

Brusel 11. března 2026  
(OR. en)

7240/26

EF 66  
ECOFIN 329  
FSC 6  
*ESMA*  
*ESRB*  
*ECB*  
*EIOPA*  
*SRB*  
*EBA*

#### **PRŮVODNÍ POZNÁMKA**

---

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2026) 119 final
Předmět:	ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU o připravenosti ve finančním sektoru EU

---

Delegace naleznou v příloze dokument COM(2026) 119 final.

---

Příloha: COM(2026) 119 final



V Bruselu dne 10.3.2026  
COM(2026) 119 final

**ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU**

**o připravenosti ve finančním sektoru EU**

## 1. Úvod

Evropská unie čelí rostoucím rizikům a bezprecedentním hrozbám v mnoha odvětvích. Tato rizika mají podobu zvýšené nejistoty, geopolitického napětí a konfliktů, kybernetických hrozeb a manipulace s informacemi, dopadů změny klimatu a zvyšujícího se výskytu přírodních katastrof. Aby mohla EU tyto hrozby lépe předvídat, předcházet jim a reagovat na ně, představila Komise spolu s Evropskou službou pro vnější činnost (ESVČ) dne 26. března 2025 Strategii unie připravenosti<sup>1</sup>. Finanční sektor EU hraje klíčovou roli při zajištění životně důležitých společenských funkcí za všech okolností. Proto provádí Komise v rámci Strategie unie připravenosti a při realizaci opatření č. 25 uvedeného v příloze příslušného společného sdělení komplexní posouzení úrovně připravenosti ve finančním sektoru. Posuzuje zejména schopnost sektoru nadále plnit své zásadní funkce, například provádět platby a financovat ekonomiku, a to za všech okolností.

Právní předpisy EU v oblasti finančních služeb jsou založeny na silné tradici obezřetnosti, opatrnosti, odolnosti a předvídavosti. Cíle jsou jasné: zachování finanční stability, řádné řešení problémů finančních institucí, které jsou v krizové situaci, krizové řízení a pojištění vkladů, ochrana investorů a integrita trhu. EU dokončila komplexní revizi svých obezřetnostních pravidel a struktury bankovního dohledu, která byla zahájena v roce 2007 po velké finanční krizi. Tyto reformy posílily finanční instituce EU, její kapitálové trhy a poskytovatele infrastruktury finančního trhu.

Finanční sektor EU dosáhl v současnosti vysoké úrovně odolnosti, a to konsolidací tří pilířů, jimiž jsou: i) kapitál založený na riziku pro banky a finanční instituce, ii) požadavky na správu a řízení a transparentnost a iii) mechanismy spolupráce v oblasti dohledu mezi členskými státy a napříč sektory. EU zavedla politiky a zásady, které umožňují průběžně vyhodnocovat rizika extrémních událostí v rámci operačních rizik, v plánech kontinuity činností a v pohotovostních plánech.

Rámec EU byl v posledních letech podroben několika krizovým situacím, jako byla pandemie COVID-19, ruská agrese vůči Ukrajině, regionální bankovní krize v USA a krize Credit Suisse v roce 2023, výpadky elektřiny, kybernetické útoky a hybridní incidenty. Tváří v tvář těmto krizím prokázal finanční sektor EU svou stabilitu a odolnost. Orgány na úrovni EU i na vnitrostátní úrovni jednaly rychle a účinně.

Obecně platí, že připravenost není statická. Je to dynamický, výhledově orientovaný stav. Vyžaduje neustálý cyklus plánování, školení, zajišťování vybavení, testování, vyhodnocování a zlepšování. Dále vyžaduje, aby byl důraz kladen na připravenost na všechna nebezpečí, a to díky předvídaní rizik, rozvoji schopností, koordinaci napříč sektory (vládním, soukromým, veřejným) a učení se z minulých událostí. Cílem je vybudovat odolné komunity, které jsou schopny krizím předcházet, chránit se před nimi a zotavit se z nich. Totéž platí i pro finanční sektor.

---

<sup>1</sup> Komise a ESVČ zveřejnily [společné sdělení](#) o [Strategii unie připravenosti](#).

Tato zpráva poskytuje přehled o současném stavu připravenosti finančního sektoru EU, přičemž vychází z průběžných diskusí s Evropskou centrální bankou, evropskými orgány dohledu, Evropskou radou pro systémová rizika, Jednotným výborem pro řešení krizí, členskými státy a odvětvím finančních služeb.

## 2. Připravenost na jednotném trhu EU

Na úrovni EU se připravenost finančního sektoru v posledních několika letech zlepšila prostřednictvím legislativních opatření a vytvořením řídicích struktur na úrovni EU, které zohledňují přeshraniční povahu finančního sektoru EU. Správa je založena na dvou pilířích: předpisech EU a orgánech EU. Tuto strukturu doplňuje soubor opatření přijímaných na úrovni eurozóny, na regionální úrovni (zahrnující několik členských států) a na úrovni členských států.

