Prohlášení o Aplikovatelnosti -> Strategie pro NIS2

Martin Kotyk

Bezpečnost informací

Administrativní řízení bezpečnosti informací

- NIS 2
  - Směrnice EU – rozšíření regulace informační bezpečnosti pro soukromou i veřejnou správu
  - Zdravotnictví -> Musí splňovat
  - Risk management – Analýza rizik jako nutný podklad pro investice od informační bezpečnosti
- ISMS
  - Systém řízení bezpečností informací
  - Zajištění systémového přístupu v oblasti bezpečnosti IT
  - Analýza rizik
- Prohlášení o Aplikovatelnosti
  - Základní dokument pro ISMS dle ISO 27001
  - Na základě analýzy rizik a pro její evidenci

Atos

ISMS – Information Security Management System

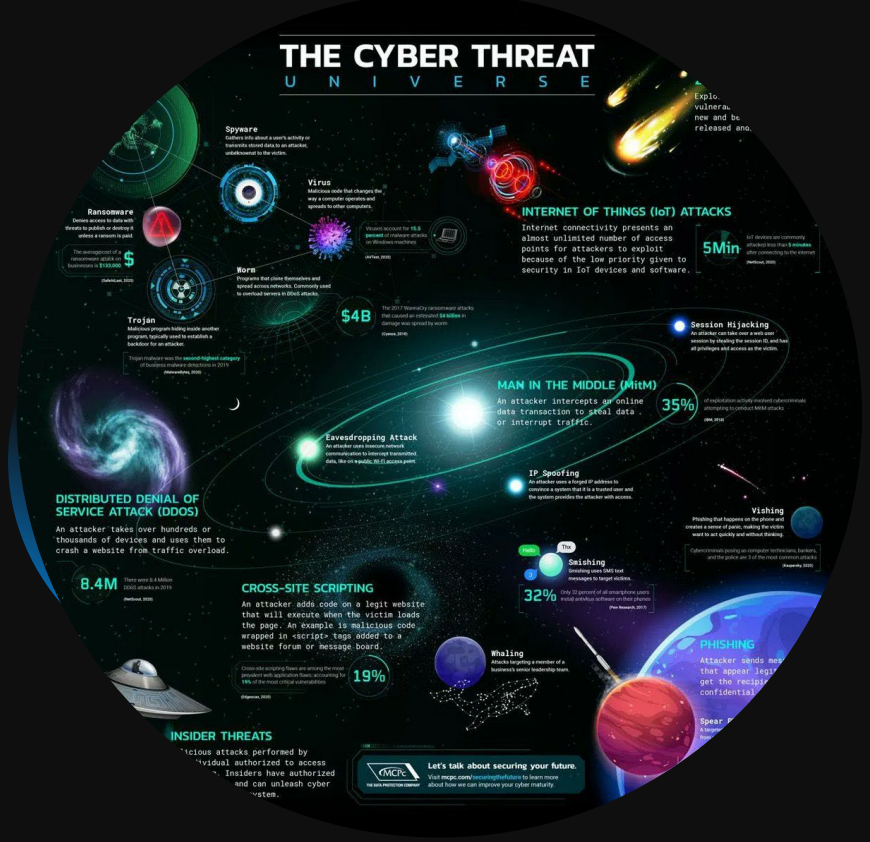
Systém řízení bezpečnosti informací pro zdravotnická zařízení

Vrstva:	*Co obsahuje?*	*Čím plnit?*
Legislativa	*Legislativní řád ČR, kterým se organizace musí řídit*	*Právní řád ČR Legislativa EU*
Bezpečnostní politika ISMS	*Interní politika, kterou organizace plní bezpečnost informací v rámci legislativy*	*Základní vzory dokumentů od NCEZ*
Prováděcí předpisy	*Předpisy, kterými se řeší naplnění bezpečnosti informací na daném místě*	*Základní vzory dokumentů od NCEZ*
IT systémy – provozní, zdravotnické, atp.	*Systémy, na kterých probíhá vytváření a zpracovávání informací*	*Dokumentace od výrobce*
Záznamy o provozu	*Záznamy, kterými se dokládá způsob fungování organizační bezpečnosti*	*SIEM/XDR/EDR/externí SOC*

Atos

Medical Internet of Things

Nekonečné množství hrozeb



In the past, much power and responsibility for life and death were concentrated in the hands of doctors. Now, this ethical burden is increasingly shared by the builders of AI software.

