC 27001:2013 a ISO/IEC 27001:2022, byla provedena analýza, při které tento program vypomáhal. Analýza současného stavu byla provedena pro podnik, v němž je již ISMS zavedené a podnik splňuje certifikaci pro normu ISO/IEC 27001:2013. V tomto případě se tedy bude jednat spíše o revizi a případné doplnění nových opatření.

Aby bylo možné analýzu vyhodnotit číselnou formou, bude výsledné hodnocení každé kapitoly vypočteno za pomoci následující formule:

$$Výsledné\ hodnocení = \frac{\text{Počet relevantních aplikovaných opatření}}{\text{Počet relevantních celkových opatření}} * 100\ (\%)$$

Níže jsou zpracovány všechny body nově revidované normy ISO/IEC 27001:2022. Tabulky jsou rozděleny do následujících oblastí:

1) Kapitola č. 5 - Organizační opatření;
2) kapitola č. 6 - Opatření v oblasti lidských zdrojů;
3) kapitola č. 7 - Opatření fyzické bezpečnosti;
4) kapitola č. 8 - Technologická opatření.

Pro vyšší hodnotu akademické práce byly autorem této práce zpracovány otázky, které byly vytvořeny na základě znění normy ISO 27001:2022. Byly zformulovány tak, aby osoba, která si bude případně zpracovávat vlastní kontrolu plnění opatření z normy, mohla jen pokládat otázky a následně na ně hledat odpověď. Níže je zobrazena tabulka která byla v praxi aplikována na existující objekt a byl tak zjištěn aktuální bezpečnostní stav ISMS v podniku. Je důležité zmínit, že aktuálně daný podnik obdržel certifikaci normy ISO/IEC:27001:2013. Je v zájmu podniku obdržet certifikaci normy ISO/IEC:27001:2022.

Tabulka 8. Kontrolní otázky: organizačních opatření

Kapitola	Dotaz	Plněno
5		
5.1	Jakým způsobem je vaše politika informační bezpečnosti definována, schválena, zveřejněna a jak často je přezkoumávána?	Ano
5.2	Jak jsou ve vaší organizaci definovány a přidělovány role a odpovědnosti v oblasti informační bezpečnosti?	Ano
5.3	Jak zajišťujete oddělení protichůdných povinností a oblastí odpovědnosti ve vaší organizaci?	Ano
5.4	Jakým způsobem vedení zajišťuje, že zaměstnanci dodržují politiku informační bezpečnosti a související postupy?	Ano
5.5	Jakým způsobem vaše organizace udržuje kontakt s příslušnými autoritami?	Ano
5.6	Jak vaše organizace udržuje kontakt se zvláštními zájmovými skupinami a odbornými fóry v oblasti bezpečnosti?	Ano
5.7	Jakým způsobem shromažďujete a analyzujete informace o hrozbách?	Ne
5.8	Jak integrujete informační bezpečnost do řízení projektů ve vaší organizaci?	Ano
5.9	Jakým způsobem vytváříte a udržujete inventář informací a aktiv, včetně jejich vlastníků?	Ano
5.10	Jak jsou definována a dokumentována pravidla pro používání informací a aktiv ve vaší organizaci?	Ano
5.11	Jakým způsobem zajišťujete, že zaměstnanci po ukončení pracovního poměru vrátí všechna aktiva organizace?	Ano
5.12	Jakým způsobem klasifikujete informace podle jejich hodnoty a důležitosti?	Ano
5.13	Jaké postupy máte zavedeny pro označování informací podle klasifikačního systému?	Ano
5.14	Jak jsou zavedena pravidla pro předávání informací pro všechny typy přenosových zařízení ve vaší organizaci?	Ano

5.15	Jakým způsobem jsou vytvořena a zavedena pravidla pro fyzický a logický přístup k informacím a aktivům ve vaší organizaci?	Ano
5.16	Jakým způsobem řídíte celý životní cyklus identit ve vaší organizaci?	Ano
5.17	Jakým způsobem spravujete a chráníte autentizační informace ve vaší organizaci?	Ano
5.18	Jak pravidelně přezkoumáváte a upravujete přístupová práva k informacím a aktivům ve vaší organizaci?	Ano
5.19	Jaké procesy máte zavedeny pro řízení rizik spojených s používáním produktů dodavatelů?	Ano
5.20	Jakým způsobem stanovujete požadavky na bezpečnost informací ve vztazích s dodavateli?	Ano
5.21	Jakým způsobem sjednáváte požadavky na informační bezpečnost s každým dodavatelem podle typu vztahu?	Ano
5.22	Jaké procesy máte zavedeny pro řízení rizik informační bezpečnosti v celém dodavatelském řetězci ICT?	Ano
5.23	Jakým způsobem zajišťujete, že procesy pro správu cloudových služeb splňují požadavky na informační bezpečnost?	Ne
5.24	Máte vytvořený plán pro řešení incidentů informační bezpečnosti, včetně definovaných procesů a odpovědností? Jak tento plán vypadá?	Ano
5.25	Jakým způsobem rozhodujete, zda události spadají do kategorie informační bezpečnosti a jak podle toho jednáte?	Ano
5.26	Jak reagujete na incidenty informační bezpečnosti podle zavedených postupů?	Ano
5.27	Jakým způsobem využíváte získané poznatky z incidentů k zlepšení opatření informační bezpečnosti?	Ano
5.28	Jak zajišťujete shromažďování a uchovávání důkazů spojených s incidenty informační bezpečnosti?	Ano
5.29	Jak zajišťujete odpovídající úroveň informační bezpečnosti během narušení?	Ano

5.30	Jak plánujete a testujete připravenost ICT na zajištění kontinuity činnosti vaší organizace?	Ne
5.31	Jakým způsobem zajišťujete splnění všech zákonných, statutárních a smluvních požadavků týkajících se informační bezpečnosti?	Ano
5.32	Jak chráníte práva duševního vlastnictví ve vaší organizaci?	Ano
5.33	Jak zajišťujete ochranu záznamů před ztrátou, zničením a neoprávněným přístupem?	Ano
5.34	Jakým způsobem zajišťujete splnění požadavků na ochranu soukromí a osobních údajů (PII)?	Ano
5.35	Jak často a jakým způsobem provádíte nezávislé přezkoumání informační bezpečnosti?	Ano
5.36	Jakým způsobem pravidelně kontrolujete a přezkoumáváte dodržování politik a norem pro informační bezpečnost?	Ano
5.37	Jak zajišťujete, aby byly provozní postupy dokumentovány a zpřístupněny pracovníkům, kteří je potřebují?	Ano

Tabulka 9. Kontrolní otázky opatření: oblast lidských zdrojů

Kapitola	Dotaz	Plněno
6		
6.1	Jakým způsobem provádíte prověřování uchazečů před nástupem i během pracovního poměru v souladu se zákony a etickými normami?	Ano
6.2	Jak jsou v pracovních smlouvách uvedeny odpovědnosti za informační bezpečnost?	Ano
6.3	Jakým způsobem školíte a informujete zaměstnance o bezpečnostních politikách a postupech?	Ano
6.4	Jaké postupy máte stanoveny pro disciplinární opatření při porušení bezpečnostních politik?	Ano
6.5	Jakým způsobem dokumentujete odpovědnosti za bezpečnost i po ukončení pracovního poměru?	Ano
6.6	Jak často přezkoumáváte a podepisujete dohody o důvěrnosti?	Ano

6.7	Jaká bezpečnostní opatření máte zavedena pro práci na dálku?	Ano
6.8	Jaký mechanismus mají zaměstnanci pro hlášení bezpečnostních událostí?	Ano

Tabulka 10. Kontrolní otázky opatření: fyzická bezpečnost

Kapitola	Dotaz	Plněno
7		
7.1	Jak definujete a používáte bezpečnostní perimetry ve vaší organizaci?	Ano
7.2	Jaká opatření máte zavedena pro ochranu vstupu do zabezpečených oblastí?	Ano
7.3	Jaká opatření pro fyzickou bezpečnost kanceláří máte zavedena?	Ano
7.4	Jak monitorujete prostory pro zajištění neoprávněného přístupu?	Ano
7.5	Jakým způsobem chráníte prostory před fyzickými a přírodními hrozbami?	Ano
7.6	Jaká bezpečnostní opatření máte zavedena pro práci v zabezpečených oblastech?	Ano
7.7	Jaká pravidla prázdného stolu a obrazovky máte zavedena pro ochranu informací?	Ano
7.8	Jak zajišťujete bezpečné umístění a ochranu zařízení?	Ano
7.9	Jakým způsobem chráníte aktiva mimo prostory organizace?	Ano
7.10	Jak nakládáte s paměťovými médii podle stanovených pravidel a postupů?	Ano
7.11	Jak chráníte zařízení pro zpracování informací před výpadky napájení a jinými poruchami služeb?	Ano
7.12	Jak chráníte kabelové rozvody před odposloucháváním, rušením nebo poškozením?	Ano
7.13	Jakým způsobem provádíte údržbu zařízení pro zajištění dostupnosti a integrity informací?	Ano
7.14	Jak zajišťujete bezpečnou likvidaci nebo opakované použití zařízení s paměťovými médii, aby byla odstraněna všechna citlivá data a software?	Ano

Tabulka 11. Kontrolní otázky opatření: Technologická opatření

Kapitola	Dotaz	Plněno
8		
8.1	Jakým způsobem chráníte informace na koncových zařízeních uživatelů?	Ano
8.2	Jakým způsobem omezujete a řídíte používání privilegovaných přístupových práv?	Ano
8.3	Jak omezujete přístup k informacím podle politiky řízení přístupu?	Ano
8.4	Jakým způsobem řídíte přístup ke zdrojovému kódu?	Ano
8.5	Jaké bezpečné autentizační postupy máte implementovány?	Ano
8.6	Jak monitorujete a upravujete využití zdrojů podle požadavků na kapacitu?	Ano
8.7	Jak implementujete a podporujete ochranu před škodlivým softwarem?	Ano
8.8	Jak získáváte a vyhodnocujete informace o technických zranitelnostech a jaká opatření přijímáte?	Ano
8.9	Jak dokumentujete, implementujete a přezkoumáváte konfigurace, včetně konfigurací bezpečnosti hardware, software a služeb?	Ne
8.10	Jakým způsobem zajišťujete vymazání informací, které již nejsou potřebné?	Ne
8.11	Jakým způsobem je zajištěno, že maskování dat je prováděno v souladu s politikou organizace a právními předpisy?	Ne
8.12	Jaká opatření pro prevenci úniku dat máte aplikována na systémy zpracovávající citlivé informace?	Ne
8.13	Jakým způsobem testujete a udržujete záložní kopie informací?	Ano
8.14	Jak zajišťujete dostatečnou redundanci vybavení pro zpracování informací?	Ano
8.15	Jakým způsobem vytvářítе, uchováváte a analyzujete logy činností, výjimek a chyb?	Ano
8.16	Jak monitorujete sítě, systémy a aplikace kvůli bezpečnostním anomáliím?	Ne

8.17	Jak zajišťujete synchronizaci hodin informačních systémů s autorizovanými zdroji času?	Ano
8.18	Jakým způsobem omezujete a kontrolujete používání privilegovaných programů?	Ano
8.19	Jaké bezpečné postupy máte zavedeny pro instalaci software na provozních systémech?	Ano
8.20	Jak zabezpečujete sítě a síťová zařízení proti neoprávněnému přístupu?	Ano
8.21	Jak identifikujete a monitorujete bezpečnostní mechanismy síťových služeb?	Ano
8.22	Jakým způsobem oddělujete sítě pro různé služby, uživatele a systémy?	Ano
8.23	Jak filtrujete přístup na webové stránky kvůli škodlivému obsahu?	Ano
8.24	Jaká pravidla máte zavedená pro bezpečné používání kryptografie a správu klíčů?	Ano
8.25	Jaké postupy máte zavedené pro bezpečný vývoj software a systémů?	Ano
8.26	Jakým způsobem zohledňujete bezpečnostní požadavky při vývoji a nákupu aplikací?	Ano
8.27	Jakým způsobem uplatňujete bezpečnostní principy architektury při vývoji systémů?	Ano
8.28	Jaké zásady bezpečného programování dodržujete při vývoji software?	Ne
8.29	Jak provádíte testování bezpečnosti během vývoje a akceptace software?	Ano
8.30	Jak řídíte a přezkoumáváte činnosti externích zdrojů pro vývoj?	Ano
8.31	Jakým způsobem zajišťujete oddělení a zabezpečení vývojového, testovacího a produkčního prostředí?	Ano
8.32	Jakým způsobem řídíte změny v systémech v souladu s postupy pro změny?	Ano
8.33	Jak chráníte a spravujete informace použité pro testování?	Ano
8.34	Jak plánujete a schvalujete auditní testy a ověřování?	Ano

3.1 Vyhodnocení analýzy stavu ISMS v podniku

Tabulka č. 8 se zaměřuje na hodnocení opatření v oblasti informační bezpečnosti v organizaci. Obsahuje 37 otázek, z nichž 34 bylo odpovězeno kladně. Organizace prokázala silné řízení informační bezpečnosti. V oblasti cloudových služeb (5.23) však organizace dosud neprokázala odpovídající opatření. Tyto mezery představují potenciální rizika, která je třeba řešit pro dosažení plné shody s požadavky na informační bezpečnost.