### 2.1 Právní předpisy EU upravující finanční sektor

Finanční sektor se řídí jak odvětvovými, tak průřezovými právními předpisy.

#### *Odvětvové právní předpisy*

Mezi odvětvové právní předpisy patří směrnice a nařízení o kapitálových požadavcích (CRD/CRR)<sup>2</sup>, Solventnost II<sup>3</sup>, směrnice o trzích finančních nástrojů II (MiFID II)<sup>4</sup>, nařízení o infrastruktuře evropských trhů (EMIR)<sup>5</sup> a nařízení o centrálních depozitářích cenných papírů (CSDR)<sup>6</sup>. Tyto právní předpisy zavádějí obezřetnostní požadavky s cílem zajistit odolnost, stabilitu a řádné fungování finančních institucí, finanční infrastruktury a finančního systému.

Z hlediska připravenosti jsou v několika odvětvových právních předpisech stanoveny požadavky na řízení operačních rizik, provozní odolnost, odolnost IKT, kontinuitu činností a krizové řízení. Například v bankovním sektoru zajišťují odolnost bank vůči široké škále možných rizik, včetně extrémních událostí, směrnice a nařízení o kapitálových požadavcích (CRR/CRD), směrnice o ozdravných postupech a řešení krize bank (BRRD)<sup>7</sup>, nařízení o

---

<sup>2</sup> „Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (CRD);

Nařízení Evropského parlamentu a rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (CRR).

<sup>3</sup> Konsolidované znění: Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II).

<sup>4</sup> Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (MIFID II).

<sup>5</sup> Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (EMIR).

<sup>6</sup> Nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnice 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012.

<sup>7</sup> Směrnice Evropského parlamentu a Rady 2014/59/EU ze dne 15. května 2014, kterou se stanoví rámec pro ozdravné postupy a řešení krize úvěrových institucí a investičních podniků a kterou se mění směrnice Rady 82/891/EHS, směrnice Evropského parlamentu a Rady 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU a 2013/36/EU a nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 a (EU) č. 648/2012 (BRRD).

jednotném mechanismu pro řešení krizí (SRMR)<sup>8</sup> a směrnice o systémech pojištění vkladů (DGSD)<sup>9</sup>. Od bank se očekává, že zavedou spolehlivé rámce správy a řízení rizik, včetně rozšířených plánů kontinuity činností, komunikace a obnovy, aby mohly účinně řešit širokou škálu rizik. Klíčové prvky opatření k řešení rizikových scénářů, a to jak preventivní, tak reaktivní, zahrnují specifické předběžné požadavky na banky, jako jsou ozdravné plány a plány řešení krize, jak ukládá nařízení o jednotném mechanismu pro řešení krizí a směrnice o ozdravných postupech a řešení krize bank.

Kromě bank podléhají podobným požadavkům na zajištění provozní odolnosti, řízení rizik pro IKT, kontinuity činností a krizového řízení také pojišťovny, které se řídí směrnicí Solventnost II, dále investiční podniky podle směrnice MiFID II a tržní infrastruktury, jako jsou ústřední protistrany a centrální depozitáře cenných papírů. Tyto požadavky jsou v případě potřeby doplněny požadavky na posílení vytváření ozdravných plánů a plánů řešení krize. Správa majetku a nebankovní finanční zprostředkování rovněž podléhají širokému a stále komplexnějšímu regulačnímu rámci EU, včetně směrnice o subjektech kolektivního investování do převoditelných cenných papírů, směrnice o správcích alternativních investičních fondů a nařízení o fondech peněžního trhu. Tyto nástroje ukládají požadavky na řízení rizik, řízení likvidity, finanční páku, oceňování a transparentnost s cílem podpořit stabilitu sektoru. Celkovou odolnost a připravenost finančního sektoru EU zlepšit opatření na rozvoj unie úspor a investic prostřednictvím budování schopnosti tohoto sektoru propojit úspory s produktivními investicemi, čímž se zlepšit sdílení rizik a diverzifikace v celém sektoru.

Evropská centrální banka (ECB) – jednotný orgán dohledu nad bankami v 21 členských státech – a příslušné vnitrostátní orgány v zemích eurozóny i mimo ni kladou finanční a provozní odolnost bank do středu svých priorit v oblasti dohledu. Banky se zejména vyzývají, aby náležitě zohlednily geopolitická rizika a začlenily je do svých procesů řízení rizik. V této souvislosti by měly zvážit expozice vůči protistranám v zemích mimo EU, potenciální dopady zahraničních sankcí na expozice a závislost na externích poskytovatelích služeb a infrastrukturách. Kromě toho by banky měly vytvořit spolehlivý rámec správy a řízení a ochrany před kybernetickými hrozbami a dalšími hrozbami, které mohou ovlivnit jejich provozní odolnost. Jde mimo jiné o opatření ke zvýšení bezpečnosti a ochrany před fyzickým poškozením. Kromě opatření specifických pro jednotlivé instituce se bankovní obezřetnostní rámec EU zabývá také širšími systémovými a přeshraničními rizikovými kanály.