— Oren Etzioni, CEO of the Allen Institute for Artificial Intelligence

Atos

Základní Nastavení ISMS

Zmapovat aktiva!

- Provést analýzu rizik na zmapovaná aktiva
  - Hrozba x Zranitelnost = Inherentní Riziko
  - Inherentní riziko – Opatření = Reziduální riziko

Zmapovat aktiva

Co je základem pro provoz nemocnic

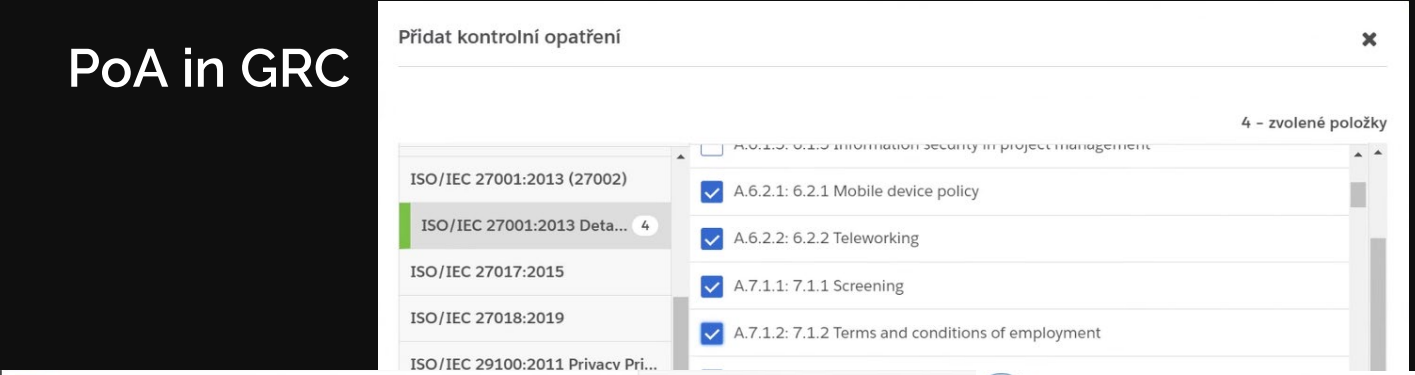
- Primární aktiva definována na základě Vyhlášky č.82/2018 § 2 g)
  - „ primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém“
- Podpůrná aktiva definována na základě Vyhlášky č.82/2018 § 2 f)
  - „podpůrným aktivem technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“
- Základní skupiny aktiv v nemocnicích
  - Ambulance
  - Klinická oddělení
  - Ekonomický provoz nemocnice
    - Zdravotní pojišťovny
  - Lidské zdroje
    - Osobní údaje pacientů
    - Osobní údaje zaměstnanců
  - Technika a provoz

