Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Navržení procesu interního IT auditu dle Zákona o kybernetické bezpečnosti

Michal Janák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Michal Janák

Informatika

Název práce

Navržení procesu interního IT auditu dle Zákona o kybernetické bezpečnosti

Název anglicky

Designing an internal IT audit process under the Cyber Security Act

---

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku IT interních auditů v oblasti kybernetické informační bezpečnosti, jejíž rámec je dán Zákonem o kybernetické bezpečnosti.
Hlavním cílem práce je navržení procesu IT interního auditu pro společnost s určenými informačními systémy základní služby.

Dílčí cíle bakalářské práce jsou:

- vydefinování potřebných rolí, jejich pravomocí, povinností a odpovědností;
- navržení způsobu prověření bezpečnostních požadavků informační kybernetické bezpečnosti definovaných vyhláškou kybernetické bezpečnosti;
- vydefinování ukazatelů procesu pro zajištění PDCA cyklu zlepšování navrženého procesu IT interních auditů.

Metodika

Metodika řešené problematiky je založena na studiu a analýze odborných informačních zdrojů a konzultací se specialisty v oboru auditů kybernetické bezpečnosti. Vlastní řešení návrhu procesu IT interních auditů je realizováno prostřednictvím kvalitativní metody focus group. Na základě rozboru teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

interní audit, informační kybernetická bezpečnost, Zákon o kybernetické bezpečnosti, ISMS, Organizační opatření, Technická opatření, Vyhláška o kybernetické bezpečnosti, ISO 27001, Bezpečnostní požadavky, auditor kybernetické informační bezpečnosti, NÚKIB, informační systém základní služby

---

Doporučené zdroje informací

Agile Auditing In:www.isaca.org [online]. 2021. ISACA

ČESKO. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) – znění od 28.5.2018

ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – znění od 6. 8. 2022

ČSN ISO/IEC 27001:2014 informační technologie – bezpečnostní techniky – systémy managementu bezpečnosti informací – požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27007:2020 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací. Praha: Český normalizační institut, 2020.

IT Audit Framework (ITAF) A Professional Framework for IT Audit 4th Edition. In:www.isaca.org [online]. 2020.

Mezinárodní rámec profesní praxe interního auditu. Český institut interních auditorů 2017. Praha: Český institut interních auditorů, 2017. ISBN 978-80-86689-55-5

SVATÁ, V. Audit informačního systému. Praha: Oeconomica, 2016. ISBN 978-80-245-2168-8.

Předběžný termín obhajoby

2022/23 ZS – PEF

Vedoucí práce

doc. Ing. Jan Tyrychtr, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 31. 10. 2022

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 26. 12. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Navržení procesu interního IT auditu dle Zákona o kybernetické bezpečnosti" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2023 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Janu Tyrychrovi, Ph.D., za cenné rady, podněty a trpělivost, se kterou ke mně a mé práci přistupoval.

Navržení procesu interního IT auditu dle Zákona o kybernetické bezpečnosti

Abstrakt

Tato bakalářská práce rozebírá problematiku navržení obecného postupu pro interní IT audity v oblasti kybernetické a informační bezpečnosti. Provádění auditů kybernetické bezpečnosti vyžaduje u určených subjektů Zákon č. 181/2014 sb. o kybernetické bezpečnosti České republiky, nicméně nestanovuje jeho formu. Cílem této bakalářské práce je navrhnout natolik univerzální proces, aby byl aplikovatelný na společnost, jejíž informační systémy byly určeny jako informační systémy základní služby. Tím na ně povinnost vykonání kybernetických auditů dopadá. Po provedení analýzy odborných a legislativních dokumentů byl proveden návrh procesu pro interní IT audity dle Zákona č. 181/2014 sb. o kybernetické bezpečnosti. Tento proces byl následně zkoumán metodou *Focus Group* na skupině odborníků v oblasti kybernetické bezpečnosti, ISO auditů a auditů informační kybernetické bezpečnosti. Na základě výsledků z odborné diskuse byla provedena revize a úprava původně navrženého procesu. Byl navržen univerzální proces pro interní IT kybernetické audity, který je v souladu s dobrou praxí v oboru interních auditů, ISO norem i mezinárodního rámce profesní praxe interního auditu. V případě, že povinná osoba s určeným informačním systémem základní služby bude využívat tento navržený proces, bude pro oblasti související s auditem kybernetické bezpečnosti v souladu se Zákonem č. 181/2014 sb. o kybernetické bezpečnosti.

Klíčová slova: interní audit, informační a kybernetická bezpečnost, Zákon o kybernetické bezpečnosti, ISMS, Organizační opatření, Technická opatření, Vyhláška o kybernetické bezpečnosti, ISO 27001, Bezpečnostní požadavky, auditor kybernetické a informační bezpečnosti, NÚKIB

Designing an internal IT audit process under the Cyber Security Act

Abstract

This bachelor's thesis discusses the design of a general procedure for IT audits in the cyber information security. Conducting cyber security audits is required by the Act n.181/2014 Cyber Security of the Czech Republic in appointed entities, however, it does not stipulate its formula. The goal of this bachelor's thesis is to design a process that is universal enough to be applicable by companies with specified elements of the basic services information system. After the analysis of professional and legislative documents, a process design for IT audits was carried out. This process was subsequently investigated, using the focus group method, on a group of cyber security expert, ISO audits and cyber security audits. Based on the results of the expert discussion, the originally proposed process was reviewed and modified. A universal process for IT cyber audits has been designed, which is in line with good practice of the ISO audits as well as the international framework for the professional practice of internal auditing. In the event that the obliged person with the determined information system of the basic service follows this designed process, then it operates in accordance with the Cyber Security Act.

Keywords: internal audit, information and cyber security, Cyber Security Act, ISMS, Organizational measures, Technical measures, Decree on cyber security, ISO 27001, Security requirements, cyber information security auditor, NÚKIB

Obsah

1 Úvod

Kybernetická a informační bezpečnost a související činnosti jsou přítomny v rámci každodenního fungování současného světa kolem nás. V závislosti na rychlosti vývoje kybernetického prostoru, informačních technologií a s tím souvisejících nových informačních systémů vznikají rizika a hrozby, které nás ovlivňují a mohou mít velký dopad na náš život. Ve společnosti dochází k jejich využívání dynamicky a živelně se zaměřením na maximální výkon, při kterém se mohou opomíjet pravidla a regulace. Regulace, které v této oblasti vznikají, nastavují základní rámec pro fungování systémů důležitých pro chod státu a návazně na to i pro veřejnost. Zásadní regulační nástroj státu pro stanovení těchto podmínek je zákon č. 181/2014 sb. o kybernetické bezpečnosti (dále jen Zákon o kybernetické bezpečnosti), který byl vydán v roce 2014, a následné prováděcí předpisy. Do té doby neexistoval žádný zákon, jenž by tuto problematiku komplexně řešil. Tento zákon dopadá zejména na subjekty a systémy, které jsou provozovány, ještě delší dobu, než je existence novodobé České republiky. Jejich fungování se dnešnímu online světu musí stále častěji přizpůsobovat.

Mezi lety 2021 a 2022 došlo k nárůstu povinných osob o 151 subjektů a 316 informačních systémů. Největší procentuální nárůst byl v soukromém sektoru u informačních systémů základní služby, a to 142 % (Kučínský a kolektiv, 2022). Důvody existence rizik a hrozeb pro informační systémy základní služby můžeme spatřovat v tom, že ochrana neboli bezpečnost společnostem prvoplánově negeneruje žádný zisk, a až v případě napadení a způsobení škod je možné porovnávat ztráty s cenou jejich zavedení.

Jedním z prvků kontroly plnění požadavků Zákona o kybernetické bezpečnosti a vyhlášky č. 82/2018 sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen Vyhláška o kybernetické bezpečnosti) jsou pravidelné audity, které Vyhláška o kybernetické bezpečnosti přímo vyžaduje: „*Povinná osoba v rámci systému řízení bezpečnosti informací zajistí provedení auditu kybernetické bezpečnosti u informačního a komunikačního systému* (dále jen „audit kybernetické bezpečnosti“) *podle § 16*“. (Vyhláška o kybernetické bezpečnosti, 2018).

Proto je klíčové sestavení takového rámce a procesu kybernetických auditů, který bude vyhovovat požadavkům zákona a vyhlášky o kybernetické bezpečnosti, a současně zajistí kontrolu nastavení zavedených postupů, odhalování jejich slabin a identifikaci příležitostí ke zlepšení procesů vůči dobré auditní praxi a mezinárodním bezpečnostním standardům.

2 Cíl práce a metodika

2.1 Cíl práce

Bakalářská práce je tematicky zaměřena na problematiku IT interních auditů v oblasti kybernetické informační bezpečnosti, jejíž rámec je dán Zákonem o kybernetické bezpečnosti.

Hlavním cílem práce je navržení procesu IT interního auditu pro společnost s určenými informačními systémy základní služby.

Dílčí cíle bakalářské práce jsou:

- vydefinování potřebných rolí, jejich pravomocí, povinností a odpovědností;
- navržení způsobu prověření bezpečnostních požadavků informační kybernetické bezpečnosti, definovaných vyhláškou kybernetické bezpečnosti;
- vydefinování ukazatelů procesu pro zajištění PDCA cyklu, zlepšování navrženého procesu IT interních auditů.

2.2 Metodika

Metodika řešené problematiky je založena na studiu a analýze odborných informačních zdrojů a konzultací se specialisty v oboru auditů kybernetické bezpečnosti. Vlastní řešení návrhu procesu IT interních auditů je realizováno prostřednictvím kvalitativní metody Focus Group. Na základě rozboru teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

3 Teoretická východiska

3.1 Legislativa a standardy v oblasti informační a kybernetické bezpečnosti

V této kapitole bude popsán legislativní rámec pro kybernetickou a informační bezpečnost a na ní navázané IT kybernetické audity. Dále související dobrá praxe, ze které dané rámce vycházejí, s plánovanými změnami, přicházejícími z prostředí Evropské unie.

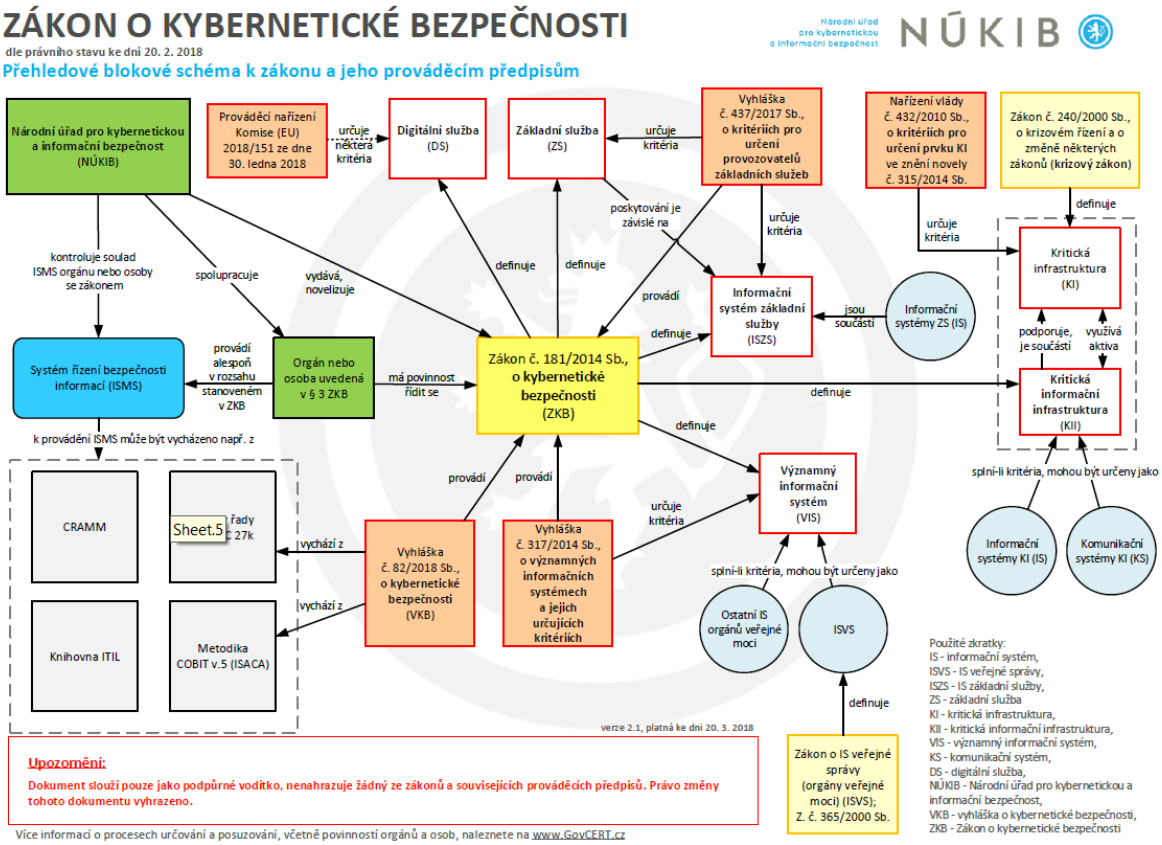
3.1.1 Zákon o kybernetické bezpečnosti

Základním právním předpisem pro oblast kybernetické bezpečnosti v České republice je Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, který *upravuje práva a povinnosti osob a působnost a pravomoc orgánů veřejné moci v oblasti kybernetické bezpečnosti.* (Zákon o kybernetické bezpečnosti, 2014)

Zákon překlápí do české legislativy směrnici Evropského parlamentu a Rady (EU) č. 2016/1148 z 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále NIS) a následně v roce 2018 prováděcí nařízení komise (EU) č. 2018/151, kterým se stanovují pravidla pro uplatňování směrnice NIS. Směrnice a nařízení mají za cíl standardizovat oblast kybernetické bezpečnosti sítí, poskytování digitální služby a informačních systémů na jednotné úrovni. Zákon o kybernetické bezpečnosti je dále rozpracován v rámci prováděcích vyhlášek a nařízení, a to vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritérií, vyhláškou č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby a nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Tyto předpisy určují pravidla, kritéria a doporučení, jakými se určené subjekty mají za povinnost chovat a jakým způsobem ke kybernetické a informační bezpečnosti přistupovat a realizovat ji. Jak je vidět na Obrázku č. 1 – *Přehledové blokové schéma k zákonu a jeho prováděcím předpisům*, existují mezi právními normami vztahy, kde jako dobrá praxe, ze které se při jejich vytváření vycházelo, byly využity standardy ISO/IEC27K a COBIT v. 5. I když zákon a prováděcí předpisy určují kritéria a podmínky, za kterých mohou subjekty pracovat s informačními systémy a informacemi, nevztahují se na informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Ty se řídí zákonem č. 412/2005 sb., o ochraně utajovaných informací a bezpečnostní způsobilosti (Oto Křivanec, 2021). Zákon kybernetické bezpečnosti dále stanovuje, kdo a jakým způsobem se stává povinnou osobou pro jeho působnost a naplňování. Povinnými osobami, na které se vztahují

následné kontroly ze strany Národního úřadu pro kritickou informační bezpečnost, jsou správce a provozovatel informačního systému kritické informační infrastruktury, správce a provozovatel významného informačního systému a správce a provozovatel informačního systému základní služby. A současně prvky podléhající tomuto zákonu jsou *„informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém, informační systém základní služby anebo informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb“*. (Zákon o kybernetické bezpečnosti, 2014, § 1). Pro potřebu naplnění cílů této bakalářské práce bude dále rozpracována oblast informačního systému základní služby a jeho určení.

Obrázek 1- Přehledové blokové schéma k zákonu a jeho prováděcím předpisům



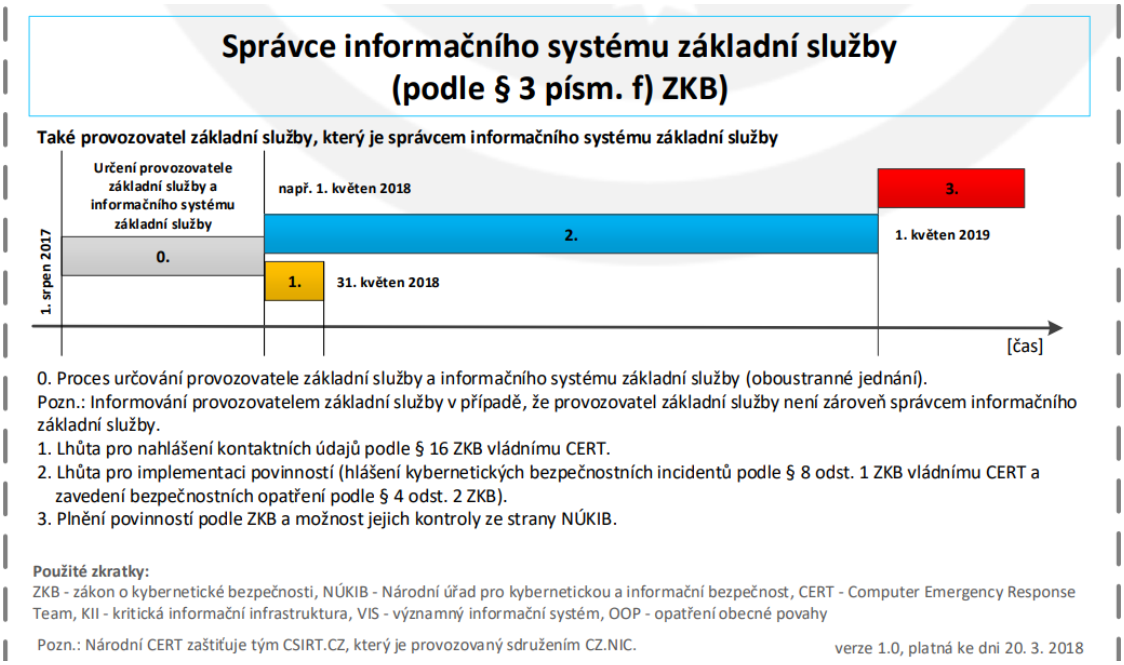
Zdroj: www.nukib.cz

3.1.1.1 Informační systém základní služby

Jak je uváděno v rámci Zákona o kybernetické bezpečnosti, jsou informační systémy základní služby (dále jen ISZS) takové systémy, bez kterých by nebylo možné provozovat a poskytovat základní služby státu. To by mělo dopad na zabezpečení společenských nebo ekonomických činností v rámci odvětví energetiky, dopravy, bankovnictví, infrastruktury, finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury nebo chemického

průmyslu (Zákon o kybernetické bezpečnosti, 2014). Pro určení takového informačního systému je nejprve nutné identifikovat základní službu. „*Základní službou se rozumí služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví*“ (NÚKIB, 2018). I když daný systém spadá do takového odvětví, je nutné, aby splňoval i odvětvová a dopadová kritéria daná vyhláškou č. 437/2017 Sb, o kritériích pro určení provozovatelů základních služeb. Odvětvová kritéria jsou závislá na druhu služby, druhu subjektu a speciálních kritériích druhu subjektu. Pro příklad uvádím v rámci odvětví Teplárenství, druh služby 1.4.1 Výrobu tepelné energie. Druh subjektu je v tom případě držitel licence na výrobu tepelné energie podle energetického zákona a speciálními kritérii jsou zdroje tepelné energie, vyvedení tepelného výkonu ze zdroje tepelné energie nebo technický dispečink využívaný k výrobě tepelné energie. Dopadovými kritérii by byly v případě nastalého kybernetického bezpečnostního incidentu v informačním systému nebo síti, které by omezovalo anebo znemožňovalo poskytovat danou základní službu pro více než 25000 osob, omezení nebo narušení provozu prvku kritické infrastruktury, hospodářskou ztrátu vyšší než 0,25 % HDP, oběti na životech s mezní hodnotou sta a více mrtvých nebo tisíce a více zraněných s nutností ošetření. Jako posledním kritériem je narušení veřejné bezpečnosti, kde by musely zasahovat složky policie, hasičů nebo záchranné služby, a to ve významné části obce s rozšířenou působností (Vyhláška č.437/2017 sb., o kritériích pro určení provozovatelů základních služeb, 2017). V případě naplnění zákonných požadavků pro určení ISZS provede národní úřad pro kybernetickou bezpečnost rozhodnutí o určení ISZS. Od tohoto momentu vzniká uvedeným společnostem povinnost začít plnit požadavky zákona o kybernetické bezpečnosti, tzn. provádět opatření vydaná ze strany NÚKIB, nahlásit kontaktní údaje a jejich změny, na což mají měsíc od určení. Od tohoto okamžiku se počítá tzv. „roční přechodná lhůta” určená na zavádění bezpečnostních opatření definovaných vyhláškou kybernetické bezpečnosti, a postupů na hlášení kybernetických bezpečnostních incidentů na národní úřad kybernetické bezpečnosti. Po skončení přechodné lhůty má úřad právo provádět kontroly dodržování zákona kybernetické bezpečnosti. Grafické znázornění je uvedeno na obrázku č. 2 - Lhůty a přechodná ustanovení Zákona o kybernetické bezpečnosti, autor NUKIB – podpůrné materiály níže. (Zákon o kybernetické bezpečnosti, 2014)

Obrázek 2 - Lhůty a přechodná ustanovení zákona o kybernetické bezpečnosti



Zdroj www.nukib.cz/sekce podpůrné materiály

Ze zprávy o stavu kybernetické bezpečnosti za rok 2021, která byla vydána v červnu roku 2022 vyplývá, že na konci roku 2021 bylo určeno 124 správců systémů základní služby a 147 informačních systémů základní služby. (Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022)

3.1.2 Vyhláška č. 82/2018, o kybernetické bezpečnosti

Z pohledu obsahu této bakalářské práce se jedná o zásadní legislativní úpravu, která obsahuje auditovatelné podmínky naplnění zákona, a to bezpečnostní opatření, povinnosti incident managementu, reaktivní opatření a náležitosti podání v oblasti kybernetické bezpečnosti a likvidace dat. Vyhláška je rozdělena do pěti částí:

První část upřesňuje úvodním ustanovením záběr, který vyhláška upravuje, a základní pojmy, se kterými se v rámci organizace pracuje.