Rámec pro krizové řízení nabízí soubor nástrojů, které lze použít v případě ohrožení životaschopnosti poskytovatele zásadní funkce. Revidovaný rámec pro krizové řízení a pojištění vkladů pro banky, ohledně něhož bylo v červnu 2025 dosaženo politické dohody, představuje důležitý krok k zajištění ještě větší účinnosti systému EU pro krizové řízení, zejména pro menší a středně velké banky.

---

<sup>8</sup> Nařízení Evropského parlamentu a Rady (EU) č. 806/2014 ze dne 15. července 2014, kterým se stanoví jednotná pravidla a jednotný postup pro řešení krize úvěrových institucí a některých investičních podniků v rámci jednotného mechanismu pro řešení krizí a Jednotného fondu pro řešení krizí a mění nařízení (EU) č. 1093/2010 (SRMR).

<sup>9</sup> Směrnice Evropského parlamentu a Rady 2014/49/EU ze dne 16. dubna 2014 o systémech pojištění vkladů (DGSD).

Jedním z důležitých aspektů připravenosti finančního sektoru je mít k dispozici platební nástroje pro veřejnost, a to jak pro hotovostní, tak elektronické platby. V zájmu dostupnosti **hotovosti** za všech okolností je třeba na úrovni Euro systému především zajistit společné strategické zásoby eurobankovek. Ústředním koordinačním a rozhodovacím orgánem je Evropská centrální banka (ECB), která pravidelně provádí cvičení v oblasti řešení krizí, včetně případné krizové komunikace. Na vnitrostátní úrovni zajišťují národní centrální banky plány kontinuity činností, aby bylo možné hotovost nadále vybírat i vkládat.

Současně má návrh týkající se postavení eurobankovek a euromincí jako zákonného platidla, který Komise předložila dne 28. června 2023, zajistit, aby eurohotovost byla i nadále obecně přijímána pro platby a snadno dostupná pro občany, podniky a veřejné subjekty v celé eurozóně. Požadavky na udržování zdravé hotovostní infrastruktury v běžných časech podporují dostupnost hotovosti v situacích, kdy nastanou nepředvídané události. Návrh Komise neobsahoval ustanovení o odolnosti, ale Rada jej začlenila v rámci svého mandátu k vyjednávání, který vyžaduje, aby členské státy přijaly plán odolnosti v oblasti hotovosti nebo zkombinovaly rovnocenná opatření.

Směrnice o platebních službách 3 (PSD3), ohledně které bylo v listopadu 2025 dosaženo politické dohody, má navíc za cíl posílit přístup k hotovosti v obchodech tím, že umožní obchodníkům nabízet výběr hotovosti bez nákupu (tzv. *cash-in-shops*), a to až do určitého limitu. Vyjasněním pravidel pro obchodníky a provozovatele bankomatů se tak zvyšuje komfort používání hotovosti, zejména ve venkovských oblastech.

Kromě dostupnosti hotovosti je zásadní zachovat kontinuitu **platebních služeb**, včetně plateb kartou, převodů z účtu na účet (včetně plateb prostřednictvím mobilních telefonů), přístupu k platebním účtům a možnosti provádět vklady, aby byla zachována důvěra veřejnosti ve finanční systém, udržen veřejný pořádek a zajištěno základní fungování ekonomiky v případě rozsáhlého narušení tím, že se veřejnosti zajistí trvalý přístup k základním službám.

Současná směrnice o platebních službách 2 (PSD2) upravuje další aspekty včetně řízení provozních a bezpečnostních rizik a hlášení závažných incidentů. Cílem je posílit bezpečnost a odolnost platebních systémů v celé EU.

Bezpečnost a účinnost platebních systémů podporuje Euro systém. Zavedl požadavky na dohled s cílem řešit klíčové rizikové scénáře identifikované pro evropský platební ekosystém. Rámec stanoví komplexní soubor požadavků na řízení provozních rizik. Patří mezi ně opatření pro řízení kontinuity činností a včasné obnovení činností spolu se zvláštními ustanoveními pro bezpečnost informací, kybernetickou odolnost, fyzickou bezpečnost, outsourcing, řízení rizik v oblasti IT a další související oblasti. Rámec zahrnuje elektronické platební nástroje (jako jsou karty, inkasa, úhrady, elektronické peníze a digitální peněženky), jakož i schémata (např. sítě platebních karet) a aplikace (např. elektronické peněženky), které umožňují jejich používání.