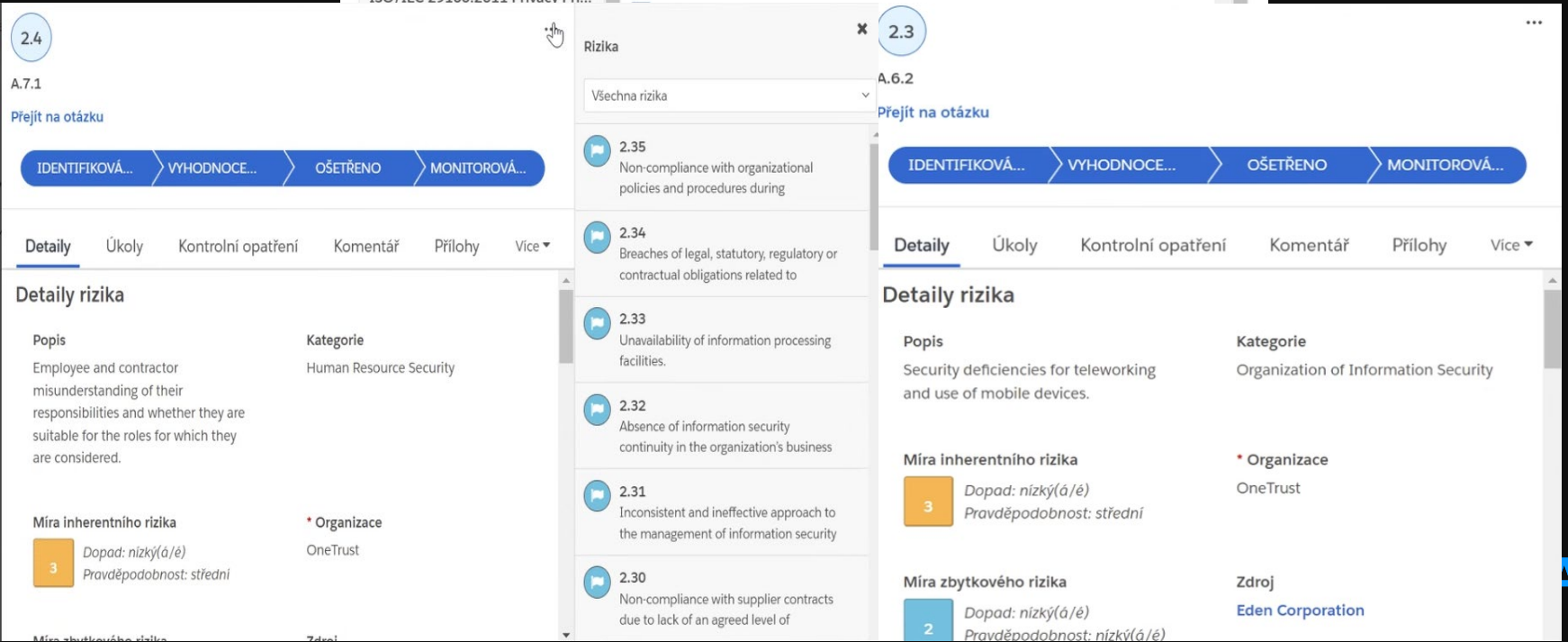
Prohlášení o aplikovatelnosti – ISO/IEC 27001 Příloha A

Evidence zavedených opatření

Příloha A ISO 27001	Název	Opatření	Aplikováno	Detaily provedení opatření	Odpovědná osoba	Důvod pro neaplikaci	Datum implementace	Poslední posouzení
A.6.2	**Mobilní zařízení a práce na dálku**							
A.6.2.1	***Politika mobilních zařízení***	Musí být přijata politika a relevantní bezpečnsotní opatření pro zvládání rizik spojených s používáním mobilních zařízení	**Ano**	Multifaktorová autentifikace Aktualizovaná politika Company portal	Ota Pavel; IT		10.4.2019	10.4.2022
A.6.2.2	***Práce na dálku***	Musí být implemetována politika a relevantní bezpečnostní opatření na ochranu informací, které jsou přístupné, zpracováváné nebo ukládáné v místech pro práci na dáklu	**Částečně**	Zavedený bitlocker Chybí BYOD politika	Petra Nová; IT		12.5.2019	12.5.2022
A.7	**Bezpečnost lidských zdrojů**							
A.7.1	**Před vznikem pracovního vztahu**							
A.7.1.1	***Prověřování***	Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků týkajících se činností organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potencionálních rizik	**Ne**	Vedení se rozhodlo neprověřovat uchazeče o práci	Jan Křeček; HR		19.7.2012	19.1.2022
A.7.1.2	***Podmínky pracovního stavu***	Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací	**Neaplikovatelné**		Petra Syslová; HR	Všichni naši zaměstnanci jsou OSVČ, pracují na smlouvu o dílo	N/A	19.1.2022