V druhé části jsou rozvedena bezpečnostní opatření, a tedy faktické podmínky, které povinné osoby musí implementovat anebo vysvětlit důvody, z jakých tak neučinili (Vyhláška o kybernetické bezpečnosti, 2018). Tyto případy vystihuje výkladový slovník kybernetické bezpečnosti, který zpracoval Národní úřad pro kybernetickou bezpečnost. Dle něj mají bezpečnostní opatření za úkol zabezpečit ochranu za účelem dostupnosti, důvěrnosti nebo integrity systémů a jejich informací. Jsou zde popsány případy bezpečnostních opatření na zabezpečení informačních systémů, ale i protiopatření takových informačních systémů v případě, že požadované podmínky provozovatel nemůže splnit.

V rámci tohoto výkladového slovníku je uvedeno, že taková opatření mají za úkol snížit dopad hrozeb nepokrytí definovaných bezpečnostních opatření. Díky protiopatřením lze hrozby úplně eliminovat nebo jen zmírnit případné škody na únosnou úroveň anebo je pouze rozpoznat a ohlásit. (Jirásek a kolektiv, 2022)

Třetí část vyhlášky se zbývá kybernetickými bezpečnostními incidenty, jejich kategorizací, formou a náležitostmi, jak je hlásit na Národní úřad pro kybernetickou a informační bezpečnost a vládního CERTu (z anglického Computer Emergency Response Team) České republiky. Dle informací prezentovaných Národním úřadem pro kybernetickou a informační bezpečnost je úkolem CERT čelit bezpečnostním výzvám, řešit bezpečnostní incidenty a předcházet jejich vzniku. Národní tým CERT zaštiťuje zájmové sdružení právnických osob CZ.NIC. (GovCERT.CZ, 2022)

Část čtvrtá popisuje reaktivní opatření, která zveřejňuje úřad národní informační kybernetické bezpečnosti na svých webových stránkách a zasílá povinným osobám. Dále je zde rozveden obsah a způsob, kterým na úřad hlásit kontaktní údaje a jak s úřadem komunikovat. (Vyhláška o kybernetické bezpečnosti, 2018, § 33 a § 34)

Část pátá popisuje přechodná ustanovení, ustanovení rušící předchozí vyhlášky č. 316/2014 Sb. o kybernetické bezpečnosti a datum účinnosti této vyhlášky, která je platná ke dni vyhlášení. (Vyhláška o kybernetické bezpečnosti, 2018, § 35, § 36 a § 37)

3.1.2.1 Bezpečnostní opatření

Bezpečnostní opatření jsou v rámci vyhlášky rozdělena na organizační a technická. Nejprve musí povinná osoba provést určení primárního informačního aktiva a informačních systémů, které doplní o podpůrná informační aktiva. Poté musí nastavit či upravit stávající systém managementu informací (dále ISMS) ve své organizaci (Zákon o kybernetické bezpečnosti, 2014). Tím vymezí jak kybernetický, tak fyzický perimetr, který je povinná osoba dle § 5 Vyhlášky o kybernetické bezpečnosti povinna provádět pravidelnou analýzou rizik a identifikovaná rizika následně řídit. Na takto identifikovaná rizika povinná osoba aplikuje přiměřená bezpečnostní opatření. A to podle § 4 ods. 2 zákona o kybernetické bezpečnosti, kde je uvedeno, že tato opatření mají být aplikována v nezbytném rozsahu a má o nich být vedena bezpečnostní dokumentace. (Kučínský, 2019)

3.1.2.2 Organizační opatření

Organizační opatření popisují požadavky na zavedení a využívání jednotlivých činností v rámci povinné osoby a její společnosti. Tyto činnosti jsou navzájem provázané a jedna bez druhé by nezaručovala funkčnost systému bezpečnosti informací dané organizace. Proto je nutné řešit jejich zavedení napříč organizační strukturou povinné osoby (Kintr, 2016). Výkladový slovník je popisuje jako: „*Procesy, které shromažďují a využívají informace k hodnocení výkonu různých organizačních zdrojů, jako jsou lidské, fyzické, finanční, a také organizace jako celek ve světle sledovaných organizačních strategií, přičemž ovlivňují chování organizačních zdrojů při implementaci organizačních strategií.*“ (Jirásek a kolektiv, 2022). Mezi organizační opatření vyhláška řadí:

„a) Systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací,

i) řízení přístupu osob,

j) akvizice, vývoj a údržba,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit.“ (Zákon o kybernetické bezpečnosti, § 5 bod 2)

Zavedením organizačních opatření organizace dokládá systémový přístup ke kybernetické a informační bezpečnosti. Nastavení organizačních opatření dává základ efektivnímu nastavení technických opatření a následně využití správných technických nástrojů k dosažení požadované úrovně kybernetické bezpečnosti dle Zákona o kybernetické bezpečnosti. (Kintr, 2016)

Vyhodnocení zavedení těchto opatření je věnován bod m), který se zabývá kontrolou a auditem. Tento bod bude rozveden níže v této práci.

3.1.2.3 Technická opatření

Technická opatření a současně i protiopatření jsou automatizované činnosti, které jsou využívány informačním systémem díky integrovaným mechanismům na zařízeních a jejich programech anebo jejich částí. (Jirásek a kolektiv, 2022)

Technická opatření oproti organizačním požadavkům vyžadují od povinné osoby zavést faktická opatření chránící daný subjekt před vnějšími hrozbami. I když se ve větší části v organizaci bude jednat o zavedení informačních a fyzických nástrojů, pravidel a postupů, které tyto činnosti budou vykonávat, je na organizaci, jakým způsobem k naplnění těchto požadavků přistoupí. Jako průvodce při zavádění těchto technických opatření mohou sloužit technické normy a dobrá praxe, například ISO normy řady 27k (Nonnemann a kolektiv, 2022). Zákon o kybernetické bezpečnosti definuje jako technická opatření následující:

„Technickými opatřeními jsou

a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací,

l) bezpečnost průmyslových a řídících systémů.“ (Zákon o kybernetické bezpečnosti, § 5 bod)

3.1.3 Normy ISO a normy řady 27k

Normy ISO rozvíjí Mezinárodní organizace pro normalizaci společně s IEC Mezinárodní elektronickou komisí specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustanovených příslušnými organizacemi pro jednotlivé technické činnosti. (ČSN EN ISO/IEC 27001, 2014). Dle informací obsažených na internetové stránce

mezinárodní organizace pro normalizaci je ISO nezávislou a mezinárodní organizací, ve které je soustředěno na 167 národních normalizačních orgánů. Normy ISO jsou postaveny na zásadách průhlednosti, otevřenosti, nestrannosti a domluvě, relevanci a účinnosti, soudržnosti a rozvoje. Sídlo této mezinárodní organizace je v Ženevě ve Švýcarsku (ISO, 2020). V rámci České republiky se norami ISO zabývá Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Organizace si zakládá na tom, že zavedení a následná certifikace je dobrovolná a není navázána na legislativu jednotlivých států. Normy ISO jsou dále rozpracovány a zlepšovány na základě nových objevů a rozvoji v rámci standardizovaných oblastí. Komplexní systém ISO norem pokrývá široký záběr oblastí, které jsou spolu kompatibilní. Normy jsou poskládány ve stejné struktuře, což je v praxi velkou výhodou oproti jiným standardům a dobré praxe, které jsou úzce zaměřené a jejich zavedení v prostředí společnosti není tak harmonizované a sourodé, jako v případě ISO norem. (ČSN EN ISO/IEC 27001, 2014). V případě, že se organizace rozhodne nechat se certifikovat certifikační autoritou dokládá svou úroveň zabezpečení certifikátem. Certifikování je v řadě ISO 27k možné jen na normu ČSN EN ISO/IEC 27001 (dále jen ISO 27001). Ostatní normy této řady jsou pouze doporučující nebo vysvětlující.

Jako zásadní pro auditování oblasti informační kybernetické bezpečnosti a nastavení této oblasti je, aby daná organizace postupovala v souladu i s dalšími normami uvedenými v tabulce č. 1 (Cuřín, 2019).

Tabulka 1- Seznam norem ISO důležitých pro proces auditu

Označení normy	Jméno normy
ČSN EN ISO 9001	Systémy managementu kvality – Požadavky
ČSN EN ISO/IEC 27000	Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník
ČSN EN ISO/IEC 27001	Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky
ČSN EN ISO 19011:2019	Směrnice pro auditování systému managementu

Zdroj: vlastní zpracování, inspirováno Cuřín, 2019

3.1.3.1 ISO 27001 Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky

Tato norma popisuje systém řízení bezpečnosti informací. Norma specifikuje požadavky pro budování, implementaci, řízení, monitorování, přezkoumávání, údržbu a zlepšování dokumentovaného ISMS s ohledem na celková podnikatelská rizika organizace. Je rozdělena na kapitoly 1–10, kde kapitoly 4–10 jsou mandatorní a jakékoliv vyřazení z implementace požadavků organizace by znemožňovalo udělení certifikace systému. Z povahy daných kapitol

by takový systém nebyl udržitelný jako celek. V odůvodněných případech a na základě podnikatelských činnosti zavádějící osoby je možné vyřadit a odůvodnit požadavky uvedené v rámci přílohy A normy. (Cuřín, 2019)

Požadavky normy jsou použitelné a aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu jejich činností. Což znamená, že jsou implementovatelné jak na soukromníka, stát, organizace nebo korporace. Organizace, která se rozhodne zavádět ISMS dle standardu ISO 27001 by měla při plánování jejího rozsahu určit rizika a příležitosti daného systému řízení. Při plánování jejího zavádění musí zajistit naplnění stanovených výsledků, předcházet nepředvídatelným jevům a snižovat jejich dopady, a definovat formu dosažení neustálého zlepšování – dokončení PDCA cyklu. (ČSN EN ISO/IEC 27001, 2014)

Dle kapitoly 9.2 normy popisující požadavky na interní audit je uvedeno, že organizace musí plánovat vykonání interních auditů, a to pravidelně v intervalech, které si naplánuje. Audit musí dát odpověď, zda daná organizace vyhovuje požadavkům normy a zároveň svým vlastním předpisům a nařízením. Dále audit dává ujištění o tom, zda je ISMS efektivně implementován a udržován. Mimo plánování auditů musí organizace také pro každý audit určit jeho rozsah a kritéria, podle kterých bude auditovanou oblast vyhodnocovat. Audit a zaměstnanci, kteří ho mají vykonávat, musí být objektivní a nestranný a jeho výsledky musí být předkládány relevantním osobám. Organizace dále musí uchovávat důkazy o programu a výsledcích interního auditu. (ČSN EN ISO/IEC 27001, 2014)

3.1.4 Připravovaná směrnice Evropské unie NIS 2

Nová směrnice Evropské unie podstatně rozšiřuje okruh institucí, které ji budou muset povinně splnit. Rozšiřuje oblast působnosti stávající směrnice NIS tím, že doplňuje nová odvětví podle jejich významu pro hospodářství a společnost. Dále zavádí jasný limit pro velikost organizace spadající pod tuto legislativu. Do oblasti působnosti směrnice NIS 2 budou zahrnuty všechny střední a velké společnosti ve vybraných odvětvích. Pro společnosti zpřísňuje a zefektivňuje požadavky na bezpečnost a podávání zpráv úřadu pro kybernetické bezpečnosti. Zavádí přísnější opatření dohledu pro vnitrostátní orgány a přísnější požadavky na vymáhání těchto požadavků. Za nedodržení pravidel stanovených směrnicí hrozí pokuta, jejíž výše začíná na částce 10 000 000 Kč nebo 2 % z celkového celosvětového ročního obratu podniku v předchozím rozpočtovém roce – podle toho, co je vyšší). Oproti NIS jsou v NIS 2 státy zavázány stanovit tyto sankce jako minimální strop. Směrnice je navržena tak, aby bylo zajištěno komplexní pokrytí všech odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu EU. Subjekty dělí do dvou kategorií

na subjekty zásadního významu (například v oblasti energetiky, dopravy, bankovnictví a infrastruktury) a důležité subjekty, do kterých patří například poštovní a kurýrní služby, nakládání s odpady a dalších. De facto bude NIS 2 po zapracování do interní legislativy závazná pro většinu komerčních subjektů. NIS 2 přinese mimo zpřísnění požadavků na ISMS oproti stávajícímu stavu navíc zvýšené náklady na informační a kybernetickou bezpečnost a potřebné zdroje. Jedná se o zavedení nebo obsazení povinných bezpečnostních rolí, zavedení bezpečnostních opatření a bezpečnostních nástrojů. Bude nutné zajistit schopnost včasné detekce bezpečnostních incidentů a reakcí na ně. Dále budou společnosti muset zajistit sdílení bezpečnostních informací s NUKIB, národním CERT a odvětvovým CERT Evropské unie. (Haller, 2022)

3.2 Procesní řízení

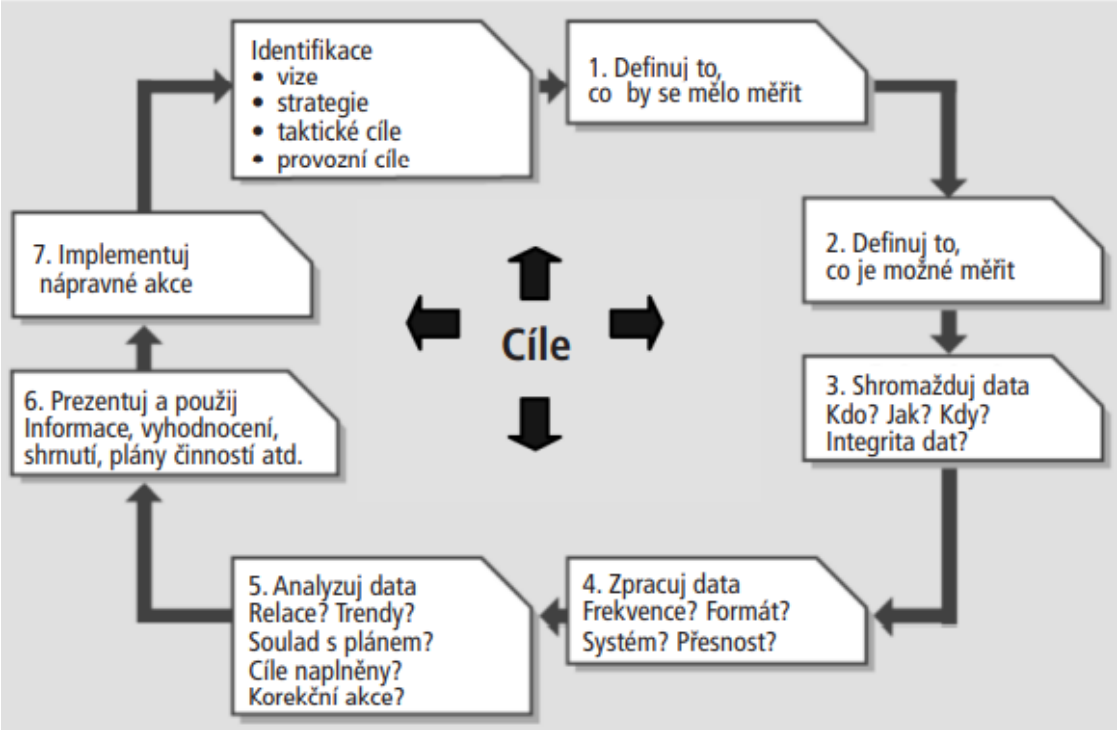
V teoretické části procesního řízení budeme vycházet z definic a popisů procesů dobré praxe v oblasti správy a IT služeb, za kterou jsou považovány standardy ITIL. Z těch následně vychází například technická norma ISO/IEC 20 000, na jejímž rozvoji se podílí například mezinárodní nezávislá a nezisková organizace itSMF (IT Service Management Forum), která má i české zastoupení ve spolku itSMF Czech Republic, z.s (ItSMF Czech Republic, 2012-2022). Standardy ITIL popisují mimo popisu zajištění služeb IT i nastavení procesů včetně těch podpůrných funkcí a jejich způsobilostí. Řízení procesu pak definuje jako *„činnost plánování a usměrňování procesu s cílem provádět proces efektivním, hospodárným a konzistentním způsobem“* (Hudec, 2012). Dále budeme vycházet z ISO norem ČSN EN ISO 9000 – Systém managementu kvality, která popisuje procesní řízení jako přístup k řízení organizace (ČSN EN ISO 9000, 2016).

3.2.1 Proces

Dle standardu ITIL se definuje proces jako *„Strukturovaná množina činností navržená pro dosažení určitého specifického cíle“* (Hudec a kolektiv, 2012), dále definuje, že může mít jeden až n vstupů, které pomocí kroků v procesu přetváří do jednoho až n výstupů. Součástí procesů můžou být definovány role, které ho vykonávají, včetně odpovědností, dále nástroje a manažerské kontrolní mechanismy. Proces může definovat řídící dokumentace ve formě norem, směrnic či jiných dokumentovaných informací, či pracovních instrukcí (Hudec, 2012). Oproti tomu norma ISO 9000 definuje za proces „jakoukoliv činnost, nebo soubor činností, při kterých se využívají zdroje k přeměně vstupů na výstupy“ (ČSN EN ISO 9000, 2016). To, v čem se oba typy norem shodují a jsou v souladu, je potřeba neustálého zlepšování

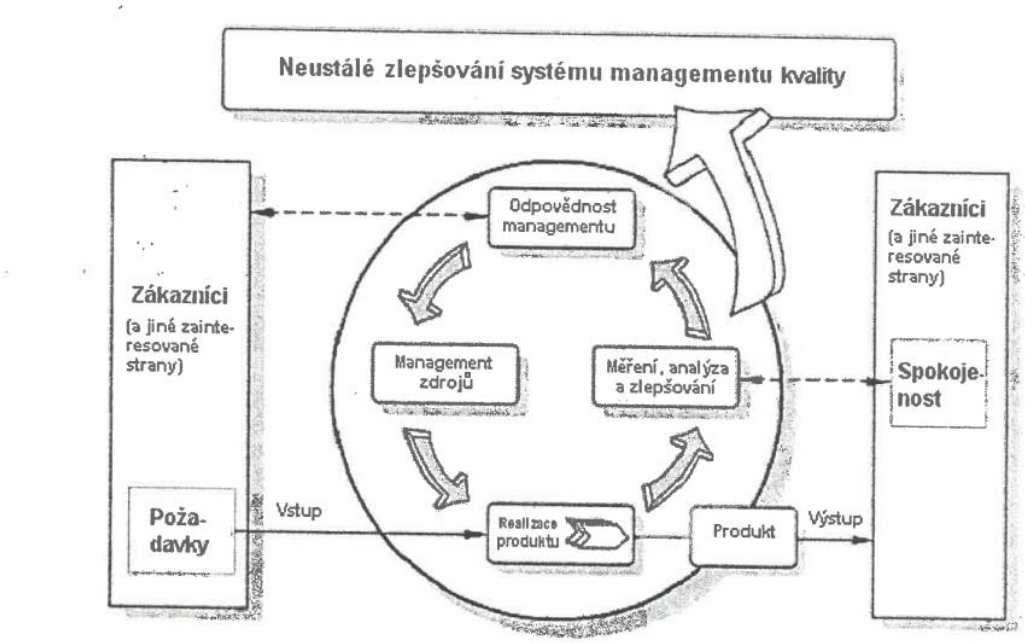
procesů, i když k tomu docházejí rozdílnými kroky, které jsou rozvedeny v následujících diagramech.

Obrázek 3 - ITIL - proces zlepšování



Zdroj: Cartlidge a kolektiv, 2007

Obrázek 4 - ISO 9001 - Proces zlepšování



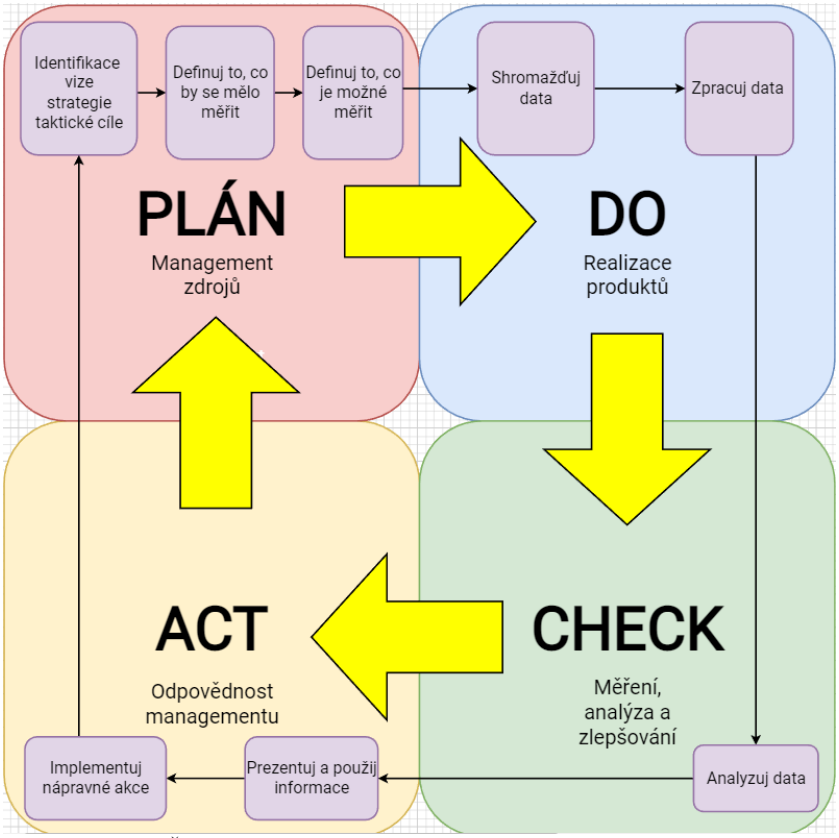
Zdroj: norma ČSN EN ISO 9001, 2016

Zjednodušenou formu zlepšování a princip, ze kterého budeme vycházet v rámci návrhu procesu kybernetických auditů, je takzvaný Demingův PDCA cyklus.

