BEARCLAVE

Report z analýzy

Soulad Microsoft 365 a Azure s nařízením DORA

Verze	1.0
Zpracoval	Bearclave s.r.o.
Klasifikace	Veřejné — vzorový dokument

Bearclave s.r.o., Třešňová 916/16, Přímětice, 669 04 Znojmo
IČO 30007534 · DIČ CZ30007534 · zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 153837
info@bearclave.cz · bearclave.cz

1. Manažerské shrnutí

DORA	21	8	11
ani vyšší, ani nižší povinnosti ZoKB	namapovaných ustanovení DORA a RTS	z nich je splněno	mezer, z toho 1 kritická

Organizace je finančním subjektem podle nařízení DORA jako platební instituce podle čl. 2 odst. 1 písm. b) a řídí se úplným rámcem podle čl. 5 až 15 a RTS 2024/1774; povinnosti ZoKB k bezpečnostním opatřením a hlášení incidentů se na ni neuplatní. Do režimu vyšších ani nižších povinností ZoKB proto nespadá.

Z 21 namapovaných ustanovení je splněno 8, částečně 5, mezera je u 7 a 1 leží mimo Microsoft 365 a Azure. Dohromady jde o 11 mezer. Kritická je jediná: organizace nemá postup klasifikace závažných incidentů a nic nehlídá lhůtu prvotního oznámení ČNB, tedy 4 hodiny od klasifikace a nejpozději 24 hodin od zjištění.

V pořádku je ověřování, síť platební brány, šifrování při uchování a přenosu, detekce a nezávislé schvalování změn. Doporučujeme začít hlášením incidentů, privilegovanými rolemi a registrem informací, ve kterém chybí Microsoft jako poskytovatel služeb pro platby.

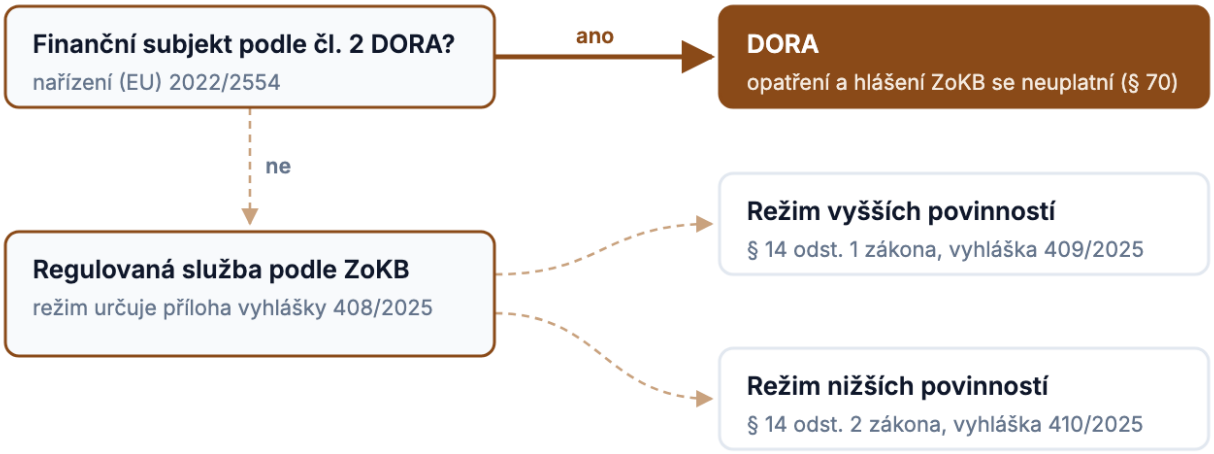
Stav 21 ustanovení DORA a RTS



2. Režim a rozsah

2.1 Určení režimu

Organizace je finančním subjektem, proto DORA



Organizace se řídí nařízením DORA; povinnosti ZoKB k bezpečnostním opatřením a hlášení se na ni neuplatní.

Vlastnost	Hodnota
Subjekt	platební instituce podle čl. 2 odst. 1 písm. b), tedy finanční subjekt
Předpis	nařízení (EU) 2022/2554 (DORA)
Rámec	úplný podle čl. 5 až 15, zjednodušený rámec podle čl. 16 se neuplatní
Technické normy	RTS 2024/1774 čl. 1 a hlava II, RTS 2025/301 pro obsah a lhůty hlášení
Hlášení	čl. 19 DORA a RTS 2025/301, příslušným orgánem je ČNB
Velikost	260 zaměstnanců, není mikropodnik (čl. 3 bod 60 DORA)
ZoKB	ani vyšší, ani nižší povinnosti; opatření a hlášení se neuplatní (§ 70)

2.1.1 Finanční subjekt

> **čl. 2 odst. 1 písm. b) nařízení (EU) 2022/2554**
>
> 1. Aniž jsou dotčeny odstavce 3 a 4, vztahuje se toto nařízení na tyto subjekty:
> ...
> b) platební instituce, včetně platebních institucí vyňatých podle směrnice (EU) 2015/2366;

2.1.2 Úplný, ne zjednodušený rámec

> **čl. 16 odst. 1 nařízení (EU) 2022/2554**
>
> 1. Články 5 až 15 tohoto nařízení se nepoužijí na malé a nepropojené investiční podniky, platební instituce vyňaté podle směrnice (EU) 2015/2366, instituce vyňaté podle směrnice 2013/36/EU, u nichž se členské státy rozhodly neuplatnit možnost uvedenou v čl. 2 odst. 4 tohoto nařízení, instituce elektronických peněz vyňaté podle směrnice 2009/110/ES a malé instituce zaměstnaneckého penzijního pojištění.

Organizace má povolení k činnosti platební instituce a platební institucí vyňatou podle čl. 32 odst. 1 směrnice (EU) 2015/2366 (čl. 3 bod 36 DORA) není. Platí pro ni proto čl. 5 až 15 a RTS 2024/1774 hlava II, přiměřeně podle zásady proporcionality:

> **čl. 4 odst. 1 nařízení (EU) 2022/2554**
>
> 1. Finanční subjekty uplatňují pravidla stanovená v kapitole II v souladu se zásadou proporcionality a s přihlédnutím ke své velikosti a celkovému rizikovému profilu a povaze, rozsahu a složitosti svých služeb, činností a operací.

2.1.3 Vztah k ZoKB

> **příloha, bod 17.4 vyhlášky č. 408/2025 Sb.**
>
> Platební instituce podle zákona o platebním styku je poskytovatelem regulované služby v režimu vyšších povinností v případě, že průměr ročních objemů jí provedených platebních transakcí, vykázaných v souladu se zákonem o platebním styku, za dobu předchozích tří účetních období přesahuje částku odpovídající 1000000000000 Kč.