Tabulka č. 9 se zaměřuje na kontrolní otázky v oblasti lidských zdrojů. Organizace odpověděla kladně na všechny otázky, což naznačuje, že má dobře zavedené procesy pro prověřování uchazečů (6.1), školení a informování zaměstnanců (6.3), disciplínu při porušení bezpečnostních politik (6.4), a ochranu bezpečnosti při práci na dálku (6.7). Tyto odpovědi ukazují na silnou kulturu informační bezpečnosti a odpovědnosti mezi zaměstnanci.

Tabulka č. 10 se věnuje opatřením pro fyzickou bezpečnost. Organizace opět odpověděla kladně na všechny otázky, což znamená, že má zavedené bezpečnostní perimetry (7.1), opatření pro ochranu vstupu do zabezpečených oblastí (7.2), a postupy pro ochranu před fyzickými a přírodními hrozbami (7.5). Tato opatření zajišťují, že fyzické prostředí organizace je dobře chráněné a přístup k citlivým oblastem je řízený.

Tabulka č. 11 obsahuje technologická opatření a pokrývá širokou škálu bezpečnostních aspektů, včetně ochrany informací na koncových zařízeních (8.1), řízení přístupu (8.3), a ochrany před škodlivým softwarem (8.7). Zatímco většina otázek byla odpovězena kladně, některé oblasti, jako dokumentace a přezkoumání konfigurací (8.9), vymazání informací (8.10), maskování dat (8.11), a prevence úniku dat (8.12) nebyly splněny. Tyto poslední zmíněné body jsou totiž nově zavedená opatření, které bude muset organizace zpracovat a implementovat do provozu. Tyto oblasti představují technologické zranitelnosti, které by měly být prioritně řešeny.

Celkově vzato všechny oblasti vykazují vysokou míru realizace opatření, přičemž lidské zdroje a fyzická bezpečnost dosáhly plné implementace (100 %). Technologická opatření a organizační opatření mají také velmi vysoké procento realizace, 82 % a 92 %.

Tabulka 12. Vyhodnocení stavu ISMS v podniku

Kapitola č. 5: Organizační opatření		Výsledek (%)
Aplikovaných opatření	34	92
Celkem opatření	37	
Kapitola č. 6: Opatření v oblasti lidských zdrojů		
Aplikovaných opatření	8	100
Celkem opatření	8	
Kapitola č. 7: Opatření fyzické bezpečnosti		
Aplikovaných opatření	14	100
Celkem opatření	14	
Kapitola č. 8: Technologická opatření		
Aplikovaných opatření	28	82
Celkem opatření	34	

4 IMPLEMENTAČNÍ PROCES PRO NORMU ISO/IEC 27001:2022

Pokud organizace neprovede kroky potřebné pro přechod na aktualizovanou verzi normy ISO/IEC 27002:2022, respektive ISO/IEC 27001:2022, skončí platnost jejich certifikátu. Přechodové období je tříleté, které končí do 31. 10. 2025. Od 1. 11. 2025 budou tedy certifikáty dle ISO/IEC 27001:2013 neplatné ve všech podnicích.

Při práci s normou ČSNE EN ISO/IEC 27002:2022 bylo zjištěno, chybí návaznost hned na několik opatření v příloze A. Chybí téměř všechny body opatření u kapitoly A.14.

V následujících bodech kapitoly č. 4 jsou sepsána nová opatření z normy ČSN EN ISO/IEC 27002:2022. Tato opatření byla upravena pro lepší a rychlejší přehled při kontrole nových požadavků.

4.1 Opatření č. 5.7 - Zpravodajství o hrozbách

4.1.1 Definice a účel

Informace týkající se hrozeb pro informační bezpečnost by měly být shromažďovány a analyzovány tak, aby poskytovaly přehled o potenciálních hrozbách. Zvýšit povědomí o prostředí hrozeb pro organizaci, což umožní přijmout vhodná opatření ke zmírnění rizik.

4.1.2 Obecné pokyny

Informace o aktuálních nebo vznikajících hrozbách by měly být shromažďovány a analyzovány za účelem:

1. Usnadnit informované rozhodování, aby se zabránilo tomu, že hrozby způsobí organizaci škodu;
2. snížit dopad těchto hrozeb.

Zpravodajství o hrozbách lze rozdělit do tří úrovní, které by měly být všechny zohledněny:

1. strategické zpravodajství o hrozbách: Obecné informace o měnícím se prostředí hrozeb (např. typy útočníků nebo typy útoků);
2. taktické zpravodajství o hrozbách: Informace o metodikách, nástrojích a technologiích útočníků;
3. operativní zpravodajství o hrozbách: Podrobnosti o konkrétních útocích, včetně technických ukazatelů.

Zpravodajství o hrozbách by mělo být:

1. Relevantní: Související s ochranou organizace;
2. zasvěcené: Poskytující přesné a podrobné porozumění prostředí hrozeb;
3. kontextové: Nabízející situační povědomí přidáním kontextu k informacím na základě času událostí, místa jejich výskytu, předchozích zkušeností a rozšíření v podobných organizacích;
4. akční: Umožňující organizaci rychle a efektivně jednat na základě informací.

Činnosti zpravodajství o hrozbách by měly zahrnovat:

1) Stanovení cílů pro tvorbu zpravodajství o hrozbách;
2) Identifikaci, prověřování a výběr interních a externích zdrojů informací, které jsou nezbytné a vhodné k poskytnutí potřebných informací;
3) Shromažďování informací z vybraných zdrojů, které mohou být interní i externí;
4) zpracování shromážděných informací pro přípravu analýzy (např. překladem, formátováním nebo potvrzením informací);
5) analyzování informací pro pochopení, jak souvisejí s organizací a jaký mají pro ni význam;
6) komunikaci relevantním jednotlivcům ve srozumitelném formátu.

4.2 Opatření č. 5.23 - Informační bezpečnost při používání cloudových služeb

4.2.1 Definice a účel

Procesy pro získávání, používání, správu a ukončení cloudových služeb musí splňovat požadavky na informační bezpečnost organizace. Je třeba specifikovat a řídit bezpečnost při používání cloudových služeb.

4.2.2 Obecné pokyny

Organizace by měla vytvořit a sdělit politiku pro používání cloudových služeb všem relevantním stranám. Je nutné definovat a komunikovat, jak budou řízena rizika spojená s cloudovými službami, případně rozšířit stávající přístupy k řízení externích služeb. Používání cloudových služeb často zahrnuje sdílenou odpovědnost za bezpečnost mezi

poskytovatelem a zákazníkem. Je důležité jasně definovat a implementovat odpovědnosti obou stran.

Organizace by měla definovat:

1) Požadavky na informační bezpečnost při používání cloudových služeb;
2) kritéria výběru a rozsah využití cloudových služeb;
3) role a odpovědnosti spojené s používáním a správou cloudových služeb;
4) opatření spravovaná poskytovatelem a opatření spravovaná organizací;
5) využití bezpečnostních možností poskytovatele;
6) ověření opatření bezpečnosti poskytovatele;
7) správu a řízení opatření při využívání více cloudových služeb;
8) postupy pro řešení bezpečnostních incidentů;
9) monitoring a vyhodnocování používání cloudových služeb;
10) postupy pro změnu nebo ukončení používání cloudových služeb.

Smlouvy a rizika: Smlouvy o cloudových službách jsou často předem definované. Organizace musí mít přístup k ověřování bezpečnostních opatření poskytovatele. Smlouvy by měly řešit požadavky na důvěrnost, integritu, dostupnost a nakládání s citlivými informacemi. Organizace by měla provést posouzení rizik spojených s používáním cloudových služeb. Zbytková rizika musí být schválena a řízena vedením organizace.

4.2.3 Bezpečnostní opatření

Organizace jako zákazník cloudových služeb by měla:

1) Řídit přístup k cloudovým službám a chránit před neoprávněným přístupem;
2) zavést monitorování a ochranu před škodlivým softwarem;
3) ukládat citlivé informace na schválených místech;
4) poskytovat podporu při bezpečnostních incidentech;
5) zajišťovat bezpečnost i při subdodávkách služeb;
6) podporovat shromažďování digitálních důkazů;
7) poskytovat podporu při ukončení používání služeb;

8) zajišťovat zálohování dat a bezpečnou správu záloh;
9) poskytovat a vracet informace při požadavku během nebo po ukončení služby.

4.2.4 Změny a kontakt s poskytovatelem

Organizace by měla požadovat, aby poskytovatel cloudových služeb předem oznámil změny ovlivňující službu. To zahrnuje změny technické infrastruktury, nové geografické nebo právní jurisdikce, a změny v subdodavatelích.

4.3 Opatření č. 5.30 - Připravenost ICT na zajištění kontinuity činnosti organizace

4.3.1 Definice a účel

Účelem opatření je zajištění dostupnosti informací organizace a dalších souvisejících aktiv během narušení. Připravenost informačních technologií má být plánována, zavedena, udržována a testována na základě cílů kontinuity činnosti organizace a požadavků na kontinuitu ICT.

4.3.2 Obecné pokyny

Požadavky na kontinuitu vycházejí z Analýzy dopadů (Business Impact Analysis, BIA), která hodnotí dopady narušení klíčových produktů, služeb a podpůrných činností. Stanoví minimální úrovně zdrojů pro obnovení kritických činností a aktivaci plánu kontinuity (BCP).

Analýza dopadů identifikuje prioritní činnosti a přiřazuje jim dobu zotavení (RTO). Z analýzy jsou určeny potřebné zdroje pro hlavní činnosti. Požadavky na výkon a kapacitu ICT systémů a cílové body obnovy (RPO) jsou také definovány. RTO a RPO určují čas od poslední zálohy dat po úplné zotavení.

Na základě analýzy dopadů musí organizace zvolit strategie kontinuity ICT a vypracovat plány zajišťující dostupnost ICT služeb po přerušení nebo selhání kritických procesů.

Organizace by měla zajistit:

1) Zavedení organizační struktury pro přípravu na narušení, jeho zmírnění a odezvu na něj. Organizační struktura musí být podporována pracovníky s potřebnou odpovědností, pravomocemi a kompetencemi;

2) plány kontinuity ICT (postupy odezvy a obnovy), které podrobně popisují, jak organizace plánuje zvládnout možný incident. Plány kontinuity musí dále být pravidelně vyhodnocovány (např. formou cvičení a testů).

4.3.3 Shrnutí pojmů

Analýza dopadů (Business Impact Analysis) je proces analýzy činností organizace a dopadů, které mohou být způsobeny jejich narušením. Analýza dopadů by měla být přezkoumávána v pravidelných intervalech nebo při podstatných změnách v organizaci.

1) RTO (Recovery Time Objective) vyjadřuje maximální dobu, za kterou by mělo dojít k zotavení po výpadku. Jedná se o důležitý ukazatel určující úroveň služby;
2) RPO (Recovery Point Objective) říká, ke kterému bodu z minulosti lze obnovit data, respektive udává maximální dobu výpadku, a tedy i ztráty dat. RPO je tak klíčovým ukazatelem dostupnosti dat;
3) BCP (Business Continuity Plan) slouží k zajištění provozuschopnosti a následné obnovy provozu v případě mimořádných událostí;

4.4 7.4 Monitorování fyzické bezpečnosti

4.4.1 Definice a účel

Účelem opatření je detekovat a nepřetržitě monitorovat prostory organizace proti neoprávněnému fyzickému přístupu a mu následně zabrání.