3.2.2 Demingův PDCA cyklus

Demingův cyklus popisuje způsob, jakým společnost může zabezpečit funkčnost systému bezpečnosti informací a zajištění jeho neustálého zlepšování. Aby byl tento cyklus naplněn, je nutné dodržet všechny jeho části, tzn. PDCA, což je plánuj (Plan), dělej (Do), kontroluj (Control) a jednej (Act). V rámci této bakalářské práce se primárně zabýváme částmi kontroluj a jednej, neboli naprav. Tyto části se vztahují k návrhu auditního procesu. Nicméně auditní proces, jakožto samostatný proces podléhá částem plánuj, kde se naplánují činnosti vedoucí ke zlepšení aktuálního systému řízení, a fázi dělej, kde se dané činnosti vykonají podle dříve schváleného plánu. Ve fázi kontroly se kontroluje, co a jakým způsobem bylo naplánováno a jestli dané činnosti naplnily stanovená očekávání. Na neshody z fáze kontroly jsou nastavena nápravná opatření, která by měla dané neshody nebo prostory pro zlepšení odstranit. PDCA cyklus je aplikovatelný na jakoukoliv dobrou praxi či metodiku, která je v rámci organizací využívána a na jejímž principu je vystavěn i Zákon o kybernetické bezpečnosti. (Cuřín, 2019)

Obrázek 5 - Aplikování PDCA cyklu na procesy zlepšování ITIL a ISO



Zdroj: vlastní zpracování dle normy ČSN EN ISO 9001, 2016 a Cartlidge a kolektiv, 2007

3.3 Principy informační a kybernetické bezpečnosti

V současné době, kdy informace mají pro organizace a společnost vzrůstající hodnotu a velkou konkurenční výhodu, mohou mít například formu fyzického nebo elektronického dokumentu, ale i mluveného slova či myšlenky. Takové informace mohou být uloženy jak na fyzických nosičích, tak ve formě dat na HW uložištích, nebo v rámci SW aplikací. Díky množství způsobů uložení a důležitosti těchto informací je nutné zaměřit se na ochranu těchto dat. V případě, že bychom informace pouze chránili, byly by nepoužitelné a stávaly by se zbytečnými daty. Z toho důvodu jsou základními kameny informační kybernetické bezpečnosti dostupnost, důvěrnost a integrita informací. To znamená, že informace mimo toho, že je musíme chránit, je nutné je sdílet mezi oprávněnými uživateli, kteří s nimi musí mít možnost pracovat, a hlavně musí být aktuální. Díky zavedení takového bezpečnostního systému si společnost zajistí udržení konkurenceschopnosti, ziskovosti, právní shody a dobrého jména organizace.

3.4 Vnitřní kontrolní systém

Jednu z metod hodnocení vnitřního kontrolního systému definují standardy sponzorských organizací COSO. Do definice pravidel se zapojily Americká účetní asociace, Americký institut certifikovaných veřejných účetních, Financial Executives International, Institut interních auditorů a Národní asociace účetních (nyní Institut manažerských účetních) (COSO, 2022). Z tohoto mezinárodně uznávaného rámce vychází při hodnocení vnitřního kontrolního systému i úřady v České republice, například národní kontrolní úřad nebo ministerstvo financí. I když prvotní využívání vnitřního kontrolního systému bylo zpočátku spojeno s oblastí financí, je nyní využití napříč oblastmi a procesy organizace. Jeden z průkopníků hodnocení vnitřního kontrolního systému je společnost Deloitte (Červený, 2012).

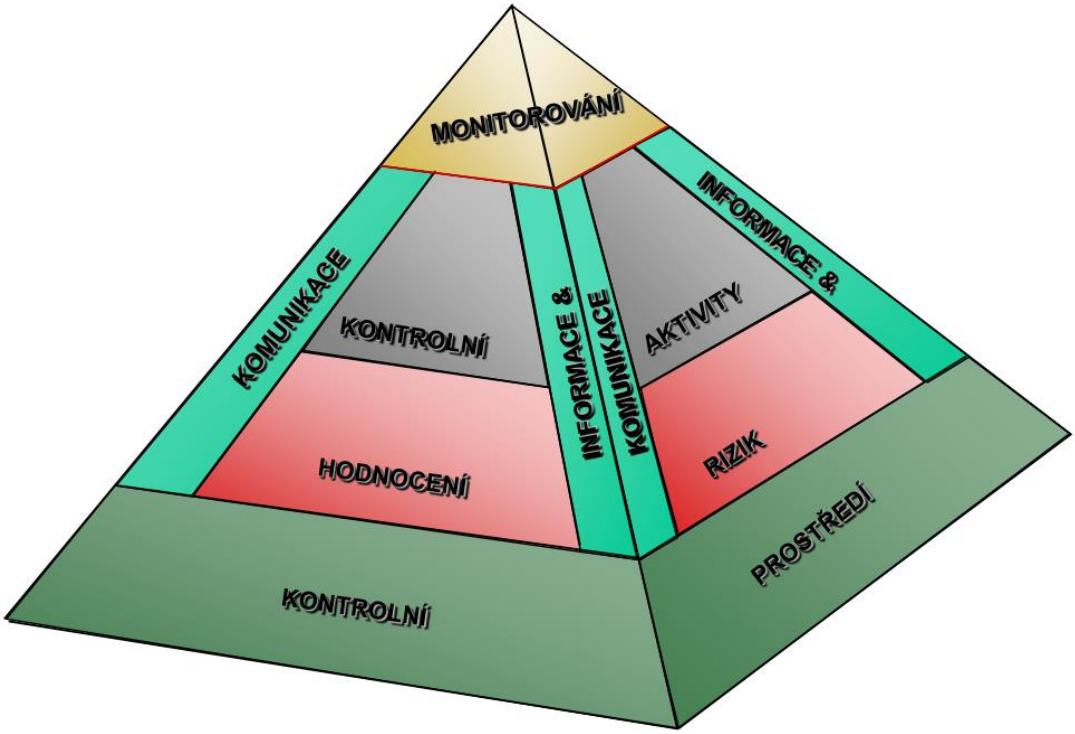
„Interní kontrolní systém je proces uskutečňovaný vedením společnosti a jinými pracovníky organizace, jehož cílem je poskytnout přiměřené ujištění o plnění cílů v následujících kategoriích:

- *efektivnost a účinnost operací,*
- *spolehlivost finančního výkaznictví,*
- *soulad s legislativou a ostatními platnými předpisy.“* (Kranecová, 2017)

Podle rámce COSO je vnitřní kontrolní systém složen z pěti komponent, a to kontrolního prostředí, hodnocení rizik, kontrolní činnosti, informací a komunikace a monitorování. Tyto oblasti jsou vzájemně provázány a tvoří jeden komplexní systém. Kontrolní prostředí stanovuje

vedení organizace zaváděním etických standardů, politik, pravidel a svým chováním, je to základní pilíř vnitřního kontrolního systému. Nad tímto základním rámcem je hodnocení rizik, které zahrnuje identifikaci a následně analýzu rizik, které mohou ohrožovat plnění cílů organizace, a to jak na úrovni organizace samotné, tak na úrovni jednotlivých aktivit. Na základě těchto rizik by mělo docházet ke kontrolní činnosti a regulacím s tím spojených tak, aby byla rizika řízena. Celým nastaveným vnitřním kontrolním systémem musí být nastavena komunikace, kde informace budou relevantní, správné, aktuální a dostupné včas na správném místě a pouze oprávněným příjemcům. Jako střecha pomyslné pyramidy je monitorování, které zajišťuje, že kontrolní činnosti jsou správně navrženy, efektivně prováděny a že dochází ke zlepšování vnitřního kontrolního systému. Grafická podoba tohoto mechanismu je zachycena v obrázku č. 6 - Vystavěný vnitřní kontrolní systém. (Červený, 2012)

Obrázek 6 - Vystavěný vnitřní kontrolní systém



Zdroj: Červený, 2012

Dle Mgr. Tomáše Pivoňky, ředitele Interního auditu ČEZ a.s., a prezidenta Českého institutu interních auditorů je vhodné, aby garantem vnitřního kontrolního systému byl interní audit společnosti a byl součástí corporate compliance dané společnosti. Vnitřní kontrolní systém pak zasahuje do činnosti celé společnosti. Dále navrhuje zlepšení systému COSO, kdy prosazuje jeho zjednodušení a přistupuje k jeho vyhodnocení na základě tří oblastí, a to hodnocení kontrolních mechanismů k souvisejícím rizikům pro části lidi,

procesy a nástroje. Auditní tým tak posuzuje lidský potenciál a jeho využití z pohledu kapacity zaměstnanců, jejich zastupitelnosti, znalostí, potřebné kompetence pro vykonávání přidělených úkolů, nebo integrity a loajality. Procesy se posuzují z pohledu toho, jak jsou popsány, definovány jejich kontroly, pravomoci a odpovědnosti. Jestli mají stanovenou strategii, identifikovaná a řízená rizika. To vše se srovnává s dobrou praxí ve zkoumaném procesu. Pro část nástrojů auditoři vyhodnocují adekvátnost, integritu a efektivnost, nebo vhodnost použitých prostředků a metod, či relevantnost a věrohodnost takových nástrojů. (Pivoňka a Kožíšková, 2014), (Pivoňka, 2017)

3.5 Audit

Dle výkladu národního úřadu pro kybernetickou bezpečnost je audit „*systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna.*“ (Jirásek a kolektiv, 2022). Jednou z možností dělení auditů je dle oblasti, do které audity spadají, například audity kybernetické, finanční, regulační, a další. Audit se dále může lišit i formou požadovaného cíle auditu, zde bychom mohli audit dělit například na certifikační, kde je cílem získání či udržení certifikátů vypovídajících o stavu společnosti, například ISO audity, či audit regulační, zkoumající naplnění požadavků zákona. Pro tuto bakalářskou práci bude zásadní definování procesu interního kybernetického auditu, prověřujícího informační a kybernetickou bezpečnost a shodu se zákonem a vyhláškou kybernetické bezpečnosti, u kterého je jasně citelný vliv dobré praxe v oblasti kybernetické a informační bezpečnosti, a to řady technických norem ISO 27k. (Přehledové blokové schéma k zákonu a jeho prováděcím předpisům, 2018)

3.5.1 Interní audit

Definice interního auditu dle Českého institutu interních auditorů zní: *„Interní audit je nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesů v organizaci. Interní audit pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy organizace.“* (Český institut interních auditorů, 2017) Oproti tomu v ISO 27001, je interní audit definován jako: „systematický, nezávislý a dokumentovaný proces získávání důkazů o auditu a jeho objektivního hodnocení s cílem stanovit rozsah, v němž jsou splněna kritéria auditu“ (ČSN ISO/IEC 27001, 2014). Z toho vyplývá, že u interních auditů dle Českého institutu interních auditorů má auditor možnost provádět v rámci auditů konzultační činnost.

Ta je u ISO auditů striktně zakázána. Vzhledem k tomu, že způsobů a organizací zastřešujících interní auditory je více, byl vytvořen Mezinárodní rámec profesní praxe interního auditora, který je využitelný v rámci kterékoli organizace a je pomůckou pro každého interního auditora. Tento rámec byl vydán společným úsilím organizací Českého institutu interních auditorů, z.s. a The Institute of Internal Auditors. (Český institut interních auditorů, 2017)

Pro účel této bakalářské práce, ve které bude návrh procesu IT auditu vytvářen, je zohledněno:

a) Vyhovění požadavkům Zákona kybernetické bezpečnosti a Vyhlášky o kybernetické bezpečnosti (kritérium je § 16):

kde povinná osoba v rámci auditu kybernetické bezpečnosti musí provádět a dokumentovat audit dodržování bezpečnostních a legislativních požadavků a jejich výsledky zohledňovat v plánu bezpečnostního povědomí a plánu zvládání rizik. Dále audit posuzuje soulad s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému. Nakonec musí stanovit nápravná opatření, aby auditovaný systém byl v souladu s těmito požadavky. (Zákon kybernetické bezpečnosti, 2018)

b) Standardy interních auditorů.

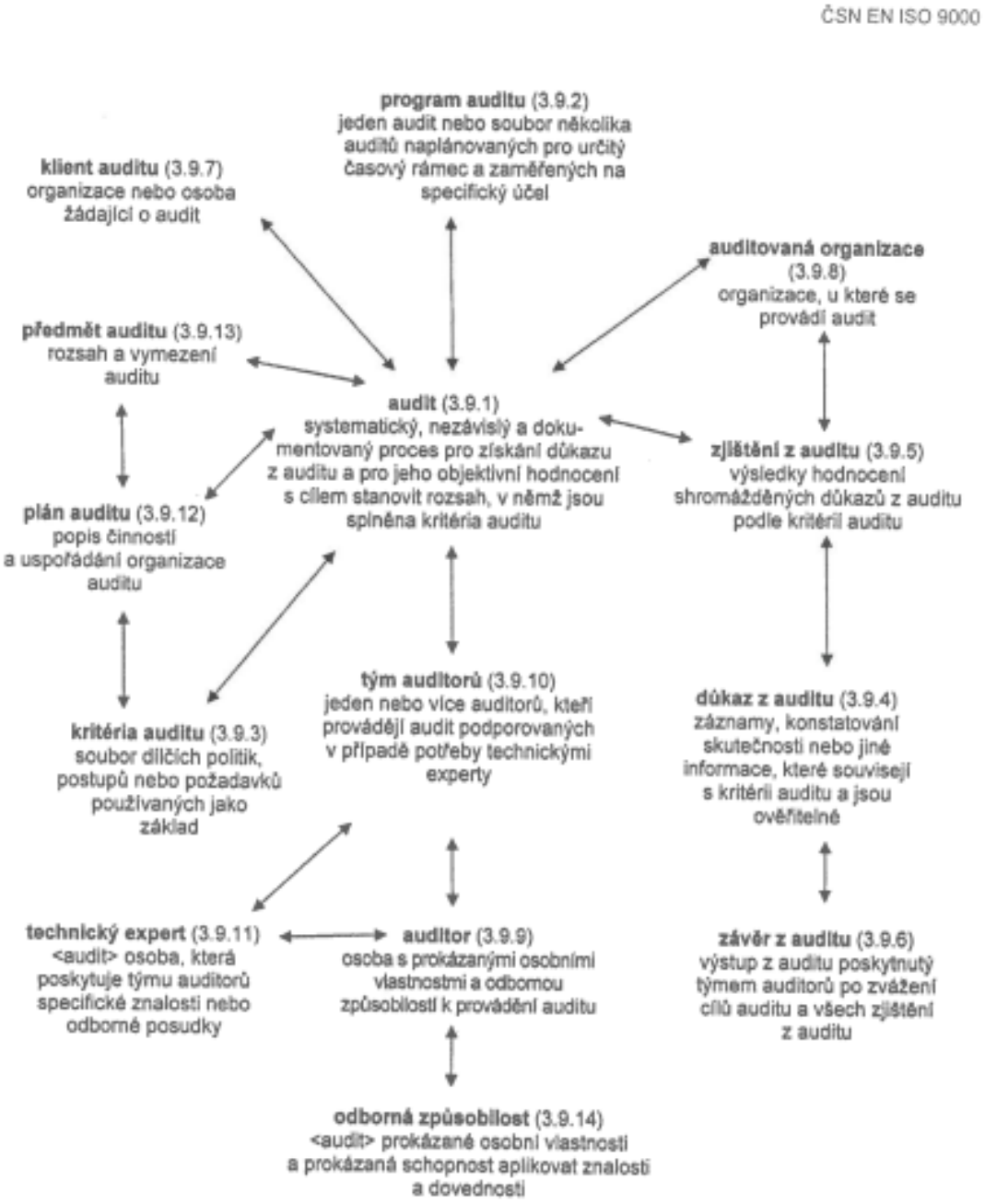
c) Normy ISO, ITIL, PCI DSS apod..

d) Smluvní požadavky společnosti, která by daný proces zaváděla.

3.5.2 Průběh auditu a základní pojmy

Na následujícím schématu z ČSN EN ISO 9000 vidíme v grafické podobě závislosti a průběh ISO auditu od jeho naplánování po ukončení.

Obrázek 7 - Základní pojmy a vazby na proces auditu ISO 9000



Zdroj: ČSN EN ISO 9000, 2016

3.5.3 Audit kybernetické bezpečnosti/ IT audit

Audit kybernetické bezpečnosti je definován v rámci Zákona o kybernetické bezpečnosti § 5, bod (2) písmeno m) Kontrola a audit (Zákon o kybernetické bezpečnosti, 2014) a dále v rámci § 16 Vyhlášky kybernetické bezpečnosti, kde je stanoveno:

„Povinná osoba v rámci auditu kybernetické bezpečnosti

a) provádí a dokumentuje audit dodržování bezpečnostní politiky, včetně přezkoumání technické shody, a výsledky auditu zohlední v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik a

b) posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu.“ (Vyhláška kybernetické bezpečnosti, 2018, § 16)

Dále je vyhláškou stanoveno, že bude audit prováděn v pravidelném intervalu 2 nebo 3 let podle druhu povinné osoby a při významných změnách. Dále vyhláška dává možnost vypracovat audit průběžně dle systematických celků, ale v takovém případě je nutné audit v celém rozsahu provést do 5 let (Vyhláška kybernetické bezpečnosti, 2018, § 16). Audit kybernetické bezpečnosti může provádět pouze osoba, která splňuje požadavky pro bezpečnostní roli auditora kybernetické bezpečnosti. Podle Aleny Rybákové, auditorky Národního úřadu pro kybernetickou bezpečnost, je možné provádět kybernetický audit podle normy ČSN ISO/IEC 27001:2014, a to z důvodu, že se principiálně neliší. Audit kybernetické bezpečnosti neboli kontrola kybernetické bezpečnosti se týká určených povinných osob a ze strany Národního úřadu pro kybernetickou bezpečnost může proběhnout po uplynutí přechodné lhůty jednoho roku po jejím určení (Rybáková, 2017).

3.5.4 Auditor kybernetické bezpečnosti

Role auditora kybernetické bezpečnosti je odpovědná za provádění auditu kybernetické bezpečnosti. Povinná osoba tuto roli, stejně jako například manažera kybernetické bezpečnosti, architekta, nebo garanta aktiv, musí určit a pověřit. Na tuto roli jsou dále kladeny další podmínky, a to že osoba musí být pověřena, vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací v minimální délce tří let, v případě že nemá vysokoškolské vzdělání, anebo jednoho roku, pokud toto vzdělání má. Povinná osoba musí dále zaručit, že provedení auditu bude nestranné a osoba provádějící audit není pověřena výkonem jiné bezpečnostní role. Tím se předchází střetu zájmů takového auditora. (Vyhláška kybernetické bezpečnosti, 2018, § 7)

Dle informací obsažených na webových stránkách Národního úřadu pro kybernetickou bezpečnost je to jedna z bezpečnostních rolí, kterou může subjekt určení řešit outsourcingem. V zákoně dále není určeno, jakými metodami nebo auditními nástroji má auditor audit vykonávat, a tudíž záleží na dobré praxi v této oblasti nebo na pravidlech zavedených ve společnosti povinné osoby. (FAQ, 2022).

3.6 Metoda Focus Group

Metoda Focus Group, neboli zaměřovaného rozhovoru soustředěných skupin, je kvalitativní metoda výzkumu. Metoda je přisuzována Robertu K. Mertonovi, který stanovil její základy ve 40. letech 20. století. Byla rozvíjena v různých částech sociální psychologie a vychází ze zaměřovaného interview. Tato metoda se soustředí na konkrétní soubor subjektivních zkušeností a situací, ze kterých tyto zkušenosti vychází. Soustředěný rozhovor, ze kterého metoda Focus Group vychází, je rozdělen na čtyři části. V rámci první části respondenti sdílejí konkrétní zkušenosti z předmětu analýzy. Ve druhé části má výzkumník k dispozici sadu hypotéz poskládaných na základě hypoteticky významných elementů a vzorců sociálních situací. Následně výzkumník vede na základě takových hypotéz rozhovor. V poslední čtvrté části je interview zaměřeno na zkušenosti dotazovaných. Výzkumník vyhodnocuje správnost připravených hypotéz a nepředvídatelné odpovědi, které tyto hypotézy mohou vyvrátit, případně zadat podnět k formulaci hypotéz nových (Toušek, 2007). Pro metodu Focus Group je dominantní role moderátora diskuse na zajištění skupinové interakce, předpokládá jeho dostatečnou znalost zkoumané oblasti. Doporučené rozmezí zkoumané skupiny je 6–10 osob, a to primárně z důvodu, že v případě větších skupin mají respondenti méně prostoru k vyjádření se k problematice. Dále má na kvalitu metody Focus Group vliv homogenita skupiny. Doporučený počet skupin v rámci výzkumu je 3–5, ale záleží na záměru daného výzkumu, nicméně primárně jde o kvalitu získaných dat (Šebek a Hoffmannová, 2010).