> **§ 70 odst. 1 a 3 zákona č. 264/2025 Sb.**
>
> (1) Pokud přímo použitelný předpis Evropské unie nebo jiný právní předpis, který zapracovává příslušný předpis Evropské unie, stanoví povinnosti v oblasti zavádění a provádění bezpečnostních opatření nebo hlášení kybernetických bezpečnostních incidentů a tyto povinnosti mají alespoň srovnatelný účinek jako povinnosti podle tohoto zákona, ustanovení tohoto zákona upravující povinnosti zavádět a provádět bezpečnostní opatření a hlásit kybernetické bezpečnostní incidenty se neuplatní, a to včetně ustanovení o dozoru nad dodržováním uvedených povinností.
>
> ...
>
> (3) Za ustanovení se srovnatelným účinkem jako povinnosti obsažené v tomto zákoně podle odstavce 1 se dále považují taková ustanovení přímo použitelného předpisu Evropské unie, o nichž to přímo použitelný předpis Evropské unie sám stanoví.

> **čl. 1 odst. 2 nařízení (EU) 2022/2554**
>
> 2. Ve vztahu k finančním subjektům určeným jako základní nebo důležité subjekty podle vnitrostátních předpisů provádějících článek 3 směrnice (EU) 2022/2555 se toto nařízení pro účely článku 4 uvedené směrnice považuje za odvětvový právní akt Unie.

Situace	Důsledek podle ZoKB
Průměrný roční objem transakcí nepřesahuje 1 bilion Kč (dnešní stav)	Organizace není poskytovatelem regulované služby, režim vyšších ani nižších povinností se neurčuje.
Objem přesahuje 1 bilion Kč	Organizace by byla v režimu vyšších povinností, ale podle § 70 odst. 1 a 3 a čl. 1 odst. 2 DORA se povinnosti ZoKB k opatřením a hlášení včetně dozoru neuplatní. Ostatní povinnosti ZoKB by se posoudily zvlášť.

2.2 Prostředí

Prostředí	Hodnota
Microsoft 365	E5 (včetně Entra ID P2) pro všechny zaměstnance, 14 hostů dodavatele brány
Azure	dvě předplatná, produkce a test, region West Europe
Platební brána	App Service za Application Gateway s WAF, API Management, Azure SQL Database, Key Vault
Dohled	Microsoft Sentinel, vlastní tým tří lidí s pohotovostí
Přístup analýzy	jen čtení, bez zásahu do provozu, záznamy za 90 dní

Zásadní nebo důležité funkce podle čl. 3 bodu 22 DORA určila organizace, analýza je přebírá

Funkce	Kde běží	Zásadní nebo důležitá	Co z ní analýza pokrývá
Provádění platebních transakcí	platební brána v Azure, správa přes Entra ID	ano	celou bránu kromě kódu aplikace, který vyvíjí dodavatel
Komunikace s klienty a dokumenty	Microsoft 365	ne	poštu, SharePoint, OneDrive, Teams a zařízení v Intune

2.3 Co analýza není

- Není to právní posouzení. Výklad DORA, technických norem a zákona patří právníkovi.
- Netestuje digitální provozní odolnost podle čl. 24 až 27 a nezahrnuje penetrační testování na základě hrozeb (TLPT).
- Nehodnotí smlouvy, nepokrývá nic mimo Microsoft 365 a Azure a nezaručuje soulad s DORA jako celkem.

3. Relevantní ustanovení

DORA je nařízení (EU) 2022/2554, RTS 2024/1774 a RTS 2025/301 jsou nařízení Komise v přenesené pravomoci, která DORA doplňují. Tabulka ukazuje, jak se oblasti promítají do Microsoft 365 a Azure.

Oblast	DORA	RTS 2024/1774	Odraz v M365 a Azure	Mapováno
Řízení a organizace, rámec a strategie	čl. 5, 6	čl. 2, 3, 27	Žádný	—
Systémy IKT a identifikace aktiv	čl. 7, 8	čl. 4, 5	Částečný	1
Řízení přístupu a identit	čl. 9 odst. 4 písm. c), d)	čl. 20, 21	Přímý	3
Šifrování a kryptografické klíče	čl. 9 odst. 4 písm. d)	čl. 6, 7	Přímý	2
Bezpečnost operací a sítí	čl. 9 odst. 2 až 4	čl. 8 až 14	Přímý	4
Projekty, vývoj a změny	čl. 9 odst. 4 písm. e)	čl. 15 až 17	Částečný	2
Fyzická bezpečnost a lidské zdroje	čl. 9 odst. 4 písm. c)	čl. 18, 19	Žádný	—
Detekce	čl. 10	čl. 22, 23	Přímý	2
Reakce, obnova a zálohování	čl. 11, 12	čl. 24 až 26	Částečný	2
Poučení, školení a komunikace	čl. 13, 14	—	Žádný	—
Zjednodušený rámec	čl. 16	hlava III	neuplatní se	—
Klasifikace a hlášení incidentů	čl. 17 až 19, 23 a RTS 2025/301	—	Částečný	2
Testování digitální provozní odolnosti	čl. 24 až 27	—	Žádný	—
Třetí strany	čl. 28 až 30	—	Částečný	3

Mapuje se 21 ustanovení z 9 oblastí s odrazem, v každé ta, která nastavení přímo naplňuje nebo dokládá. Nejde o výčet všech povinností oblasti. Oblasti bez odrazu a organizační povinnosti jsou v příloze Povinnosti mimo rozsah.

4. Mapování

U každého ustanovení je doslovné znění, překlad do nastavení Microsoft 365 a Azure a zjištěný stav.

Přehled ustanovení. Splněno: platí v celém rozsahu Microsoft 365 a Azure. Částečně: s výjimkami. Mezera: chybí. Mimo rozsah: leží mimo Microsoft 365 a Azure, uveden je jen podklad.