4.4.2 Obecné pokyny

Fyzické prostory organizace musí být monitorovány dohledovými systémy, které zahrnují např. ostrahu, poplašné systémy, kamerové systémy, software pro management informací o fyzické bezpečnosti apod. Tyto systémy je možné řídit jak interně organizací, tak externím poskytovatelem (outsourcing).

Přístup do objektů, kde jsou umístěny kritické systémy, má být nepřetržitě monitorován, aby se odhalil neoprávněný přístup nebo podezřelé chování. Toho se dá docílit zejména:

1) Instalací monitorovacích systémů (kamerový systém) pro sledování a záznam přístupu do citlivých oblastí v prostorách organizace.

2) instalací a pravidelného testování kontaktních, zvukových nebo pohybových detektorů pro spuštění poplachu proti narušení, jako například:
    a. nasazením kontaktních detektorů, které spustí poplach, když dojde k navázání nebo přerušení kontaktu;
    b. použití detektorů pohybu založených na infračervené technologii;
    c. instalací detektorů tříštění skla;
3) použitím alarmů k pokrytí všech vnějších dveří a přístupných oken. Neobsazené prostory mají být vždy zabezpečeny alarmem.

Návrh monitorovacích systémů musí zůstat důvěrný, neboť jeho zveřejnění může usnadnit neodhalené vniknutí do prostor organizace.

Ovládací panel poplachového systému by měli být umístěn na vhodném místě v poplachové zóně a disponovat mechanismy odolnými proti neoprávněné manipulaci. Je vhodné také praktikovat pravidelná testování, aby se zajistilo, že systémy fungují správně.

Využívání monitorovacího a záznamového mechanismu musí být použit s ohledem na vnitrostátní zákony a předpisy, včetně právních předpisů o ochraně dat a osobních údajů, a to zejména pokud jde o monitorování zaměstnanců organizace a doby uchovávání nahraných záznamů.

4.5 Opatření č. 8.9 - Management konfigurací

4.5.1 Definice a účel

Nastavení, dokumentace, implementace, monitorování a přezkoumávání konfigurací hardwaru, softwaru, služeb a sítí. Zajistit také, aby hardware, software, služby a sítě fungovaly bezpečně a aby konfigurace nebyly neoprávněně nebo nesprávně měněny.

4.5.2 Obecné pokyny

Organizace by měla zavést procesy a nástroje pro vynucení definovaných konfigurací, včetně bezpečnostních konfigurací, pro hardware, software, služby a sítě, a to pro nové i stávající systémy. Organizace musí zavést role, odpovědnosti a postupy pro kontrolu změn konfigurací. Standardní šablony by měly být pro bezpečnou konfiguraci:

1) Založeny na veřejně dostupných pokynech;
2) přizpůsobeny úrovni ochrany potřebné v organizaci;
3) podporovány politikami informační bezpečnosti;
4) pravidelně přezkoumávány a aktualizovány.

4.5.3 Klíčové aspekty konfigurace

1) Minimalizaci administrátorských přístupových práv;
2) Blokování nepotřebných identit;
3) Omezení nepovolených funkcí a služeb;
4) Omezení přístupu k důležitým programům a nastavením;
5) Synchronizaci hodin;
6) Změnu implicitních hesel po instalaci;
7) Nastavení časových limitů pro automatické odhlášení;
8) Ověření splnění licenčních požadavků.

4.5.4 Management konfigurací

Konfigurace musí být zaznamenány a změny protokolovány. Záznamy by měly být bezpečně uloženy v konfiguračních databázích nebo šablonách. Konfigurační záznamy by měly obsahovat:

1) Informace o vlastníkovi;
2) datum poslední změny;
3) verzi šablony;
4) vztah ke konfiguracím jiných aktiv.

4.5.5 Monitorování konfigurací

Konfigurace by měly být monitorovány pomocí nástrojů pro správu systému a pravidelně přezkoumávány. Skutečné konfigurace by měly být porovnávány s cílovými šablonami a případné odchylky řešeny automatickým vynucením nebo manuální analýzou.

4.5.6 Další informace

Management konfigurací je nutné integrovat s procesy správy aktiv a efektivně automatizovat. Konfigurační informace, šablony a by měly být chráněny před neoprávněným přístupem. K řízení bezpečné konfigurace je obvykle efektivnější automatizace (např. pomocí infrastruktury jako kódu).

4.6 Opatření č. 8.10 - Mazání informací

4.6.1 Definice a účel

Toto opatření pojednává o nutnosti a možnostech výmazu informací uložených v informačních systémech, zařízeních nebo jiných paměťových médiích v případě, kdy již nejsou potřebné. Účelem opatření je zabránit zbytečnému vystavení citlivých informací a současně dodržovat zákonné a smluvní požadavky.

4.6.2 Obecné pokyny

Citlivé informace by neměly být uchovávány déle, než je nezbytně nutné, aby se snížilo riziko jejich prozrazení. Při procesu mazání informací je třeba vzít v úvahu převážně výběr metody vymazání (např. elektronický přepis nebo kryptografické vymazání) v souladu s interními požadavky vyplývajícími z činnosti organizace s ohledem na příslušné zákony a předpisy. Nedílnou součástí procesu je i zaznamenání výsledku výmazu jako důkazu o provedení, které by organizace měla vést ve své dokumentaci. Oficiální záznam lze poté využít při analýze příčiny možného úniku dat.

Dle informací výše by měly být citlivé informace vymazány v případě, že již nejsou potřebné. Z hlediska způsobu výmazu musíme pak brát v úvahu, o jaký typ informace, podléhající likvidaci se jedná. Například likvidace osobních údajů zaměstnance má jiná pravidla než výmaz specifických citlivých informací z fyzického zařízení (mobilní telefon, paměťová média apod.).

4.6.3 Metody vymazání

Způsobů vymazání informací je celá řada a organizace by měla zvážit, jakou vhodnou metodu použít v závislosti na konkrétních typech informací.

1) Použití schváleného softwaru pro bezpečné mazání k trvalému výmazu informace bez možnosti obnovení

2) použití schválených certifikovaných poskytovatelů služeb bezpečné likvidace informací;
3) mechanismy likvidace vhodných pro typ likvidovaného nosiče informace;
4) demagnetizace pevných disků a jiných paměťových médií;
5) skartace dokumentů obsahující citlivé informace;
6) vymazání dat prostřednictvím zabudovaných funkcí fyzického zařízení (např. obnovení továrního nastavení chytrého telefonu);
7) likvidace dat v souladu s právními předpisy (např. osobní údaje, pracovněprávní dokumenty apod.).

Vzhledem k tomu, že bezpečné vymazání některých zařízení lze dosáhnout pouze zničením nebo funkcí zabudovaných v těchto zařízeních dle bodu d), měla by organizace zvolit vhodnou metodu podle klasifikace informací, s nimiž tato zařízení pracují.

4.6.4 Vymazání informací v cloudových službách

Pokud jsou využívány cloudové služby, měla by organizace ověřit, jaký způsob likvidace konkrétní cloudová služba poskytuje. Následně, pokud je to přijatelné, lze požádat poskytovatele cloudových služeb o vymazání informací. Tyto procesy by měly být automatizované. V závislosti na citlivosti vymazaných dat lze také sledovat nebo ověřit, zda procesy likvidace proběhly.

4.7 Opatření č. 8.11 - Maskování dat

4.7.1 Definice a účel

Smyslem tohoto opatření je omezit vystavení citlivých údajů včetně osobních údajů a dodržovat zákonné a smluvní požadavky. Maskování dat má být používáno v souladu s interní politikou organizace týkající se řízení přístupu a dalšími požadavky vyplývající z činnosti organizace, přičemž je třeba brát v úvahu platnou legislativu.

4.7.2 Obecné pokyny

Pokud se jedná o ochranu citlivých údajů (např. osobní údaje), měla by organizace zvážit skrytí těchto údajů pomocí technik, jako je maskování dat, pseudonymizace a anonymizace, přičemž je stále zachován formát integrita dat.

Pseudonymizace je postup, při kterém je z osobních údajů oddělena jejich část umožňující určení konkrétního člověka (např. odstraněním jména, rodného čísla), přičemž je stále lze přiřadit k určitému subjektu. Zpětné přiřazení je poté možné pomocí jedinečných identifikátorů.

Anonymizace je technika maskování dat, zpravidla osobních údajů, kdy dochází k odstranění nebo úpravě identifikačních prvků subjektu tak, že osobu není možné identifikovat a zjistit její totožnost. Výsledkem jsou anonymizovaná data, která nelze přiřadit k žádné konkrétní osobě. Proces anonymizace je nevratný.

4.7.3 Další techniky maskování

1) Šifrování – vyžaduje, aby oprávnění uživatelé disponovali klíčem;
2) substituce – záměna jedné hodnoty za jinou;
3) nulování nebo mazání znaků – brání neoprávněným uživatelům vidět celé zprávy;
4) různá čísla a data.

Při implementaci technik maskování dat je třeba vzít v úvahu následující:

1) Neudělovat všem uživatelům přístup ke všem datům, ale řídit přístupy pouze pro zaměstnance s určitými rolemi, aby ze souboru dat viděli pouze to, co spadá do jejich kompetence;
2) skutečnost, že jsou data zamaskována, což dává subjektu osobních údajů možnost požadovat, aby uživatelé nemohli zjistit, zda jsou data zamaskována (zamaskování maskování).

4.8 Opatření č. 8.12 - Prevence úniku dat

4.8.1 Definice a účel

Jedná se o opatření, které má za cíl odhalit a zabránit neoprávněnému vyzrazení a získání informací společnosti. Opatření z hlediska prevence úniku dat mají být aplikována na systémy, sítě a jakákoliv další zařízení, jež zpracovávají, ukládají nebo přenášení citlivé informace.

4.8.2 Obecné pokyny

Pro snížení rizika úniku dat je třeba zvážit následující dílčí opatření, která lze najít v normě ISO/IEC 27002:

1) Identifikace a klasifikace informací;
2) monitorování kanálů;
3) opatření k zabránění úniku informací;
4) identifikace a klasifikace informací.

Aby organizace vůbec věděla a měla přehled o tom, jaké informace vlastní a jakou mají hodnotu a kdo s nimi nakládá, je třeba informace identifikovat a vést potřebnou dokumentaci. Je potřeba nastavit jak správné řízení přístupu, tak značení dané informace dle její citlivosti, aby se zabránilo jejímu úniku. Informace musí být klasifikovány podle potřeb organizace na základě atributů důvěrnosti, dostupnosti a integrity. Zpravidla se jedná o osobní údaje, obchodní smlouvy, strategické plány, personální údaje, ale i o přístupová hesla, zdrojové kódy atd.

4.8.3 Monitorování kanálů

Pod pojmem monitorování kanálů si můžeme představit softwarová řešení umožňující aktivní sledování přenosů souborů síťovou infrastrukturou, včetně e-mailu a přenosných paměťových zařízení za účelem ochrany před únikem dat. V rámci organizace je pro tyto účely nasazen nástroj pro prevenci úniku dat DLP (Data Loss Prevention), který na základě nastavených politik chrání přenos citlivých informací.

4.8.4 Kroky k zabránění úniku informací

Tyto kroky úzce souvisí s monitorováním kanálů. Ze své podstaty se jedná především o monitorování komunikace a online aktivit pracovníků, používaných zařízení a dodržování klasifikace informací a případné akce za účelem zabránění ztráty dat. Z hlediska aktivního zásahu k zabránění úniku dat lze využít rovněž nástroj DLP, který je schopen detekované citlivé informace blokovat, pokud dojde k neoprávněnému přenosu. V případě zálohování dat je třeba dbát na ochranu citlivých informací pomocí opatření, jako je šifrování, řízení přístupu a fyzická ochrana paměťových médií, na kterých je záloha uložena.

4.9 Opatření č. 8.16 - Monitorovací činnosti

4.9.1 Definice a účel

Sítě, systémy a aplikace lze monitorovat z hlediska poruchového chování a měla by být přijata vhodná opatření k vyhodnocení potencionálních incidentů informační bezpečnosti.

4.9.2 Obecné pokyny

Rozsah a úroveň monitorování mají být stanoveny v souladu s požadavky vyplývajícími z činnosti organizace a požadavky na informační bezpečnost a s ohledem na příslušné zákony a předpisy. Záznamy z monitorování mají být uchovávány po stanovenou dobu.