PoA in GRC


Přidat kontrolní opatření
4 – zvolené položky
ISO/IEC 27001:2013 (27002)
ISO/IEC 27001:2013 Deta... 4
ISO/IEC 27017:2015
ISO/IEC 27018:2019
ISO/IEC 29100:2011 Privacy Pri...
A.6.2.1: 6.2.1 Mobile device policy
A.6.2.2: 6.2.2 Teleworking
A.7.1.1: 7.1.1 Screening
A.7.1.2: 7.1.2 Terms and conditions of employment

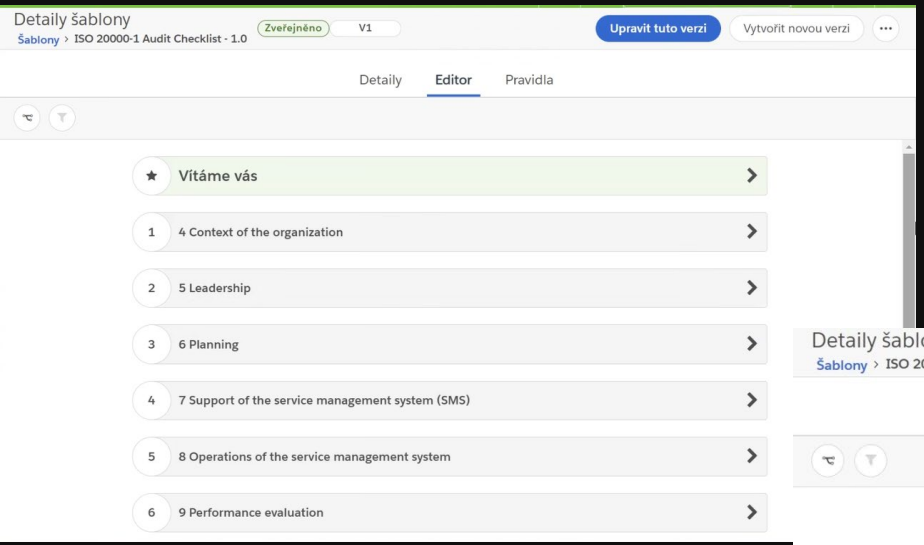

2.4
A.7.1
Přejít na otázku
IDENTIFIKOVÁ...
VYHODNOCE...
OŠETŘENO
MONITOROVÁ...
Detaily
Úkoly
Kontrolní opatření
Komentář
Přílohy
Více
Detaily rizika
Popis
Employee and contractor misunderstanding of their responsibilities and whether they are suitable for the roles for which they are considered.
Kategorie
Human Resource Security
Míra inherentního rizika
3
Dopad: nízký(á/é)
Pravděpodobnost: střední
* Organizace
OneTrust
Rizika
Všechna rizika
2.35
Non-compliance with organizational policies and procedures during
2.34
Breaches of legal, statutory, regulatory or contractual obligations related to
2.33
Unavailability of information processing facilities.
2.32
Absence of information security continuity in the organization's business
2.31
Inconsistent and ineffective approach to the management of information security
2.30
Non-compliance with supplier contracts due to lack of an agreed level of
2.3
A.6.2
Přejít na otázku
IDENTIFIKOVÁ...
VYHODNOCE...
OŠETŘENO
MONITOROVÁ...
Detaily
Úkoly
Kontrolní opatření
Komentář
Přílohy
Více
Detaily rizika
Popis
Security deficiencies for teleworking and use of mobile devices.
Kategorie
Organization of Information Security
Míra inherentního rizika
3
Dopad: nízký(á/é)
Pravděpodobnost: střední
* Organizace
OneTrust
Míra zbytkového rizika
2
Dopad: nízký(á/é)
Pravděpodobnost: nízký(á/é)
Zdroj
Eden Corporation