Předpis	Ustanovení	Obsah	Stav	Mezera
DORA	čl. 8 odst. 4	Soupis aktiv a závislostí	Splněno	—
RTS 2024/1774	čl. 21 písm. e) bod ii)	Privilegovaný přístup podle potřeby	Mezera	M-01
RTS 2024/1774	čl. 21 písm. e) bod iv)	Přezkum přístupových práv	Mezera	M-02
RTS 2024/1774	čl. 21 písm. f) bod ii)	Silné ověření	Splněno	—
RTS 2024/1774	čl. 6 odst. 1 a 2 písm. a)	Šifrování při uchování a přenosu	Splněno	—
RTS 2024/1774	čl. 7 odst. 2	Ochrana kryptografických klíčů	Částečně	M-03
RTS 2024/1774	čl. 10 odst. 2	Skenování zranitelností	Splněno	—
RTS 2024/1774	čl. 10 odst. 4 písm. d)	Lhůty pro instalaci oprav	Mezera	M-04
RTS 2024/1774	čl. 12 odst. 2	Doba uchovávání protokolů	Mezera	M-05
RTS 2024/1774	čl. 13 písm. a) a g)	Segmentace a hranice sítě	Splněno	—
RTS 2024/1774	čl. 16 odst. 5 písm. a)	Produkční data mimo produkci	Mezera	M-06
RTS 2024/1774	čl. 17 odst. 1 písm. b)	Nezávislé schvalování změn	Splněno	—
DORA	čl. 10 odst. 2	Prahové hodnoty a výstrahy	Splněno	—
RTS 2024/1774	čl. 23 odst. 2	Výstrahy u zásadních funkcí	Splněno	—
DORA	čl. 17 odst. 3 písm. b)	Evidence a klasifikace incidentů	Částečně	M-07
RTS 2025/301	čl. 5 odst. 1 písm. a) až c)	Lhůty hlášení incidentu	Mezera	M-07
DORA	čl. 12 odst. 1 písm. a)	Rozsah a frekvence zálohování	Částečně	M-08
DORA	čl. 12 odst. 2	Záložní systémy a test obnovy	Částečně	M-09
DORA	čl. 28 odst. 3	Registr informací	Částečně	M-10
DORA	čl. 28 odst. 8	Strategie ukončení	Mezera	M-11
DORA	čl. 30 odst. 2 písm. b) a d)	Smluvní ujednání s Microsoftem	Mimo rozsah	—

4.1 Identifikace aktiv

čl. 8 odst. 4 — Soupis aktiv a závislostí (DORA)

> **čl. 8 odst. 4 nařízení (EU) 2022/2554**
>
> 4. Finanční subjekty identifikují všechna informační aktiva a aktiva v oblasti IKT, včetně těch na vzdálených pracovištích, síťové zdroje a hardwarové vybavení a evidují ta, která jsou považovaná za kritická. Evidují konfiguraci informačních aktiv a aktiv v oblasti IKT a propojení a vzájemné závislosti různých informačních aktiv a aktiv v oblasti IKT.

Překlad do Microsoft 365 a Azure

- Zařízení v Intune, prostředky Azure v Resource Graph se značkou kritičnosti.
- Závislosti platební brány: mapa aplikace v Application Insights.

Zjištěno	Stav	Mezera
V rozsahu Microsoft 365 a Azure úplné: 284 zařízení v Intune, prostředky produkce se značkami kritičnosti a funkce, mapa závislostí brány.	Splněno	—

4.2 Řízení přístupu a identit

čl. 21 písm. e) bod ii) — Privilegovaný přístup podle potřeby (RTS 2024/1774)

> **čl. 21 písm. e) bod ii) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> e) postupy v oblasti správy účtů pro udělování, změnu nebo odebírání přístupových práv k uživatelským a obecným účtům, včetně obecných účtů správců, zahrnující všechny následující prvky:
>
> …
>
> ii) přidělování privilegovaného, nouzového a administrátorského přístupu podle potřeby nebo v režimu ad hoc u všech systémů IKT;

Překlad do Microsoft 365 a Azure

- PIM pro role Entra ID a Azure: jen oprávněná přiřazení, aktivace na omezenou dobu.
- Aktivaci nejvyšších rolí schvaluje druhá osoba, trvale jen nouzové účty.

Zjištěno	Stav	Mezera
Všech 11 přiřazení privilegovaných rolí v Entra ID a 6 přiřazení role Vlastník v produkci je trvalých. PIM z licence E5 (Entra ID P2) se nepoužívá.	Mezera	M-01

čl. 21 písm. e) bod iv) — Přezkum přístupových práv (RTS 2024/1774)

> **čl. 21 písm. e) bod iv) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> e) postupy v oblasti správy účtů pro udělování, změnu nebo odebírání přístupových práv k uživatelským a obecným účtům, včetně obecných účtů správců, zahrnující všechny následující prvky:
>
> ...
>
> iv) aktualizace přístupových práv, pokud je nezbytné provést změny a jinak nejméně jednou ročně u všech systémů IKT, které nepodporují zásadní nebo důležité funkce, a nejméně jednou za šest měsíců u systémů IKT, které podporují zásadní nebo důležité funkce;

Překlad do Microsoft 365 a Azure

- Přezkumy přístupu v Entra ID po šesti měsících pro všechny přístupy k platební bráně.
- Ostatní skupiny, aplikace a hosté jednou ročně, nepotvrzený přístup se odebere.

Zjištěno	Stav	Mezera
Přezkumy přístupu nastavené nejsou, i když je licence E5 obsahuje. Poslední ruční kontrola přístupů k bráně je z listopadu 2025 a nemá zapsaný výsledek.	**Mezera**	M-02

čl. 21 písm. f) bod ii) — Silné ověření (RTS 2024/1774)

> **čl. 21 písm. f) bod ii) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> f) metody ověřování zahrnující všechny tyto prvky:
>
> ...
>
> ii) používání metod silného ověření v souladu s osvědčenými postupy a technikami pro vzdálený přístup do sítě finančního subjektu, pro privilegovaný přístup, pro přístup k aktivům v oblasti IKT podporujícím zásadní nebo důležité funkce nebo k veřejně přístupným aktivům v oblasti IKT;

Překlad do Microsoft 365 a Azure

- Conditional Access: vícefaktorové ověření pro všechny, starší protokoly blokované.
- Síla ověření odolná proti phishingu pro správcovské role a správu Azure.
- Veřejné rozhraní brány: API Management ověřuje obchodníky certifikátem klienta a tokenem OAuth 2.0.

Zjištěno	Stav	Mezera
Vícefaktorové ověření platí pro všechny účty, správci používají klíč FIDO2, obchodníci certifikát a token.	**Splněno**	—

4.3 Šifrování a kryptografické klíče

čl. 6 odst. 1 a 2 písm. a) — Šifrování při uchování a přenosu (RTS 2024/1774)

> **čl. 6 odst. 1 a 2 písm. a) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 1. V rámci svých politik, postupů, protokolů a nástrojů v oblasti bezpečnosti IKT uvedených v čl. 9 odst. 2 nařízení (EU) 2022/2554 finanční subjekty vypracují, zdokumentují a zavedou politiku šifrování a kryptografických kontrol.
> 2. Finanční subjekty navrhnou politiku šifrování a kryptografických kontrol uvedenou v odstavci 1 na základě výsledků schválené klasifikace dat a posuzování rizika v oblasti IKT. Tato politika obsahuje pravidla pro všechny následující oblasti:
> a) šifrování údajů během jejich uchovávání a přenosu;

Překlad do Microsoft 365 a Azure

- Minimálně TLS 1.2 na bráně aplikací, API Management, App Service a Azure SQL.
- Data v klidu: šifrování Azure SQL a úložiště, BitLocker na zařízeních přes Intune.