V rámci systému monitorování se má zvážit zahrnutí následujících informací:

1) odchozí a příchozí síťový, systémový a aplikační provoz;
2) přístupy k systémům, serverům, síťovému vybavení, monitorovacímu systému, kritickým aplikacím atd.;
3) logy z bezpečnostních nástrojů [např. antivir, IDS, systém prevence průniku (IPS), webové filtry, firewally, prevence úniku dat];
4) logy událostí týkající se aktivity systému a sítě;
5) kontrola, zda je spouštěný kód oprávněn běžet v systému a zda do něj nebylo zasahováno (např. rekompilací nebo přidáním dalšího nežádoucího kódu);
6) využití zdrojů (např. CPU, pevných disků, paměti, šířky pásma) a jejich výkonnost.

Konfigurace monitorovacího systému:

Monitorovací systém má být nakonfigurován na základě stanovené základní linie, aby bylo možné identifikovat anomální chování, jako například:

1) Neplánované ukončení procesů nebo aplikací;
2) činnost typicky spojená se škodlivým softwarem;
3) známé charakteristiky útoků (např. odepření služby a přetížení vyrovnávací paměti);
4) neobvyklé chování systému (např. zaznamenávání stisků kláves, injektování procesů a odchylky v používání standardních protokolů);
5) neoprávněný přístup (skutečný nebo pokus o něj) k systémům nebo informacím;

6) neoprávněné skenování podnikových aplikací, systémů a sítí;
7) úspěšné a neúspěšné pokusy o přístup k chráněným zdrojům (např. DNS serverům, webovým portálům a souborovým systémům).

Monitorování má probíhat v reálném čase nebo v pravidelných periodách podle potřeb a schopností organizace. Automatizovaný monitorovací software má být nakonfigurován tak, aby generoval výstrahy (např. prostřednictvím kontrol pro management, e-mailových zpráv nebo systémů rychlého zasílání zpráv) na základě předem definovaných parametrů. Výstrahy by měly být vyřizovány a zaměřeně na základní úrovni organizace, aby se minimalizovaly nesprávné pozitivní výstrahy. Pro odezvu na výstrahy by měli být vyčleněni pracovníci, kteří by měli být řádně vyškoleni, aby efektivně reagovali na generované výstrahy.

O abnormálních událostech mají být informovány příslušné strany, aby se zlepšily následující činnosti: audit, hodnocení bezpečnosti, skenování zranitelností a monitorování.

Monitorování anomální komunikace pomáhá identifikovat botnety (tj. soubor zařízení řízených vlastníkem botnetu pod vlivem), distribuovaným útokům typu odepření služby (DDoS) na jiných počítačích jiných organizací. Pokud je počítač ovládán uživatelem jenž jedná v rozporu se zájmem organizace, dochází ke komunikaci s externím zařízením a řídicím zařízením.

4.10 Opatření č. 8.23 - Filtrování webu

4.10.1 Definice a účel

Hlavním účelem tohoto opatření je ochrana systémů před napadením škodlivým softwarem a zabránění přístupu k neautorizovaným webovým zdrojům.

4.10.2 Obecné pokyny

Organizace má snižovat riziko přístupu svých zaměstnanců na webové stránky, které obsahují nelegální informace nebo o nichž je známo, že obsahují viry či phishingový materiál. Účinná technika, jak toho dosáhnout, spočívá v blokování IP adresy nebo domény konkrétních webových stránek. Výhodou je, že některé prohlížeče toto vykonávají automaticky nebo je lze takto nakonfigurovat. Každá organizace si sama určí typy webových stránek, ke kterým budou nebo nebudou mít zaměstnanci přístup. Je třeba zvážit zablokování přístupu k následujícím typům stránek:

1) Webové stránky s možností nahrávání informací – s výjimkou oprávněných pracovních důvodů
2) známé nebo podezřelé škodlivé stránky;
3) stránky s nevhodným obsahem (zpravidla se jedná např. o pornografii, hazardní hry, webové stránky bez certifikátu HTTPS, darkweb atd.);
4) příkazové a řídicí servery;
5) webové stránky sdílející nelegální obsah.

Před zavedením opatření by organizace měla nastavit pravidla pro bezpečné a vhodné používání online zdrojů, která mají být stále aktuální. Jedná se o vytvořenou interní politiku, jejíž rozsah nasazení je regulován legislativními požadavky.

4.10.3 Bezpečnostní povědomí

Zaměstnanci by měli být vhodně proškoleni o bezpečném používání online zdrojů včetně přístupu na web. Takové školení vychází z interních pravidel organizace a má zahrnovat i případné způsoby nahlašování bezpečnostních událostí, popřípadě incidentů. Dále by školení mělo obsahovat i proces udělování výjimek v případech, kdy je z legitimních důvodů nutné přistupovat k webovým zdrojům s omezeným přístupem. V rámci zvyšování povědomí o problematice je nutné také zajistit, aby uživatelé nepřehlíželi žádné upozornění prohlížeče, který oznamuje, že webová stránka není bezpečná, ale umožní uživateli pokračovat.

4.11 Opatření č. 8.28 - Bezpečné programování

4.11.1 Definice a účel

Při vývoji softwaru je třeba dodržovat zásady bezpečného programování. Dále je potřeba zajistit bezpečnost softwaru a snížit potenciální zranitelnosti.

4.11.2 Obecné pokyny

Organizace by měla zavést celopodnikové procesy pro správu a řízení bezpečného programování s minimální bezpečnostní úrovní, včetně softwarových komponent třetích stran a open-source softwaru. Je třeba sledovat reálné hrozby a aktuální rady pro neustálé zlepšování a implementaci efektivních postupů. Před programováním se mají uplatňovat zásady bezpečného programování:

1) Očekávání organizace a schválené zásady;
2) běžné postupy programování a chyby;
3) konfigurace vývojových nástrojů (IDE);
4) dodržování pokynů poskytovatelů nástrojů;
5) aktualizace vývojových nástrojů;
6) kvalifikace vývojářů;
7) bezpečný návrh a architektura;
8) standardy bezpečného programování;

Při programování je třeba:

1) Uplatňovat bezpečné postupy specifické pro jazyky a techniky;
2) používat techniky jako programování ve dvojici, refaktoring, odborné posouzení a testování;
3) používat strukturované programování;
4) dokumentovat kód a odstraňovat chyby;
5) zakázat nezabezpečené techniky (pevně zakódovaná hesla, neschválené knihovny).

Přezkoumávání a údržbě programu by organizace měla:

1) Aktualizace začlenit do bezpečného balíčku;
2) řešit nahlášené zranitelnosti;
3) zaznamenávat chyby a podezření na útoky;
4) chránit zdrojový kód před neoprávněným přístupem a manipulací.

U externích nástrojů a knihoven by organizace měla:

1) Spravovat a aktualizovat externí knihovny;
2) používat prověřené komponenty;
3) zajistit bezpečnost a historii komponent;
4) zajistit sledovatelnost zdrojových souborů;
5) zajistit dlouhodobou dostupnost vývojových zdrojů.

Při úpravách softwaru je třeba zvážit:

1) Riziko kompromitace kontrol;
2) riziko zásahu dohodnutého dodavatele;
3) oznámení změn formou standardní aktualizace;
4) možné změny odpovědnosti za údržbu;
5) kompatibilitu s jiným softwarem.

Bezpečné programování se zaměřuje na dodržování zásad bezpečného programování během vývoje softwaru s cílem snížit potenciální zranitelnosti. Organizace by měla implementovat procesy správy a řízení bezpečného programování, včetně aktualizace vývojových nástrojů a školení vývojářů. Důraz zde také musí být kladen na používání bezpečných postupů, jako je programování ve dvojici, testování a správa externích nástrojů a knihoven, aby byla zajištěna dlouhodobá bezpečnost a dostupnost.

5 NÁSTROJ PRO KOMPARACI NOREM ISO 27001:2013/2022

Pro komparaci těchto norem existuje poměrně rozsáhlé množství dokumentů které jsou zaměřené na hlavní změny. Co se týče aplikací nebo programů, tak na České scéně se nenalézá ani jeden program v kterém by bylo možné porovnávat normy ISO/IEC 27001:2013 a 2022. Co se týče světového měřítka, tak v tomto případě zde je placená aplikace „CONFORMIO: ISO 27001 Software for Small Businesses“. S touto aplikací se dá provádět audit normy ISO 27001:2022. Jak již ale bylo zmíněno, jedná se o aplikaci placenou, kde samotná licence stojí: 999, 1699 a 1999 USD / 1 rok.

5.1 Volba platformy pro vytvoření programu

Pro vytvoření programu byl sepsán seznam několika aplikacích a nástrojů, ve kterých by se dala práce vytvořit. Zde jsou některé z nich:

1) Microsoft Excel;
2) Microsoft Access;
3) Google Forms;
4) Microsoft Forms;
5) LibreOffice Base;
6) FileMaker Pro;
7) Zoho Creator;
8) Ninja Forms;
9) JotForm;
10) Knack.

5.1.1 Zvolení aplikace ACCESS

Pro zpracování programu na komparaci normy byla zvolena aplikace Access od Microsoftu. Níže jsou odůvodnění, proč byla dána přednost aplikaci Access, před jinými platformami:

Excel: Zatímco Excel je skvělý pro analýzu dat, Access nabízí robustnější databázové funkce, lepší možnosti pro automatizaci a spravování většího množství dat.

Webové aplikace: Vývoj webových aplikací může být časově i finančně náročný. Access poskytuje rychlejší a jednodušší způsob, jak vytvořit databázová řešení bez potřeby hlubokých znalostí programování a webových technologií.

SQL Server: Access je ideální pro menší až středně velké aplikace, kde není potřeba složitější infrastruktura a administrace, kterou vyžaduje SQL Server. Navíc je Access vhodnější pro rychlé nasazení a uživatelsky přívětivé řešení.

5.1.2 Přednosti aplikace Access

Microsoft Access poskytuje integrované prostředí pro správu databází, což umožňuje snadnou tvorbu, úpravu a správu formulářů. Tato integrace s ostatními nástroji Microsoft Office usnadňuje práci v rámci jednoho systému protože je součástí balíčku Microsoft 365. Při vlastnění tohoto balíčku není potřeba zakupovat licenci zvlášť. Níže jsou zmíněny přednosti aplikace Access:

