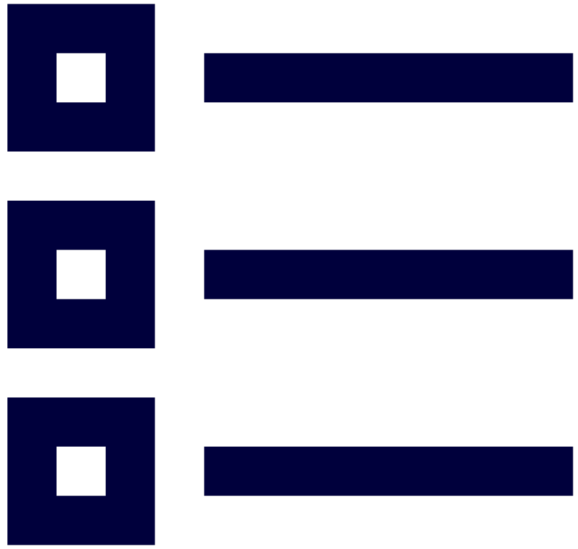

TÜVNORD
NIS2
TISAX® 6.0
ENX VCS - ISO/SAE 21434
AIMS – ISOIEC 42001
Ing. Martin Drastich MBA, Ph.D.
Adobe Stock | #816845178

Obsah



TÜVNORD

NIS2 - Novinky týkající se připravovaných prováděcích předpisů ke směrnici NIS2

TÜVNORD

NIS2

Nový zákon o kybernetické bezpečnosti by měl nabýt účinnosti 1. ledna 2025

https://portal.nukib.gov.cz/

1

Dopadá regulace na vaši organizaci?

Vyplňte si naši kalkulačku k ověření, zda budete podle nové právní úpravy spadat mezi regulované subjekty. Informace k chystané regulaci jsme pro vás připravili v článcích Koho se nové povinnosti týkají a také Rozdělení povinných organizací.

2

Splňujete podmínky pro registraci. Co teď?

Nový zákon je stále v legislativním procesu a očekáváme jeho platnost od ledna roku 2025. Aktuální informace o případných legislativních změnách můžete sledovat na webu NÚKIB a v Informačním servisu. Poradíme, jak se připravit na novou právní úpravu.

3

Co dělat až nový zákon vstoupí v platnost?

Nejprve bude potřeba provést ohlášení regulované služby skrze Portál NÚKIB. Konkrétní rozsah zákonných povinností záleží na vašem režimu povinností. Bezpečnostní opatření pro nižší a vyšší režim specifikují určené vyhlášky, které naleznete na webu PSP ČR.

TÜVNORD

NIS2

Výběr služby

V této rychlé kalkulačce můžete zjistit, zda vámi poskytovaná služba bude regulovaná a do jakého režimu (vyšší/nižší) bude pravděpodobně spadat. Pokud poskytujete více služeb a některé z nich budou regulované, pak bude celá organizace regulovaná podle nejvyššího režimu, na který některá ze služeb dosáhne.

Odvětví poskytované služby Vyberte odvětví

Poskytovaná služba Vyberte službu

Dále

TÜVNORD

NIS2

Registrace organizace

Aktuálně registrace organizace probíhá na základě zaslání pozvánky ze strany NÚKIB směrem k subjektu a neřídí se zákonem o kybernetické bezpečnosti. Nejedná se tak o hlášení dle připravovaného nového zákona.

Registrační formulář do Portálu NÚKIB **slouží k registraci subjektů, které byly do platformy** (dříve Neveřejný web) **pozvány. Do přijetí nového zákona o kybernetické bezpečnosti je registrace určena** primárně pro vybrané povinné osoby dle aktuálně platné legislativy, a to pro **správce systémů kritické informační infrastruktury, významných informačních systémů a provozovatelů základní služby** (správců informačních systémů základní služby).

Platforma Portál NÚKIB není náročková a **zatím je zapojení pro povinné osoby zcela dobrovolné.**Registrace aktuálně slouží pro organizace, které byly ze strany NÚKIB oficiálně osloveny. **Pokud nám registrační formulář zašlete, aniž byste byli jedním ze subjektů popsaných výše, žádost o přístup může být zamítnuta.**

Registrační formulář zároveň slouží jako formulář pro aktualizaci správců účtů, například po odchodu dřívějšího správce z organizace. **Vygenerovaný dokument ve formátu PDF nám spolu s přílohami zašlete do datové schránky Úřadu: zzfnkp3.**

Zpět | Dále

1. **Základní informace**
2. Identifikace orgánu nebo osoby
3. Oprávněný zástupce organizace
4. Další zástupce organizace (volitelné)
5. Hlavní správce uživatelských účtů
6. Další správci uživatelských účtů
7. Kontrola a potvrzení
8. Konec

TÜVNORD

NIS2

Hlášení kontaktních údajů

Aktuálně hlášení kontaktních údajů probíhá na základě stávajícího zákona o kybernetické bezpečnosti. Nejedná se tak o hlášení dle připravovaného nového zákona.

Orgány a osoby, které jsou regulovány na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, mají povinnost hlásit kontaktní údaje osob, které jsou za organizaci oprávněny jednat ve věcech upravených zákonem. Hlášení je potřeba provést po určení či identifikaci daného subjektu a dále v případě jakékoli změny.

Formulář pro hlášení kontaktních údajů je určen pro správce a provozovatele informačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby, stejně tak jako pro provozovatele základní služby.