K zajištění větší ochrany stanoví článek 15 nařízení ECB o systémově významných platebních systémech (SIPS) další požadavky. Požaduje například, aby systémy zajistily obnovení činnosti do dvou hodin (včetně využití sekundárních míst) a aby provozovatelé SIPS byli

schopni dokončit zúčtování všech plateb splatných v daný den do konce pracovního dne, kdy k incidentu došlo.

Projekt na vytvoření digitálního eura – digitální formy hotovosti, která by doplnila fyzickou hotovost a soukromá platební řešení – by veřejnosti nabídl další způsob placení a zároveň by podpořil digitální a finanční začlenění. Digitální euro jako první jednotný celoevropský platební systém by rovněž pomohlo ochránit mezinárodní roli eura. Posílením otevřené strategické autonomie EU a rozšířením nabídky dostupných platebních nástrojů má projekt digitálního eura dále posílit celkovou odolnost platebních služeb. Pokud jde o návrh týkající se zákonného platidla, Rada doplnila další ustanovení, která mají odolnost digitálního eura dále posílit. V této souvislosti budou evropské peněženky digitální identity (EUDI) interoperabilní s uživatelskými rozhraními digitálního eura, což zajistí bezpečné a bezproblémové ověřování uživatelů<sup>10</sup>.

### *Meziodvětvové právní předpisy ve finančním sektoru*

Doplňkem k výše uvedeným právním předpisům ve finanční oblasti je nařízení o digitální provozní odolnosti (nařízení DORA), které je odvětvovým právním předpisem a platí pro celý finanční sektor EU. Zahrnuje 20 různých typů finančních subjektů včetně úvěrových institucí, poskytovatelů platebních služeb, infrastruktur finančního trhu, pojišťoven, ratingových agentur a správců aktiv.

Nařízení DORA klade velký důraz na odolnost finančních subjektů, na úroveň jejich připravenosti čelit případným narušením v oblasti IKT a na řízení rizik vyplývajících ze závislosti finančních subjektů na poskytovatelích služeb IKT z řad třetích stran, včetně systémových rizik a rizik koncentrace, která představují poskytovatelé IKT, kteří jsou pro finanční sektor EU kriticky významní. Toto nařízení tvoří harmonizovaný a spolehlivý rámec pro posílení schopnosti finančního sektoru EU předcházet narušením souvisejícím s IKT, odolávat jim, reagovat na ně a zotavovat se z nich. Finanční subjekty musí přijmout komplexní rámec pro řízení rizik v oblasti IKT, který zahrnuje správu, inventarizaci aktiv, identifikaci rizik, ochranu, odhalování, reakci, obnovu a neustálé zlepšování. Tím se zajistí proaktivní řízení zranitelných míst a odolnosti systémů a procesů. Od finančních subjektů se rovněž vyžaduje, aby odhalovaly, klasifikovaly a oznamovaly příslušným orgánům závažné incidenty související s IKT za použití dohodnutých definic, prahových hodnot a lhůt, aby bylo možné v rámci různých jurisdikcí koordinovaně reagovat. Nařizuje pravidelné testování a hodnocení jejich procesů, nástrojů a opatření v oblasti odolnosti a připravenosti.

Finanční subjekty musí rovněž řídit rizika spojená s využíváním poskytovatelů služeb IKT z řad třetích stran, zejména kritických poskytovatelů služeb IKT z řad třetích stran (CTPPs). Nařízení DORA ukládá finančním subjektům, aby před uzavřením nových smluv s

---

<sup>10</sup> Evropský rámec pro digitální identitu vytváří bezpečný a důvěryhodný ekosystém pro digitální identifikaci a autentizaci a používání digitálních důkazů, který bude do konce roku 2026 k dispozici všem občanům EU. Evropské peněženky digitální identity přímo přispějí k odolnosti a připravenosti finančního sektoru EU na krizi, jelikož jej ochrání před podvody a krádežemi totožnosti při platbách, přijímání zákazníků a v rámci dalších finančních služeb.

poskytovateli z řad třetích stran provedly hloubkovou kontrolu rizik koncentrace. Nařízení stanoví mechanismus dohledu, v jehož rámci tři evropské orgány dohledu<sup>11</sup> dohlížejí na kritické poskytovatele služeb IKT z řad třetích stran v celoevropském měřítku, čímž se zvyšuje celková digitální provozní odolnost v celém finančním sektoru EU. V listopadu 2025 zveřejnily evropské orgány dohledu seznam určených kritických poskytovatelů služeb IKT z řad třetích stran podle nařízení DORA. Rámec podle nařízení DORA je obzvláště vhodný pro řízení kybernetické bezpečnosti, konektivity, připravenosti a pro řešení provozních rizik se silným mezinárodním rozměrem.