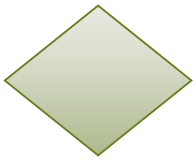
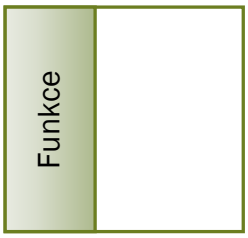
Silné stránky této metody jsou ve flexibilitě, se kterou může moderátor debaty přistupovat k připraveným otázkám a hypotézám na základě odezvy a odpovědí debatující skupiny. Metodou Focus group je možné dojít k posouzení zkoumané hypotézy z hlediska jednotlivých účastníků debaty, které by v rámci rozhovoru s jednotlivci nebyly rozkryty. Slabou stránkou této metody může být nedostatečně kvalitní moderátor debaty, který nedokáže debatu dostatečně usměrňovat a neomezovat její přínos. Je nutné, aby se účastníci aktivně zapojovali, ale přiměřeně dominantně, aby nedocházelo k odrazování ostatních debatujících. Tato metoda není vhodná, pokud by měla sloužit k získání statistických dat, které by nebyly ovlivňovány pocity a zkušenostmi účastníků debaty. (Sedláková, 2014)

3.7 Metoda BPMN

Pro grafické znázornění procesních diagramů existuje řada způsobů a metod a současně i řada podpůrných systémů, v rámci kterých lze strukturované diagramy tvořit. Pro tuto bakalářskou práci bude využita syntaxe BPMN (z anglického Business Process

Model and Notation), kterou rozvíjí organizace Business Process Management Initiative. Jedná se o syntaxí podporovanou řadou informačních systémů jako například MS Visio, nebo Enterprice Architekt. Grafické modely procesů se vyznačují jednoduše pochopitelnou syntaxí, díky které lze popisovat i složité procesy a systémy. Hlavní elementy, které budeme v rámci této práce využívat jsou uvedeny v tabulce č. 2 – Syntaxe BPMN. (Kanisová a Müller, 2006)

Tabulka 2- Syntaxe BPMN

	**Počáteční událost** – zahajuje řetěz úloh v rámci procesu		**Brány –** modelová rozhodnutí, řídí divergenci a konvergenci sekvenčního toku
	**Průběžná událost –** slouží k provázání procesních map mezi sebou		**Sekvenční tok –** vyjadřuje následnost procesních prvků
	**Koncová událost –** slouží k ukončení řetězu činností v procesní mapě		**Dráha zodpovědnosti -** reprezentuje účastníka / roli jemuž je svěřeno vykonávání předepsaných činností
	**Činnost –** reprezentují předepsanou činnost která má být vykonána v daném procesním kroku		

Zdroj: vlastní zpracování, inspirováno Kanosová a Müller, 2006

4 Vlastní práce

4.1 Výzkum v oblasti Focus Group

Nejprve jsem provedl analýzu dostupných informačních zdrojů, na které odkazuji v rámci literární rešerše. Dále jsem čerpal znalosti z certifikace ISMS ISO/IEC 27001 Lead Auditor a vykonávané praxe auditora kybernetické bezpečnosti mezi lety 2019–2022 ve společnosti ČEZ a.s. Na základě těchto podkladů jsem připravil návrh procesu IT kybernetických auditů, který sloužil jako podklad pro uskutečnění řízené diskuse podle metody Focus Group. Hlavním cílem řízené diskuse měla být optimalizace navrženého procesu IT kybernetického auditu. Dílčími cíli měly být profesní poznatky v rámci dané problematiky.

4.1.1 Příprava uskutečnění Focus Group

Pro výzkum a zhodnocení IT auditů metodou *Focus Group* v rámci praktické části jsem uskutečnil jeden řízený rozhovor. Na tento rozhovor jsem pozval 12 možných účastníků z profesní a akademické praxe kybernetické informační bezpečnosti, auditů kybernetické informační bezpečnosti a ISO auditů. Mezi respondenty nebyly žádné osobní nebo rodinné vztahy. V rámci přípravy jsem stanovil, že dle nastudované teorie musí dorazit na diskusi minimálně 6 osob, tzn. minimálně 50procentní účast pozvaných účastníků a minimálně 2ze4 oslovených rolí povinných ze Zákona o kybernetické bezpečnosti. Vedení debaty, a tedy roli moderátora jsem se rozhodl provádět já osobně.

Výzkum byl naplánován na 24. 11. 2022 od 19:00 v salónku v restauraci La casa Havana, Opatovická 28, Praha – Nové město. Z důvodu zajištění příjemné atmosféry bylo objednáno drobné pohoštění. Respondentům byl v rámci zaslané pozvánky předložen i návrh procesu IT auditů k prostudování. Pro danou diskusi byla pro každého účastníka připravena tištěná verze navrženého procesu, a propisovací tužka pro možnost zaznamenávání si poznámek. Diskuse byla zaznamenávána psanou formou zápisu, v rámci, kterého budou shrnuty výsledky diskuze na položené otázky. Zápis provedla osoba nezasahující do diskuse. Zápis je přiložen formou přílohy do této práce.

4.1.1.1 Hypotézy

Pro diskusi Focus Group jsem připravil základní hypotézy a otázky spadající pod tyto hypotézy, které v rámci připravované akce poskytly osnovu řízené diskuse.

Hypotéza 1: IT kybernetický audit má být sestaven z činností seskládaných dle Demingova PDCA cyklu.

Otázky: Jsou dle Vašeho názoru kybernetické IT audity něčím specifické, čím se liší od jiných auditních činností? Jaké činnosti je nutné vykonávat v části plánování interního auditu a jakou s nimi máte zkušenost, jakým způsobem je vykonáváte ve Vaší organizaci, či s jakým způsobem jste se setkali v rámci Vaší dosavadní praxe? Na jaké činnosti se zaměřoval kybernetický audit, když Vás kontroloval, na jaké činnosti se zaměřujete vy? Stalo se někdy, že Vás auditor kontroloval a došel k chybným závěrům? Můžete uvést příklad? Kdo na to přišel a jakým způsobem? Byly nějaké činnosti auditora podle Vás za hranou nebo nekorektní? Jakým způsobem Vám auditor dokazoval nálezy a závěry, které učinil? Zaměřoval se auditor na Vaše prováděné kontroly nebo spíše prověřoval Vaše činnosti? Prováděl to na vzorku nebo na celém spektru případů, které prověřoval? Jakým způsobem a v jakých termínech Vám auditor prověřil efektivitu nasazených nápravných opatření? Jakým způsobem? Jak je dle Vašeho názoru možné vyhodnotit vnitřní kontrolní systém v oblasti kybernetického auditu?

Hypotéza 2: Pro vykonání kybernetických auditů je možné vydefinovat potřebné role, které zaručí jeho kvalitní vykonání a současně i ujištění o jeho korektnosti.

Otázky: Jaké role v rámci vaší zkušenosti v interním auditu vystupovaly a jaké měly pravomoci a odpovědnosti? Chybělo nebo chybí vám v rámci auditních týmů zastoupení nějaké činnosti, které je dle vašeho názoru nezbytné pro naplnění cílů kybernetických auditů? Je auditor kybernetické bezpečnosti ve vaší společnosti zastoupen v rámci Výboru kybernetické bezpečnosti vaší společnosti? Vykonává daný auditor ještě jinou nežli auditní roli ve vaší organizaci?

Hypotéza 3: Existují kvantitativní metriky pro vyhodnocení kybernetických auditů, které budou vést k neustálému zlepšování procesu IT interních kybernetických auditů.

Otázky: Jaké činnosti v rámci kybernetických auditů se z vašeho pohledu dají kvantifikovat a mohly by sloužit pro vyhodnocení kvality daného procesu kybernetických auditů? Jakým způsobem u vás probíhá hodnocení realizovaného kybernetického auditu? Je možné a za vás přínosné provádět sebehodnocení po skončení auditu? Máte s tím zkušenost, jakou? V čem vidíte největší přínos kybernetických auditů?

Hypotéza 4: Zaslaný proces IT kybernetických auditů je beze změny aplikovatelný v rámci povinných osob ISZS dle ZKB.

Otázky: Na základě proběhlé debaty a materiálu, který vám byl poskytnut v rámci přípravy na tuto debatu, napadá vás něco, co daný proces nepopisuje, nebo je nedostatečně detailní? Chybí vám nějaké oblasti či role v daném procesu?

4.1.2 Vykonání diskuse Focus Group

Řízená diskuse proběhla 24. 11. 2022 od 19:00 v restauraci La casa Havana Opatovická 28, Praha – Nové město. Diskuse se zúčastnilo 9 z 12 pozvaných účastníků, což zajišťovalo 75procentní účast a následnou vypovídající hodnotu zaznamenaných odpovědí. Diskuse byla rozdělena do čtyř oddělených bloků, vymezených stanovenými hypotézami. Z důvodu zajištění příjemné atmosféry byly bloky odděleny pauzami s drobným občerstvením. Diskuse v rámci jednotlivých bloků byla dynamická a leckdy přesahovala i přes snahu moderátora nastolená témata. Z debaty vznikl zápis, který je přiložen v rámci přílohy č. 2. Během debaty vzhledem k časovým možnostem nebyly odpovězeny veškeré připravené otázky. Všichni přítomní souhlasili se zaznamenáváním formou zápisu z debaty a dohodli se na požadavku anonymizace osobních údajů daných účastníků, z důvodu zveřejňování této bakalářské práce. Tím se zajistilo to, že mohli účastníci mluvit bez obav ze zneužití jejich odpovědí proti vlastní osobě. Na konci debaty dostali respondenti možnost k rozhovoru mezi čtyřma očima v případě, že by chtěli provést i rozhovor mimo danou skupinu a tím pádem mimo využívanou metodu Focus Group. Tato možnost nebyla využita.

4.1.3 Vyhodnocení metody Focus Group

Z provedených rozhovorů jsem provedl shrnutí závěrů s konsensy pro úpravu navrhovaného procesu kybernetických auditů, a to v následujících oblastech:

1) Plán auditů je nutné rozšířit o možnost neplánovaných auditů a v rámci plánu musí být jasná periodicita vykonávání auditu, včetně rozvržení plánovaných kontrol, a to s možnostmi na 2 až 5 let dle požadavků vyhlášky kybernetické bezpečnosti,

2) V rámci procesu by se neměly vyskytovat neurčité a sporné termíny jako například přiměřeně, dostatečně atd.

3) V navrženém procesu je nutné vydefinovat i roli, která nemusí naplňovat požadavky kladené vyhláškou na auditora kybernetické informační bezpečnosti, ale její role musí být čistě kontrolní. Je nutné, aby byla znalá auditních postupů a požadavků auditních standardů,

ale nemusí být zběhlá v problematice kybernetické bezpečnosti a oblasti IT. Není nutné, aby tato role byla zastávána interním zaměstnancem.

4) V navrženém procesu není vhodné uvádět vedoucího auditovaného subjektu, protože tato role nemusí mít dostatečné pravomoci pro jednání za celý auditovaný útvar. Z toho důvodu bylo doporučeno uvádět osobu odpovědnou za auditovaný útvar.

5) Jako metriky úspěšnosti auditované oblasti bylo doporučeno nezařazovat počty zjištěných nápravných opatření, ale dosahování zlepšení vnitřního kontrolního systému, a to na základě například průměru provedených kontrol v oblastech lidí, procesů a nástrojů, s tím, že výkonnost musí být hodnocena na každém auditu. Z vícenásobného vyhodnocování auditů v definované periodě provádění plánovaných auditů, a i těch mimořádných neplánovaných, pak následně vyjde trend zlepšování nebo zhoršování daného procesu.

6) Proces interního auditu by měl být pro dané role, které v tomto procesu vystupují, jednoduše pochopitelný a aplikovatelný pro dané osoby. Z toho důvodu účastníci doporučili diskutovaný návrh dokumentu zjednodušit a doplnit ideálně procesními diagramy, tak aby se zaměstnanci v jednotlivých rolích dostatečně zorientovali v rámci připravovaného dokumentu.

7) Proces auditu by měl být průkazný, ale neměl by být zatížen zvýšenou byrokratickou činností a dokumentací, bez zjevného přínosu, proto by mělo dojít k sloučení zprávy o stavu informační a kybernetické bezpečnosti určeného ISZS, zprávy o činnosti auditu za hodnocené období a zprávy z vyhodnocení funkčnosti a efektivnosti řídicího a kontrolního systému do jednoho dokumentu.

8) V rámci návrhu by měl být kladen důraz na maximální digitalizaci procesu a výstupů z něj.

4.2 Proces interního IT auditu dle Zákona o kybernetické bezpečnosti

4.2.1 Základní ustanovení procesu interního IT auditu

Účelem tohoto dokumentu je stanovit proces interního IT auditu dle Zákona o kybernetické bezpečnosti (dále jen auditu), který bude respektovat poslání, nezávislost, odpovědnosti, pravomoci a postupy pro činnost auditu v rámci společnosti XXXX (dále jen „XXXX“ nebo společnosti).

4.2.1.1 Závaznost

Tento dokument se týká všech organizačních útvarů společnosti „XXXX“.

4.2.1.2 Účel a poslání auditu

Posláním auditu ve společnosti „XXXX“ je zvyšovat a chránit hodnotu společnosti tím, že poskytuje objektivně ujišťovací služby založené na vyhodnocení rizik, poskytuje poradenství ve věci dosažení souladu se Zákonem o kybernetické bezpečnosti pro povinné osoby a informační systémy základní služby. Toho je dosahováno zejména poskytováním nezávislé, objektivní ujišťovací a poradenské činnosti.

Audit má za cíl pomáhat vedení společnosti dosahovat stanovených cílů managementu společnosti a ujišťovat jí o stavu souladu se Zákonem o kybernetické bezpečnosti.

4.2.2 Role a odpovědnosti

Odpovědná osoba za audit

Pravomoci:

- vytvářet a předkládat rizikově zaměřený plán auditů s požadavky na zdroje, včetně jejich průběžných významných změn, k posouzení a schválení vedení společnosti „XXXX“;
- účastnit se porad vedení a představenstva společnosti „XXXX“
- přidělovat auditory kybernetické bezpečnosti na audity i mimo plán v případě identifikované potřeby posílení auditních týmů;
- nahlížet do auditních složek auditů z důvodu jejich kontroly;
- dávat zpětnou vazbu členům auditního týmu pro dosažení jeho zlepšování.

Odpovědnosti a povinnosti:

- respektovat a nenarušovat, pokud je to možné, plynulý výkon činností auditovaných subjektů;
- zabezpečit veškeré získané informace (materiály, soubory na médiích i vlastní dokumentaci) proti jejich zneužití nepovolanou osobou;
- zachovávat diskrétnost a mlčenlivost o všech skutečnostech zjištěných v průběhu své činnosti;
- neprodleně informovat vedení společnosti „XXXX“ o závažných zjištěných skutečnostech, které významným způsobem ovlivňují nebo mohou ovlivňovat činnost společnosti „XXXX“;
- zajišťovat zohlednění nových trendů a osvědčených postupů v oblasti interního auditu a kybernetické bezpečnosti;
- zavést a zajistit dodržování zásad a postupů určených k řízení činnosti auditu společnosti;

- vykonávat auditorské práce s náležitou profesní péčí, a přitom dodržovat vysokou úroveň chování a jednání v souladu s etickým kodexem interního auditora;
- pravidelně předávat vedení společnosti „XXXX“ zprávy o stavu informační kybernetické bezpečnosti a jejího souladu se zákonem o kybernetické informační bezpečnosti;
- nenarušovat nezávislost podřízených auditorů kybernetické bezpečnosti;
- neprodleně předávat informace související s informační a kybernetickou bezpečností z porady vedení společnosti na auditory kybernetické bezpečnosti;
- provádět pravidelnou kontrolu auditních složek auditu,
- zajistit soulad činnosti auditu s mezinárodními standardy pro profesní praxe interního auditu (dále jen standardy IA), s následujícími výjimkami:
    - pokud jsou standardy IA používány ve spojení s požadavky vydanými jinými odbornými organizacemi, nebo standardy a existují rozdíly mezi standard IA a ostatními použitými požadavky, pokud jsou jejich ustanovení přísnější než standardy IA,
    - pokud by standardy IA měli být v rozporu s požadavky Zákona o kybernetické bezpečnosti.

Auditor kybernetické bezpečnosti

Pravomoci:

je oprávněn za účelem plnění funkce kybernetického interního auditu:

- vyžadovat informace o veškerých skutečnostech souvisejících s ověřovanou činností a kontrolami;
- jednat se všemi zaměstnanci společnosti „XXXX“ bez ohledu na jejich pracovní pozici a postavení v úrovni řízení,
- jednat se všemi významnými i nevýznamnými dodavateli společnosti „XXXX“ a vyžadovat si jejich součinnost přes pověřené osoby definované v rámci smluvní dokumentace. V souladu s těmito pravidly, vstupovat na pracoviště v rámci celé společnosti „XXXX“ a nahlížet do písemných a elektronických podkladů, dokumentace, médií a informačních systémů;
- vyžadovat ústní nebo písemná vysvětlení k ověřované činnosti a ke zjištěným skutečnostem v případě potřeby vyžadovat informace a jejich doložení i od třetích osob;

- vyhotovovat fotokopie, audiozáznamy, videozáznamy, opisy, popřípadě výpisy z originálních dokladů a ze souborů uložených na elektronických a paměťových nosičích;
- mít přístup k výsledkům interních a externích kontrol;
- účastnit se všech důležitých jednání s externími orgány týkajících se řídícího a kontrolního systému společnosti „XXXX“, interního auditu a rizik vyplývajících z činnosti společnosti „XXXX“.

Odpovědnosti a povinnosti

- nesmí být pověřen výkonem jiných bezpečnostních rolí definovaných Zákonem o kybernetické bezpečnosti;
- nesmí postupovat tak, aby při činnosti a vztazích byla narušena jeho nezávislost a objektivita;
- nesmí řídit činnost ostatních zaměstnanců společnosti „XXXX“;
- nesmí nastavovat řídící a kontrolní systém společnosti „XXXX“;
- nesmí zavádět nebo se podílet na výkonu řídicích a kontrolních mechanismů, mimo těch, které se týkají auditních činností;
- nesmí hodnotit procesy, za které byl během předchozího roku odpovědný nebo na jejichž rozvoji či zavádění se podílel nebo za které je odpovědný.

Odpovědná osoba za auditovaný útvar

Pravomoci

- požádat odpovědnou osobu za audit o provedení neplánovaného (mimořádného) auditu;
- vyjádřit se k závěrečné zprávě kybernetického auditu;
- definovat nápravná opatření a odpovědné osoby pro jejich odstranění.

Odpovědnosti a povinnosti

- zajistit součinnosti auditovaného subjektu, odpovědných rolí a personálu při provádění kybernetického auditu;
- provádět činnosti pro odstranění a mitigace identifikovaných rizik a nedostatků;
- zajišťovat činnosti a provozování informačních systémů základní služby v souladu s platnou legislativou, řídící dokumentací a pravidly společnosti.

Vedení společnosti

Pravomoci

- připomínkovat střednědobý plán auditu a roční plán auditu,

- dostávat informace o změnách střednědobého a ročního plánu auditu;
- dostávat informace a ujištění o stavu auditované oblasti.

Odpovědnosti a povinnosti

- schválení střednědobého a ročního plánu auditů
- poskytnout součinnost v rámci připomínkování střednědobého a ročního plánu auditů
- rozhodnout o akceptaci auditem identifikovaných rizik, nebo schválení postupu odstranění formou nápravných opatření

Subjekt externího hodnocení procesu auditu

Pravomoci

- vyžadovat informace o veškerých skutečnostech souvisejících s procesem auditu;
- jednat se všemi zaměstnanci a členy vedení společnosti „XXXX“ bez ohledu na jejich pracovní pozici a postavení v úrovni řízení;
- jednat se všemi významnými i nevýznamnými dodavateli společnosti „XXXX“ a vyžadovat si jejich součinnost přes pověřené osoby definované v rámci smluvní dokumentace v rozsahu revidovaných auditních zakázek. V souladu s těmito pravidly, vstupovat na pracoviště v rámci celé společnosti „XXXX“ a nahlížet do podkladů, dokumentace, médií a informačních systémů;
- vyžadovat ústní nebo písemná vysvětlení k ověřované činnosti a kontrol ke zjištěným skutečnostem a v případě potřeby vyžadovat informace i od třetích osob a jejich doložení;
- vyhotovovat fotokopie, audiozáznamy, videozáznamy, opisy, popřípadě výpisy z originálních dokladů a ze souborů uložených na elektronických a paměťových nosičích;
- mít přístup k práci a výstupům ostatních interních a externích kontrol.

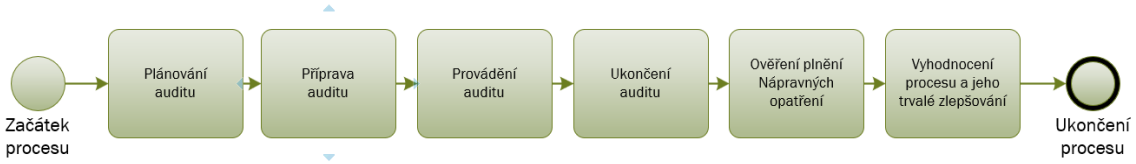
Odpovědnosti a povinnosti;

- nesmí být pověřen výkonem jiných bezpečnostních rolí definovaných zákonem o kybernetické bezpečnosti;
- nesmí postupovat tak, aby při činnosti a vztazích byla narušena jeho nezávislost a objektivita;
- nesmí řídit činnost ostatních zaměstnanců společnosti „XXXX“;
- nesmí nastavovat řídící a ani kontrolní systém společnosti „XXXX“;

- nesmí zavádět nebo se podílet na výkonu řídicích a kontrolních mechanismů, mimo těch, které se týkají auditních činností;
- nesmí hodnotit procesy, za které byl během předchozího roku odpovědný nebo na jejichž rozvoji či zavádění se podílel nebo za které je odpovědný.
- musí postupovat v souladu s dobrou praxí v oblasti auditů a v souladu s mezinárodními standardy interních auditorů.