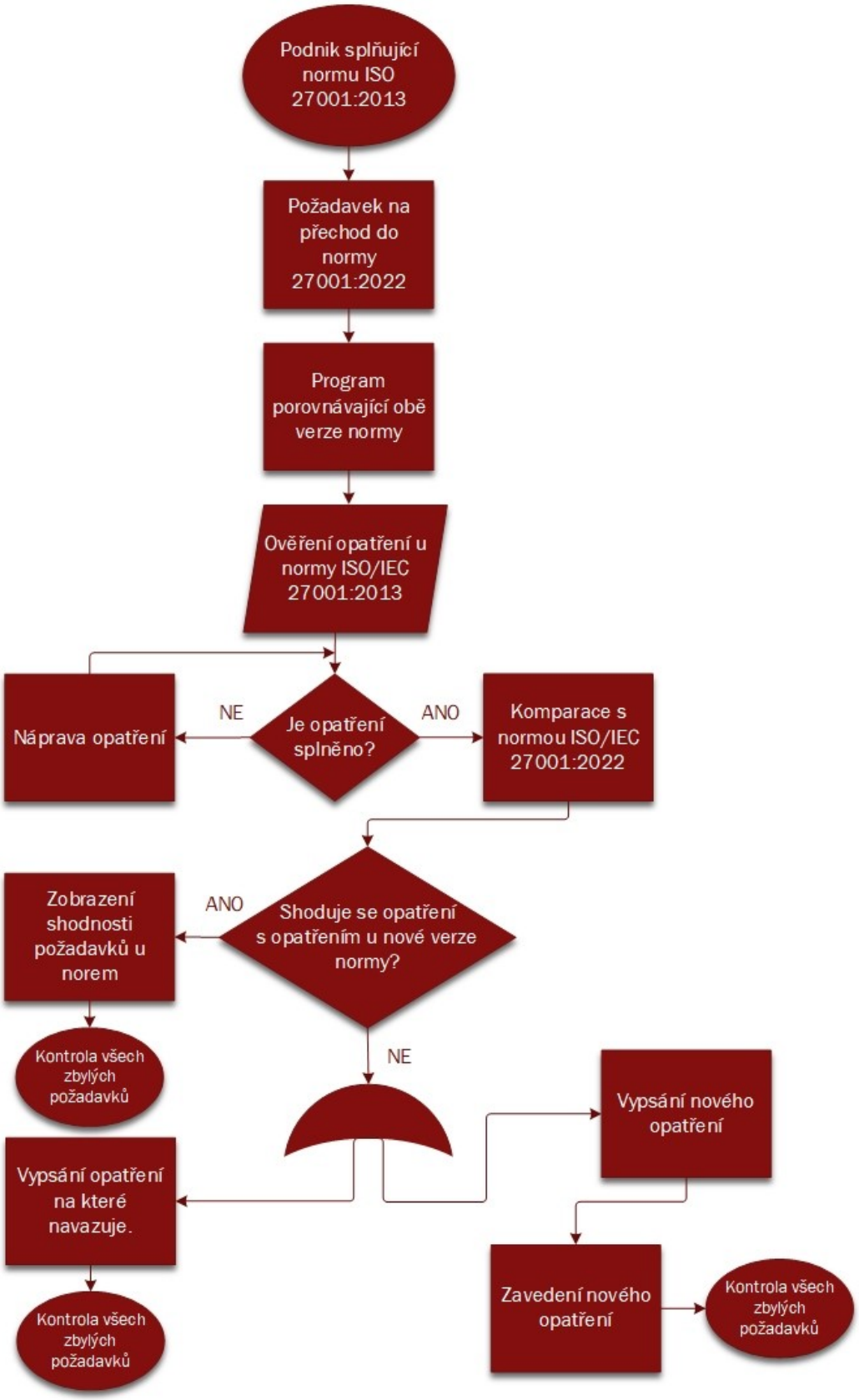
1) **Jednoduché použití**: Access nabízí uživatelsky přívětivé rozhraní s množstvím předdefinovaných šablon a průvodců, které usnadňují tvorbu formulářů i pro uživatele bez hlubokých technických znalostí. Toto usnadnění zvyšuje efektivitu práce a snižuje časovou náročnost vývoje;
2) **flexibilita a přizpůsobitelnost**: Formuláře v Accessu lze snadno přizpůsobit specifickým potřebám uživatele díky širokému spektru ovládacích prvků a možností úprav. Uživatelé mohou přidávat tlačítka, textová pole, rozbalovací nabídky a další interaktivní prvky pro práci s daty;
3) **pokročilé funkce a automatizace**: Access umožňuje využití VBA (Visual Basic for Applications) pro pokročilou automatizaci úkolů a tvorbu složitějších aplikací. To poskytuje možnosti pro automatizaci opakujících se procesů a zlepšení efektivity práce s databázemi;
4) **bezpečnost a řízení přístupu**: Access poskytuje robustní nástroje pro řízení přístupu k datům, což umožňuje nastavení různých úrovní oprávnění pro různé uživatele. To je zvláště důležité pro ochranu citlivých informací a zajištění integrity dat;
5) **integrace s externími datovými zdroji**: Access umožňuje snadnou integraci s různými externími datovými zdroji, jako jsou Excel, SQL Server a další databázové systémy. To zajišťuje flexibilitu a umožňuje využívat data z různých platforem v rámci jednoho systému.

Díky těmto vlastnostem byla zvolena aplikace Microsoft Access jako nejvhodnější kandidát pro tvorbu aplikace na komparaci normy ISO/IEC 27001:2013/2022.

5.2 Diagram pro komparaci normy

Diagram zobrazuje samotnou logiku postupu při revidování a také část funkcí vytvořeného programu. Detailnější popsání diagramu je znázorněno níže:

1) Podnik splňující normu ISO 27001:2013 – Výchozí stav podniku, který aktuálně splňuje starší verzi normy;
2) požadavek na přechod do normy 27001:2022 – Podnik se rozhodne přejít na novou verzi normy z vlastní vůle nebo z povinnosti;
3) program porovnávající obě verze normy – Využije se program, který porovná požadavky obou verzí normy. (není nutností);
4) ověření opatření u normy ISO/IEC 27001:2013 – Kontrola stávajících opatření podle starší verze normy;
5) naplněná jednotlivých opatření – Kontrola, zda jsou opatření splněna:
    a. NE: Náprava opatření – Pokud nejsou opatření splněna, provede se jejich náprava;
    b. ANO: Komparace s normou ISO/IEC 27001:2022 – Pokud jsou opatření splněna, pokračuje se porovnáním s novou verzí normy;
6) shoduje-li se opatření s opatřením u nové verze normy – Kontrola, zda se stávající opatření shodují s požadavky nové verze normy:
    a. ANO: Zobrazení shodnosti požadavků u norem – Pokud se shodují, zobrazí se shodnost požadavků a pokračuje se kontrolou všech zbývajících požadavků;
    b. NE: Vypsání nového opatření – Pokud se neshodují, zapíše se nové opatření a pokračuje se jeho zavedením. Poté se kontrolují všechny zbývající požadavky;
7) kontrola všech zbývajících požadavků – Tento krok se opakuje jak pro shodná opatření, tak pro nově zavedená opatření, aby bylo zajištěno splnění všech požadavků nové verze normy.



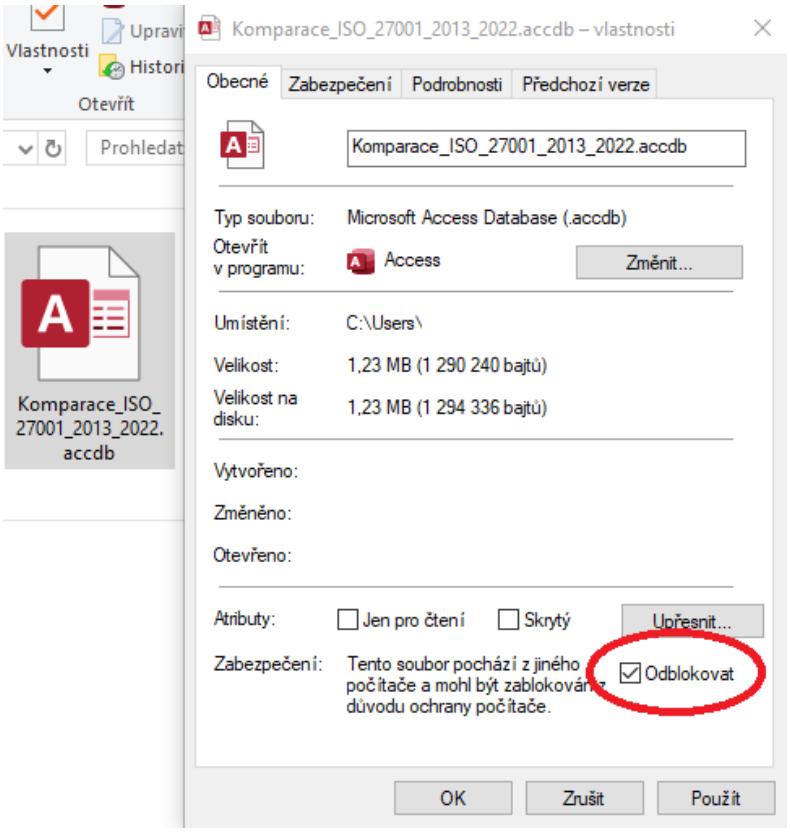
Obrázek 10. Diagram pro komparaci normy

5.3 Návod k využívání programu v prostředí Access

Jak již bylo zmíněno, program je vytvořen pro asistenci při případném auditu nebo revizi stavu ISMS v podniku. Je důležité tento program nebrat jako přesnou příručku, ale spíše jako pomocníka pro usnadnění práce s normou ISO 27001:2013 a ISO 27001:2022. Při zpracování tohoto programu bylo pracováno s normami ISO 27001:2013, ISO 27001:2022 a ISO 27002:2022. Ovšem informace získané z normy nejsou exaktně přesné. Jsou mnohdy zkrácené, jednodušeji formulované nebo obohacené o poznatky z vlastní zkušenosti. Výše zmíněná fakta je potřeba brát v potaz.

5.3.1 Odemknutí souboru Access

Při stažení a prvotním spuštění bude program zablokovaný. Na obrázku č. 12 je vidět okno vlastností souboru v systému Windows. Pro odblokování přístupu k zabezpečenému dokumentu, je potřeba otevřít vlastnosti dokumentu a kliknout na zaškrtávací políčko s názvem "Odblokovat," které je zvýrazněno červeným oválem. Toto políčko se nachází v dolní části karty "Obecné." Kliknutím na toto políčko se odstraní omezení, která bylo na soubor uvalena z důvodu ochrany počítače, a umožní se tak jeho plné otevření a úpravy.

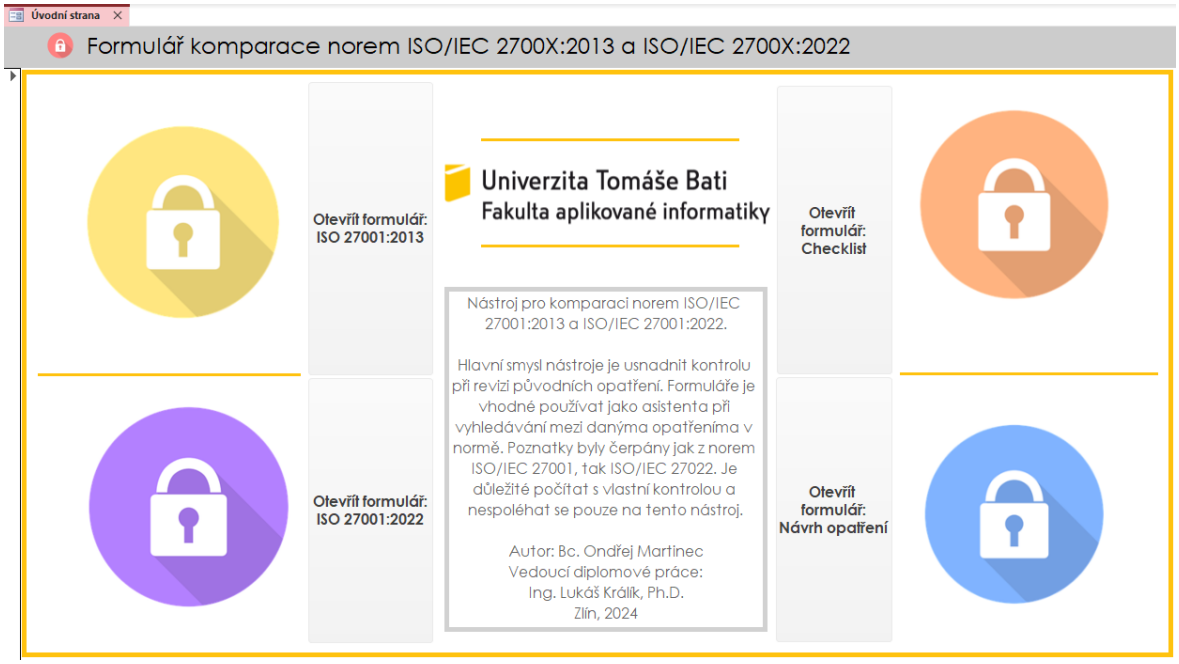


Obrázek 11. Odblokování dokumentu

5.3.2 Úvodní strana

Jak už z názvu vyplývá, pro úspěšné používání je potřeba a mít nainstalovaný program Access. Ten je ale převážně součástí balíčku Office 365. Tudíž je jeho síť uživatelů široká. Pro úspěšný start otevřeme soubor: „Komparace_ISO_27001_2013_2022.accdb“. Po spuštění a načtení je nastaveno zobrazení úvodní strany. Na úvodní straně jsou zmíněny údaje ohledně používání dokumentu. Formulář je navržen a rozdělen do čtyř sekcí, tudíž zde nalezneme čtyři tlačítka ve tvaru šedých obdélníků, které mají vlastní funkční význam. Uživatel si tak může zvolit, který formulář si bude chtít otevřít.

1) Formulář: ISO 27001:2013;
2) formulář: ISO 27001:2022;
3) formulář: Checklist;
4) formulář: Návrh opatření.