Kromě nařízení DORA, které je *lex specialis* pro finanční sektor, se na tento sektor vztahují také horizontální ujednání o spolupráci v oblasti fyzické a digitální odolnosti v rámci směrnice o odolnosti kritických subjektů<sup>12</sup> a směrnice NIS2.

Směrnice o odolnosti kritických subjektů vytváří zastřešující rámec, který se věnuje odolnosti kritických subjektů vůči všem nebezpečím. Nařizuje posouzení rizik, sestavení vnitrostátní strategie a přijetí konkrétních opatření k zajištění odolnosti určených kritických subjektů, aby byly schopny i nadále zajišťovat životně důležité společenské funkce. Ačkoli se směrnice vztahuje na bankovní sektor a infrastruktury finančního trhu coby kritická odvětví, na finanční sektor se nevztahují všechny věcné požadavky na odolnost kritických subjektů, protože se ho týkají mnohem specifitější požadavky podle nařízení DORA. Finanční sektor nicméně zůstává v oblasti působnosti směrnice o odolnosti kritických subjektů, pokud jde o horizontální ujednání o spolupráci.

Směrnice NIS2 poskytuje širší rámec pro kybernetickou bezpečnost v různých kritických odvětvích. Nařízení DORA je ve vztahu ke směrnici NIS2 považováno za *lex specialis*, což znamená, že požadavky týkající se řízení rizik a hlášení incidentů stanovené v nařízení se použijí jako odvětvový právní akt Unie namísto směrnice NIS2. Jak Komise sdělila ve svých pokynech k uplatňování čl. 4 odst. 1 a 2 směrnice NIS2<sup>13</sup>, nadále platí některá ustanovení stanovená ve směrnici NIS2, která jsou zásadní pro zajištění připravenosti a dosažení vysoké úrovně odolnosti finančních subjektů, včetně požadavků na přijetí strategie kybernetické bezpečnosti a vytvoření vnitrostátního rámce pro řešení kybernetických krizí (s povinností jmenovat orgány pro řešení kybernetických krizí a přijmout vnitrostátní plány reakce na kybernetické incidenty a krize velkého rozsahu), které se vztahují na sektory bankovní a infrastruktur finančního trhu. Dále by měly své úkoly s ohledem na odvětví bankovní infrastruktury a infrastruktury finančního trhu plnit týmy pro reakce na počítačové bezpečnostní incidenty (tým CSIRT) a Síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe).

---

<sup>11</sup> Třemi evropskými orgány dohledu jsou Evropský orgán pro bankovníctví (EBA), Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění (EIOPA) a Evropský orgán pro cenné papíry a trhy (ESMA).

<sup>12</sup> Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES. Ustanovení čl. 5 odst. 5 této směrnice stanoví, že Komise ve spolupráci s členskými státy vytvoří dobrovolný společný vzor pro podávání zpráv pro účely dodržování čl. 5 odst. 4 směrnice.

<sup>13</sup> C(2023)6068.

Opatření pro připravenost finančního sektoru jsou navržena tak, aby vyvážila potřebu odolnosti se zásadou proporcionality. Regulační požadavky a požadavky v oblasti dohledu jsou přizpůsobeny velikosti, složitosti a systémovému významu institucí, aby nedocházelo k neúměrnému zatěžování menších subjektů. Aby se zabránilo zbytečné administrativní zátěži, harmonizované rámce, jako je nařízení DORA, zefektivňují požadavky v celém odvětví, zajišťují konzistentnost a zároveň snižují duplicitu úsilí.

## 2.2 Orgány EU: nástroje a spolupráce

Orgány EU jsou pověřeny zvláštními nástroji, které mohou být aktivovány při mimořádných situacích a které udržují opatření za účelem připravenosti k zajištění kontinuity činností. Například tři uvedené evropské orgány dohledu mají podle svých zřizovacích nařízení přiděleny pravomoci pro mimořádné situace. Jakmile Rada mimořádnou situaci formálně uzná (podle článku 18 nařízení o zřízení evropských orgánů dohledu), může prostřednictvím individuálních rozhodnutí dočasně omezit finanční činnosti podle článku 9. Plní také obecnou koordinační funkci mezi vnitrostátními orgány a v rámci Evropského systému dohledu nad finančním trhem (ESFS) (článek 31).

Jak bylo uvedeno výše, ECB je jednotným orgánem dohledu nad bankami v 21 členských státech, které se účastní jednotného mechanismu dohledu, a zajišťuje tak konzistentní obezřetnostní dohled v celé oblasti. Jednotný výbor pro řešení krizí je jednotným orgánem pro řešení krizí v těchto členských státech, který je odpovědný za řádné řešení problémů bank v krizové situaci, čímž zajišťuje finanční stabilitu a minimalizuje náklady pro daňové poplatníky.