4.2.3 Proces auditu

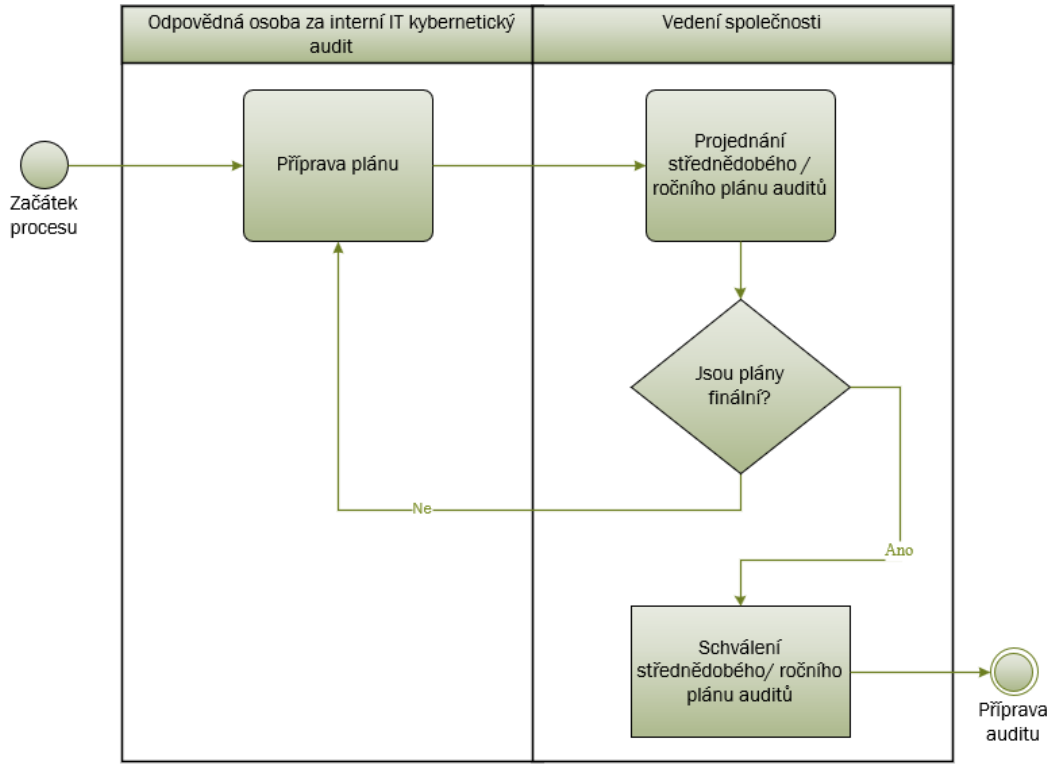
Obrázek 8 - Schéma procesu IT kybernetických auditů



Zdroj: vlastní zpracování

4.2.3.1 Plánování auditu – Plan

Obrázek 9 - procesní krok plánování IT kybernetických auditů



Zdroj: vlastní zpracování

Cílem plánování auditu je stanovit pro určité časové období úkoly auditu zejména na základě vyhodnocení významných rizik při dosahování cílů společnosti „XXXX“.

Příprava auditního plánu

Při přípravě auditního plánu se vychází zejména z:

- cílů, úkolů, strategických záměrů, ukončených významných změn na prvcích ISZS;
- analýzy rizik činností společnosti „XXXX“;
- legislativních požadavků zákona o kybernetické bezpečnosti a souvisejících předpisů;
- výsledků externích kontrol;
- požadavků regulatorních orgánů;
- výsledků již proběhlých auditů na prvcích ISZS,
- analýzy dalších zdrojů informací.

Odpovědná osoba za audit sestavuje každoročně plán auditu obsahující střednědobý plán auditu a roční plán auditu.

Střednědobý plán činnosti auditu je sestavován na období 2 nebo 5 let tak aby pokryl všechny zásadní činnosti a procesy společnosti „XXXX“, související se Zákonem o kybernetické bezpečnosti. Střednědobý plán je každý rok aktualizován. V případě 5letého období je nutné provést auditní činnosti po ucelených logických a odůvodněných celcích, tak, aby došlo k auditu celého určeného informačního systému základní služby a systému bezpečnosti organizace.

Roční plán auditních zakázek navazuje na plán střednědobý. Upřesňuje rozsah, věcné zaměření auditu, jeho cíle, časové rozvržení, personální zajištění a významné změny ukončené v roce předchozím auditním období. Musí být sestaven v roce, který předchází roku, na nějž je sestavován.

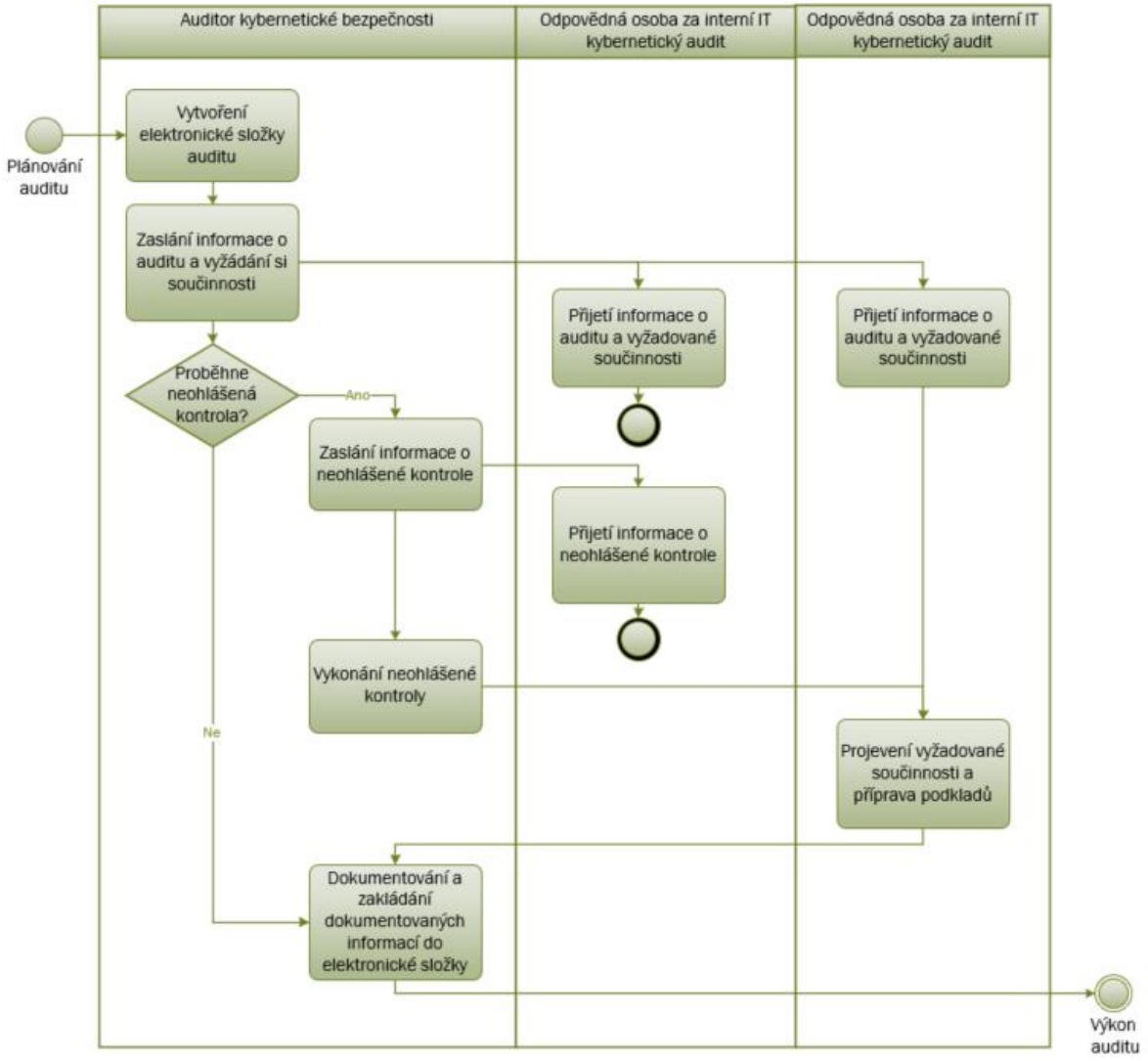
Projednání a schválení plánu auditů

Návrh plánu auditu, včetně analýzy rizik, je předložen na projednání a odsouhlasení vedení společnosti „XXXX“. Důvody případných změn plánu auditu nebo odlišné názory na analýzu rizik jsou zdokumentovány.

Dle vývoje situace ve společnosti „XXXX“, identifikovaných a odstraněných slabin určených prvků informačních systémů základních služeb, dokončených významných změn lze formou neplánovaných auditů roční plán auditních zakázek přehodnotit v průběhu roku. Změnu ročního plánu kybernetických auditů schvaluje vedení společnosti.

4.2.3.2 Příprava auditu

Obrázek 10 - Procesní krok příprava auditu



Zdroj: vlastní zpracování

Audit před zahájením auditu shromáždí a prostuduje potřebné podkladové materiály (např. aktuální znění Zákona o kybernetické bezpečnosti a prováděcích předpisů, další související zákony, regulatorní požadavky, vnitřní předpisy a řídící dokumentaci, zprávy regulátorů a externích auditorů, předchozí zprávy auditu, doporučení auditu pro danou oblast, odpovídající vstupy z mapy aktiv a mapy rizik, reporting pro vedení společnosti „XXXX“ apod.) Součástí individuální přípravy na provedení auditu může být i předběžná prohlídka auditované lokality na základě předchozího informování auditovaného útvaru.

Před zahájením plánovaného auditu jsou na auditovaný subjekt (Odpovědnou osobu za auditovaný útvar) a v kopii na odpovědnou osobu za audit zaslány elektronickou formou informace o termínu auditu, jeho zaměření, základní informace oficiálním emailem o složení

auditorského týmu a seznam podkladů, které auditor požaduje připravit ke dni zahájení auditu. Dále je v oficiálním emailu zaslána informace, že v odůvodněných případech má audit právo provádět předem neohlášené kontroly v místě výkonu auditu. Na tyto audity se nevztahuje povinnost předchozího informování auditovaného subjektu. O těchto případech musí být v podobě dokladovatelné informace uvědomena osoba odpovědná za interní IT kybernetický audit.

Oficiální email slouží zároveň jako písemné oprávnění uvedených auditorů k výkonu auditu.

Veškerá dokumentace a podklady pořízené auditorem jsou ukládány do elektronické složky daného auditu. Do složky auditu (tzv. auditního spisu) jsou průběžně zakládány tyto povinné dokumenty:

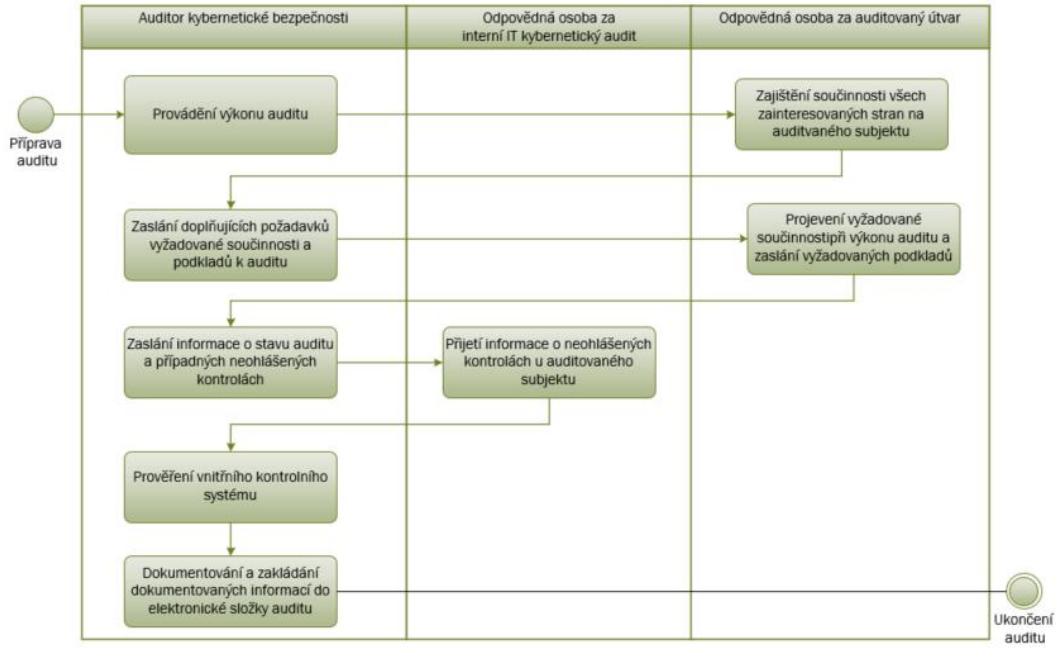
- oznámení o zahájení auditu;
- plán realizace auditu;
- pracovní výkaz auditora (Audit tracking log, dále také jako „ATL“) včetně podkladové dokumentace ke zjištěním;
- zpráva interního auditu (včetně korespondence);
- záznam z projednání výsledků auditu;
- záznam z ověření plnění nápravných opatření (včetně podkladové dokumentace).

Auditor kybernetické bezpečnosti má v této fázi auditu za úkol nastudovat auditovanou oblast a platné interní a externí předpisy, směrnice, mezinárodní standardy ISO apod. a pochopit zařazení auditovaného subjektu / oddělení / pracovníků a jejich pravomocí.

Dále musí stanovit jasné zadání a hypotézy či hlavní rizika auditované oblasti a také pečlivě rozplánovat celkový harmonogram průběhu auditu, včetně termínů zahájení a ukončení auditu.

4.2.3.3 Výkon auditu - Do

Obrázek 11 - Procesní krok výkon auditu



Zdroj: vlastní zpracování

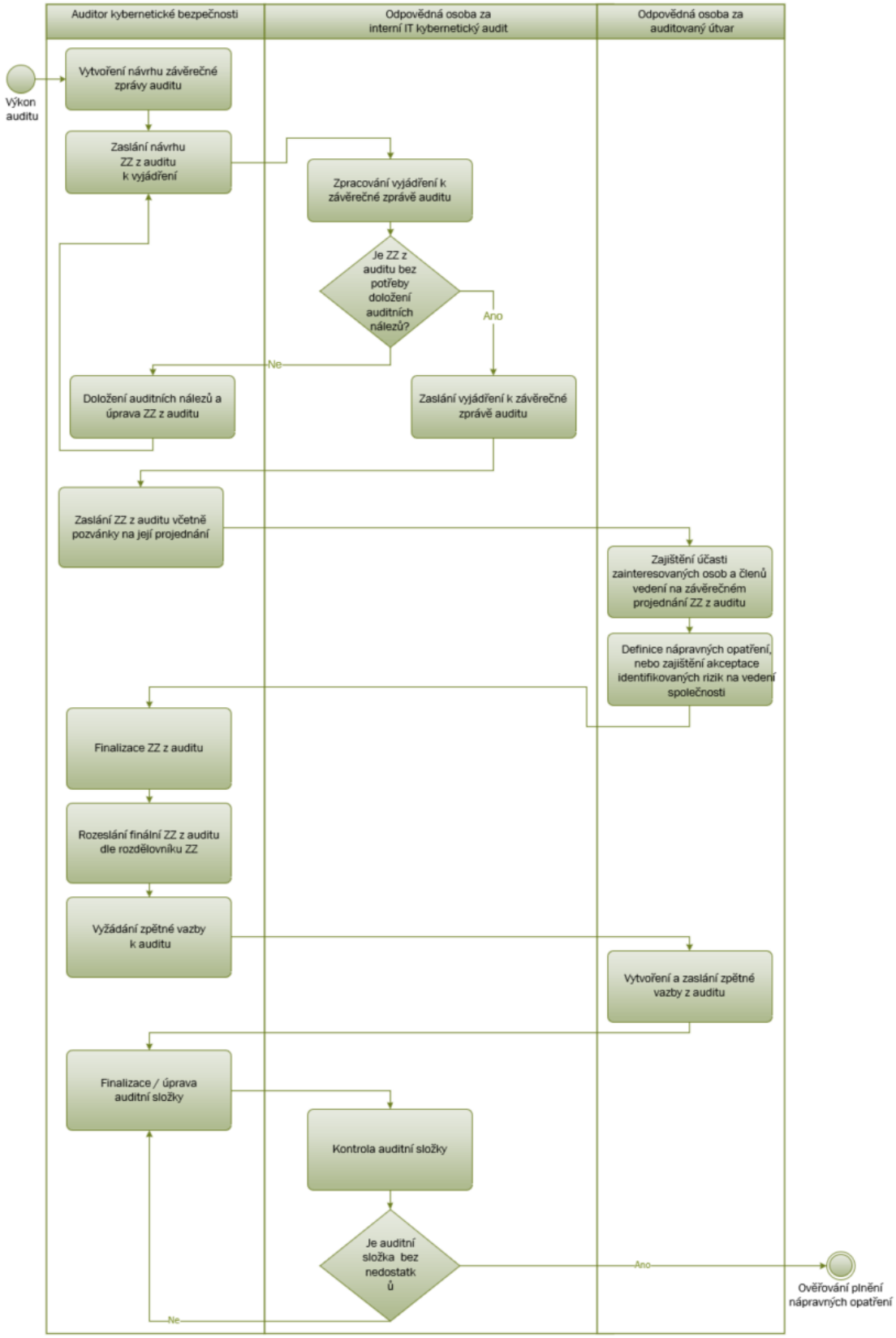
Audit je prováděn v souladu se standardními auditorskými postupy (Standardy IA) a dle vytvořeného plánu auditu.

Cílem auditních činností v této fázi auditu je získat dostatečnou auditní dokumentaci, která by umožnila kvalifikovaně posoudit auditovanou oblast a formulovat případná auditní doporučení ke zjištěným nesrovnalostem.

Prověření bezpečnostních požadavků informační kybernetické bezpečnosti je prováděno na základě kontrol definovaných vyhláškou kybernetické bezpečnosti v souladu s plánem auditu. Auditor zváží na základě prováděných pravidelných kontrol systému, zda bude provádět kontrolu systému samotného, nebo efektivnost vydefinovaných, prováděných a dokumentovaných kontrol. Vyhodnocení těchto kontrol jsou provedena principem ověření funkčnosti vnitřního kontrolního systému, a to v oblastech lidí, procesů a nástrojů. Funkčnost vnitřního kontrolního systému probíhá na 3 kontrolách za každou oblast. Auditor má právo provádět kontroly jak za pomocí sebou připravených materiálů a podkladů, tak pomocných materiálů distribuovaných Národním úřadem pro kybernetickou bezpečnost. V případě provádění neohlášených kontrol na straně auditovaného je auditor kybernetické bezpečnosti povinen před provedenou kontrolou informovat odpovědnou osobu audit. Při kontrolách (jak fyzických, tak elektronických) musí auditor kybernetické bezpečnosti postupovat neinvazivně. Odpovědná osoba za auditovaný útvar zajistí součinnost všech zainteresovaných stran a zaměstnanců.

4.2.3.4 Ukončení auditu

Obrázek 12 - Procesní krok ukončení auditu, dílo autora



Zdroj: vlastní zpracování

Po ukončení auditních prací zpracuje auditor kybernetické bezpečnosti návrh závěrečné zprávy auditu (dále jen „ZZ“), která obsahuje cíl a rozsah auditu, příslušné závěry, zjištěné rozpory s definovaným systémem řízení a požadavky Vyhlášky a Zákona o kybernetické bezpečnosti a doporučení k jejich odstranění. Dále jsou zde uvedeny kontroly v oblastech lidí, procesů a nástrojů tak, aby mohlo dojít k odečtení trendu zlepšování či zhoršování efektivnosti nastavených technických a organizačních bezpečnostních opatření (minimálně 3 kontroly za každou oblast).

Návrh ZZ odešle auditor odpovědné osobě za audit k vyjádření. Odpovědná osoba za audit se může k návrhu ZZ do 5 pracovních dnů vyjádřit, případně zaslat požadavek (požadavky) na doložení identifikovaných nálezů. Následně je návrh ZZ zaslán na odpovědnou osobu za auditovaný subjekt k připomínkám a definici nápravných opatření k identifikovaným nálezům do pěti pracovních dnů. Po posouzení objektivnosti připomínek auditovaného útvaru vypracuje interní audit konečné znění ZZ.

Konečné znění ZZ je následně zasláno, současně s pozvánkou k závěrečnému projednání, odpovědné osobě za auditovaný útvar. O způsobu projednání rozhoduje auditor kybernetické bezpečnosti.

Audit je ukončen projednáním konečného znění ZZ s odpovědnou (odpovědnými) osobou (osobami) auditovaného (auditovaných) útvaru (útvarů), členem vedení zastřešujícím danou auditovanou oblast a vyjádřením odpovědných vedoucích pracovníků k auditním doporučením (akceptace rizika vedením společnosti „XXXX“ nebo přijetí nápravných opatření).

Přijatá opatření musí být vždy konkrétní, jednoznačná, dokladovatelná, termínovaná (konkrétní datum) a s uvedením odpovědnosti za jejich plnění na osobu s dostatečnými pravomocemi a odpovědnostmi. Opatření formuluje auditovaný útvar na základě doporučení auditu a musí být promítnuta do prohlášení aplikovatelnosti společnosti a následně do implementačního plánu na další rok případně období. Odstraněné nedostatky musí být součástí přezkumu auditorem a následně přezkumu následného auditu auditované oblasti.

Ze závěrečného projednání ZZ se vyhotovuje záznam, který tvoří součást finálního znění zprávy kybernetické informační bezpečnosti. Výsledkem závěrečného projednání musí být akceptace konečného znění zprávy nebo dohoda o způsobu vyřešení rozporů.

Audit zašle naskenovanou kopii konečného znění zprávy (vč. záznamu z projednání) příslušným stranám podle kontaktní matice, která je uvedena ve zprávě. Společně se zprávou zasílá auditor kybernetické bezpečnosti na odpovědnou osobu za auditovaný útvar požadavek

na zpětnou vazbu spokojenosti s ukončeným auditem s důrazem na identifikované nedostatky činnosti auditora a jeho postupů.