Zjištěno	Stav	Mezera
Pravidla politiky šifrování pro uchování a přenos jsou zavedená: všude TLS 1.2 a vyšší, data v klidu šifrovaná, BitLocker na všech zařízeních s Windows.	Splněno	—

čl. 7 odst. 2 — Ochrana kryptografických klíčů (RTS 2024/1774)

> **čl. 7 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 2. Finanční subjekty určí a zavedou kontrolní mechanismy na ochranu kryptografických klíčů během celého jejich životního cyklu před ztrátou, neoprávněným přístupem, zveřejněním a modifikací. Finanční subjekty navrhnou tyto kontrolní mechanismy na základě výsledků schválené klasifikace dat a posuzování rizika v oblasti IKT.

Překlad do Microsoft 365 a Azure

- Šifrování Azure SQL vlastním klíčem v Key Vault Premium nebo v Managed HSM.
- Key Vault s ochranou proti vymazání, rolemi v PIM a zásadou rotace klíčů.

Zjištěno	Stav	Mezera
Politika organizace předepisuje pro platební údaje vlastní klíč, databáze brány má klíč spravovaný Microsoftem. Nařízení vlastní klíč nepředepisuje, jde o rozpor s vlastní politikou.	Částečně	M-03

4.4 Bezpečnost operací a sítí

čl. 10 odst. 2 — Skenování zranitelností (RTS 2024/1774)

> **čl. 10 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 2. Postupy řízení zranitelností uvedené v odstavci 1:
>
> …
>
> b) zajišťují provádění automatizovaného skenování a posuzování zranitelností aktiv v oblasti IKT, přičemž četnost a rozsah těchto činností musí být úměrné klasifikaci stanovené v souladu s čl. 8 odst. 1 nařízení (EU) 2022/2554 a celkovému rizikovému profilu aktiva v oblasti IKT;
>
> …
>
> Pro účely písmene b) u aktiv v oblasti IKT podporujících zásadní nebo důležité funkce provádějí finanční subjekty automatizované skenování a posuzování zranitelností alespoň jednou týdně.

Překlad do Microsoft 365 a Azure

- Defender Vulnerability Management z licence E5 posuzuje zařízení průběžně.
- Defender for SQL a plánovaný běh kanálu skenují databázi a knihovny brány týdně.

Zjištěno	Stav	Mezera
Zařízení se posuzují průběžně, databáze brány i knihovny aplikace každý týden, knihovny navíc při každém sestavení.	**Splněno**	—

čl. 10 odst. 4 písm. d) — Lhůty pro instalaci oprav (RTS 2024/1774)

> **čl. 10 odst. 4 písm. d) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 4. Postupy řízení oprav uvedené v odstavci 3:
>
> …
>
> d) stanoví lhůty pro instalaci oprav a aktualizací softwaru a hardwaru a postupy eskalace v případě, že tyto lhůty nelze dodržet.

Překlad do Microsoft 365 a Azure

- Okruhy aktualizací v Intune s termínem vynucení instalace a restartu.
- Defender Vulnerability Management: náprava s termínem podle závažnosti.

Zjištěno	Stav	Mezera
Lhůty ani eskalace stanovené nejsou. Okruhy aktualizací nemají termín, 31 % zařízení je víc než dva měsíce pozadu, 18 kritických zranitelností je otevřených přes 30 dní.	**Mezera**	M-04

čl. 12 odst. 2 — Doba uchovávání protokolů (RTS 2024/1774)

čl. 12 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1774

2. Postupy, protokoly a nástroje pro vedení protokolů uvedené v odstavci 1 obsahují všechny níže uvedené náležitosti:
a) identifikace událostí, které mají být protokolovány, doba uchovávání protokolů a opatření k zabezpečení a zpracování dat z protokolů s ohledem na účel, pro který jsou protokoly pořizovány;
…

Pro účely písmene a) stanoví finanční subjekty dobu uchovávání s přihlédnutím k obchodním cílům a cílům v oblasti bezpečnosti informací, důvodu pro zaznamenání události do protokolů a výsledkům posouzení rizik v oblasti IKT.

Překlad do Microsoft 365 a Azure

- Doba uchovávání podle druhu protokolu, zapsaná v postupu vedení protokolů.
- Celková retence tabulek v Log Analytics podle ní (až 12 let), včetně záznamů Entra ID.

Zjištěno	Stav	Mezera
Doba stanovená není, platí výchozí nastavení: Sentinel 90 dní pro všechny tabulky včetně protokolů brány, přihlášení v Entra ID 30 dní.	Mezera	M-05

čl. 13 písm. a) a g) — Segmentace a hranice sítě (RTS 2024/1774)

čl. 13 písm. a) a g) nařízení v přenesené pravomoci (EU) 2024/1774

Finanční subjekty v rámci ochranných opatření zajišťujících bezpečnost sítí proti vniknutí a zneužití údajů vypracují, zdokumentují a zavedou politiky, postupy, protokoly a nástroje pro řízení bezpečnosti sítí, včetně všech následujících prvků:
a) oddělení a segmentace systémů a sítí IKT s ohledem na:
i) zásadnost nebo důležitost funkce, kterou tyto systémy a sítě IKT podporují;
…
g) zabezpečení síťového provozu mezi interními sítěmi a internetem a dalšími externími připojeními;

Překlad do Microsoft 365 a Azure

- Brána v samostatné virtuální síti, z internetu jen přes Application Gateway s WAF.
- Azure SQL a Key Vault jen přes privátní koncové body, veřejný přístup vypnutý.

Zjištěno	Stav	Mezera
Z internetu je dostupná jen brána aplikací s WAF v režimu blokování. API Management, App Service, databáze a Key Vault přijímají provoz jen z vnitřní sítě.	Splněno	—

4.5 Vývoj a změny

čl. 16 odst. 5 písm. a) — Produkční data mimo produkci (RTS 2024/1774)

> **čl. 16 odst. 5 písm. a) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 5. Postup uvedený v odstavci 2 stanoví, že:
> a) v neprodukčních prostředích jsou uchovávána pouze anonymizovaná, pseudonymizovaná nebo náhodně vybraná produkční data;

Překlad do Microsoft 365 a Azure

- Testovací databáze s anonymizovanými nebo pseudonymizovanými daty.
- Export produkční databáze jen pro provoz, dynamické maskování nestačí.