Pro zvýšení provozní odolnosti vypracovaly všechny orgány EU interní opatření pro zajištění kontinuity činnosti, připravenosti a řízení kritických událostí, aby mohly zvládat různá nebezpečí. Pravidelně tato opatření testují, aby zajistily kontinuitu činností a určily, které obchodní procesy jsou nejnáročnější, pokud jde o včasnost, a na jaké úrovni je třeba je v případě mimořádné situace provést.

Vzhledem k potřebě zachovat integritu a řádné fungování jednotného trhu a vzhledem k vysokému stupni vzájemné propojenosti a riziku vedlejších účinků ve finančním sektoru EU je nezbytná koordinace mezi různými orgány EU a zapojení členských států, aby bylo možné předvídat a zvládat krize, které mohou ovlivnit více částí EU současně. Zajistit včasné zapojení a rychlou spolupráci je třeba jak ve fázi plánování, tak ve všech jednotlivých fázích krize. Aby se usnadnila spolupráce a výměna informací, které mohou být důležité i v případě krize, dohodlo se několik orgánů EU na nástrojích spolupráce mezi sebou nebo s příslušnými vnitrostátními orgány či vnitrostátními orgány pro řešení krizí, případně podepsalo memoranda o porozumění (např. memorandum o porozumění mezi ECB a Jednotným výborem pro řešení krizí). Zároveň se provádějí simulace krizí, aby se zajistila odpovídající připravenost na případnou krizi.

Jedním z důležitých milníků v této práci je Rámec Evropské unie pro koordinaci systémových kybernetických incidentů (EU-SCICF), který v lednu 2025 vytvořily evropské orgány dohledu. Tento rámec poskytuje strategický základ pro spolupráci při významných kybernetických

incidentech<sup>14</sup>. Jeho cílem je usnadnit rychlé sdílení informací a společnou reakci zavedením protokolů pro vyhodnocování a zmírňování hrozeb v členských státech EU.

Kromě toho přijala Rada v červnu 2025 plán pro řešení kybernetických bezpečnostních krizí<sup>15</sup> jako důležitý návod pro členské státy, jak posílit jejich připravenost, schopnost odhalovat kybernetické bezpečnostní incidenty a adekvátně na ně reagovat, a to na základě všech příslušných mechanismů, včetně mechanismů vytvořených směrnicí NIS2, nařízením DORA (EU-SCICF) a nařízením o kybernetické solidaritě.

V tomto rámci lze provádět pravidelná cvičení, aby se zajistilo, že připravenost a schopnost reakce zůstanou stabilní a účinné. Kromě toho byl na mezinárodní úrovni přijat protokol G7 o reakci na kybernetické incidenty, jehož cílem je sjednotit celosvětovou snahu o zajištění reakce na kybernetické bezpečnostní hrozby, které mají dopad na finanční sektor, a zajistit včasnou a koordinovanou reakci napříč jurisdikcemi.

Každý orgán EU provádí pravidelné hodnocení rizik a přijímá další opatření, aby s ohledem na mandát a funkce každého orgánu určil nejvýznamnější rizika. Hodnocení rizik se provádí ve spolupráci s vnitrostátními orgány, což přispívá ke společnému a hlubšímu pochopení rizikového prostředí a rizik, na něž je třeba se přednostně zaměřit. Výsledky posouzení rizik se často promítají do systémů včasného varování, které jsou zase součástí rámců připravenosti orgánů EU. Stávající regulační ujednání a ujednání v oblasti dohledu mezi orgány EU a zúčastněnými stranami ze soukromého sektoru navíc umožňují pokračovat v dialogu o vzájemných očekáváních ohledně připravenosti<sup>16</sup>.

### 2.3 Rámce na národní a regionální úrovni

Kromě právních předpisů na úrovni EU vypracovaly členské státy vlastní vnitrostátní systémy připravenosti<sup>17</sup>. Ty zpravidla překračují finanční sektor a týkají se připravenosti společnosti jako celku na vnitrostátní úrovni. Z tohoto důvodu se vnitrostátní systémy v jednotlivých členských státech liší – odrážejí rozdílné vnitrostátní vládní a správní struktury a rozsah pravomocí. Zároveň fungují v soudržném rámci EU a stále více se propojují s opatřeními na úrovni EU a přeshraničními koordinačními mechanismy.