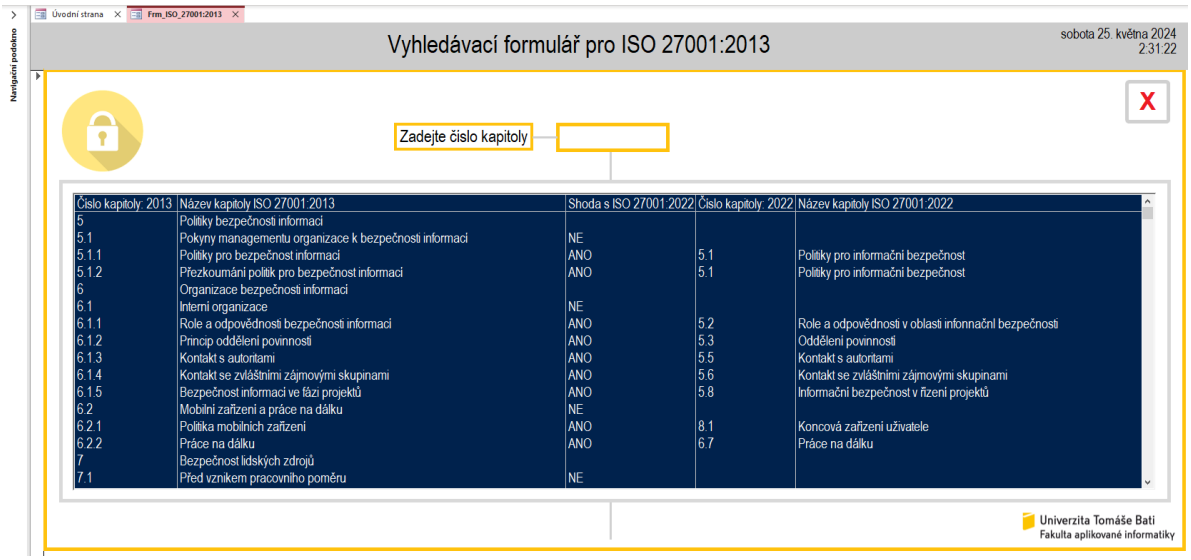


Obrázek 12. Úvodní strana formuláře

5.3.3 Formulář: ISO 27001:2013

Práce s formulářem je prostá. Do prázdného pole, umístěného uprostřed (vedle pole “Zadejte číslo kapitoly“) napíšeme námi hledanou kapitolu z normy ISO 27001:2013. Při práci na menších obrazovce je možné že formulář nebude zobrazený celý. Proto je vhodné při zapsání hodnoty do vyhledávacího pole následně stisknout klávesu „Enter“. Okno se nám následně přesune na začátek tabulky. V pravém horním rohu je umístěno tlačítko pro uzavření

formuláře. Druhá možnost, jak zavřít formulář je stisknout křížek na horní liště otevřených dokumentů (červeně zabarvený obdélník). Tímto způsobem se vrátíme na úvodní stranu. Výše zmíněné body platí i pro následující formuláře. Obrázek č. 15 znázorňuje jak je možné s formulářem pracovat. V tabulce pod vyhledávacím pole je zabarvená žlutozlatou barvou kapitola 10.1, kterou si uživatel vyhledal. Také jsou níže zobrazeny další kapitoly, které mají stejný číselný základ.



Číslo kapitoly: 2013	Název kapitoly ISO 27001:2013	Shoda s ISO 27001:2022	Číslo kapitoly: 2022	Název kapitoly ISO 27001:2022
5	Politiky bezpečnosti informací			
5.1	Pokyny managementu organizace k bezpečnosti informací	NE		
5.1.1	Politiky pro bezpečnost informací	ANO	5.1	Politiky pro informační bezpečnost
5.1.2	Přezkoumání politik pro bezpečnost informací	ANO	5.1	Politiky pro informační bezpečnost
6	Organizace bezpečnosti informací			
6.1	Interní organizace	NE		
6.1.1	Role a odpovědnosti bezpečnosti informací	ANO	5.2	Role a odpovědnosti v oblasti infonnačnl bezpečnosti
6.1.2	Princip oddělení povinnosti	ANO	5.3	Oddělení povinnosti
6.1.3	Kontakt s autontami	ANO	5.5	Kontakt s autontami
6.1.4	Kontakt se zvláštními zájmovými skupinami	ANO	5.6	Kontakt se zvláštními zájmovými skupinami
6.1.5	Bezpečnost informací ve fázi projektů	ANO	5.8	Informační bezpečnost v řízení projektů
6.2	Mobilní zařízení a práce na dálku	NE		
6.2.1	Politika mobilních zařízení	ANO	8.1	Koncová zařízení uživatele
6.2.2	Práce na dálku	ANO	6.7	Práce na dálku
7	Bezpečnost lidských zdrojů			
7.1	Před vznikem pracovního poměru	NE		

Obrázek 13. Vyhledávací formulář pro ISO 27001:2013

Číslo kapitoly: 2013	Název kapitoly ISO 27001:2013	Shoda s ISO 27001:2022	Číslo kapitoly: 2022	Název kapitoly ISO 27001:2022
10.1	Kryptografická opatření	NE		
10.1.1	Politika použití kryptografických opatření	ANO	8.24	Používání kryptografie
10.1.2	Správa klíčů	ANO	8.24	Používání kryptografie

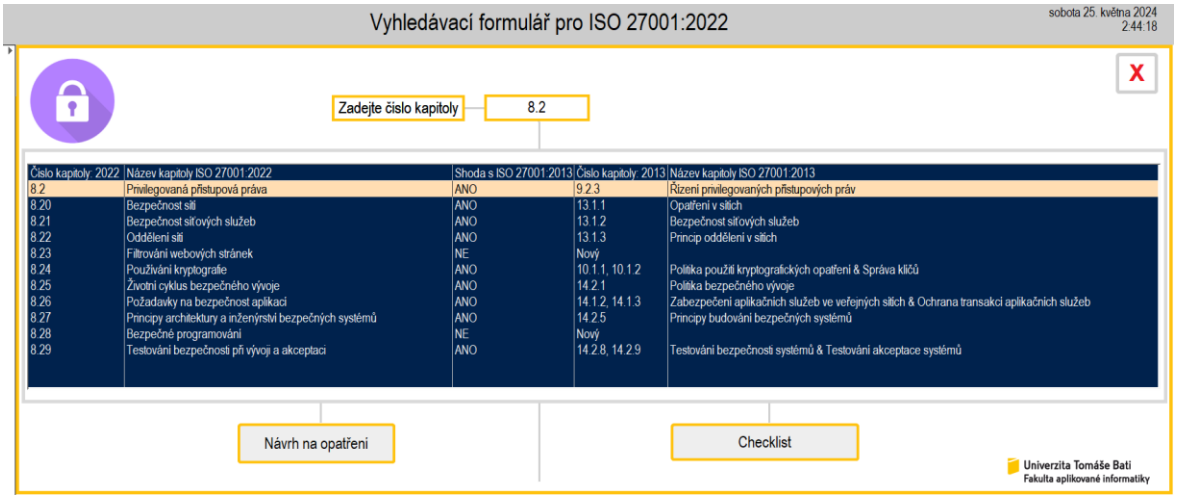
Obrázek 14. Vyhledávací formulář pro ISO 27001:2013

5.3.4 Formulář: ISO 27001:2022

Práce s tímto formulářem je podobná jako v předchozím případě, což usnadňuje jeho používání. Do prázdného pole umístěného uprostřed vedle pole označeného "Zadejte číslo kapitoly" jednoduše napíšeme číslo kapitoly z normy ISO 27001:2022, kterou hledáme.

Tento intuitivní krok nám umožňuje rychle vyhledat potřebné informace. Pro zjednodušení práce jsou v dolní části formuláře umístěna tlačítka, která umožňují přímý přístup k formulářům „Návrh opatření“ a „Checklist“. Tato tlačítka významně urychlují navigaci a práci s formulářem. Obrázek č. 16 a č. 17 názorně ilustrují, jak s formulářem pracovat a využívat jeho funkcí k efektivnímu vyhledávání a správě informací dle normy ISO 27001:2022.

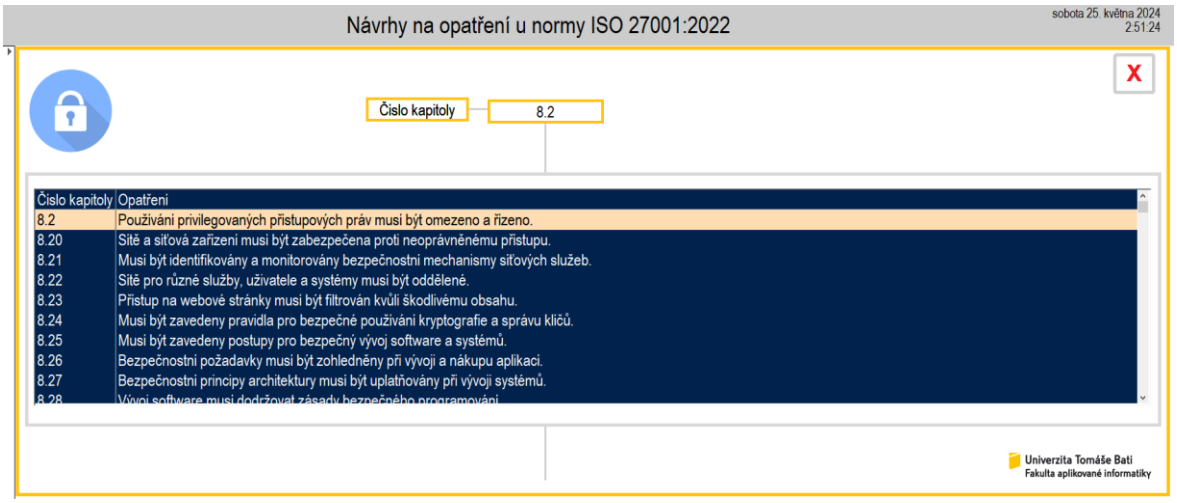
Obrázek 15. Vyhledávací formulář pro ISO 27001:2022



Obrázek 16. Vyhledávací formulář pro ISO 27001:2022

5.3.5 Formulář: Návrh na opatření

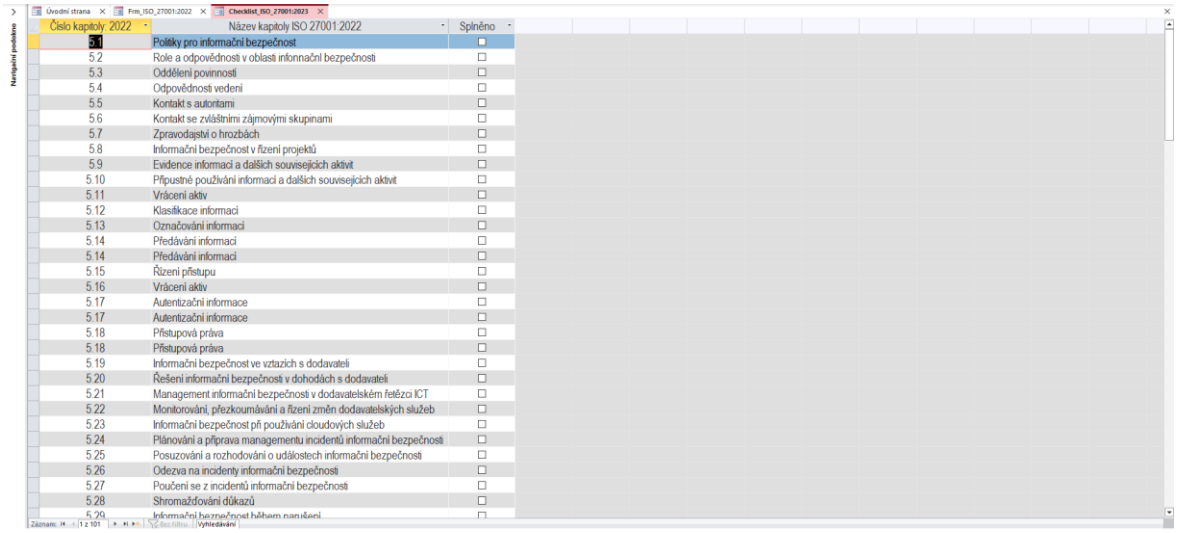
Zde se opět formulář neliší od předchozích případů. Do prázdného pole, umístěného uprostřed (vedle pole “Zadejte číslo kapitoly“) napíšeme námi hledanou kapitolu z normy ISO 27001:2022. Po zapsání hodnoty se nám zobrazí zvýrazněné pole s návrhem na splnění konkrétního opatření (obrázek č. 18). Formulář můžeme zavřít opět dvěma způsoby (červený křížek nebo křížek na horní liště).