Zjištěno	Stav	Mezera
Testovací databáze je obnovená produkční záloha z března 2026 s úplnými údaji o klientech a platbách. Výjimku podle odst. 6 nikdo neschválil.	Mezera	M-06

čl. 17 odst. 1 písm. b) — Nezávislé schvalování změn (RTS 2024/1774)

> **čl. 17 odst. 1 písm. b) nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 1. V rámci ochranných opatření pro zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů finanční subjekty zahrnou do postupů řízení změn v oblasti IKT uvedených v čl. 9 odst. 4 písm. e) nařízení (EU) 2022/2554 v souvislosti se všemi změnami softwarových, hardwarových a firmwarových komponent, systémů nebo bezpečnostních parametrů všechny následující prvky:
> ...
> b) mechanismy zajišťující nezávislost funkcí, které schvalují změny, a funkcí, které jsou odpovědné za žádosti o tyto změny a jejich provádění;

Překlad do Microsoft 365 a Azure

- Do produkce jen kanálem v Azure DevOps se schválením jinou osobou než autorem.
- Vývojáři a dodavatel bez zápisu v produkci, změny mimo kanál ukáže protokol aktivit.

Zjištěno	Stav	Mezera
Každé nasazení za 90 dní schválil někdo jiný než autor změny. Přímá změna produkce mimo kanál se neobjevila.	Splněno	—

4.6 Detekce

čl. 10 odst. 2 — Prahové hodnoty a výstrahy (DORA)

> **čl. 10 odst. 2 nařízení (EU) 2022/2554**
>
> 2. Detekční mechanismy uvedené v odstavci 1 umožňují vícestupňovou kontrolu, stanoví prahové hodnoty a kritéria výstrah pro spuštění a zahájení postupů reakce na incidenty související s IKT, mimo jiné automatické výstražné mechanismy pro příslušné pracovníky odpovědné za reakce na incidenty související s IKT.

Překlad do Microsoft 365 a Azure

- Analytická pravidla Sentinelu a incidenty Defender XDR se závažností jako prahem.
- Incident vysoké a střední závažnosti jde automaticky do Teams a na telefon pohotovosti.

Zjištěno	Stav	Mezera
Sentinel má 71 aktivních pravidel, pohotovost dostává incidenty automaticky i mimo pracovní dobu.	Splněno	—

čl. 23 odst. 2 — Výstrahy u zásadních funkcí (RTS 2024/1774)

> **čl. 23 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1774**
>
> 2. Mechanismus včasné detekce neobvyklých aktivit, včetně problémů s fungováním sítě IKT a incidentů souvisejících s IKT, jak je uveden v čl. 10 odst. 1 nařízení (EU) 2022/2554, umožní finančním subjektům:
>
> …
>
> b) určit neobvyklé aktivity a chování a zavést nástroje, které zasílají výstrahy týkající se neobvyklých aktivit a chování, přinejmenším u aktiv v oblasti IKT a informačních aktiv podporujících zásadní nebo důležité funkce;
>
> …
>
> Pro účely písmene b) zahrnují nástroje uvedené v tomto písmenu i nástroje, které zasílají automatické výstrahy na základě předem stanovených pravidel pro identifikaci anomálií, které mají dopad na úplnost a integritu zdrojů údajů nebo sběru protokolů.

Překlad do Microsoft 365 a Azure

- Pravidla Sentinelu nad protokoly WAF, API Management, App Service, SQL, Key Vault.
- Monitorování zdraví Sentinelu a pravidlo na zdroj protokolů, který přestal posílat data.

Zjištěno	Stav	Mezera
Nad aktivy platební brány běží 14 pravidel. Zdroj protokolů, který mlčí přes dvě hodiny, vytvoří incident.	Splněno	—

4.7 Klasifikace a hlášení incidentů

čl. 17 odst. 3 písm. b) — Evidence a klasifikace incidentů (DORA)

> **čl. 17 odst. 3 písm. b) nařízení (EU) 2022/2554**
>
> 3. Proces řízení incidentů souvisejících s IKT uvedený v odstavci 1:
>
> ...
>
> b) stanoví postupy k identifikaci, sledování, evidenci, kategorizaci a klasifikaci incidentů souvisejících s IKT podle jejich priority a závažnosti a podle toho, jak zásadní jsou zasažené služby v souladu s kritérii vymezenými v čl. 18 odst. 1;

Překlad do Microsoft 365 a Azure

- Incident v Sentinelu s kategorií, závažností a zasaženou službou podle watchlistu aktiv.
- Úkol v incidentu: posoudit kritéria čl. 18 odst. 1 a zapsat výsledek klasifikace.
- Provozní výpadky brány ve stejné evidenci, klasifikují se i incidenty související s platbami (čl. 23).

Zjištěno	Stav	Mezera
Incidenty mají závažnost a řešitele, chybí kategorie, zasažená služba i posouzení podle čl. 18 odst. 1. Výpadky brány jsou jen v tiketech provozu.	Částečně	M-07

čl. 5 odst. 1 písm. a) až c) — Lhůty hlášení incidentu (RTS 2025/301)

> **čl. 5 odst. 1 písm. a) až c) nařízení v přenesené pravomoci (EU) 2025/301**
>
> 1. Finanční subjekty předloží prvotní oznámení a průběžnou a závěrečnou zprávu podle čl. 19 odst. 4 písm. a), b) a c) nařízení (EU) 2022/2554 v těchto lhůtách:
> a) v případě prvotní zprávy: co nejdříve, v každém případě však do čtyř hodin od klasifikace incidentu souvisejícího s IKT jako závažného incidentu souvisejícího s IKT a nejpozději do 24 hodin od okamžiku, kdy se finanční subjekt o incidentu souvisejícím s IKT dozvěděl;
> b) v případě průběžné zprávy: nejpozději do 72 hodin od předložení prvotního oznámení, a to i v případech, kdy se stav nebo způsob řešení incidentu nezměnily, jak je uvedeno v čl. 19 odst. 4 písm. b) nařízení (EU) 2022/2554. Aktualizovanou průběžnou zprávu předloží finanční subjekty bez zbytečného odkladu a v každém případě po obnovení běžných činností;
> c) v případě závěrečné zprávy: nejpozději jeden měsíc buď po předložení průběžné zprávy, nebo po předložení případné poslední aktualizované průběžné zprávy.