Vyplněný formuláře s hlášením kontaktních údajů prosím zasílejte do datové schránky NÚKIB, ID: zzfnkp3 nebo elektronicky podepsané na e-mail regulace@nukib.gov.cz.

Zpět Dále

1 **Základní informace**
2 Výběr regulované osoby
3 Identifikace regulované osoby
4 Identifikace regulovaného systému
5 Identifikace kontaktních osob
6 Kontrola a potvrzení

TÜVNORD

NIS2

Hlášení incidentu

Aktuálně hlášení incidentů slouží primárně pro povinné subjekty, na které se vztahuje zákonná povinnost dle aktuálního zákona o kybernetické bezpečnosti.

Orgány a osoby, které jsou regulovány na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, mají povinnost hlásit kybernetické bezpečnostní incidenty (KBI) v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury (KII), informačním systému základní služby (ISZS) nebo významném informačním systému (VIS).

V případě, že je nám nahlášen incident, který nespadá do oblasti působnosti Vládního CERT týmu (KII, VIS, ISZS), jsou informace předány dále příslušnému bezpečnostnímu týmu (např. Národní CSIRT).

Na Vládní CERT je možné dobrovolně hlásit i další kybernetické bezpečnostní incidenty a kybernetické bezpečnostní události (KBU).

Více informací o tom, jaké kybernetické bezpečnostní incidenty je nutné hlásit můžete najít v Metodice k hlášení kybernetického bezpečnostního incidentu.

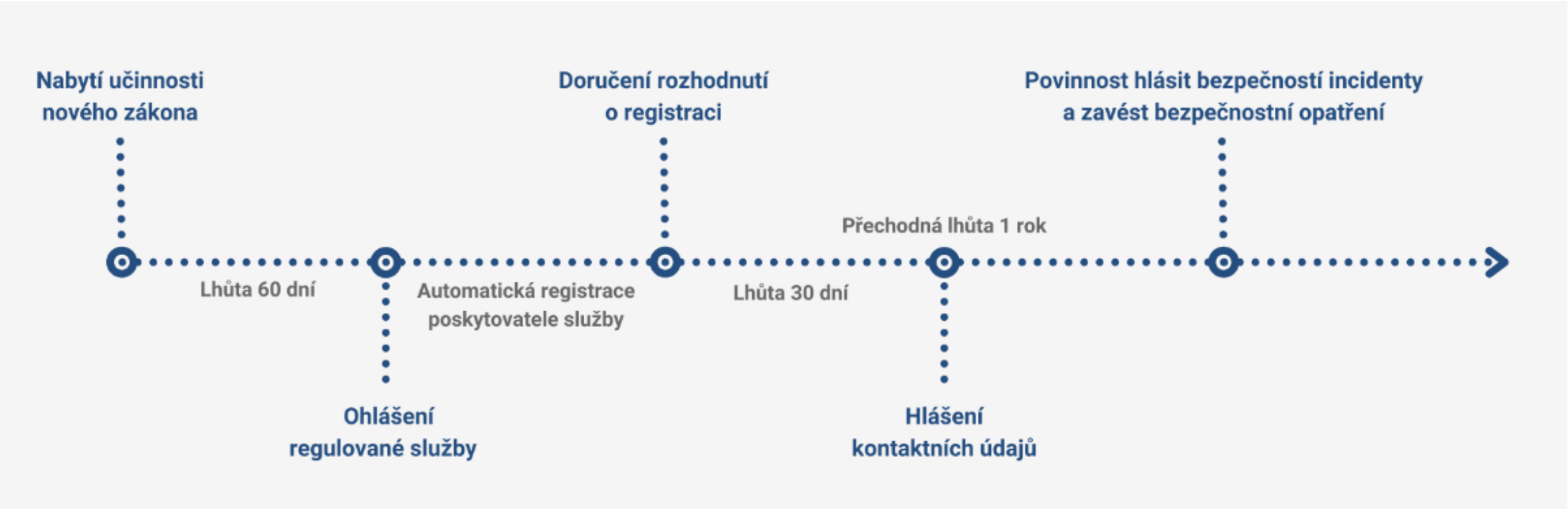
Zpět | Dále

1. **Základní informace**
2. Kdo nahlašuje
3. Upřesnění
4. Typ incidentu
5. Informace o incidentu
6. Kontaktní informace
7. Kontrola a potvrzení
8. Vygenerovat formulář

TÜVNORD

NIS2

Harmonogram zavádění nového zákona



TÜVNORD

NIS2

Základní povinností společnou pro oba režimy povinností je zavádění a provádění bezpečnostních opatření. Při stanovení úrovně zabezpečení a výběru konkrétních bezpečnostních opatření bude potřeba v souladu s novým zákonem a vyhláškami zohlednit specifika organizace a důležitost jednotlivých systémů a služeb (není cílem zavádět nesmyslná a nákladná řešení tam, kde to pro organizaci nemá význam). Pokud vaše organizace kybernetickou bezpečnost do této chvíle systematicky neřešila, lze doporučit jako výchozí krok především:

- **zmapování aktuálního stavu organizace** (tzn. audit aktuálního stavu kybernetické bezpečnosti a potenciálních slabých míst) a
- vypracování tzv. **business impact analýzy** (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat).

Již v této fázi je dobré se zaměřit na **školení relevantních osob v organizaci**. Doporučujeme základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost a nezapomínat přitom i na vrcholový management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci).

Z technických opatření lze obecně doporučit nasadit **firewally** (zejména perimetrové), **antiviry** (zejména sofistikovanější EDR) a **zálohovací řešení**. Společně s prováděním **aktualizací** (tam, kde je to možné) se jedná o věci, které by měly být dávno běžnou součástí chodu každé organizace.