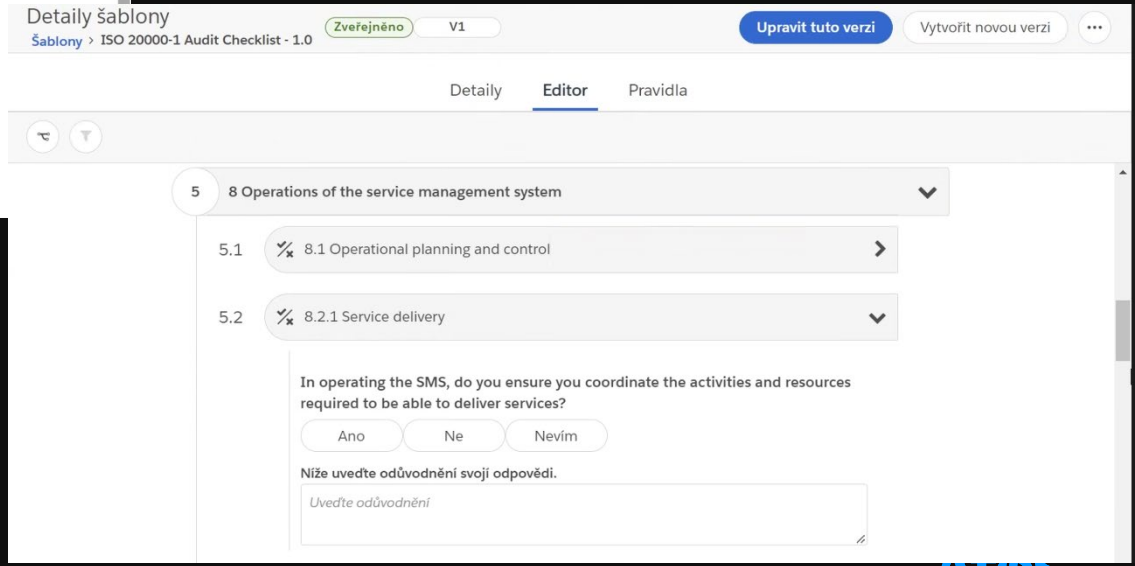
GRC – Governance, Risk, Compliance

Správa komplexu předpisů, bezpečnostních rámců a compliance na jednotné platformě pro stanovení priorit a řízení rizik.