Překlad do Microsoft 365 a Azure

- Po klasifikaci jako závažný vytvoří automatizace úkoly s termíny 4 hodiny od klasifikace a 24 hodin od zjištění.
- Playbook upozorní před lhůtou 72 hodin na průběžnou a měsíce na závěrečnou zprávu.
- Časy zjištění, klasifikace a hlášení ČNB zapsané v incidentu jako doklad.

Zjištěno	Stav	Mezera
Postup ani hlídání lhůt neexistuje. Nejde doložit, kdy se organizace o incidentu dozvěděla, kdy ho klasifikovala a kdy hlásila ČNB.	Mezera	M-07

4.8 Zálohování a obnova

čl. 12 odst. 1 písm. a) — Rozsah a frekvence zálohování (DORA)

> **čl. 12 odst. 1 písm. a) nařízení (EU) 2022/2554**
>
> 1. Pro účely zajištění obnovy systémů IKT a dat s minimální odstávkou, omezenými výpadky fungování a ztrátami finanční subjekty jako součást svého rámce pro řízení rizika v oblasti IKT vypracují a zdokumentují:
> a) politiky a postupy zálohování uvádějící rozsah dat, která se zálohují, a minimální frekvenci zálohování, a to na základě významu informací nebo úrovně důvěrnosti dat;

Překlad do Microsoft 365 a Azure

- Azure SQL: obnova k bodu v čase a dlouhodobé zálohy podle politiky.
- Microsoft 365: Microsoft 365 Backup nebo zálohovací služba třetí strany.

Zjištěno	Stav	Mezera
Politika určuje rozsah a frekvenci jen pro databázi brány. Data Microsoft 365 se nezálohují a za retenčními lhůtami je Microsoft neobnoví.	Částečně	M-08

čl. 12 odst. 2 — Záložní systémy a test obnovy (DORA)

> **čl. 12 odst. 2 nařízení (EU) 2022/2554**
>
> 2. Finanční subjekty zřídí záložní systémy, které lze aktivovat v souladu s politikami a postupy zálohování, jakož i postupy a metodami obnovy provozu. Aktivace záložních systémů nesmí ohrozit bezpečnost sítí a informačních systémů ani dostupnost, hodnověrnost, integritu nebo důvěrnost údajů. Pravidelně se provádí testování postupů zálohování a postupů a metod obnovy.

Překlad do Microsoft 365 a Azure

- Pravidelná obnova Azure SQL do samostatné databáze s kontrolou dat a protokolem.
- Geo-redundantní zálohy nebo skupina převzetí služeb pro obnovu v jiném regionu.

Zjištěno	Stav	Mezera
Databáze má obnovu k bodu v čase 14 dní a geo-redundantní zálohy. Obnova se nikdy nezkoušela, protokol ani změřená doba obnovy nejsou.	Částečně	M-09

4.9 Třetí strany

čl. 28 odst. 3 — Registr informací (DORA)

> **čl. 28 odst. 3 nařízení (EU) 2022/2554**
>
> 3. Jakožto součást svého rámce pro řízení rizika v oblasti IKT finanční subjekty na úrovni subjektu a na subkonsolidované a konsolidované úrovni vedou a aktualizují registr informací s ohledem na všechna smluvní ujednání o využívání služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran.
> Smluvní ujednání uvedená v prvním pododstavci se řádně zdokumentují, přičemž se rozlišuje mezi těmi, která se týkají služeb IKT podporujících zásadní nebo důležité funkce a těmi, která se jich netýkají.

Překlad do Microsoft 365 a Azure

- Microsoft v registru s ujednáními pro Microsoft 365 a Azure, služby z Resource Graph.
- Služby Azure platební brány označené jako podpora zásadní nebo důležité funkce.

Zjištěno	Stav	Mezera
Registr uvádí Microsoft jedním řádkem jako dodavatele Microsoft 365. Azure v něm není a služby brány nejsou označené jako podpora zásadní funkce.	Částečně	M-10

čl. 28 odst. 8 — Strategie ukončení (DORA)

čl. 28 odst. 8 nařízení (EU) 2022/2554

8. U služeb IKT podporujících zásadní nebo důležité funkce zavedou finanční subjekty strategie ukončení smluvního vztahu.

...

Plány ukončení smluvního vztahu musí být komplexní, zdokumentované a splňovat kritéria vymezená v čl. 4 odst. 2, musí být dostatečně otestovány a pravidelně přezkoumávány.
Finanční subjekty identifikují alternativní řešení a vypracují plány přechodu, které jim umožní odebrání nasmlouvaných služeb IKT a příslušných dat od poskytovatele služeb IKT z řad třetích stran a jejich bezpečný a integrovaný přenos k alternativnímu poskytovateli, nebo jejich začlenění v rámci vlastní organizace.

Překlad do Microsoft 365 a Azure

- Strategii a plán zpracuje organizace. Podklad z Azure: celá brána popsaná kódem.
- Vyzkoušený export dat Azure SQL a konfigurace API Management mimo Azure.

Zjištěno	Stav	Mezera
Strategie ani plán ukončení pro Azure neexistují. Kódem je popsaná jen App Service, zbytek brány vznikl ručně v portálu.	Mezera	M-11

čl. 30 odst. 2 písm. b) a d) — Smluvní ujednání s Microsoftem (DORA)

čl. 30 odst. 2 písm. b) a d) nařízení (EU) 2022/2554

2. Smluvní ujednání o využívání služeb IKT obsahují přinejmenším tyto prvky:

...

b) místa, konkrétně regiony nebo země, kde mají být nasmlouvané nebo subdodavatelem zajišťované funkce a služby IKT poskytovány a kde mají být zpracovávána data, včetně místa jejich uchovávání, a povinnost poskytovatele služeb IKT z řad třetích stran oznámit finančnímu subjektu předem, plánuje-li změnu těchto míst;

...

d) ustanovení o zajištění přístupu, obnovy a vrácení ve snadno přístupném formátu osobních a jiných než osobních údajů zpracovávaných finančním subjektem v případě platební neschopnosti, řešení krize nebo přerušení činností poskytovatele služeb IKT z řad třetích stran nebo v případě ukončení smluvních ujednání;

Překlad do Microsoft 365 a Azure

- Organizace porovná smluvní dokumenty Microsoftu pro finanční služby s čl. 30.
- Podklad k písm. b): regiony Azure a umístění dat Microsoft 365.