Připravenost finančního sektoru je vždy klíčovým prvkem vnitrostátních strategií připravenosti. Tento sektor je v otázce připravenosti na předním místě a je vzorem pro ostatní odvětví. Vnitrostátní strategie připravenosti pro finanční sektor jdou nad rámec *acquis* EU a zaměřují se na vnitrostátní provozní otázky. Rozdíly mezi vnitrostátními finančními systémy (např. hlavní rysy vnitrostátního bankovního sektoru, rozsah používání hotovosti, přijetí eura, účast

---

<sup>14</sup> Rámec EU-SCICF rovněž provádí článek 49 nařízení DORA s cílem posílit koordinaci s ostatními krizovými rámci EU.

<sup>15</sup> Doporučení Rady ze dne 6. června 2025 o plánu EU pro řešení kybernetických bezpečnostních krizí (*Úř. věst. C, C/2025/3445, 20.6.2025, <http://data.europa.eu/eli/C/2025/3445/oj>*).

<sup>16</sup> Strategie unie připravenosti uznává význam těchto partnerství. Klíčová opatření č. 36 a 37 mají za cíl zřídit pracovní skupinu veřejného a soukromého sektoru pro připravenost a vypracovat protokoly veřejného a soukromého sektoru pro mimořádné události ve všech odvětvích.

<sup>17</sup> V rámci úsilí o realizaci opatření č. 25 přílohy společného sdělení o Strategii unie připravenosti Komise rovněž navázala na pokračující diskuse s členskými státy o systémech připravenosti.

v bankovní unii) se přirozeně odrážejí ve způsobu hodnocení a zajištění úrovně připravenosti finančního sektoru na vnitrostátní úrovni.

Vzhledem ke klíčové úloze, kterou hrají orgány veřejné moci, zejména v případě krize nebo závažného incidentu, musí být i nadále k dispozici spolehlivé funkce krátkodobého financování, aby se zabránilo nedostatku likvidity nebo financování na úrovni státu a veřejného sektoru v širším smyslu a aby se zabránilo širším dopadům na společnost, pokud jde o důvěru veřejnosti a finanční stabilitu. To však neplatí pro všechny krizové rámce stejně: zejména řešení krize bank je koncipováno tak, aby omezilo závislost na veřejných prostředcích, a to prostřednictvím mechanismů rekapitalizace z vnitřních zdrojů a mechanismů řešení krize financovaných sektorem.

Aby byla zajištěna odolnost vládních funkcí krátkodobého financování, vypracovaly vnitrostátní úřady pro správu dluhu plány pro nepředvídané události a plány kontinuity činností, aby mohly pokračovat v činnosti i v případě krize. Tato opatření jsou stále více doplňována výměnou osvědčených postupů a koordinací na úrovni EU i na regionální úrovni.

Kromě toho nabízí Evropský mechanismus stability (ESM) několik nástrojů finanční pomoci, které mají zajistit finanční stabilitu poskytováním pomoci členům ESM, aby se zvýšila schopnost eurozóny zvládat krizové situace států a bank. Tyto nástroje jsou určeny k řešení systémových krizí a doplňují provozní připravenost členských států a EU o konkrétnější scénáře narušení. Některé členské státy vypracovaly dvoustranné dohody, které zajišťují dostupnost krátkodobého financování v případě, že některá ze základních funkcí úřadu pro správu dluhu nebude k dispozici. Dokončení očekávané změny Smlouvy o ESM by záchrannou sítí eurozóny dále posílilo.

Souběžně existují regionální koordinační fóra, jako je například Mechanismus spolupráce severských a baltických zemí, což je důležitá regionální iniciativa zaměřená na pobaltské země. Tato fóra podporují spolupráci v oblasti finančního dohledu a krizového řízení, výměnu informací o hodnocení rizik a strategickém plánování. Ukazují, jak může regionální spolupráce přispět k posílení připravenosti.

Několik členských států vytvořilo v rámci svých vnitrostátních systémů připravenosti zvláštní partnerství nebo fóra soukromého a veřejného sektoru (zahrnující zástupce soukromého sektoru z několika odvětví).

Celkově jsou tato opatření na úrovni EU, na regionální a vnitrostátní úrovni součástí mnohvrstvého rámce připravenosti, kde koordinaci a spolupráci na úrovni EU a na regionální úrovni doplňují opatření na vnitrostátní úrovni.

### 3. Zátěžové testování

Zátěžové testování je klíčovým aspektem připravenosti, jak je uznáno v doporučení Rady o posílení odolnosti kritické infrastruktury<sup>18</sup>. Ve finančním sektoru je zátěžové testování již nedílnou a nezbytnou součástí dohledu nad finančními institucemi a poskytovateli infrastruktury finančního trhu. Zátěžové testy posilují připravenost finančního sektoru tím, že simulují závažné krize (jako je recese, klimatické šoky nebo kybernetické útoky), aby odhalily zranitelnost kapitálu a likvidity finančních institucí. Instituce a poskytovatelé jsou tak nuceni řízení rizik zlepšovat, zvyšovat kapitálové rezervy, zdokonalovat strategické plánování a budovat odolnost vůči budoucím otřesům, čímž se zvyšuje celková finanční stabilita a buduje důvěra trhu.