NIS2

Požadavky na funkci manažera kybernetické bezpečnosti vs. osobu odpovědnou za kybernetickou bezpečnost

Dle připravovaného nového zákona bude obsazení bezpečnostní role manažera kybernetické bezpečnosti povinností pro poskytovatele regulované služby v režimu vyšších povinností.
Organizace spadající do režimu nižších povinností pouze určují tzv. osobu odpovědnou za kybernetickou bezpečnost.

Manažer kybernetické bezpečnosti (režim vyšších povinností)

Manažer kybernetické bezpečnosti je jedna z klíčových bezpečnostních rolí poskytovatele regulované služby, musí být pro výkon své činnosti řádně vyškolena a musí prokázat odbornou způsobilost praxí s řízením kybernetické bezpečnosti nebo s řízením bezpečnosti informací

- po dobu nejméně tří let, nebo
- po dobu jednoho roku, pokud absolvoval studium na vysoké škole.

Příloha č. 5 k návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností pak shrnuje doporučené znalosti, zkušenosti, vzdělání a praxi, relevantní certifikaci a další případné podmínky spojené s výkonem funkce manažera kybernetické bezpečnosti.

Osoba odpovědná za kybernetickou bezpečnost (režim nižších povinností)

S ohledem na nedostupnost osob v oboru kybernetické bezpečnosti v ČR musí organizací určená osoba odpovědná za kybernetickou bezpečnost pouze absolvovat odborné školení, nebo jinak prokázat odbornou způsobilost v oblasti kybernetické bezpečnosti. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností nestanovuje žádné konkrétní požadavky, znalosti či praxi těchto osob, aby posouzení dostatečné odborné způsobilosti osoby odpovědné za kybernetickou bezpečnost mohl stanovit samotný poskytovatel regulované služby.

TÜVNORD

NIS2

Základní povinnosti regulovaných organizací

- Ohlášení poskytování regulované služby Úřadu.
- Nahlášení kontaktních údajů osob odpovědných za kybernetickou bezpečnost.
- Postupné zavádění bezpečnostních opatření.
- Hlášení kybernetických bezpečnostních incidentů.
- Provádění protiopatření vydaných NÚKIB.

TISAX® 6.0 – Trusted Information Security Assessment Exchange

Novinky TISAX® 6.0 oproti verzi 5.1

TÜVNORD

TISAX® 6.0

8.800
TISAX Participants

18
TISAX Audit Providers

>50.000
Improvements of information security since 2018

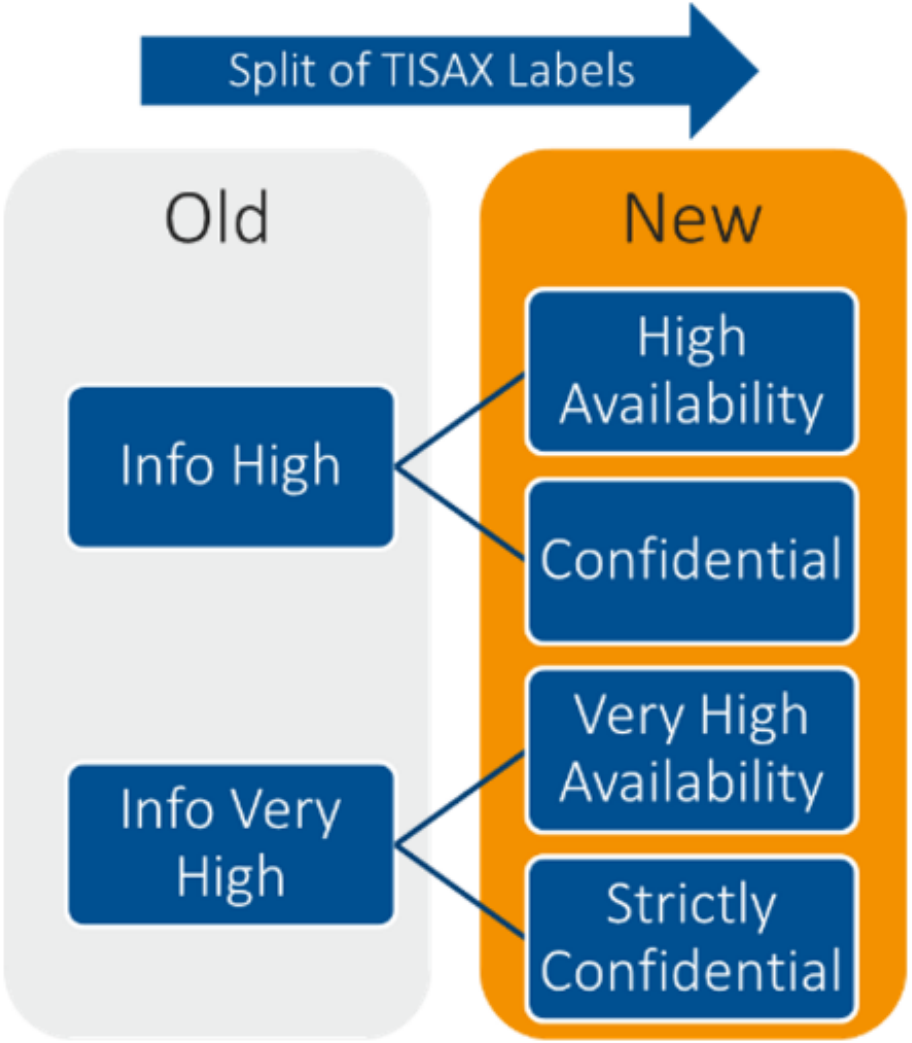
Among them >5000 critical risks that could be identified and addressed

18.800
Registered Locations

11.500
Assessed Locations with valid labels

TÜVNORD

TISAX® 6.0



Nové Tisax Labely – „Availability“ a „Confidential“

V poslední době získala pozornost významná hrozba – útoky ransomware.