Zjištěno	Stav	Mezera
Nastavením splnit nejde, výsledek porovnání patří do registru. Azure běží ve West Europe, Microsoft 365 v EU.	Mimo rozsah	—

5. Mezery

Tři mezery v plném znění, seřazené podle priority. Všech 11 je v registru mezer v příloze: kritická 1, vysoká 6, střední 4.

5.1 M-07 — Chybí klasifikace závažných incidentů a hlídání lhůt hlášení

Vlastnost	Hodnota
Ustanovení	DORA čl. 17 odst. 3 písm. b); RTS 2025/301 čl. 5 odst. 1 písm. a) až c)
Priorita	**Kritická**
Pracnost	Střední

5.1.1 Zjištěný stav

Incidenty v Sentinelu mají závažnost a řešitele, ale ne kategorii, zasaženou službu ani posouzení podle kritérií čl. 18 odst. 1. Výpadky brány jsou jen v tiketech provozu. Za 90 dní vzniklo 164 incidentů, 9 z nich se týkalo platební brány.

Ověření: incidenty a jejich značky za 90 dní

```
SecurityIncident
| where CreatedTime > ago(90d)
| summarize arg_max(LastModifiedTime, *) by IncidentNumber
| summarize Incidenty = count(),
    SeZnackou = countif(array_length(Labels) > 0),
    Uzavrene = countif(Status == "Closed")
    by Severity
```

5.1.2 Dopad

Prvotní oznámení ČNB je nutné do 4 hodin od klasifikace incidentu jako závažného a nejpozději do 24 hodin od zjištění. Bez postupu lhůta běží, aniž o ní kdo ví, a dodržení nejde doložit. U platební instituce se to týká i provozních nebo bezpečnostních incidentů souvisejících s platbami (čl. 23 DORA).

5.1.3 Doporučení

- Postup klasifikace podle čl. 18 DORA a kritérií a prahových hodnot nařízení v přenesené pravomoci (EU) 2024/1772 schválí organizace, včetně toho, kdo klasifikuje a kdo hlásí ČNB.

- V Sentinelu watchlist aktiv platební brány a automatizační pravidlo, které incidentu nad nimi přidá značku a úkol posoudit závažnost. Do stejné evidence převádět i provozní výpadky brány.
- Po označení incidentu jako závažného vytvoří playbook úkoly s termíny 4 hodiny od klasifikace a 24 hodin od zjištění a upozorní odpovědnou osobu, stejně před lhůtou 72 hodin a jednoho měsíce.
- Časy zjištění, klasifikace a odeslání hlášení zapisovat do incidentu. Doklad pro ČNB pak vznikne dotazem.

5.2 M-01 — Privilegované role jsou trvalé, PIM se nepoužívá

Vlastnost	Hodnota
Ustanovení	RTS 2024/1774 čl. 21 písm. e) bod ii)
Priorita	**Vysoká**
Pracnost	Nízká
Licence	Entra ID P2, součást Microsoft 365 E5

5.2.1 Zjištěný stav

V Entra ID je 11 trvalých přiřazení privilegovaných rolí, z toho 4 globální správci.
V předplatném produkce má 6 účtů trvale roli Vlastník. Správci mají oddělené správcovské účty, PIM ale není nasazený, přestože ho licence E5 obsahuje.

Ověření: vlastníci předplatného produkce

```
az role assignment list --all --role Owner \
  --subscription sub-platby-prod -o table
```

5.2.2 Dopad

Ukradený nebo zneužitý účet správce má okamžitě a trvale plnou kontrolu nad Entra ID i nad produkcí platební brány. Nejde doložit, kdy a proč kdo privilegovaný přístup potřeboval.

5.2.3 Doporučení

- Zapnout PIM pro role Entra ID a role Azure a všechna trvalá přiřazení převést na oprávněná s aktivací nejvýš na 8 hodin, vícefaktorovým ověřením a odůvodněním.

- Aktivaci globálního správce a vlastníka produkce schvaluje druhá osoba, trvale zůstanou jen dva nouzové účty.

5.3 M-10 — V registru informací chybí služby Microsoftu pro platby

Vlastnost	Hodnota
Ustanovení	DORA čl. 28 odst. 3
Priorita	**Vysoká**
Pracnost	Nízká

5.3.1 Zjištěný stav

Registr informací má pro Microsoft jeden řádek: Microsoft 365 jako kancelářský software, bez vazby na funkce. Předplatné Azure, na kterém běží platební brána, v registru není.

Služby Microsoftu, které v registru chybějí

Služba	Použití	Podporuje provádění plateb
Azure App Service	aplikace platební brány	ano
Azure API Management	rozhraní pro obchodníky	ano
Application Gateway s WAF	vstup z internetu	ano
Azure SQL Database	transakce a klienti	ano
Azure Key Vault	klíče a certifikáty brány	ano
Entra ID	přihlášení správců a dodavatele	ano

5.3.2 Dopad

Registr se na žádost zpřístupňuje ČNB (čl. 28 odst. 3) a chybí v něm nejdůležitější závislost organizace.

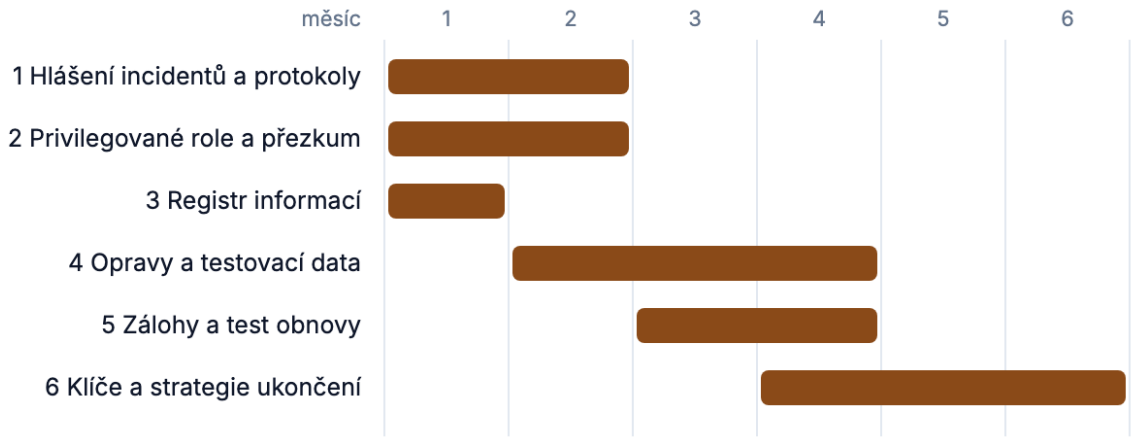
5.3.3 Doporučení

- Zapsat Microsoft jako poskytovatele služeb IKT z řad třetích stran se samostatnými ujednáními pro Microsoft 365 a Azure a u služeb z tabulky označit podporu zásadní nebo důležité funkce.
- Porovnat smluvní dokumenty Microsoftu pro finanční služby s čl. 30 a výsledek zapsat do registru.