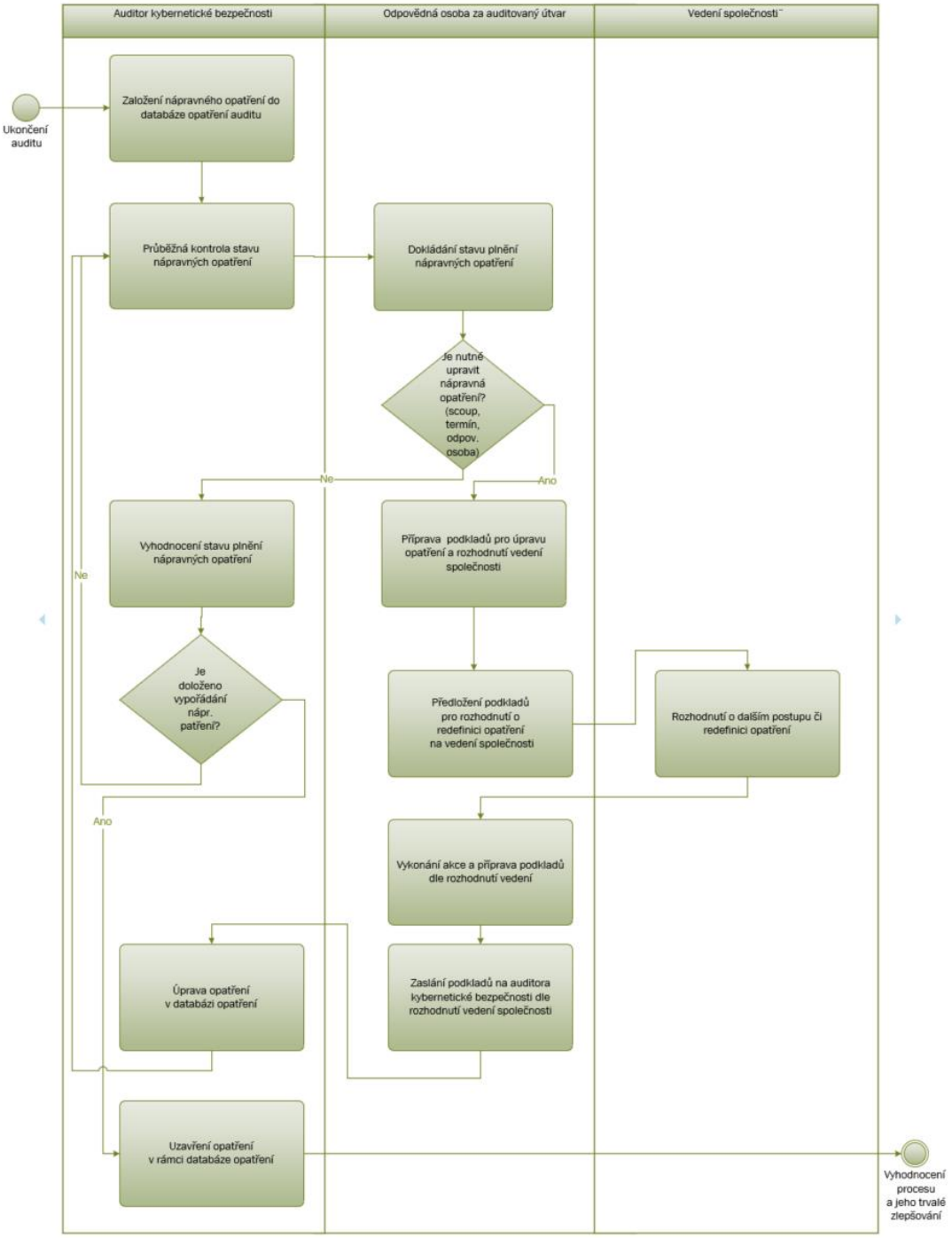
Odpovědná osoba za auditovaný útvar dodá zpětnou vazbu z auditu do 2 dnů po obdržení požadavku zpět na auditora kybernetické bezpečnosti.

Jednotlivá nápravná opatření k auditním doporučením jsou předmětem následné kontroly ze strany auditu formou průběžného ověřování jejich plnění s pravidelným hlášením o celkovém stavu pro vedení společnosti „XXXX“.

Po vydání závěrečné zprávy z auditu provede odpovědná osoba za interní audit kontrolu úplnosti auditní složky a v případě nedostatků auditní složky jej vrátí k dopracování auditoru kybernetické bezpečnosti.

4.2.3.5 Ověřování plnění nápravných opatření - Check

Obrázek 13 - Procesní krok ověřování plnění nápravných opatření



Zdroj: vlastní zpracování

Ověřování plnění nápravných opatření poskytuje zpětnou vazbu k ujištění o snížení rizik, odstranění nedostatků nebo zlepšení procesů, činností či kontrolních mechanismů. Informace o plnění nápravných opatření je součástí ročního plánu.

4.2.3.6 Evidence nápravných opatření

Audit vede databázi opatření. Databáze obsahuje popis nálezů a přijatých opatření, odpovědné osoby za implementaci, termíny realizace, status plnění opatření a po jejich odstranění i dokumentovatelné doklady o odstranění.

Podmínkou pro zařazení opatření do evidence je, aby opatření bylo:

- konkrétní;
- jednoznačné;
- termínované;
- dokladovatelné;
- aktuální (s ohledem na určený termín plnění);
- s určenou jednoznačnou odpovědností za implementaci.

Kontrolu úplnosti formálních náležitostí pro jednotlivá opatření provádí auditor kybernetické bezpečnosti před zařazením do evidence přijatých opatření.

Ověřování plnění jednotlivých opatření provádí auditor kybernetické bezpečnosti průběžně a vytváří samostatný záznam z ověření plnění opatření.

Ověřují se veškerá opatření, jejichž termín plnění nastal.

Projednání výsledku ověření plnění opatření probíhá elektronicky, zasláním záznamu k vyjádření odpovědné osobě za opatření.

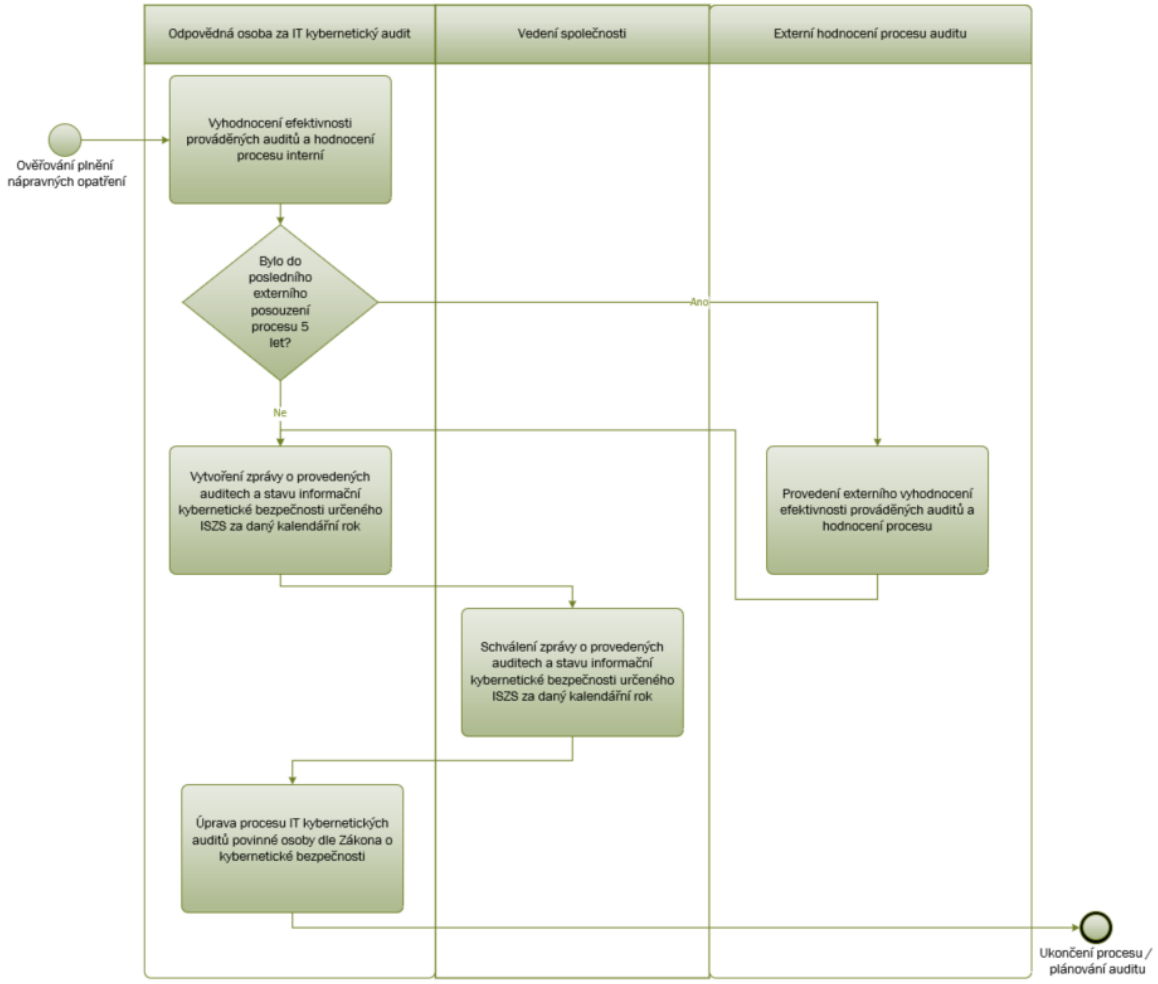
V případě, že nápravná opatření z důvodu změny technologie, nebo jiných odůvodněných případech pozbyla platnosti, nebo je nutné změnit jejich termín, předkládá odpovědná osoba za auditovaný útvar požadavek na vedení společnosti, které rozhoduje o dalším postupu, tak aby byla mitigována rizika z nálezů auditu. V případě nedostatků týkajících se zákonných požadavků subjektu ISZS, zajistí Odpovědná osoba za auditovaný útvar ve spolupráci s odpovědnými rolemi dle Zákona o kybernetické bezpečnosti analýzu rizik a další standardní kroky v naplňování legislativních, jakožto zanesení do prohlášení o aplikovatelnosti daného stavu a promítnutí do implementačního plánu společnosti. Dokumentované informace předkládá vedení společnosti a auditoru kybernetické bezpečnosti k založení do auditního elektronického spisu.

Auditor kybernetické bezpečnosti na základě předložených dokumentovaných informací upravuje nebo uzavírá záznam v rámci databáze opatření a dokládá kroky dokumentovanými informacemi.

4.2.3.7 Vyhodnocení procesu auditu a jeho trvalé zlepšování - Act

Odpovědná osoba za audit připravuje jednou za kalendářní rok souhrnnou zprávu o provedených auditech a stavu informační kybernetické bezpečnosti určeného ISZS za daný kalendářní rok.

Obrázek 14 - Procesní krok vyhodnocení procesu a jeho trvalé zlepšování



Zdroj: vlastní zpracování

Zpráva o provedených auditech a stavu informační kybernetické bezpečnosti určeného ISZS za daný kalendářní rok

Dokument obsahující závěrečné výsledky auditních akcí (podle ročního plánu auditů) včetně přijatých opatření. Dále informuje vedení společnosti o:

- nezávislosti funkce auditu;
- plánu auditů a jeho plnění současného období;
- výsledcích auditních činností;
- souladu s etickým kodexem a se standardy IA;

- odpovědi vedení společnosti na identifikovaná rizika;
- souhrnu identifikovaných nesouladů se Zákonem o kybernetické bezpečnosti;
- plánu kybernetických auditů se stanovenými cíli na nadcházející rok dle střednědobého plánu auditů;
- návrhy na změnu střednědobého plánu auditů;
- soupis auditovaných významných změn ukončených v rámci auditovaného období;
- kybernetický audit dále vyhodnocuje stav vnitřního kontrolního systému, a to na základě průměru provedených kontrol v oblastech lidí, procesů a nástrojů a srovnává ho s předešlými roky. První rok po zavedení tohoto procesu jen informuje o stavu vnitřního kontrolního systému;
- informuje o hodnocení odpovědných osob za auditované útvary;
- obsahuje informace pro úpravu procesu auditu z důvodu neustálého zlepšování.

Odpovědná osoba za audit vytváří, aktualizuje a provádí průběžné sledování efektivnosti způsobu vykonání auditů v roční periodě. Interní hodnocení procesu provádí formou sebehodnocení a o jeho výsledcích informuje vedení společnosti „XXXX“ součástí Zprávy o provedených auditech a stavu informační kybernetické bezpečnosti určeného ISZS za daný kalendářní rok.

V souladu se standardy IA jsou prováděna externí hodnocení procesu jednou za pět let, a to odborně způsobilým a nezávislým externím hodnotitelem, jehož výstup podléhá schválení vedení společnosti „XXXX“. Nálezy, které jsou externím hodnotitelem identifikovány, budou v souladu s tímto procesem evidovány, analyzovány a odstraněny. Následně jsou externím hodnotitelem vyhodnocovány.

Na základě výsledků z hodnocení odpovědných osob za auditované útvary, hodnocení odpovědné osoby za audit, výsledků hodnocení vnitřního kontrolního systému, podnětů ze strany vedení společnosti a externích hodnocení procesu a kontrol regulátorů, provádí osoba odpovědná za audit úpravy procesu auditů. Tím je dosahováno neustálého zlepšování definovaného procesu.

5 Výsledky a diskuse

V rámci bakalářské práce jsem navrhl procesu IT interního auditu pro společnost s určenými informačními systémy základní služby. Nejprve jsem navrhl proces na základě analýzy a teoretického bádání v rámci dostupných materiálů. Takto navržený proces jsem dále zkoumal na základě organizované diskuse se specialisty v oboru kybernetické informační bezpečnosti metodou Focus Group. Oproti nastudovaným autorům se v rámci praktické části a konfrontaci procesu ukázalo, že praktická funkčnost v běžném životě společnosti může být přínosnější, nežli zaznamenání veškerých legislativních požadavků a složitosti povinností. Z debaty s odborníky v této oblasti vyplývá, že v takovém případě jsou dokumenty, které v sobě nesou veškeré povinnosti a poznatky dané oblasti, velice rozsáhlé a v běžném prostředí společnosti leckdy nevyužitelné. I z toho důvodu jsem v rámci praktické části a v definici procesu na základě těchto poznatků proces zjednodušil a doplnil o grafické znázornění procesu metodou BPMN. Navrhl jsem samostatný proces tak, aby byl transparentní a dokumentovatelný. Proces je zaznamenán ve formě řídícího dokumentu, který může společnost implementovat do své předpisové základny. Následně zaměstnance účastnící se daného procesu s řídícím dokumentem prokazatelně seznámit. Dokumenty popisující proces ve společnosti často slouží i jako vzorová příručka pro daného zaměstnance, který v určité roli v procesu vystupuje. Proto musí být popis procesu dostatečně návodný a musí srozumitelně udávat pravomoci a odpovědnosti rolí, které v takovém procesu vystupují. Dále jsem došel k závěru, že není nutné jednotlivé fáze procesu rozpracovávat do činností mikro managementu a je vhodné dávat zaměstnancům dostatečně volné ruce při naplňování požadovaných cílů. Nicméně, netýká se to formy vyžadovaných závěrů takových činností. V rámci závěru tvorby práce jsem proces návrhu provádění auditů konzultoval se dvěma společnostmi, které s největší pravděpodobností spadnou do regulace infomační kybernetické bezpečnosti při zavedení směrnice NIS 2 do české legislativy. Obě společnosti se vyjádřily kladně a uvažovaly by v takovém případě o začlenění definovaného procesu do svého systému interních předpisů a postupů. Stojím si za tím, že v případě kontroly ze strany Národního úřadu kybernetické informační bezpečnosti (NÚKIB) by daná kontrola neshledala v procesu IT interních auditů neshodu se zákonem (aktuálně platným, tj. 181/2014 Sb.), avšak mohla by případně identifikovat místa ke zlepšení, což by bylo v souladu s demingovým PDCA cyklem, na což je daný proces připraven. Zvolený způsob analýzy vhodnosti navržených postupů pomocí metody Focus Group považuji za velice přínosný a za výbornou zkušenost pro svou další profesní praxi. Je ovšem nutné přemýšlet o tom, zda by stejných poznatků bylo dosaženo,

pokud by nad rámec přiděleného časového limitu pro zpracování této bakalářské práce bylo skupin více, což by bylo v souladu s nastudovanými doporučeními, či v případě, že by se řízených rozhovorů účastnili i jiní odborníci z dané praxe, například zaměření méně na praktickou stránku výkonu kybernetické bezpečnosti a auditních kontrol, ale spíše na stránku teoretickou či akademickou. Z tohoto důvodu považuji toto téma dostatečně nosné pro další možné zkoumání. Pro případnou diplomovou práci bych uvažoval o nasazení daného procesu a bezpečnostních kontrol do regulované společnosti a provedení auditů dle tohoto procesu a následně vyhodnocení a úpravu na základě vyhodnocení jeho přínosů a nedostatků.

Lze konstatovat, že i další dílčí stanovené cíle byly naplněny. V oblasti navržení kontrol organizačních a bezpečnostních opatření není jak ve zkoumaných zdrojích, tak ani mezi respondenty shoda na tom, jakou formou by kontroly měly probíhat. Z tohoto důvodu, dále z komplexnosti navrženého procesu a nezávislosti auditora kybernetické bezpečnosti jsou kontroly v souladu se standardy interního auditu plně v kompetencích auditora, který je stanovuje ve fázi přípravy auditu a následně při výkonu auditu kontroly provádí. Jako pomůcku může využít pomocné materiály od Národního úřadu pro kybernetickou a informační bezpečnost. I přes relativní volnost v nastavení kontrol, došlo k definování rámců, dle kterých auditor kybernetické bezpečnosti musí postupovat.

6 Závěr

Cíl práce, tj. navržení procesu IT interního auditu pro společnost s určenými informačními systémy základní služby dle Zákona o kybernetické bezpečnosti, a i ostatní dílčí cíle, tzn. vydefinování potřebných rolí, jejich pravomocí, povinností a odpovědností, navržení způsobu prověření bezpečnostních požadavků informační kybernetické bezpečnosti, definovaných Vyhláškou kybernetické bezpečnosti a vydefinování ukazatelů procesu pro zajištění PDCA cyklu, zlepšování navrženého procesu IT interních auditů, byly splněny. Vytvořením a nastavením procesu interních IT auditů byl definován univerzální rámec pro začlenění tohoto procesu do společností s určenými prvky informačních systémů základní služby tak, aby jej zákonem regulované společnosti vykonávaly v souladu s požadavky Zákona o kybernetické informační bezpečnosti.

7 Seznam použitých zdrojů

[1] CARTLIDGE, Alison a kolektiv. itSMF The IT Service Management Forum: Úvodní přehled ITIL ® V3, itSMF Czech Republic, o.s. a Hewlett-Packard, s.r.o., ISBN 0-9551245-8-1, Praha 2007.

[2] CUŘÍN, Jan. TAYLORCOX S.R.O. ISMS Lead Auditor: Školící materiály [školící materiál]. 2019. taylorcox Institute U.K., Verze 2015.1.

[3] ČERVENÝ, Vlastimil. Vnitřní kontrolní systém a jeho audit: 7. setkání auditorů průmyslu. Praha: Deloitte Touche Tohmatsu, 2012, 27 s. Dostupné také z: www.interniaudit.cz/download/sekce/prumysl/VRKS_a_jeho_audit_100512.pdf

[4] ČESKO. zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 6. 8. 2022. In: Zákony pro lidi.cz . © AION CS 2010-2023. Dostupné z: www.zakonyprolidi.cz/cs/2014-181

[5] ČESKO. vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) - znění od 28. 5. 2018. In: Zákony pro lidi.cz. © AION CS 2010-2023 Dostupné z: www.zakonyprolidi.cz/cs/2018-82

[6] ČESKO. vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby – znění od 1. 1. 2021. In: Zákony pro lidi.cz © AION CS 2010-2022. Dostupné z: www.zakonyprolidi.cz/cs/2017-437

[7] ČSN EN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak

[8] ČSN EN ISO 9001: Systémy managementu kvality – Požadavky. Páté vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016, 48 s. Třídící znak 010321

[9] ČSN EN ISO 9000. Systémy managementu kvality - Základní principy a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016, 79 s. Třídící znak 010300

[10] GovCERT.CZ: govcert.cz. Národní úřad kybernetické bezpečnosti, Brno: Národní úřad pro kybernetickou a informační bezpečnost, 6. 9. 2022. Dostupné z: nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/govcert-cz

[11] HALLER, Martin. CyberCon 2022: Směrnice NIS2 a hlavní plány její transpozice v ČR. In: Www.cybercon.cz/ [. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 14.9.2022 . Dostupné z: www.youtube.com/watch?v=aowHkz1FOiQ

[12] HUDEC, Jiří a kolektiv. ItSMF Czech Republic the IT Service Management Forum: ITIL - výkladový slovník a zkratky v češtině. Praha, itSMF Czech Republic the IT Service Management Forum, 2012.

[13] ISO . iso.org. Dostupné z: www.iso.org/foreword-supplementary-information.html

[14] ItSMF Czech Republic: The IT Service Management Forum. Česká Republika: itSMF Czech Repoublic, 2012 -2022. Dostupné z: itsmf.cz/o-spolku

[15] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.

[16] KANISOVÁ, Hana a Miroslav MÜLLER. UML srozumitelně. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1083-4.

[17] KINTR, Lukáš. Bezpečnostní opatření podle zákona o kybernetické bezpečnosti: 1. část - organizační opatření. Interní auditor: čtvrtletník českého institutu interních auditorů. Praha: Český institut interních auditorů, 2016, 20(4), 4 - 8. ISSN 1213-8274.

[18] KRANECOVÁ, Jana. Vývoj zákonného rámce vnitřního kontrolního systému: Centrální harmonizační jednotka | Ministerstvo financí České republiky. In: NKÚ: Česká Republika Nejvyšší kontrolní úřad. Praha, 5.10.2017. Dostupné z: https://www.nku.cz/assets/o-nas/konference-seminare/2017/seminar-vnitrni-kontrolni-system/prezentace-kranecova.pdf

[19] KŘIVANEC, Oto. Legislativa a regulace kybernetické bezpečnosti. Auditor: časopis Komory auditorů České republiky. Mělník: Komora auditorů České republiky, 2022, 2021(3), ISSN 1210-9096.