I když je to také hrozba pro důvěrnost, může mít způsobená škoda ovlivněná dostupností ještě větší dopad

Největší škody ve výrobě jsou způsobeny výpadky dodávek produktů a služeb v dodavatelském řetězci

TISAX® 6.0

Requested asessment objectives/Labels		Selection
Confidential	Confidential Information	n
Strictly Confidential	Strictly Confidential Information	n
Avail High	High Availability	n
Avail Very High	Very High Availability	n
Data	Data Protection	n
Special Data	Data Protection with Special Categories of Personal Data	n
Proto Parts	Protection of Prototype Parts and Components	n
Proto Vehicles	Protection of Prototype Vehicles	n
Test Vehicles	Handling of Test Vehicles	n
Proto Events	Protection of Prototypes durings Events and Film or Photo Shoots	n

TISAX® 6.0

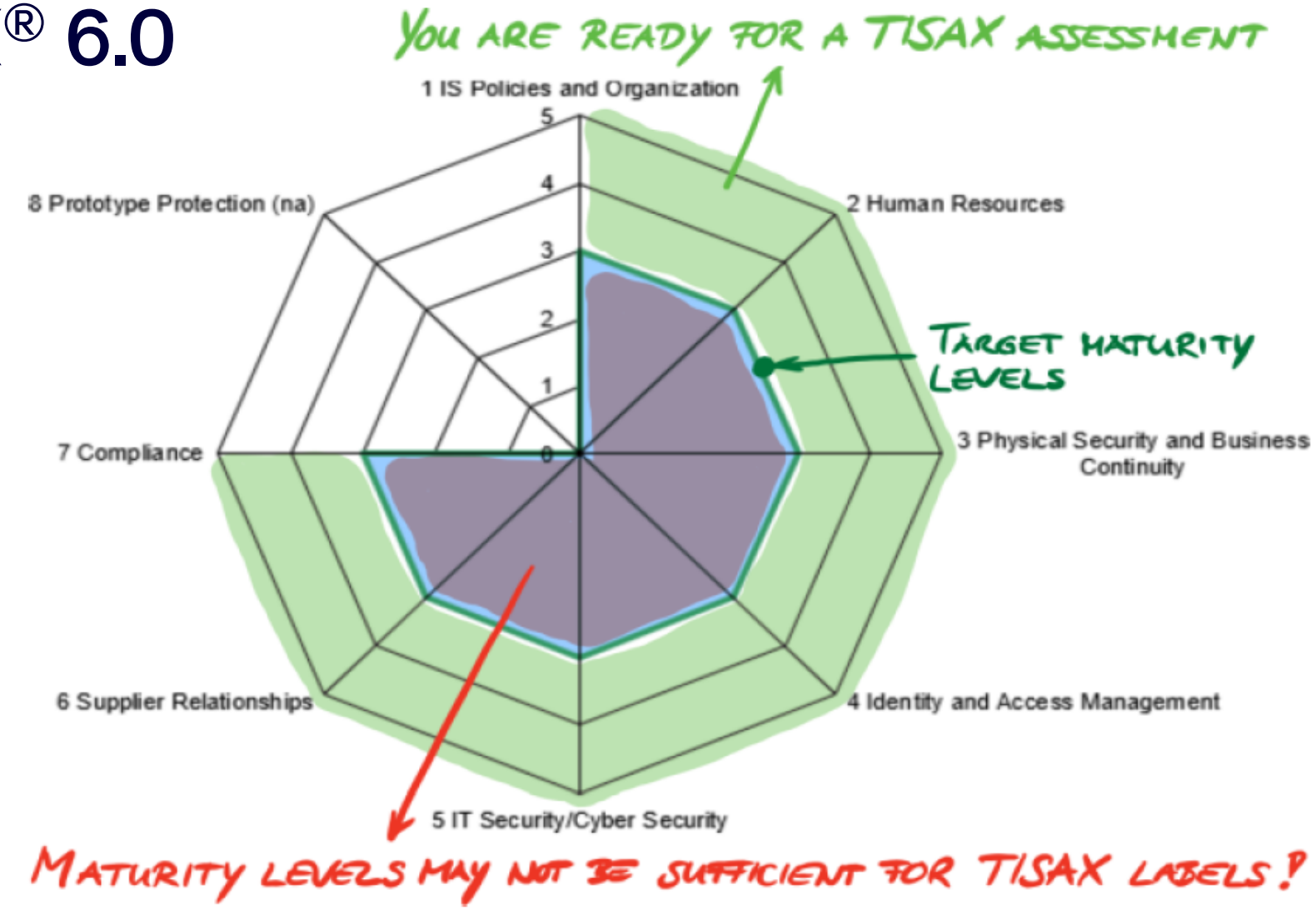
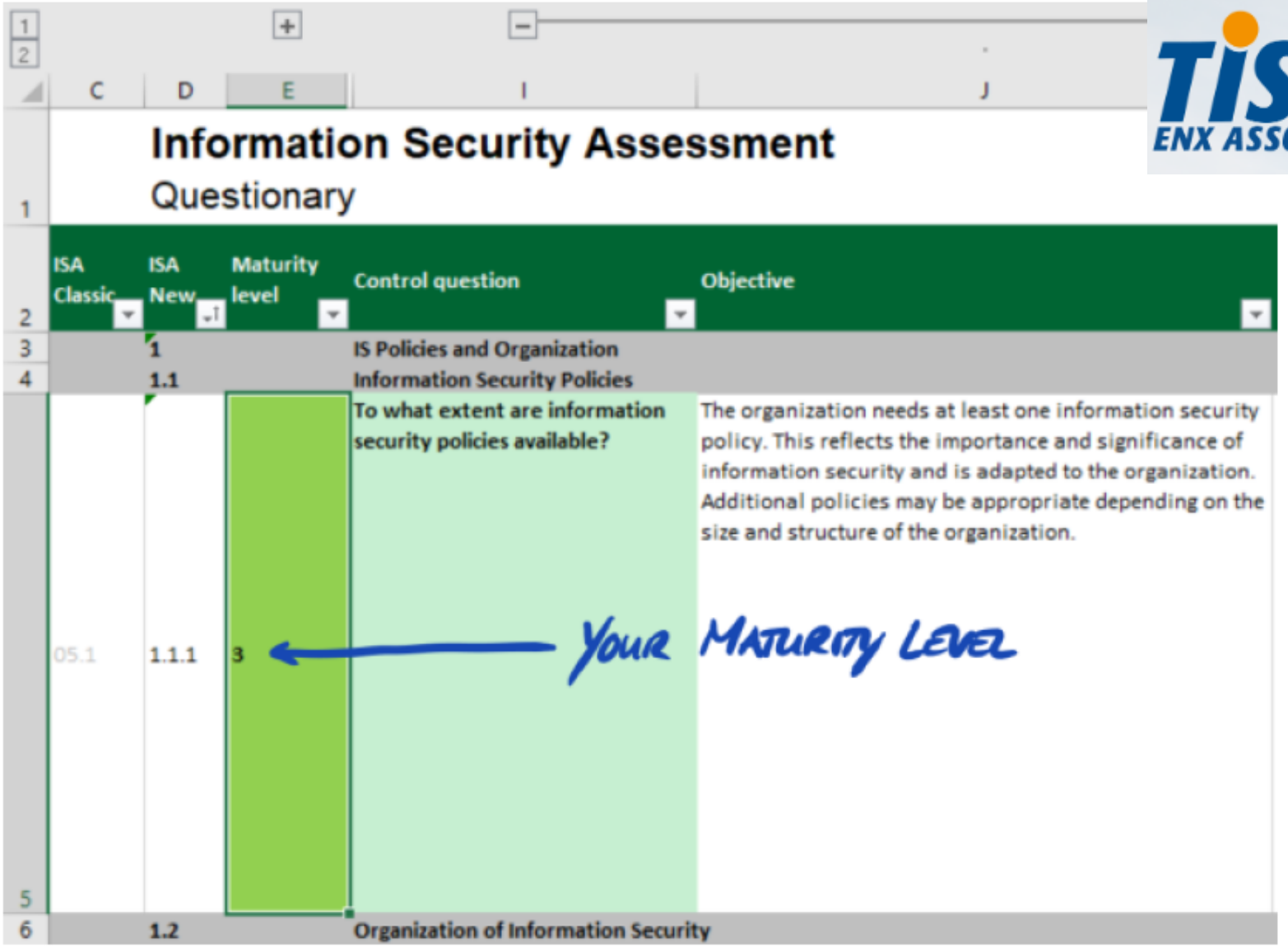