6. Roadmapa

Pořadí je podle priority a závislostí. Krok 1 řeší jedinou kritickou mezeru a dobu uchovávání protokolů, u které každý den odkladu znamená nevratně ztracené záznamy. Kroky 1 až 3 nepotřebují nové licence.

Harmonogram (měsíce)



Krok	Obsah	Mezery	Pracnost
1	Postup klasifikace, hlídání lhůt 4, 24 a 72 hodin v Sentinelu, doba uchovávání protokolů	M-05, M-07	Střední
2	PIM pro role Entra ID a Azure, přezkum přístupu k platební bráně po šesti měsících	M-01, M-02	Nízká
3	Microsoft jako poskytovatel služeb pro platby, služby Azure podle Resource Graph	M-10	Nízká
4	Lhůty oprav podle závažnosti s eskalací, anonymizovaná testovací databáze	M-04, M-06	Střední
5	Zálohy Microsoft 365, test obnovy Azure SQL s protokolem	M-08, M-09	Střední
6	Vlastní klíč pro databázi brány, brána popsaná kódem, plán ukončení pro Azure	M-03, M-11	Vysoká

Pracnost kroku je nejvyšší pracnost z jeho mezer.

7. Přílohy

7.1 Registr mezer

ID	Mezera	Ustanovení	Priorita	Pracnost
M-01	Privilegované role jsou trvalé, PIM se nepoužívá	RTS 2024/1774 čl. 21 písm. e) bod ii)	Vysoká	Nízká
M-02	Přístupy k platební bráně se nepřezkoumávají	RTS 2024/1774 čl. 21 písm. e) bod iv)	Střední	Nízká
M-03	Databáze brány nemá vlastní klíč, který předepisuje politika	RTS 2024/1774 čl. 7 odst. 2	Střední	Střední
M-04	Lhůty pro instalaci oprav a eskalace chybějí	RTS 2024/1774 čl. 10 odst. 4 písm. d)	Vysoká	Střední
M-05	Doba uchovávání protokolů není stanovená	RTS 2024/1774 čl. 12 odst. 2	Vysoká	Nízká
M-06	Testovací databáze obsahuje úplná produkční data	RTS 2024/1774 čl. 16 odst. 5 písm. a)	Vysoká	Střední
M-07	Chybí klasifikace závažných incidentů a hlídání lhůt hlášení	DORA čl. 17 odst. 3 písm. b); RTS 2025/301 čl. 5 odst. 1 písm. a) až c)	Kritická	Střední
M-08	Data Microsoft 365 se nezálohují	DORA čl. 12 odst. 1 písm. a)	Střední	Střední
M-09	Obnova databáze brány se nikdy nezkoušela	DORA čl. 12 odst. 2	Vysoká	Nízká
M-10	V registru informací chybí služby Microsoftu pro platby	DORA čl. 28 odst. 3	Vysoká	Nízká
M-11	Pro Azure chybí strategie a plán ukončení	DORA čl. 28 odst. 8	Střední	Vysoká

7.2 Důkazní balík

Doklady s datem a zdrojem, které jde kdykoli zopakovat. Doklady k mezerám vzniknou po jejich odstranění.

Doklad	Odkud se exportuje	Ustanovení
Soupis zařízení a prostředků se značkami	Intune, Defender for Endpoint, Azure Resource Graph	DORA čl. 8 odst. 4
Conditional Access, PIM a přezkumy přístupu	Entra ID, Microsoft Graph	RTS 2024/1774 čl. 21
TLS, šifrování a klíče	Azure Resource Graph, Key Vault	RTS 2024/1774 čl. 6 a 7

Doklad	Odkud se exportuje	Ustanovení
Zranitelnosti a plnění lhůt oprav	Defender Vulnerability Management, Intune	RTS 2024/1774 čl. 10
Retence tabulek	Log Analytics	RTS 2024/1774 čl. 12
Pravidla, automatizace a zdraví zdrojů	Sentinel	DORA čl. 10, RTS 2024/1774 čl. 23
Incidenty s časy zjištění, klasifikace a hlášení	Sentinel, tabulka SecurityIncident	DORA čl. 17, RTS 2025/301 čl. 5
Schválení nasazení do produkce	Azure DevOps, protokol aktivit Azure	RTS 2024/1774 čl. 17
Nastavení záloh a protokol testu obnovy	Azure SQL, Microsoft 365 Backup	DORA čl. 12
Soupis služeb Microsoftu pro registr	Azure Resource Graph, centrum pro správu Microsoft 365	DORA čl. 28 odst. 3

7.3 Povinnosti mimo rozsah

Nejde o mezery analýzy. Organizace je zajistí a doloží mimo nastavení Microsoft 365 a Azure.

Ustanovení	Povinnost	Co dodá Microsoft 365 nebo Azure
DORA čl. 5 a 6, RTS 2024/1774 čl. 2, 3 a 27	Řízení a organizace, rámec a strategie, zpráva o přezkumu rámce	tuto analýzu a důkazní balík jako podklad přezkumu
DORA čl. 8 odst. 1 až 3 a 7, RTS 2024/1774 čl. 5	Klasifikace funkcí a aktiv, posouzení rizik, původní systémy	soupis prostředků a značky kritičnosti
DORA čl. 11, RTS 2024/1774 čl. 24 až 26	Zachování provozu, analýza dopadů, plány reakce a obnovy a jejich test	protokol testu obnovy (M-09)
DORA čl. 13 a 14	Poučení a školení, krizová komunikace	simulace útoků a školení v Defender for Office 365 z licence E5
DORA čl. 19 odst. 1 a 3	Hlášení ČNB a informování klientů	časy a průběh incidentu ze Sentinelu (M-07)
DORA čl. 24 až 27	Testování digitální provozní odolnosti, TLPT	výsledky Defender Vulnerability Management a Defender for Cloud jako vstup
DORA čl. 28 odst. 2 a 4 až 7, čl. 29 a 30	Strategie pro třetí strany, posouzení před smlouvou, riziko koncentrace, smluvní ujednání	auditní zprávy v Service Trust Portal; smluvní dokumenty Microsoftu pro finanční služby porovná organizace
RTS 2024/1774 čl. 15, 18 a 19	Řízení projektů IKT, fyzická bezpečnost, lidské zdroje	—