[20] KUČÍNSKÝ, Adam, Hana KROUPOVÁ a Jakub ONDERKA. Aktuální vývoj v oblasti kybernetické bezpečnosti: Kontrola plnění zákona o kybernetické bezpečnosti. In: ISSS. Hradec Králové: Národní úřad pro kybernetickou a informační bezpečnost, 17.5.2022. Dostupné z: www.isss.cz/archiv/2022/download/audio/kyberneticka-bezpecnost_1kucinsky-kroupova-onderka.mp3

[21] KUČÍNSKÝ, Adam. Zákon o kybernetické bezpečnosti a jeho implementace aktuálně: Aktuality z oblasti regulace. In: ISSS Hradec Králové: Traida, spol. s. r. o, 2. 4. 2019 Dostupné z: www.youtube.com/watch?v=Lw155n-ommU

[22] MEZINÁRODNÍ RÁMEC PROFESNÍ PRAXE INTERNÍHO AUDITU. Český institut interních auditorů 2017. Praha: Český institut interních auditorů, 2017. ISBN 978-80-86689-55-5.

[23] Národní úřad pro kybernetickou bezpečnost: FAQ. Národní úřad pro kybernetickou bezpečnost, Brno: Národní úřad pro kybernetickou bezpečnost, 2022, Dostupné z: nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/

[24] NONNEMANN, František, Vlastimil ČERVENÝ a Dominik VÍTEK. Kybernetický bezpečnostní incident 3D: IT, právo a compliance. Praha: Wolters Kluwer, 2022. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7676-515-3.

[25] PIVOŇKA, Tomáš a Vendula KOŽÍŠKOVÁ. Dílna interního auditu: VŘKS © 2014 Ernst & Young, s.r.o, 2014. Dostupné z: www.interniaudit.cz/download/ konference-spindl14/Pivonka_Tomas_prezentace.pdf

[26] PIVOŇKA, Tomáš. VKS pohledem interního auditora. In: 2017. Dostupné z: www.nku.cz/assets/o-nas/konference-seminare/2017/seminar-vnitrni-kontrolni-system/prezentace-pivonka.pdf

[27] Přehledové blokové schéma k zákonu a jeho prováděcím předpisům, In : Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2018, 20.2.2018. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf

[28] RYBÁKOVÁ, Alena. Audit a auditor kybernetické bezpečnosti. Interní auditor. Praha: Český institut interních auditorů, 2017, ISSN 1213-8274.

[29] SEDLÁKOVÁ, Renáta. VÝZKUM MÉDIÍ Nejužívanější metody a techniky. Praha: Grada Publishing, 2014. ISBN 978-80-247-3568-9.

[30] Schéma - Proces určení provozovatele základní služby a IS základní služby dle zákona o KB a vyhlášky o kritériích pro určení provozovatelů základních služeb: Základní služba. In: Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2018, 27.3.2018. Dostupné z: www.nukib.cz/download/publikace/podpurne_materialy/Schema_rozhodovani_PZS_v2.1.pdf

[31] ŠEBEK, L., a Hoffmannová, J. (2010). Metoda focus group a možnosti jejího využití v kinantropologickém výzkumu. Tělesná kultura,. doi: 10.5507/tk.2010.009

[32] TOUŠEK, Ladislav. Zaměřované interview a focus groups: Přehledová studie 07/2. CAAT 2007, 30.12.2022. Dostupné také z: www.antropologie.org/sites/default/files/publikace/downloads/153_153_ladislav_tousek_zamerovane_interview_a_focus_groups.pdf. Katedra antropologických věd FF ZČU.

[33] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 30.6.2022. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

8 Seznam obrázků, tabulek a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

Tabulka 3 – Seznam použitých zkratek

Audit	interní IT audit dle zákona o kybernetické bezpečnosti
BPMN	Business Process Model and Notation. Jedná se o syntaxy pro grafické znázornění procesních modelů
CERT	Computer Emergency Reponse Team. Skupina pro reakci na počítačové hrozby.
COBIT	Control Objectives for Information and Related Technology. Jedná se o framework pro správu a řízení IT
COSO	Committee of Sponsoring Organizations. Dobrá praxe pro hodnocení vnitřního kontrolního systému
EU	Evropská unie
H1, H2, H3, H4	Hypotézy stanovené pro metodu Focus Group
HDP	Hrubý domácí produkt
HW	Hardware. Fyzické kompotenty IT
IA	Interní audit

ISMS	Information security management systém. Systém řízení bezpečnosti informací.
ISO	International Organization for Standardization. Ve spojení s číslem se jedná o označení technické normy.
ISZS	Informační systém základní služby
IT	Informační technologie
ITIL	Information Technology Infrastructure Library. Standard pro řízení a nastavení podnikových procesů
itSMF	The IT Service Management Forum. T Service Management Forum je nezávislá organizace věnující se propagaci profesionálního přístupu ke správě služeb IT
NIST	Označení směrnice evropské unie o bezpečnosti sítí a informací

Zdroj: vlastní zpracování

9 Přílohy

Seznam příloh

Příloha A

Připravený dokument pro výzkum procesu interních auditů metodou Focus Group – pro realizační fázi

1. Základní ustanovení Procesu kybernetických auditů

Účelem tohoto dokumentu je stanovit proces Interního auditu, který bude respektovat poslání, nezávislost, odpovědnosti, pravomoci a postupy pro činnost kybernetického interního auditu v rámci společnosti ORGANIZACE (dále jen „XXXX“ nebo společnosti).

1.1. Závaznost

Tento vnitřní předpis se týká všech organizačních útvarů společnosti „XXXX“.

1.2. Definice pojmů a použité zkratky

Výraz	Definice	Zkratka
Interní audit	Je nezávislá, objektivně ujišťovací a poradenská činnost zaměřená na přidávání hodnoty a zdokonalování procesů v organizaci. Interní audit pomáhá organizaci dosahovat jejích cílů tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a řízení a správy společnosti.	IA
Řízení a správa společnosti	Je kombinace procesů a struktur zavedených orgány společnosti za účelem informování, kontroly, řízení a monitorování činností společnosti směrem k dosažení jejích cílů.	--
Řídící a kontrolní procesy	Zásady, postupy (jak manuální, tak automatizované) a činnosti, které jsou součástí rámce řízení a kontroly, který je navržen a vykonáván s cílem zajistit, aby se rizika nacházela v míře, kterou je společnost ochotna přijmout.	--
Řízení rizik	Proces identifikace, ohodnocení, řízení a kontroly možného výskytu událostí a situací za účelem poskytnutí přiměřeného ujištění ohledně dosažení cílů společnosti.	--
Interní auditor	Osoba, která ve společnosti vykonává funkci interního auditu.	--
Zakázka	Konkrétní zadání auditní akce, úkol nebo prověřovací činnost (jako jsou např. šetření interního auditu, prověrka sebehodnocení řídicího a kontrolního systému, vyšetřování podvodu nebo poradenství). Zakázka může zahrnovat více dílčích úkolů nebo činností, jejichž cílem je splnění konkrétních stanovených cílů.	--
Zjištění	Je prokazatelná skutečnost, kterou mohou potvrdit postupy auditu a která identifikuje chybějící nebo neúčinné kontroly či stav, který je nutno řešit s ohledem na možnost ohrožení stanovených cílů.	--
Doporučení	Názory a podněty interního auditu formulované k odstranění zjištěných nedostatků, ke zdokonalení postupů a zlepšení řízení.	--
Opatření	Popis činností přijatých vedením nebo orgány společnosti směřující k nápravě zjištěného nedostatku s cílem ošetřit související rizika a zvýšit pravděpodobnost realizace záměrů a dosažení cílů.	--

1.3. Statut kybernetického auditu

1.3.1. Účel a poslaní

Posláním kybernetického interního auditu ve společnosti „XXXX“ je zvyšovat a chránit hodnotu společnosti tím, že poskytuje objektivně ujišťovací služby založené na vyhodnocení rizik, poskytuje poradenství ve věci dosažení souladu se zákonem o kybernetické bezpečnosti pro povinné osoby a informační systémy a základní služby. Toho je dosahováno zejména poskytováním nezávislé, objektivní ujišťovací a poradenské činnosti zaměřené na přidávání hodnoty a zdokonalování procesů ve společnosti „XXXX“.

Kybernetický audit má za cíl pomáhat vedení společnosti dosahovat stanovených cílů managementu společnosti s tím, že přináší systematický metodický přístup k hodnocení a zlepšování účinnosti systému řízení rizik, řídicích a kontrolních procesů a správy a řízení.

1.3.2. Standardy pro profesní praxi kybernetického interního auditu

Kybernetický interní audit se ve výkonu svých funkcí řídí závaznými prvky mezinárodního rámce profesní praxe interního auditu tzn. hlavními principy profesní praxe interního auditu, etickým kodexem, mezinárodními standardy pro profesní praxi interního auditu (dále jen „Standardy IA“), definicí interního auditu a požadavky zákona o kybernetické informační bezpečnosti č. 181/2014 Sb.

1.3.3. Pravomoci

Auditor kybernetické bezpečnosti je oprávněn za účelem plnění funkce kybernetického interního auditu:

- vyžadovat informace o veškerých skutečnostech souvisejících s ověřovanou činností,
- jednat se všemi zaměstnanci a členy představenstva společnosti „XXXX“ bez ohledu na jejich pracovní pozici a postavení v úrovni řízení,
- jednat se všemi významnými i nevýznamnými dodavateli společnosti „XXXX“ a vyžadovat si jejich součinnost přes pověřené osoby společnosti, vstupovat na pracoviště v rámci celé společnosti „XXXX“ a nahlížet do písemných podkladů, dokumentace, médií a informačních systémů,
- vyžadovat ústní nebo písemná vysvětlení k ověřované činnosti a ke zjištěným skutečnostem a v případě potřeby vyžadovat informace i od třetích osob,
- vyhotovovat fotokopie, audiozáznamy, videozáznamy, opisy, popřípadě výpisy z originálních dokladů a ze souborů uložených na elektronických a paměťových médiích,
- mít přístup k práci ostatních interních a externích poskytovatelů ujištění,
- účastnit se porad vedení a představenstva společnosti „XXXX“ (v případech hodných zvláštního zřetele může být toto právo jednotlivě omezeno odůvodněným rozhodnutím představenstva „XXXX“),
- účastnit se všech důležitých jednání s externími orgány týkajících se řídícího a kontrolního systému XXXX, interního auditu a rizik vyplývajících z činnosti „XXXX“.

1.3.4. Nezávislost a objektivita

Kybernetický audit je při své činnosti nezávislý na všech výkonných činnostech „XXXX“.

Postavení a činnosti interního kybernetického auditu v „XXXX“ jsou vymezeny v Organizačním řádu a v Kompetenčním řádu „XXXX“.

Auditor kybernetické bezpečnosti nesmí:

- vykonávat jakékoli výkonné činnosti pro XXXX, mimo činnosti interního auditu, v souladu s § 7 Bezpečnostní role, číslo (4) Auditor kybernetické bezpečnosti bod c) nesmí být pověřen výkonem jiných bezpečnostních rolí.
- postupovat tak, aby při činnosti a vztazích interního auditora v rámci „XXXX“ byla narušena jeho nezávislost a objektivita (tzn. nezapojovat se do těch činností, které by vedly k oslabení nezávislosti kybernetického auditora),
- řídit činnost ostatních zaměstnanců XXXX, kteří nejsou auditory, vyjma případů, kdy tito zaměstnanci jsou řádně zařazeni do auditorského týmu,
- nastavovat řídící a kontrolní systém XXXX,
- zavádět nebo se podílet na výkonu řídicích a kontrolních mechanismů, mimo těch, které se týkají činnosti auditu,
- hodnotit procesy, za které byl během předchozího roku odpovědný nebo na jejichž rozvoji či zavádění se podílel nebo za které je odpovědný.

1.3.5. Rozsah poskytovaných služeb

[redacted]Ujišťovací služby

Za ujišťovací služby jsou v podmínkách společnosti „XXXX“ považovány tyto zakázky:

- audit plánovaný,
- audit na vyžádání „XXXX“ (mimořádné audity),
- ověřování a vyhodnocení funkčnosti a efektivnosti vnitřního kontrolního systému,
- ověřování plnění nápravných opatření.

Poskytování ujišťovacích služeb probíhá v souladu s ročním plánem auditních zakázek. Výstupy pro vedení společnosti „XXXX“.

[redacted]Poradenské služby

Za poradenské služby jsou v podmínkách společnosti „XXXX“ považovány tyto zakázky:

- monitoring činností útvarů, aktivit, projektů XXXX,
- účast v připomínkovém řízení k vnitřním předpisům XXXX,
- spolupráce s externím auditorem, kontrolními orgány apod.,
- účast interního auditora ve výběrových komisích (poradní hlas),
- metodická pomoc při koncipování zavádění nebo zlepšování řídicího a kontrolního systému.

1.3.6. Odpovědnosti

Kybernetický audit je povinen:

- vytvářet a předkládat rizikově zaměřený plán zakázek a požadavky na zdroje, včetně jejich průběžných významných změn, k posouzení a schválení představenstvu společnosti „XXXX“ (v případě omezení zdrojů též informovat o dopadech vzniklých v důsledku omezení zdrojů),
- respektovat a v rámci svých možností nenarušovat plynulý výkon činností auditovaných subjektů,
- zabezpečit veškeré získané informace (materiály, soubory na médiích i vlastní dokumentaci) proti jejich zneužití nepovolanou osobou,
- zachovávat diskrétnost a mlčenlivost o všech skutečnostech zjištěných v průběhu své

činnosti,

- neprodleně informovat vedení společnosti „XXXX“ o závažných zjištěných skutečnostech, které významným způsobem ovlivňují nebo v budoucnu mohou ovlivňovat činnost společnosti XXXX,
- poskytovat pouze takové služby, pro které má nezbytné znalosti, zkušenosti a schopnosti,
- zajišťovat zohlednění nových trendů a osvědčených postupů v oblasti interního auditu a kybernetické bezpečnosti,
- zavést a zajistit dodržování zásad a postupů určených k řízení činnosti kybernetického auditu společnosti,
- vykonávat auditorské práce s náležitou profesní péčí, a přitom dodržovat vysokou úroveň chování a jednání v souladu s Etickým kodexem interního auditora, který tvoří přílohu tohoto vnitřního předpisu,
- pravidelně předávat vedení společnosti „XXXX“ zprávy o stavu informační kybernetické bezpečnosti a jejího souladu se Zákonem o kybernetické informační bezpečnosti, týkající se účelu,
- zajistit soulad činnosti kybernetického auditu s Mezinárodními standardy pro profesní praxe interního auditu (dále jen Standardy IA), s následujícími výjimkami:
  - Pokud jsou Standardy IA používány ve spojení s požadavky vydanými jinými odbornými organizacemi, v případech, kdy je to vhodné, mohou auditní zprávy také odkazovat na tyto požadavky. Pokud v takovém případě vykazuje interní audit soulad se Standardy a existují rozdíly mezi Standardy IA a ostatními použitými požadavky, interní auditoři a interní audit musí být v souladu se Standardy IA; mohou se však také přizpůsobit ostatním požadavkům, pokud jsou jejich ustanovení přísnější než Standardy IA.
  - Pokud by Standardy IA měli být v rozporu s požadavky Zákona o kybernetické bezpečnosti.

1.3.7. Program pro zabezpečení a zvýšení kvality

Interní audit vytváří a aktualizuje Program pro zabezpečení a zvyšování kvality kybernetického auditu (dále je „Program“), jehož součástí jsou všechny aspekty činnosti interního auditu a provádí průběžné sledování jeho efektivnosti a způsobu vykonání auditů v daném roce.

Interní hodnocení Programu provádí kybernetický audit formou sebehodnocení a o jeho výsledcích informuje vedení společnosti „XXXX“ ve zprávě o stavu kybernetické informační bezpečnosti a o činnosti IA za hodnocené období. Součást auditního týmu, provádějícího tuto kontrolu, musí být i interní pracovník nepodléhající internímu auditu. Je to nutné pro zajištění nestrannosti tohoto hodnocení.

V souladu se Standardy IA jsou prováděna externí hodnocení Programu jednou za pět let, a to odborně způsobilým a nezávislým externím hodnotitelem, jehož výstup podléhá schválení vedení společnosti „XXXX“.

2. Proces kybernetických auditů

Plánování – Plan

Provádění auditní akce – Do

Ověřování plnění opatření – Control

Reporting – Act

2.1. Proces:

2.1.1. Plánování – Plan

Cílem plánování kybernetického auditu je stanovit pro určité časové období úkoly interního auditu zejména na základě vyhodnocení významných rizik při dosahování cílů společnosti „XXXX“.

2.1.2. Příprava plánu

Při přípravě plánu se vychází zejména z:

- cílů, úkolů, strategických záměrů a rozhodnutí XXXX,
- analýzy rizik činností společnosti XXXX,
- legislativních požadavků zákona o kybernetické bezpečnosti a souvisejících prováděcích předpisů,
- výsledů externích kontrol,
- požadavků regulatorních orgánů,
- analýzy dalších zdrojů informací.

Kybernetický audit sestavuje každoročně plán interního auditu obsahující střednědobý plán auditu a roční plán auditu.

Střednědobý plán činnosti interního auditu je sestavován na období 5 let tak aby pokryl všechny zásadní činnosti a procesy „XXXX“, související se Zákonem o kybernetické bezpečnosti. Střednědobý plán je každý rok aktualizován.

Roční plán auditních zakázek navazuje na plán střednědobý. Upřesňuje rozsah, věcné zaměření a typ auditu, jeho cíle, časové rozvržení, personální zajištění a významné změny ukončené v roce předchozím. Musí být sestaven v roce, který předchází roku, na nějž je sestavován.

2.1.3. Projednání a schválení plánu

Návrh plánu auditu včetně analýzy rizik je předložen interním auditem k projednání a odsouhlasení vedení společnosti „XXXX“. Důvody případných změn plánu interního auditu nebo odlišné názory na analýzu rizik jsou zdokumentovány.

Dle vývoje situace ve společnosti XXXX, identifikovaných a odstraněných slabin určených prvků informačních systémů základních služeb a dokončených významných změn je možné roční plán auditních zakázek v průběhu roku přehodnotit. Změnu ročního plánu auditních zakázek předkládá interní audit opět vedení společnosti „XXXX“ ke schválení.

2.2. Provádění auditu kybernetické bezpečnosti – DO

Auditní akce (dále jen „audit“) je prováděna v souladu s ročním plánem.

Veškerá dokumentace pořízená auditorem v průběhu auditu je ukládána do elektronické složky daného auditu. Elektronické dokumenty jsou průběžně ukládány do elektronické složky interního auditu na společném disku.

Do složky auditu (tzv. auditního spisu) jsou průběžně zakládány tyto povinné dokumenty:

- oznámení o zahájení auditu,
- plán realizace auditu,
- pracovní záznam auditora (Audit tracking log) včetně podkladové dokumentace ke zjištěním,
- zpráva interního auditu (včetně korespondence),
- záznam z projednání výsledků auditu,
- záznam z ověření plnění nápravných opatření (včetně podkladové dokumentace).

2.2.1. Příprava

Audit před prováděním auditu shromáždí a prostuduje potřebné podkladové materiály (např. aktuální znění Zákona o kybernetické bezpečnosti a prováděcích předpisů, další související zákony, regulatorní požadavky, vnitřní předpisy, zprávy regulátorů a externích auditorů, předchozí zprávy auditu, doporučení auditu pro danou oblast, odpovídající vstupy z mapy rizik, reporting pro vedení společnosti „XXXX“ apod.) Součástí individuální přípravy na provedení auditu může být i předběžná prohlídka auditované lokality, o které je auditovaný útvar předem informován.

Před zahájením plánovaného termínu auditu zašle audit vedoucímu auditovaného útvaru oznamovací dopis, kterým auditovaný subjekt seznámí se zaměřením auditu a obdobím, ve kterém bude audit proveden, a základní informace o složení auditorského týmu. Součástí oznamovacího dopisu je zpravidla i seznam podkladů, které auditor požaduje připravit ke dni zahájení auditu.

Oznamovací dopis slouží zároveň jako písemné oprávnění uvedených auditorů k provedení auditu.

V odůvodněných případech má audit právo provádět předem neohlášené kontroly na místě. Na tyto audity se nevztahuje povinnost předchozího informování dotčených vedoucích pracovníků.

2.2.2. Provádění auditu

Interní audit je prováděn v souladu se standardními auditorskými postupy (viz Standardy IA) a dle vytvořeného plánu auditu.

Cílem auditních činností v této fázi auditu je získat dostatečnou a přiměřenou auditní dokumentaci, která by umožnila kvalifikovaně posoudit auditovanou oblast a formulovat případná auditní doporučení ke zjištěným nesrovnalostem.

2.2.3. Ukončení auditu

Po ukončení auditních prací zpracuje vedoucí auditu návrh zprávy kybernetického auditu (dále je „zpráva IA“), která obsahuje cíl a rozsah auditu, příslušné závěry a doporučení.

Návrh zprávy IA odešle vedoucí auditor vedoucím auditovaného útvaru k vyjádření. Vedoucí auditovaného útvaru se může k návrhu zprávy IA do 5 pracovních dnů vyjádřit, případně zaslat návrh (návrhy) konkrétních nápravných opatření. Po posouzení objektivnosti připomínek auditovaného útvaru interní audit vypracuje konečné znění zprávy IA.

Konečné znění zprávy IA je následně zasláno, současně s pozvánkou k závěrečnému projednání, vedoucímu auditovaného útvaru. O způsobu projednání rozhoduje vedoucí auditor.

Audit je ukončen projednáním konečného znění zprávy IA s vedoucím auditovaného (auditovaných) útvaru (útvarů), členem vedení zastřešujícím danou auditovanou oblast a vyjádřením odpovědných vedoucích pracovníků k auditním doporučením (akceptace rizika vedením společnosti „XXXX“ nebo přijetí nápravných opatření).

Přijatá opatření musí být vždy konkrétní, jednoznačná, dokladovatelná, termínovaná (konkrétní datum) a s uvedením odpovědnosti za jejich plnění. Opatření formuluje auditovaný útvar na základě doporučení auditu a musí být promítnuta do Prohlášení aplikovatelnosti společnosti a následně do implementačního plánu na další rok případně období.

Ze závěrečného projednání se vyhotovuje záznam z projednání, který tvoří součást finálního znění zprávy o kybernetické informační bezpečnosti. Výsledkem závěrečného projednání musí být akceptace konečného znění zprávy nebo dohoda o způsobu vyřešení rozporů.