Figure 30. Screenshot: Target maturity level fulfilment in the ISA spider web diagram (Excel sheet "Results (ISA5)")

TISAX® 6.0



Information Security Assessment

Questionary

ISA Classic	ISA New	Maturity level	Control question	Objective
	1		IS Policies and Organization	
	1.1		Information Security Policies	
05.1	1.1.1	3	To what extent are information security policies available?	The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.
	1.2		Organization of Information Security	

Figure 15. Screenshot: Example of maturity level selection in the ISA document (Excel sheet "Information Security")

TISAX® 6.0

Level	Name	Description
0	Incomplete	There is no process, or the process does not work. Neexistuje žádný proces nebo proces nefunguje
1	Performed	There is a process and the result shows it works, but the process is not documented and nobody knows for sure why the process works. Existuje proces a výsledek ukazuje, že funguje, ale tento proces není zdokumentován a nikdo neví, proč tento proces funguje.
2	Managed	There are processes that work and are documented, but there are different processes for the same objective. Existují procesy, které fungují a jsou dokumentovány, ale pro stejný cíl existují různé procesy.
3	Established Implemented	There is a process that works and has documentation that is up-to-date and maintained. Existuje proces, který funguje a má dokumentaci, která je aktuální a udržovaná.
4	Predictable	Same as for level 3, plus the process is measured. 3 plus měří se procesy.
5	Optimizing	Same as for level 4, plus dedicated staff is responsible for continual improvements. 4 plus odpovědný personál je zodpovědný za neustálé zlepšování.

TISAX® 6.0

1.1 Information Security Policies

1.1.1 To what extent are information security policies available?

Do jaké míry jsou dostupné zásady bezpečnosti informací?

Organizace potřebuje alespoň jednu politiku zabezpečení informací. To odráží důležitost a význam informační bezpečnosti a je přizpůsobeno organizaci. V závislosti na velikosti a struktuře organizace mohou být vhodné další zásady.