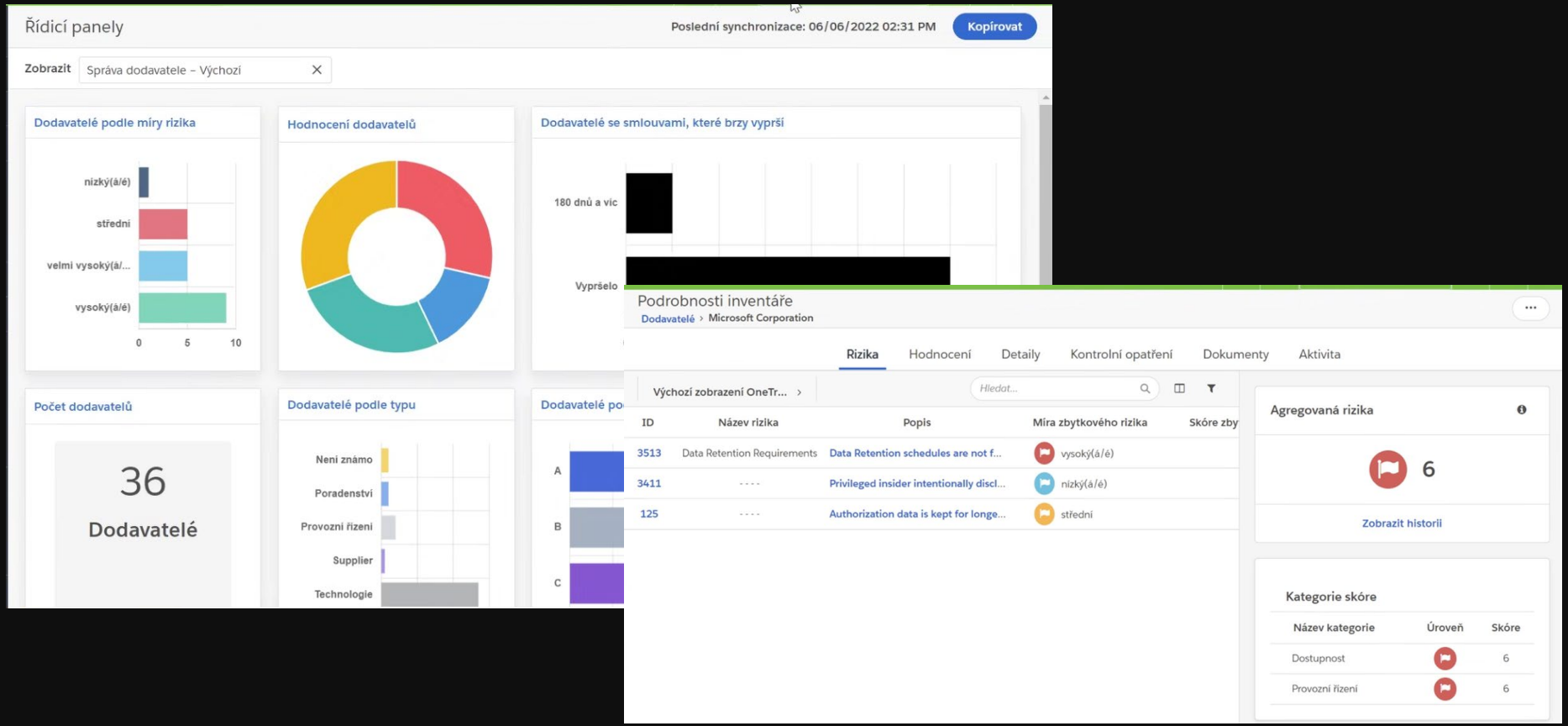
- Dosažení integrovaná správy systému (cloud/on premise/vendor)
  - Governance & Policy Management
  - Audit & Compliance Management
  - IT Risk & Security Assurance
    - Security Certification Compliance
    - IT & Security Risk Management
    - Security Incident Management
  - Third Party Risk
- Pro kontinuální audit a pomocí něj optimalizaci systému
- Pro kontinuální vyhodnocování rizik a přesné nastavování bezpečnostních opatření
- Kontinuální dohled nad dodavateli

Audit in GRC


Detaily šablony
Šablony › ISO 20000-1 Audit Checklist - 1.0
Zveřejněno
V1
Upravit tuto verzi
Vytvořit novou verzi
Detaily
Editor
Pravidla
Vítáme vás
1 4 Context of the organization
2 5 Leadership
3 6 Planning
4 7 Support of the service management system (SMS)
5 8 Operations of the service management system
6 9 Performance evaluation


Detaily šablony
Šablony › ISO 20000-1 Audit Checklist - 1.0
Zveřejněno
V1
Upravit tuto verzi
Vytvořit novou verzi
Detaily
Editor
Pravidla
5 8 Operations of the service management system
5.1 8.1 Operational planning and control
5.2 8.2.1 Service delivery
In operating the SMS, do you ensure you coordinate the activities and resources required to be able to deliver services?
Ano
Ne
Nevím
Níže uveďte odůvodnění svojí odpovědi.
Uveďte odůvodnění

Dodavatelé i GRC



NIS 2

The EU´s Cybersecurity Strategy for the Digital Decade

- *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*
  - *V platnosti od 2023*
- Nutnost přijmout technická a organizační opatření k řízení rizik ohrožujících bezpečnost sítí a informačních systémů organizace
  - Analýza rizik musí předcházet změně ve společnosti
  - Zvládání incidentů
  - Business continuity
  - Zajištění dodavatelského řetězce

Vaše dotazy?

Děkuji za pozornost