Audit zašle naskenovanou kopii konečného znění zprávy (vč. záznamu z projednání) příslušným stranám podle distribučního seznamu, který je uveden ve zprávě.

Jednotlivá nápravná opatření k auditním doporučením jsou předmětem následného kontroly ze strany auditu formou průběžného ověřování jejich plnění s pravidelným hlášením o celkovém stavu pro vedení společnosti „XXXX“

2.3. Ověřování plnění opatření – Check

Ujišťovací služba ověřování plnění opatření poskytuje zpětnou vazbu k ujištění o snížení rizik, odstranění nedostatků nebo zlepšení procesů, činností či kontrolních mechanismů, ke kterým opatření směřovala. Služba je součástí ročního plánu.

2.3.1. Evidence opatření

Audit vede databázi opatření. Databáze obsahuje popis nálezů a přijatých opatření, odpovědné osoby za implementaci, termíny realizace a status plnění opatření.

Podmínkou pro zařazení opatření do evidence je, aby opatření bylo:

- konkrétní,
- jednoznačné,
- racionální,
- termínované,
- dokladovatelné,

- aktuální (s ohledem na určený termín plnění),
- s určenou jednoznačnou odpovědností za implementaci.

Kontrolu úplnosti formálních náležitostí pro jednotlivá opatření provádí audit před zařazením do evidence přijatých opatření.

2.3.2. Průběžné ověřování

Ověřování plnění jednotlivých opatření provádí interní audit průběžně a vytváří samostatný záznam z ověření plnění opatření (dále jen „záznam“) ke každému opatření.

Ověřují se veškerá opatření, jejichž termín plnění nastal, včetně opatření, u nichž je předpoklad, že jsou již splněna.

Projednání výsledku ověření plnění opatření probíhá elektronicky, zasláním záznamu k vyjádření odpovědné osobě.

2.3.3. Souhrnné hlášení

Interní audit vytváří pro vedení společnosti „XXXX“ roční hodnotící informaci o stavu plnění přijatých opatření jako součást zprávy o činnosti IA za hodnocené období.

2.4. Reporting – Act

K zabezpečení poslání auditu v XXXX je stanoven základní systém reportingu, který zahrnuje následující výstupy z ujišťovacích a poradenských služeb auditu pro představenstvo „XXXX“.

2.4.1. Zpráva o stavu informační kybernetické bezpečnosti určeného ISZS

Dokument obsahující závěrečné výsledky auditní akce (podle plánu nebo na vyžádání) včetně přijatých opatření.

2.4.2. Zpráva o činnosti auditu za hodnocené období

Souhrnný dokument, který informuje o:
- statutu kybernetického auditu,
- nezávislosti funkce auditu,
- plánu auditů a jeho plnění současného období,
- výsledcích auditních činností,
- souladu s Etickým kodexem a se Standardy IA,
- odpovědi vedení společnosti na identifikovaná rizika, která jsou dle úsudku auditu pro společnost „XXXX“ nepřijatelná.
- souhrn identifikovaných nesouladů s legislativními požadavky se Zákonem o kybernetické bezpečnosti.

2.4.3. Zpráva z vyhodnocení funkčnosti a efektivnosti řídicího a kontrolního systému

Souhrnná zpráva z vyhodnocení funkčnosti vnitřního kontrolního systému, kterou zpracovává kybernetický audit.

2.5. Závazné prvky mezinárodního rámce profesní praxe interního auditu a ISO

- Hlavní principy profesní praxe interního auditu
- Etický kodex
- Mezinárodní standardy pro profesní praxi interního auditu (Standardy IA)
- Definice interního auditu
- Normy ISO

Příloha B

Zápis z provedené řízené diskuse dle metody Focus Group

Administrativa diskuse: Moderátor, Zapisovatel

Účastníci diskuse – role:3x Auditor kybernetické bezpečnosti, 3x Manažer kybernetické bezpečnosti, 1x Architekt kybernetické bezpečnosti, 1x Garant aktiva ISZS, 1x Garant aktiva KII

Datum: 24.11.2022

Místo: Praha

Tabulka 4- Zápis z provedené řízené diskuse dle metody Focus Group

Otázky	**Závěry z řízené debaty**
H1: IT kybernetický audit má být sestaven z činností seskládaných dle Demingova PDCA cyklu.	
Jsou dle Vašeho názoru kybernetické IT audity něčím specifické, čím se liší od jiných auditních činností?	Účastníci se shodli. že specifika kybernetických auditů spočívají, oproti jiným, jako jsou například procesní audity nebo finanční, v specifickém zaměření. Výsledek finančních auditů vidí ve prověření správnosti finančních transakcí a správnosti jednotlivých kontrol plateb, účtování a dalších. Naproti tomu kybernetické audity prověřují nastavení a funkčnost bezpečnostních kontrol a činností. Dále se zaměřují na rizika spojené s externími útočníky, bezpečnostní hrozby informačních systémů a úniku dat. Do debaty se zapojili všichni účastníci.
Jaké činnosti je nutné vykonávat v části plánování interního auditu a jakou s nimi máte praxi, jakým způsobem je vykonáváte ve Vaší organizaci, či s jakým způsobem jste se setkali v rámci Vaší dosavadní praxe?	Kybernetičtí interní auditoři: V části plánování je pro auditory nutné zejména nastudovat auditovanou oblast a platné interní a externí předpisy, směrnice, mezinárodní standardy ISO apod. a pochopit zařazení auditovaného subjektu / oddělení / pracovníků a jejich pravomocí. Dále je nutno stanovit jasné zadání a hypotézy či hlavní rizika auditované oblasti a také pečlivě rozplánovat celkový harmonogram průběhu auditu včetně termínů zahájení a ukončení. Je kladen důraz především na správné určení rizik. Další názor auditora byl, že audity jsou plánovány zejména s důrazem na hypotézy – tj. následné potvrzení či vyvrácení hypotéz v auditu. Ve srovnání s mezinárodním auditním standardem však upřednostňuji pracovat s riziky a tyto příp. dále rozpracovat na podrizika a ověřovat je podobně jako hypotézy. Manažeři kybernetické bezpečnosti: Internímu auditu jsou předávány v pravidelné periodě (u každého z této role byl časový úsek jiný - 1x kvartálně, 2x jednou ročně), jako vstup do plánování auditních činností, a to nejen kybernetických auditů. Dále

Otázky	Závěry z řízené debaty
	v případě dokončování významných změn na prvcích jak KII tak ISZS dochází k plánování a součinnosti na tomto plánování. Architekt kybernetické bezpečnosti: Na plánování auditů se nikterak nepodílí a nemá zkušenost z tohoto procesního kroku. V případě že by byla nutná jeho interakce, provede jí na základě požadavku svého nadřízeného / osoby odpovědné za interakci s interním auditem. Garant aktiv určených prvků KII: 2x ročně probíhají mezi týmové kontroly procesu, které spadají pod zákon o kybernetické bezpečnosti, v rámci, kterých jsou vytipovány zásadní oblasti, na které je nutné se v rámci plánovaní auditu kybernetické bezpečnosti primárně zaměřit. Garant aktiv určených prvků ISZS: S plánováním interního auditu nebo jeho součinnosti nemá žádnou profesní zkušenost. Zapojení do této fáze je pro něj maximálně v případě oslovení odpovědné osoby ze společnosti o případné doložení podkladů.
Na jaké činnosti se zaměřoval kybernetický audit, když Vás kontroloval, na jaké činnosti se zaměřujete vy?	**Kybernetičtí interní auditoři:** Manažeři kybernetické bezpečnosti: shodli se, že provedené kybernetické audity se zaměřovaly na naplňování zákona a vyhlášky kybernetické bezpečnosti, kde v jednom případě bylo zjevné, že pro danou činnost využívají vodítka Národního úřadu pro kybernetickou bezpečnost, u zbytku probíhala kontrola primárně v procesní rovině se zaměřením na dokumentační stránku věci. Manažeři kybernetické bezpečnosti se shodli, že je až překvapilo, že auditoři kybernetické bezpečnosti v jejich společnostech (ať už externí nebo interní) nešli do technických podrobností a kontroly funkčnosti systémů, ale šlo jim pouze o doložení provedených kontrol, seznámení a proškolení zaměstnanců, či pokrytí řídící dokumentace. Architekt kybernetické bezpečnosti: Zaměřoval se na navržení auditovaných systémů, nastavené a prováděné kontroly. Dále zkoumal, zda existují a jsou aktuální vyžadované dokumenty typu prohlášení o aplikovatelnosti či akční plán, a také jakým způsobem probíhá identifikování významných změn v rámci určených systémů. Garant aktiv určených prvků KII: S kontrolou ze strany kybernetického auditu i kontroly ze strany kontrolního úřadu byl konfrontován formou rozhovorů s auditory, kteří se primárně zaměřovaly na dokumentování jeho činností na prvcích kritické informační infrastruktury. Dále auditoři kontrolovali nastavení těchto systémů a doptávali se na technické záležitosti, pro které nebyl kompetentní odpovídat. Z toho důvodu (a od první kontroly) se těchto rozhovorů účastnil také dodavatel celého řešení. V neposlední řadě pro dané kontroly musel vypracovat podklady jako jsou záznamy ze schůzek, prokázat že byl seznámen s řídící dokumentací organizace a dodat analytická data ze systémů pro další analýzy. Vzhledem k tomu, že nebyl zaznamenán nedostatek v rámci jeho činností, nedostal zpětnou vazbu ani informaci o tom co se s danými podklady stalo, a ani o tom co s nimi auditoři/ kontrola úřadu dělala.

Otázky	Závěry z řízené debaty
	Garant aktiv určených prvků ISZS: Zatím s kontrolou auditu neprošel. V rámci svojí činnosti se zaměřuje primárně na faktickou funkčnost určených informačních systémů a do konfrontace s kybernetickým auditem se dostal pouze formou přípravy podkladů.
Stalo se někdy, že Vás auditor kontroloval a došel k chybným závěrům? Můžete uvést příklad?	Kybernetičtí interní auditoři: Ano, i auditoři jsou jen lidé, ale souhrnně se účastníci shodli, že chyby nastávají většinou jen na základě dodaných chybných informací či podkladů od auditovaných subjektů. Manažeři kybernetické bezpečnosti: Nikdo z manažerů nemá zkušenost, že by v rámci identifikovaných nedostatků byla ze strany auditorů pochybení. Architekt kybernetické bezpečnosti: Ano, chyby jsou často zapříčiněné neznalostí detailu daných systémů a argumentací dobrou praxí, která ale nezohledňuje daná specifika. Jako typický příklad takové chyby považuje vyžadování antiviru, či dvojité autentizace na zařízení terminálového typu, odpojeného od venkovní sítě se zaslepenými externími vstupy, u kterého je nutné, aby běželo bez odhlašování, a sloužícího jako výstupní, nikoliv vstupní zřízení. Garant aktiv určených prvků KII: Není si vědomí, že by k chybě auditora došlo. Garant aktiv určených prvků ISZS: díky tomu, že účastník zatím s touto formou kontroly neměl zkušenost, nedostal se do situace, kdy by auditor chyboval. V rámci debaty účastníci došli ke shodě, že spíše, nežli by auditor došel k chybnému závěru, tak nastavenými testy neodhalil nedostatky auditovaných řešení a jeho zpětná vazba tím pádem nebyla kompletní.
Kdo na to přišel a jakým způsobem?	Auditovaní se shodli, že na dané pochybení/ nenalezení chyby se přišlo buď následnou kontrolou/ auditem, případně při výskytu problému provozního charakteru.
Byly nějaké činnosti auditora podle Vás za hranou nebo nekorektní?	V rámci debaty účastníků došlo k vydefinování termínu nekorektního chování. Hlavní zmiňovaný problém s auditory byl v tom, že si neuvědomovali, že mimo dané kontroly musí účastníci řešit každodenní provozní záležitosti a že daná kontrola znamená více práce. Jediný účastník, který se setkal za něj s nekorektním jednáním auditora kybernetické bezpečnosti byl architekt kybernetické bezpečnosti, a to v rámci toho, že z jeho zkušenosti auditor odmítal vyslechnout argumenty o nastavených řešeních a definoval zjištění do závěrečné práce i přes to, že při provedené kontrole hodnotil stav systému jako bez závad.
Jakým způsobem Vám auditor dokazoval nálezy a závěry, které učinil?	Účastníci se shodli, že dané nálezy byly vypsány v závěrečné zprávě z auditu. K dokazování nálezů nedošlo. Došlo k vyjasňování při tvorbě nápravných opatření. Dle názorů auditora kybernetické bezpečnosti by k danému vysvětlování ani nemuselo dojít. Správný postup dle jeho názoru by byl, kdyby vedení společnosti sepsané nálezy vzalo, rizikově posoudilo a nastavilo na ně opravné nebo akceptující mechanismy.

Otázky	Závěry z řízené debaty
Zaměřoval se auditor na Vaše prováděné kontroly nebo spíše prověřoval Vaše činnosti?	V rámci debaty se nenašel mezi účastníky konsenzus a ani jednotliví účastníci na danou otázku nebyly schopni odpovědět. Za shrnutí se dá považovat, že by auditor měl systém prověřit komplexně, tj. jak kontroly, tak i činnosti.
Prováděl to na vzorku nebo na celém spektru případů, které prověřoval?	V rámci této otázky se primárně zapojovali auditoři kybernetické bezpečnosti. Zajímavá diskuse mezi účastníky a auditory byla zakončena shodou, že záleží případ od případu. Auditor musí dát názor o nastavení systému bezpečnosti informací a stavu bezpečností na určených prvcích jako celku a tím v závislosti na nastaveném harmonogramu auditu se daný auditor musí rozhodnout co prověří a jestli danou činnost/ kontrolu na vzorku, nebo celou škálu. Manažer kybernetické bezpečnosti nad rámec ostatních uvedl, že v jeho zkušenosti daný auditor dodával informaci i o tom, s jakou pravděpodobností jsou výsledky korektní.
Jakým způsobem a v jakých termínech Vám auditor prověřil efektivitu nasazených nápravných opatření?	Účastníci se shodli na tom, že termíny nápravných opatření byly řešeny individuálně a nedá se říci pravidlo na základě kterého by byly termíny určovány. Co se týče prověřování efektivity v nápravných opatřeních nedochází. Auditoři kontrolují stav naplnění a pro uzavření nebo akceptaci plnění nápravných opatření musí být vždy doložena dokumentovaná informace o splnění, případně proběhnout další kontrola auditora.
Jak je dle Vašeho názoru možné vyhodnotit vnitřní kontrolní systém v oblasti kybernetického auditu?	Auditoři kybernetické bezpečnosti se shodli na metodice COSO pro hodnocení vnitřního kontrolního systému, která je použitelná i pro kybernetické audity. V rámci diskuse došlo na základě impulzu ze strany Manažerů kybernetické bezpečnosti a architektů k vyjasnění co to vnitřní kontrolní systém je, a ke stanovisku, že principy COSO, které vysvětlovali auditoři jsou zbytečně složité a nedávají dostatečnou zpětnou vazbu. Garanti aktiv se dané debaty neúčastnili.
H2: Pro vykonání kybernetických auditů je možné vydefinovat potřebné role, které zaručí jeho kvalitní vykonání a současně i ujištění o jeho korektnosti.	
Jaké role v rámci Vaší zkušenosti v interním auditu vystupovaly a jaké měly pravomoci a odpovědnosti?	Manažer kybernetické bezpečnosti vydefinoval role: „Manažer dojednávající rozsah auditu a časový rámec, senior konzultant který měl na starosti provedení auditu a komunikaci s auditovanými, juniorní auditor připravující a vyhodnocující podklady a řídící dokumentaci.“ V rámci debaty účastníci došli k závěru, že by měla být osoba odpovědná vrcholově za prováděný audit, dále osoby vykonávající daný audit a komunikující s auditovanými přes odpovědnou osobu na straně businessu. Jejich povinnosti a pravomoci by měli být někde zachyceny a dodržovány. Další role přijdou účastníkům nadbytečné, nicméně záleží na velikosti a náročnosti auditu.
Chybělo nebo chybí Vám v rámci auditních týmů zastoupení nějaké činnosti, které je dle Vašeho	Účastníci se shodli, že v rámci kybernetických auditů by měl auditor kybernetické bezpečnosti mít znalosti nejen v rámci kontroly procesních činností, ale i technickou zdatnost v provádění technických úkonů, jako jsou testy zranitelnosti, nebo penetrační

Otázky	Závěry z řízené debaty
názoru nezbytné pro naplnění cílů kybernetických auditů?	testy. Další podstatná činnost, na kterou by se auditoři měli zaměřit, je komunikace mezi auditory a auditovanými a projednávání nálezů, ideálně po jejich nálezu.
Je auditor kybernetické bezpečnosti ve Vaší společnosti zastoupen v rámci Výboru kybernetické bezpečnosti Vaší společnosti?	U části účastníků debaty ano, a daný auditor kybernetické bezpečnosti je účasten, je možné se ho doptat na jeho názor, ale nikdy se neúčastní definice činností, nastavení kontrol a dalších činností souvisejících s činností výboru. U druhé části není účasten, ale dostává výstupy z daného výboru kybernetické bezpečnosti. Garanti aktiv se debaty účastnili, ale neměli zkušenost s výborem kybernetické bezpečnosti.
Vykonává daný auditor ještě jinou nežli auditní roli ve Vaší společnosti?	Účastníci se shodli na tom, že ani externí ani interní auditoři žádnou jinou roli ve společnosti nezastávají.
H3: Existují kvantitativní metriky pro vyhodnocení kybernetických auditů, které budou vést k neustálému zlepšování procesu IT interních kybernetických auditů.	
Jaké činnosti v rámci kybernetických auditů se z Vašeho pohledu dají kvantifikovat a mohly by sloužit pro vyhodnocení kvality daného procesu kybernetických auditů?	V rámci debaty byla diskutována možnost jako metriku procesu dávat počty nálezů a definovaných zjištění či nápravných opatření z auditů. Tato možnost byla nakonec účastníky zavržena, protože by dle nich mohla vést k navyšování zátěže na auditované a provádění nálezů z důvodu naplnění požadovaných parametrů. V návaznosti na předchozí debatu zazněl názor, že by dobrým kvantifikátorem mohl být výstup z hodnocení vnitřního kontrolního systému, který by ale musel být standardizován, aby mohlo dojít k posouzení trendu zjištěných výsledků.
Jakým způsobem u Vás probíhá hodnocení realizovaného kybernetického auditu?	Auditoři kybernetické bezpečnosti uvedli shodně, že hodnocení z auditu probíhá formou sebehodnocení, dále hodnocení nadřízeným a zpětnou vaznou od auditovaných. Zvláště sebehodnocení je nutné a to zejména pro zlepšení prováděných činností do budoucích auditů. 2 manažeři kybernetické bezpečnosti uvedli, že po vykonání auditu odevzdávají zpětnou vazbu z auditu na vedení interního auditu společnosti. Zbytek účastníků s předáváním zpětné vazby nemá zkušenost.
Je možné a za Vás přínosné provádět sebehodnocení po skončení auditu?	Z časových důvodů a toho, že byla otázka částečně odpovězena v rámci předchozí otázky byla otázka přeskočena.
Máte s tím zkušenost, jakou?	Z časových důvodů a toho, že byla otázka částečně odpovězena v rámci předchozí otázky byla otázka přeskočena.
H4 – Zaslaný proces IT kybernetických auditů je beze změny aplikovatelný v rámci povinných osob ISZS dle ZKB.	

Otázky	Závěry z řízené debaty
V čem vidíte největší přínos kybernetických auditů?	V rámci debaty došlo k následující shodě: „Ve zhodnocení stavu informační kybernetické bezpečnosti v rámci organizace a regulovaných systémů. Dále v ujištění vedení společnosti o stavu prověřovaných oblastech společnosti a stavu rizik a hrozeb v nich.“
Na základě proběhlé debaty Vás napadá něco, co daný proces nepopisuje, nebo je nedostatečně detailní?	V rámci procesu byly identifikované neurčité a sporné termíny. Účastníci se shodli, že v ideálním případě by měly být jako požadavky auditu, tak požadavky na audit jednoznačné a počitatelné. Účastníci se shodli, že v rámci navrhovaného procesu jsou nedostatečně definované role, odpovědnosti a pravomoci účastníků procesu. Zvláště chyběla role kontrolující auditora kybernetické bezpečnosti, která by fungovala formou supervize postupů v souladu s principy PDCA cyklu. Auditoři kybernetické bezpečnosti se shodli, že taková osoba nemusí naplňovat požadavky na roli auditora kybernetické bezpečnosti definované v Zákoně o kybernetické bezpečnosti. Dále byly rozdiskutovány jednotlivé role podílející se na procesu auditu, hlavní téma bylo definování odpovědné osoby za auditovatelnou oblast a zda to může být vedoucí té oblasti, či kdokoli do takové role dosazený.
Chybí Vám nějaké oblasti či role v daném procesu?	Manažeři kybernetické bezpečnosti se shodli, že není zcela jasné, jak se definovaný proces staví k auditům, které nebudou součástí střednědobého, či ročního plánu. Z jejich zkušenosti jsou takové audity často potřebné a přínosnější nežli ty plánované. Auditoři kybernetické bezpečnosti, z důvodu transparentnosti a na základě požadavku zákona navrhli explicitní vypsání termínů střednědobého plánu (2-5 let v odůvodněných případech). Účastníci se shodli, že vydefinovaná kritéria pro hodnocení procesu nejsou ideální a v rámci diskuse se došlo k závěru, že stačí i jeden parametr vyhodnocující daný proces, který bude jasně vyjadřovat trend zlepšování procesu Navrhovaný proces hodnotili účastníci jako velmi dokumentačně zatěžující a bez dostatečného přihlédnutí na digitalizaci společností. I z toho důvodu navrhovali zpružnění daného procesu, doplněného o procesní diagramy aby v případě potřeby bylo možné jej jednoduše virtualizovat.

Zdroj: vlastní zpracování