ISO 27005

a) řízení přístupu (viz kapitola 9);
b) klasifikaci informací (a zacházení s informacemi) (viz 8.2);
c) fyzickou bezpečnost a bezpečnost prostředí (viz kapitola 11);
d) témata orientovaná na koncového uživatele, jako jsou:
   1) přijatelné použití aktiv (viz 8.1.3);
   2) čistý stůl a čistý displej (viz 11.2.9);
   3) přenos informací (viz 13.2.1);
   4) mobilní zařízení a práce na dálku (viz 6.2);
   5) omezení týkající se instalací a použití softwaru (viz 12.6.2);
e) zálohování (viz 12.3);
f) přenos informací (viz 13.2);
g) ochrana před malwarem (viz 12.2);
h) správa a řízení technických zranitelností (viz 12.6.1);
i) kryptografická opatření (viz kapitola 10);
j) bezpečnost komunikací (viz kapitola 13);
k) soukromí a ochrana osobních údajů (viz 18.1.4);
l) dodavatelské vztahy (viz kapitola 15).

TISAX® 6.0

1.4 IS Risk Management

1.4.1 To what extent are information security risks managed?

Do jaké míry jsou řízena rizika informační bezpečnosti?

Řízení rizik informační bezpečnosti se zaměřuje na včasnou detekci, hodnocení a řešení rizik za účelem dosažení cílů ochrany informační bezpečnosti. Umožňuje tak organizaci zavést adekvátní opatření na ochranu svých informačních aktiv s ohledem na související vyhlídky a rizika. Doporučuje se udržovat řízení rizik informační bezpečnosti organizace co nejjednodušší, aby bylo možné její efektivní a efektivní provoz.

ISO 27005

B.1 Příklady identifikace aktiv

B.1.1 Obecně

Aby provedla ocenění aktiv, potřebuje organizace nejprve identifikovat svá aktiva (na příslušné úrovni podrobnosti). Mohou být rozlišovány dva druhy aktiv:

- primární aktiva:
  - podnikatelské procesy a činnosti;
  - informace;
- podpůrná aktiva (na která se spoléhají primární prvky v oblasti působnosti) všech typů:
  - hardware;
  - software;
  - síť;
  - zaměstnanci;
  - lokalita;
  - struktura organizace.

TISAX® 6.0

4 Identity and Access Management

4.2 Access Management

4.2.1 To what extent are access rights assigned and managed?

Do jaké míry jsou přidělována a spravována přístupová práva?

Správa přístupových práv zajišťuje, že k informacím a IT službám mají přístup pouze oprávnění uživatelé. Za tímto účelem jsou uživatelským účtům přidělena přístupová práva.

NIS2 - Správa a ověřování identit § 20

- Použití hesel je pouze **poslední** a **dočasná** možnost!
- Min. požadavky na hesla
  - Uživatel 12 znaků
  - Admin 17 znaků
  - Technická aktiva 22 znaků
  - Možnost 64 znaků
  - Možnost všech typů znaků
  - Změna po 30 min
  - Povinná změna po 18 měsících

- **MFA** jako základ
  - Jinak evidence výjimky a **klíče/certifikáty**
    - Jinak v nástroji **ID a heslo**

- **Nástroj** pro správu a ověření identity (admina, uživatele technického aktiva) – adresářové služby, např. MS AD, RADIUS, OpenLDAP, apod.
  - Ověření identity
  - Řízení počtu neúspěšných pokusů o přihlášení
  - Zabezpečení údajů
  - Znovu ověření po nečinnosti
  - Bezpečné předání výchozích údajů (náhodné, hned změna, zneplatnění po 24 hod)
  - Centralizovaná správa

TISAX® 6.0

5 IT Security / Cyber Security

5.2 Operations Security

5.2.4 To what extent are event logs recorded and analysed?

Do jaké míry jsou logy událostí zaznamenávány a analyzovány?

Protokoly událostí podporují sledovatelnost událostí v případě bezpečnostního incidentu. To vyžaduje, aby události nezbytné k určení příčin byly zaznamenány a uloženy. Kromě toho je nutné protokolování a analýza činností v souladu s platnou legislativou (např. zákon o ochraně osobních údajů nebo zákoník práce), aby bylo možné určit, který uživatelský účet provedl změny v systémech IT.

NIS2 - Logování § 22 Požadované minimální typy logovaných událostí – min. 18 měsíců

- Přihlašování/odhlašování
- Privilegované činnosti (i neúspěšný pokus)
- Manipulace s oprávněními (i neúspěšný pokus)
- Zahájení/ukončení činnosti technických aktiv
- Kritická chybová hlášení technických aktiv
- Přístup k záznamům událostí a pokus o změnu
- Další činnosti – plyne např. z analýzy rizik

TISAX® 6.0

5.2.6 To what extent are IT systems and services tech checked (system and service audit?
Do jaké míry jsou IT systémy a služby technicky kontrolovány (systém. a servisní audit)?
Cílem technických kontrol je odhalování stavů, které mohou ohrozit dostupnost, důvěrnost nebo integritu IT systémů a služeb.

NIS2 – Aplikační bezpečnost § 25

- Používat pouze podporovaná technická aktiva a všechny aktualizace – jinak **Evidence** a **Bezpečnostní opatření**
- Pravidelné **skenování zranitelností** min. 1x/rok (z interní a externí sítě),

  Následně zhodnocení rizik a opatření
- **Penetrační testování** dle rizik min. 1x/2 roky
  - Před uvedením do provozu
  - Při významné změně

  Následně hodnocení rizik, opatření a **retest**

TISAX® 6.0

5 IT Security / Cyber Security

5.2 Operations Security

5.2.7 To what extent is the network of the organization managed?

Do jaké míry je spravována síť organizace?