Obrázek 17. Návrh na opatření pro ISO 27001:2022

5.3.6 Datový list: Checklist pro ISO 27001:2022

Datový list, zobrazený na obrázcích č. 19 a č. 20 znázorňuje podobu checklistu. Práce s checklistem je opět snadná. Pomocí posuvného jezdce nebo kolečka myši můžeme projíždět seznam a zaškrtnout si tak splněná opatření. Ve spodní liště je také možnost napsat do bílého pole číslo kapitoly a seznam se nám posune na námi zapsanou hodnotu. V případě zavření checklistu zůstanou zaškrtnuté hodnoty uloženy do příštího otevření. Na obrázku č. 20 je znázorněna práce s checklistem.



Obrázek 18. Checklist pro ISO 27001:2022

Číslo kapitoly: 2022	Název kapitoly ISO 27001:2022	Splněno
5.1	Politiky pro informační bezpečnost	☐
5.2	Role a odpovědnosti v oblasti infonnačnl bezpečnosti	☐
5.3	Oddělení povinnosti	☐
5.4	Odpovědnosti vedení	☐
5.5	Kontakt s autoritami	☐
5.6	Kontakt se zvláštními zájmovými skupinami	☐
5.7	Zpravodajství o hrozbách	☐
5.8	Informační bezpečnost v řízení projektů	☑
5.9	Evidence informací a dalších souvisejících aktivit	☑
5.10	Přípustné používání informací a dalších souvisejících aktivit	☑
5.11	Vrácení aktiv	☑
5.12	Klasifikace informací	☑
5.13	Označování informací	☑
5.14	Předávání informací	☐
5.14	Předávání informací	☐
5.15	Řízení přístupu	☐
5.16	Vrácení aktiv	☐
5.17	Autentizační informace	☐
5.17	Autentizační informace	☐
5.18	Přístupová práva	☐
5.18	Přístupová práva	☐
5.19	Informační bezpečnost ve vztazích s dodavateli	☐

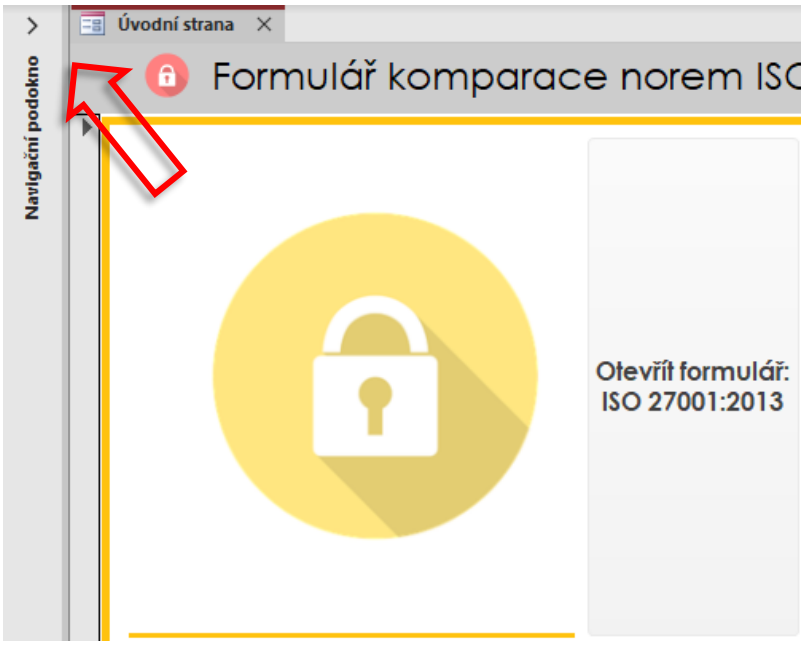
Obrázek 19. Práce s checklistem

5.4 Úprava dat ve formulářích

Pro potřeby úprav nebo vlastního doplnění bude program dostupný pro změnu parametrů. Na následujících obrázcích je znázorněno, jak postupovat pro změnu dat v jednotlivých tabulkách.

5.4.1 Navigační podokno

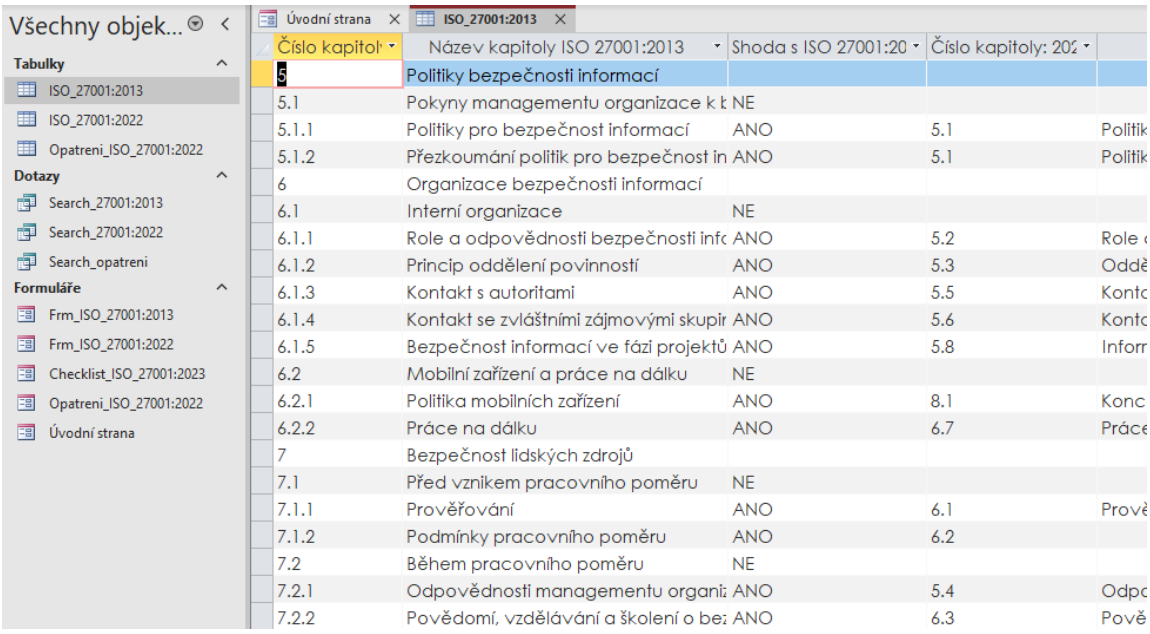
Při spuštění programu se nám jako první zobrazí „Úvodní strana“. Je možné, že navigační okno zůstane zavřené. Navigační okno bude pravděpodobně skryto z důvodu, lepší přehlednosti ve formuláři. Pro jeho zobrazení je šipkou na obrázku č. 21 znázorněno, kde se podokno rozklikne.



Obrázek 20. Otevření navigačního podokna

5.4.2 Úprava dat v tabulce normy ISO 27001:2013

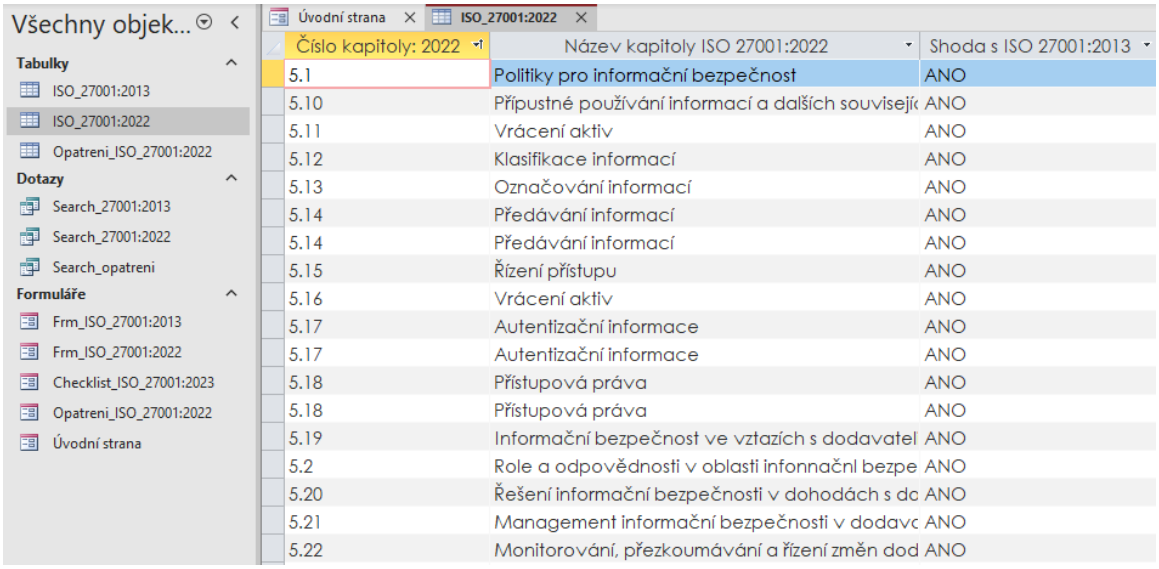
Pro úpravu dat je potřeba dvakrát kliknout myší na tabulku v které chceme měnit nebo přidávat data. Při každé změně dat je potřeba soubor uložit.



Obrázek 21. Úprava dat v tabulce ISO_27001:2013

5.4.3 Úprava dat v tabulce normy ISO 27001:2022

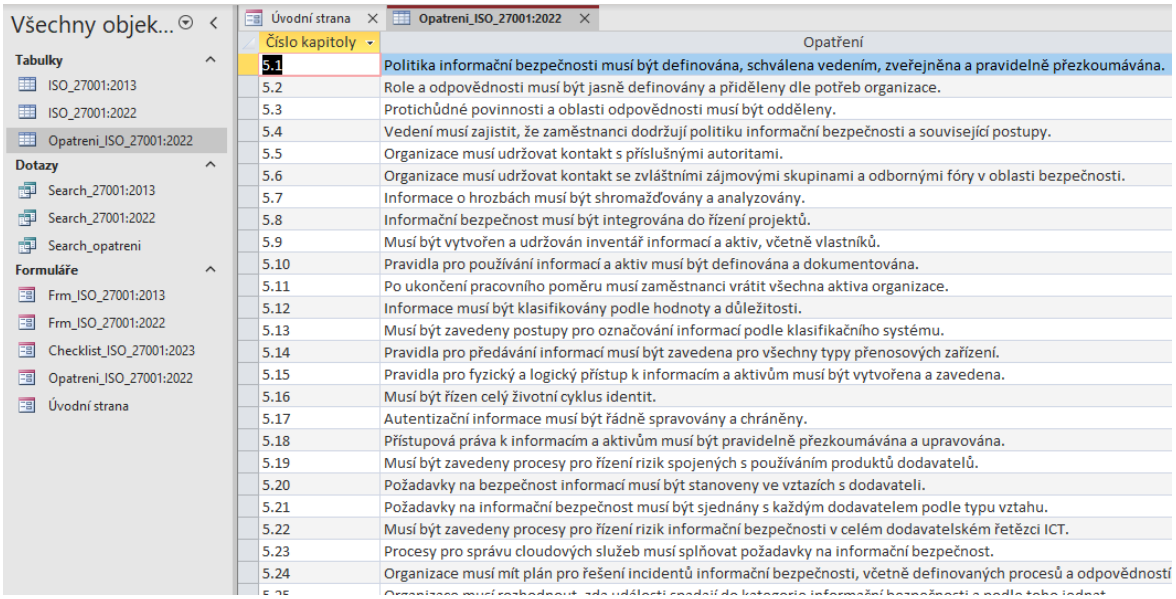
Pro úpravu dat je potřeba dvakrát kliknout myší na tabulku v které chceme měnit nebo přidávat data. Při každé změně dat je potřeba soubor uložit



Obrázek 22. Úprava dat v tabulce ISO_27001:2022

5.4.4 Úprava dat v tabulce opatření normy ISO 27001:2022

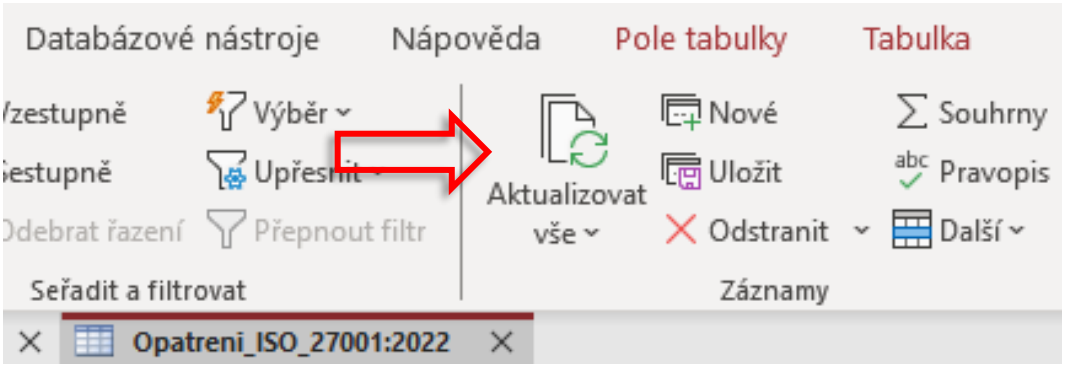
Pro úpravu dat je potřeba dvakrát kliknout myší na tabulku v které chceme měnit nebo přidávat data. Při každé změně dat je potřeba soubor uložit



Obrázek 23. Úprava dat v tabulce Opatreni_ISO_27001:2022

5.4.5 Aktualizace dat

Jelikož jsou tabulky provázány s formuláři, tak při změně dat v tabulce nastane změna i ve formuláři. Tato synchronizace zajišťuje, že všechna data zůstávají aktuální napříč celým programem. Pokud se ale změny v tabulce automaticky neprojeví ve formuláři a data se neaktualizují, je možné tento krok provést i manuálně pomocí tlačítka "Aktualizovat vše". Toto tlačítko umožňuje uživatelům ručně spustit proces aktualizace, čímž se zajistí, že všechny formuláře budou obsahovat nejnovější informace z tabulek. Znázorněno na obrázku č. 25.