Připravenost podporuje rovněž zátěžové testování – zachycuje celosystémové a přeshraniční rizikové kanály, včetně zdrojů globální finanční nestability, geopolitického napětí, kybernetických incidentů a narušení kritické infrastruktury.

V **bankovním systému** má mandát iniciovat a koordinovat zátěžové testy bankovního sektoru v celé EU Evropský orgán pro bankovníctví (EBA). Na základě tohoto mandátu provádí orgán EBA každé dva roky zátěžový test v celé EU, který se týká přibližně 75 % bankovního sektoru. Směrnice o kapitálových požadavcích rovněž pověřuje příslušné orgány, aby podle potřeby, nejméně však jednou ročně, prováděly zátěžové testy v rámci dohledu u institucí, nad nimiž vykonávají dohled. Orgán EBA navíc vydal pokyny, jimiž se má zajistit, aby orgány při provádění ročního zátěžového testování v rámci dohledu používaly společnou metodiku.

V rámci bankovní unie provádí ECB pravidelně zátěžové testy, analýzy scénářů a simulace, které slouží jako podklad pro proces přezkumu a hodnocení v rámci dohledu. ECB rovněž provádí cílené přezkumy kybernetické odolnosti a outsourcingových opatření.

V **odvětví pojišťoven a institucí zaměstnaneckého penzijního pojištění** provádí orgán EIOPA pravidelně každé tři roky celoevropské zátěžové testy u pojišťoven a zajišťoven a institucí zaměstnaneckého penzijního pojištění (IZPP)<sup>19</sup>, včetně složky kybernetických rizik a klimatických rizik.

Evropský orgán pro cenné papíry a trhy (ESMA) provádí pravidelné celoevropské zátěžové testy odolnosti ústředních protistran v rámci hodnocení podle článku 32 nařízení o ESMA a článku 24a nařízení EMIR. Ačkoli se tyto testy zaměřují na odolnost ústředních protistran vůči nepříznivému vývoji na trhu, orgán ESMA posuzuje i další typy exogenních rizik.

Evropská rada pro systémová rizika (ESRB) vypracovává nepříznivé scénáře pro zátěžové testy orgánu EBA (banky), orgánu EIOPA (pojišťovny, instituce penzijního pojištění) a orgánu ESMA (ústřední protistrany).

---

<sup>18</sup> Doporučení Rady ze dne 8. prosince 2022 o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury (2023/C 20/01).

<sup>19</sup> V několika členských státech nespádají instituce zaměstnaneckého penzijního pojištění do oblasti působnosti směrnice IZPP II, a proto se na ně nevztahují pravidla EU. Tyto instituce penzijního pojištění nepodléhají zátěžovým testům prováděným orgánem EIOPA.

Směrnice 2014/49/EU o systémech pojištění vkladů vyžaduje, aby členské státy plnily své úkoly podle této směrnice. Výsledky těchto testů pak orgán EBA využívá k provádění vzájemných hodnocení, jejichž cílem je prověřit odolnost systémů pojištění vkladů.

#### **4. Výhled**

Finanční sektor EU se opírá o pevný a vícerozměrný rámec připravenosti. Rámec se skládá ze specifických odvětvových právních předpisů, průřezových právních předpisů a mechanismů spolupráce mezi odvětvími a napříč členskými státy. Připravenost finančního sektoru EU má také vnější rozměr, kterým EU posiluje nejen svou finanční stabilitu, ale také svou roli spolehlivého a důvěryhodného finančního sektoru na celosvětové úrovni.

Finanční sektor EU prokázal během minulých krizí svou odolnost. Prokázal, že je schopen přečkat bouři v podobě pandemie COVID-19, ruskou agresi vůči Ukrajině, finanční krize v jiných jurisdikcích, kybernetické útoky a mnoho dalších událostí.

Nicméně vzhledem k bezprecedentním hrozbám a nejistějším geopolitickému prostředí, kterému EU čelí, je důležité průběžně vyhodnocovat úroveň připravenosti finančního sektoru EU. EU pokračuje v této práci a může zahájit veškeré úpravy potřebné k zajištění rychlých, sladěných a přiměřených preventivních a reaktivních opatření na úrovni EU i členských států s cílem udržet pevný kurz a zachovat životně důležité funkce finančního sektoru EU. Do budoucna se očekává, že rozvoj unie úspor a investic a zavedení digitálního eura zlepší celkovou odolnost finančního sektoru EU a dále zvýší úroveň jeho připravenosti.