IT systémy v síti jsou vystaveny různým rizikům nebo mají různé potřeby ochrany. Aby bylo možné odhalit nebo zabránit nechtěné výměně dat nebo přístupu mezi těmito IT systémy, jsou tyto systémy rozděleny do vhodných segmentů a přístup je řízen a monitorován pomocí bezpečnostních technologií.

NIS2 – Vyhodnocování kybernetických bezpečnostních událostí § 22

- **Nástroj** pro vyhodnocování kybernetických bezpečnostních událostí
  - SIEM (Security Information and Event Management)
  - Schopnost kombinovat informace z více zdrojů (např. uživatel neprošel vstupním turniketem, ale přihlásil se na počítači v objektu, apod.)
- **Aktualizovat** nastavení nástroje, užitých pravidel a alertingu
  - (**nekonečný proces**, nastavení musí odpovídat měnícím se potřebám)

TISAX® 6.0

8 Prototype Protection

Prototypová ochrana chrání fyzické prototypy, které jsou klasifikovány jako vyžadující ochranu. Prototypy zahrnují vozidla, komponenty a díly. Vlastník duševního vlastnictví k prototypu je považován za vlastníka prototypu.

Za klasifikaci potřeby ochrany prototypu je odpovědné oddělení uvádění do provozu majitele. Pro prototypy klasifikované jako vyžadující vysokou nebo velmi vysokou ochranu musí být uplatněny minimální požadavky na ochranu prototypu.

8.1 Physical and Environmental Security

Fyzická prostředí a bezpečnost prostředí

Požadavky popsané v této části platí pro všechny společnosti, které na základě svých vlastních vlastností vyrábějí, skladují nebo poskytují k použití vozidla, součásti nebo díly klasifikované jako vyžadující ochranu.

ENX VCS (Vehicle CyberSecurity) ISO/SAE 21434

TÜVNORD

ENX VCS – ENX Vehicle CyberSecurity

Rostoucí digitalizace systémů vozidel prostřednictvím automatizace, konektivity a nových konceptů mobility zvyšuje požadavky na kybernetickou bezpečnost při vývoji produktů a jejich údržbě napříč velkými částmi hodnotového řetězce automobilového průmyslu a během životního cyklu vozidel.

To vyžaduje, aby výrobci a dodavatelé řídili rizika na základě standardizovaných postupů, aby byla zachována bezpečnost vozidel a součástí v celém hodnotovém řetězci. Prostřednictvím ENX Vehicle Cyber Security Audit (ENX VCS) vytvořila asociace ENX certifikační standard pro automobilový průmysl.

Schéma ENX VCS bylo vyvinuto a je neustále vyvíjeno odborníky z automobilového průmyslu (OEM, dodavatelé a poskytovatelé služeb) v pracovní skupině ENX.

ISO/SAE 21434

ENX VCS umožňuje dodavatelům automobilového průmyslu poskytovat standardizovaný důkaz o implementovaném systému řízení kybernetické bezpečnosti (CSMS) v souladu se směrnicí ISO/PAS 5112.

To může být použito k prokázání, že společnosti splňují technické požadavky pro implementaci CSMS v dodavatelském řetězci v souladu s mezinárodní normou ISO/SAE 21434.

To znamená, že byly zavedeny nezbytné standardizované postupy pro řízení rizik. Typové schvalování vozidel podléhá velkému množství regulačních požadavků EHK OSN (Evropská hospodářská komise Organizace spojených národů). S UN R 155 se nyní rozšiřují také na kybernetickou bezpečnost vozidla. Součástí těchto požadavků je systém řízení dodavatelů zaměřený na informační a kybernetickou bezpečnost.

TÜVNORD

EU AI Act 2024/1689

TÜVNORD

EU AI Act 2024/1689

Dne 21. května 2024 – Evropská rada formálně přijala zákon EU o umělé inteligenci.

Červen–červenec 2024 – Zákon o umělé inteligenci bude zveřejněn v Úředním věstníku Evropské unie. To slouží jako formální oznámení nového zákona.

O 20 dní později – Zákon o AI „vstoupí v platnost“ 20 dní poté, co byl zveřejněn v Úředním věstníku. Od tohoto data budou následovat následující milníky podle článku 113:

Zákon přijat 1.8.2024

- ***O 6 měsíců později*** –začne platit kapitola I a kapitola II (zákazy nepřijatelného rizika AI).
- ***O 12 měsíců později*** –použije se kapitola III oddíl 4 (oznamující orgány), kapitola V (všeobecné modely umělé inteligence) , kapitola VII (správa), kapitola XII (důvěrnost a sankce) a článek 78 (důvěrnost), s výjimkou článku 101 (pokuty pro poskytovatele GPAI).
- ***O 24 měsíců později*** – Použije se zbytek zákona o AI, kromě;
- ***O 36 měsíců později*** – použije se čl. 6 odst. 1 a odpovídající povinnosti v tomto nařízení.

Kodexy správné praxe musí být připraveny 9 měsíců po vstupu v platnost podle článku 56 .