Obrázek 24. Aktualizování dat

ZÁVĚR

Tato diplomová práce se zabývala implementací systému řízení bezpečnosti informací (ISMS) podle aktuálních norem ISO/IEC 27001:2022 a ISO/IEC 27002:2022, s důrazem na jejich využití ve výrobních podnicích. Hlavními cíli byly komparace aktualizovaných verzí norem ISO/IEC 27000:2022 s verzí 2013 a vytvoření metodiky pro zavedení ISMS v praxi.

V teoretické části jsme definovali klíčové pojmy a koncepty informační bezpečnosti, přičemž jsme se zaměřili na význam certifikací a standardů jako jsou ISO/IEC 27001 a 27002. Byly popsány historické milníky ve vývoji informační bezpečnosti, role mezinárodních organizací pro standardizaci (ISO a IEC), a význam implementace ISMS pro moderní organizace. Metodika PDCA (Plan-Do-Check-Act) se ukázala jako klíčový nástroj pro systematické zavádění, provoz, monitorování a zlepšování ISMS.

Praktická část práce zahrnovala podrobnou analýzu změn mezi normami ISO/IEC 27002:2013 a 2022. Zjistili jsme, že nová verze normy přináší důležité úpravy, které reflektují současné technologické a bezpečnostní požadavky. Snížení celkového počtu kontrol z 114 na 93 zjednodušuje proces implementace a zvyšuje jeho efektivitu. Zavedení nových kontrol, sloučení a odstranění některých kontrol pomáhá lépe odpovídat aktuálním potřebám organizací.

Praktická aplikace metodiky byla demonstrována na konkrétním výrobním podniku, kde byla provedena analýza současného stavu ISMS. Výsledky ukázaly vysokou míru realizace opatření, s plnou implementací v oblasti lidských zdrojů a fyzické bezpečnosti. Technologická opatření a organizační opatření dosáhla také velmi vysokého procenta realizace, což potvrzuje efektivitu navržené metodiky.

Zavedení ISMS podle normy ISO/IEC 27001:2022 přináší podnikům mnoho výhod, včetně zvýšení úrovně bezpečnosti informací, zajištění souladu s legislativními požadavky a zlepšení firemní kultury. Pravidelné audity a kontinuální zlepšování ISMS umožňují organizacím pružně reagovat na nové hrozby a udržovat vysokou úroveň bezpečnosti. Implementace ISMS také podporuje vyšší důvěru zákazníků a obchodních partnerů, což je klíčové pro dlouhodobý úspěch a konkurenceschopnost na trhu.

Významným přínosem práce je vytvoření metodiky pro zavedení ISMS, která je prakticky využitelná pro výrobní podniky. Metodika byla navržena tak, aby byla snadno adaptovatelná

na různé organizační struktury a specifické potřeby podniků. Zároveň poskytuje nástroje pro efektivní řízení rizik a zajištění kontinuity podnikových procesů.

Celkově lze konstatovat, že tato práce poskytla komplexní přehled o implementaci ISMS podle aktuálních norem a vytvořila prakticky využitelnou metodiku pro výrobní podniky. Důležitost informační bezpečnosti v dnešním digitálním světě nelze podceňovat, a proto je zavedení efektivního systému řízení bezpečnosti informací klíčové pro dlouhodobou udržitelnost a úspěch každé organizace.

SEZNAM POUŽITÉ LITERATURY

[1] ONDRÁK, Viktor; SEDLÁK, Petr a MAZÁLEK, Vladimír. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 9788072048724.

[2] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

[3] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

[4] SEDLÁK, Petr a KONEČNÝ, Martin. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.

[5] Jaké změny přinesla nová norma ISO 27002:2022? Jaký má vliv na certifikaci systémů informační bezpečnosti? Jaký je rozdíl mezi ISO/IEC 27001 a ISO/IEC 27002? [online]. In: . s. 1 [cit. 2024-05-09]. Dostupné z: doi:https://eucert.cz/jake-zmeny-prinesla-nova-norma-iso-270022022-jaky-ma-vliv-na-certifikaci-systemu-informacni-bezpecnosti-jaky-je-rozdil-mezi-iso-iec-27001-a-iso-iec-27002/

[6] The differences between ISO 27002: 2013 and ISO 27002: 2022. In: Strike Graph [online]. s. 1 [cit. 2024-05-10]. Dostupné z: https://www.strikegraph.com/blog/the-differences-between-iso-27002-2013-and-iso-27002-2022#:~:text=Most%20recently%E2%80%94on%20February%2015,the%20introduction%20of%20new%20controls.

[7] Aktualizace normy ISO 27001 – Informační bezpečnost, 2023. In: Q-COM [online]. s. 1 [cit. 2024-05-13]. Dostupné z: https://www.qcom.cz/2023/11/24/aktualizace-normy-iso-27001/

[8] POLÁCH, David. Cyber Security Framework 2 – americká obdoba NIS2 a ISO 27001? [online]. In: . [cit. 2024-05-25]. Dostupné z: https://cybrela.com/cyber-security-framework-2-obdoba-nis2-a-iso-27001/

[9] JEGELKA, Markus, 2023. Nová norma ISO/IEC 27001:2022 - klíčové změny [online]. In: . [cit. 2024-05-25]. Dostupné z: https://www.dqsglobal.com/cs-cz/vzdelavani/blog/new-iso-27001-2022-key-changes

[10] PDCA – Dr Deming's Gift To The World [online], 2019. In: . s. 1 [cit. 2024-05-25]. Dostupné z: https://www.siobhaindanaher.com/pdca-dr-demings-gift-to-the-world/

[11] Norma ISO/IEC 27001:2022. Jaké jsou klíčové změny v normě ISO/IEC 27001:2022?, 2023. In: Eucert [online]. s. 1 [cit. 2024-05-25]. Dostupné z: https://eucert.cz/norma-iso-27001-2022/

[12] JANŮ, František. V zajištění kybernetické bezpečnosti je proces víc než program. IT Systems [online]. [cit. 2024-05-26]. Dostupné z: https://www.systemonline.cz/it-pro-verejny-sektor-a-zdravotnictvi/v-zajisteni-kyberneticke-bezpecnosti-je-proces-vic-nez-program.htm?mobilelayout=false

[13] PRAVIDLA OCHRANY JEDNOTLIVÝCH ÚROVNÍ AKTIV – MINISTERSTVO PRO CERTIFIKACI SENZORŮ [online]. In: . NÚKIB, s. 12 [cit. 2024-05-26]. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Ploha%205%20-%20Vzorov%20pravidla%20ochrany%20jednitlivch%20rovn%20aktiv.pdf

[14] Klasifikace důvěrnosti informací (Classified information scheme), 2018. Management mania [online]. [cit. 2024-05-26]. Dostupné z: https://managementmania.com/cs/klasifikace-duvernosti-informaci-classified-information-scheme

[15] Co je ISO 27001? Nqa [online]. 1 [cit. 2024-05-26]. Dostupné z: https://www.nqa.com/cs-cz/certification/standards/iso-27001-2022#:~:text=Norma%20ISO%2027001%3A%202013%20(zn%C3%A1m%C3%A1,pro%20ochranu%20va%C5%A1ich%20nejd%C5%AFle%C5%BEit%C4%9Bj%C5%A1%C3%ADch%20aktiv)

[16] Jaký je rozdíl mezi ISO/IEC 27001 a ISO/IEC 27002. CeMS-CO s.r.o. [online]. 1 [cit. 2024-05-26]. Dostupné z: https://www.cems-cz.com/blog/471-jaky-je-rozdil-mezi-iso-iec-27001-a-iso-iec-27002

[17] GOLL, Jan, 2019. Z norem řízení bezpečnosti informací se postupně vytrácí řada užitečných věcí. IT SYSTEMS [online]. 1 [cit. 2024-05-26]. Dostupné z: https://www.systemonline.cz/clanky/normy-rizeni-bezpecnosti-informaci.htm?mobilelayout=false

[18] Nový zákon o kybernetické bezpečnosti je před schválením. Arion [online]. 1 [cit. 2024-05-26]. Dostupné z: https://arion.cz/aktuality/bezpecnost/novy-zakon-o-kyberneticke-bezpecnosti-je-pred-schvalenim/

[19] NEJEDLÝ, Matěj. Damoklův meč jménem NIS2. Dopadne na ajťáky, vadí i mobilním operátorům. IDnes [online]. 1 [cit. 2024-05-26]. Dostupné z: https://www.idnes.cz/zpravy/domaci/kyberbezpecnost-evropska-smernice-nis2-nukib-firmy-pruzkum.A240520_132720_domaci_nema

[20] Enerex achieves ISO-27001 Certification [online]. In: . [cit. 2024-05-27]. Dostupné z: https://enerex.com/iso-27001-certification/

[21] Timeline of the History of Information Security [online]. [cit. 2024-05-27]. Dostupné z: https://learn.saylor.org/mod/book/tool/print/index.php?id=29635&chapterid=5183

[22] Enigma - legenda za miliony korun [online]. In: DOROTHEUM. [cit. 2024-05-27]. Dostupné z: https://artplus.cz/cs/aukcni-zpravodajstvi/1/enigma-legenda-za-miliony-korun

[23] MURPHEY, Dakota. A history of information security [online]. [cit. 2024-05-27]. Dostupné z: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

[24] A brief history of ISO 27001. Secureframe [online]. 1 [cit. 2024-05-27]. Dostupné z: https://secureframe.com/hub/iso-27001/history

[25] What is ISO 27001 information security management? Secureframe [online]. 1 [cit. 2024-05-27]. Dostupné z: https://www.itgovernance.co.uk/iso27001#:~:text=ISO%2FIEC%2027001%20is%20the,addressing%20people%2C%20processes%20and%20technology.

[26] EDWARDS, Max. The Ultimate Guide to ISO 27001. IT Governance [online]. 1 [cit. 2024-05-27]. Dostupné z: https://www.isms.online/iso-27001/

[27] BENEFITS OF ISO 27001 CERTIFICATION. Moore ClearComm [online]. 1 [cit. 2024-05-27]. Dostupné z: https://mooreclear.com/services/iso-27001/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIA	Business Impact Analysis
ČSN	Česká technická norma
DLP	Data Loss Prevention
DLP	Data Loss Prevention
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPS	Intrusion Prevention System
IPS	Intrusion Prevention System
IS	Information System (Informační systém)
IS	Information System (Informační systém)
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KII	Kritická informační infrastruktura
NIS2	Network and Information Systems Directive 2
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan, Do, Check, Act
PII	Personally Identifiable Information
RPO	Recovery Point Objective
RTO	Recovery Time Objective
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SEZNAM PŘIOŽENÝCH SOUBORŮ

\ Komparace_ISO_27001_2013_2022.accdb	program v podobě formulářů v aplikaci Microsoft Access
\ Tabulka shody ISMS.xlsx	tabulka porovnávající dvě verze normy ISO/IEC 27001
\ 27001_opatreni.xlsx	tabulka se seznamem doporučených opatření