TÜVNORD

EU AI Act 2024/1689

- **Založeno na riziku:** Zakázaná AI » Vysoce riziková AI » Omezeně riziková AI » Minimálně riziková AI

Zakázaná AI

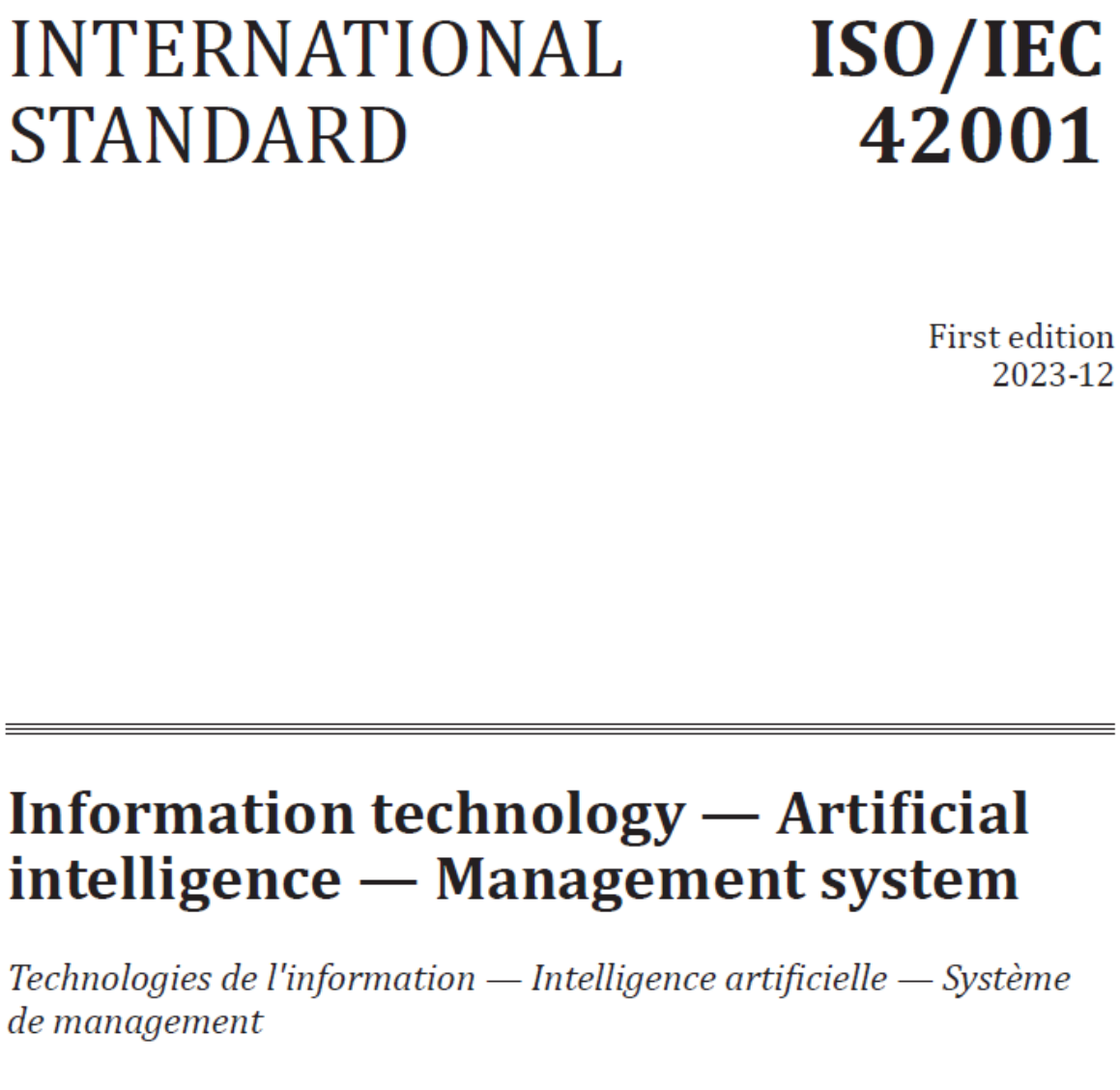
- Systémy sociálního kreditního hodnocení
- Systémy rozpoznávání emocí v práci a ve vzdělávání s výjimkou hlídání ostražitosti řidiče v dopravě
- AI využívající lidské zranitelnosti (např. věk, postižení)
- Manipulace s chováním a obcházení svobodné vůle
- Hromadný scraping obličejů pro vytváření databáze pro rozpoznávání obličejů (příklad Clearview AI)
- Biometrické kategorizační systémy využívající citlivé charakteristiky (rasa, sexuální orientace, politické či náboženské názory apod.)
- Specifické aplikace prediktivního policejního dohledu
- Použití biometrické identifikace v reálném čase policií ve veřejných prostorách (kromě omezených, předem autorizovaných situací)

Vysoce riziková AI

- Zdravotnické přístroje
- Vozidla
- Nábor, HR a řízení pracovníků
- Vzdělávání a odborný výcvik
- Ovlivňování voleb a voličů
- Přístup ke službám (např. pojištění, bankovnictví, úvěry, dávky atd.)
- Správa kritické infrastruktury (např. voda, plyn, elektřina atd.)
- Systémy rozpoznávání emocí
- Biometrická identifikace
- Vymáhání práva, pohraniční kontrola, migrace a azyl
- Správa spravedlnosti
- Specifické produkty a/nebo bezpečnostní komponenty specifických produktů

TÜVNORD

EU AI Act 2024/1689



INTERNATIONAL STANDARD

ISO/IEC 42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système de management

TÜVNORD

TÜVNORD

Otázky?

Ing. Martin Drastich, MBA, Ph.D.

M.: 604 857 854

E.: drastich@tuev-nord.cz