EURÓPSKA
KOMISIA

V Bruseli 23. 6. 2020
COM(2020) 255 final

ANNEX

PRÍLOHA

k

návrhu rozhodnutia Rady

o pozícii, ktorá sa má v mene Európskej únie zaujať v spoločnom výbore zriadenom Dohodou medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov v súvislosti s prijatím spoločných operačných postupov

ROZHODNUTIE č. 1/2020 SPOLOČNÉHO VÝBORU ZRIADENÉHO DOHODOU MEDZI EURÓPSKOU ÚNIOU A ŠVAJČIARSKOU KONFEDERÁCIOU O PREPOJENÍ ICH SYSTÉMOV OBCHODOVANIA S EMISIAMI SKLENÍKOVÝCH PLYNOV

z ...

o spoločných operačných postupoch

SPOLOČNÝ VÝBOR

so zreteľom na Dohodu medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov[1] (ďalej len „dohoda“), a najmä na jej článok 3,

keďže:

(1) Rozhodnutím spoločného výboru č. 2/2019 z 5. decembra 2019 sa zmenili prílohy I a II k dohode, čím sa splnili podmienky pre prepojenie stanovené v dohode.

(2) Po prijatí rozhodnutia spoločného výboru č. 2/2019 a podľa článku 21 ods. 3 dohody si zmluvné strany vymenili svoje listiny o ratifikácii alebo schválení, pretože sa domnievajú, že všetky podmienky na prepojenie uvedené v dohode boli splnené.

(3) V súlade s článkom 21 ods. 4 dohody nadobudla dohoda platnosť 1. januára 2020.

(4) Podľa článku 3 ods. 6 dohody by švajčiarsky správca registra a ústredný správca registra Únie mali určiť spoločné operačné postupy týkajúce sa technických alebo iných záležitostí potrebných na fungovanie prepojenia medzi protokolom transakcií Európskej únie (ďalej len „EUTL“) registra Únie a dodatkovým protokolom transakcií Švajčiarska (SSTL) švajčiarskeho registra, pričom by sa mali zohľadniť priority vnútroštátnych právnych predpisov. Spoločné operačné postupy vypracované správcami začnú platiť po prijatí rozhodnutia spoločného výboru.

(5) V súlade s článkom 13 ods. 1 dohody by mal spoločný výbor odsúhlasiť technické usmernenia s cieľom zabezpečiť riadne vykonávanie dohody vrátane technických alebo iných záležitostí potrebných na fungovanie prepojenia a s prihliadnutím na priority vnútroštátnych právnych predpisov. Technické usmernenia môže vypracovať pracovná skupina zriadená podľa článku 12 ods. 5 dohody. Pracovná skupina by mala zahŕňať minimálne švajčiarskeho správcu registra a ústredného správcu registra Únie a mala by pomáhať spoločnému výboru pri výkone jeho funkcií podľa článku 13 dohody.

(6) Vzhľadom na technickú povahu usmernení a potrebu prispôsobiť ich aktuálnemu vývoju by sa technické usmernenia vypracované švajčiarskym správcom registra a ústredným správcom registra Únie mali predložiť spoločnému výboru na účely informovania alebo v prípade potreby na účely schválenia,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Týmto sa prijímajú spoločné operačné postupy, ktoré tvoria prílohu k tomuto rozhodnutiu.

[1] Ú. v. EÚ L 322, 7.12.2017, s. 3.

Článok 2

Týmto sa zriaďuje pracovná skupina podľa článku 12 ods. 5 dohody. Spoločnému výboru bude pomáhať zabezpečovať riadne vykonávanie dohody vrátane vypracovania technických usmernení na vykonávanie spoločných operačných postupov.

Členmi pracovnej skupina musia byť minimálne švajčiarsky správca registra a ústredný správca registra Únie.

Článok 3

Toto rozhodnutie nadobúda účinnosť v deň jeho prijatia.

V anglickom jazyku v Bruseli, dňa XX 2020.

Za spoločný výbor

tajomník za Európsku úniu	*predseda*	*tajomník za Švajčiarsko*

DODATOK

PRÍLOHA

SPOLOČNÉ OPERAČNÉ POSTUPY (SOP)

podľa článku 3 ods. 6 dohody medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov
- Postupy pre predbežné riešenia -

1. GLOSÁR

Tabuľka 1-1 – Skratky a definície

Skratka/Termín	Definícia
Certifikačný orgán (CA)	Subjekt, ktorý vydáva digitálne certifikáty
CH	Švajčiarska konfederácia
ETS	Systém obchodovania s emisiami
EÚ	Európska únia
IMT	Tím pre riadenie incidentov
Informačné aktívum	Informácia, ktorá je cenná pre spoločnosť alebo organizáciu
IT	Informačné technológie
ITIL	Knižnica pre infraštruktúru informačných technológií
ITSM	Riadenie služieb v oblasti informačných technológií
LTS	Prepájacie technické normy
Register	Systém účtovania kvót vydaných v rámci ETS, ktorý sleduje vlastníctvo kvót vedených na elektronických účtoch.
RFC	Žiadosť o zmenu
SIL	Zoznam citlivých informácií
SR	Žiadosť o službu
Wiki	Webové sídlo, na ktorom si používatelia môžu vymieňať informácie a poznatky pridaním alebo prispôsobením obsahu priamo prostredníctvom webového prehliadača.

2. ÚVOD

V dohode medzi Európskou úniou a Švajčiarskou konfederáciou o prepojení ich systémov obchodovania s emisiami skleníkových plynov z 23. novembra 2017 (ďalej len „dohoda“) sa stanovuje vzájomné uznávanie emisných kvót, ktoré možno použiť na dosiahnutie súladu v rámci systému obchodovania s emisiami Európskej únie (ďalej len „EU ETS“) alebo systému obchodovania s emisiami Švajčiarska (ďalej len „ETS Švajčiarska“). S cieľom realizovať prepojenie medzi EU ETS a ETS Švajčiarska sa zriadi priame prepojenie medzi protokolom transakcií Európskej únie (European Union Transaction Log – EUTL) registra Únie a dodatkovým protokolom transakcií Švajčiarska (Swiss Supplementary Transaction Log – SSTL) švajčiarskeho registra, čím sa umožní prenos emisných kvót vydaných v rámci ktoréhokoľvek z týchto dvoch ETS medzi registrami (článok 3 ods. 2 dohody). S cieľom sfunkčniť prepojenie medzi EU ETS a ETS Švajčiarska sa bude od mája 2020 alebo čo najskôr po uvedenom mesiaci uplatňovať predbežné riešenie. zmluvné strany sú povinné spolupracovať na čo možno najvčasnejšom nahradení predbežného riešenia trvalým prepojením registrov (príloha II dohody).

Podľa článku 3 ods. 6 dohody švajčiarsky správca registra a ústredný správca registra Únie sú povinní stanoviť spoločné operačné postupy týkajúce sa technických alebo iných záležitostí, ktoré sú potrebné na fungovanie prepojenia, pričom sú povinní vziať do úvahy priority domácich právnych predpisov. Spoločné operačné postupy vypracované správcami nadobudnú účinnosť po prijatí rozhodnutia spoločného výboru.

Spoločné operačné postupy uvedené v tomto dokumente, má prijať spoločný výbor rozhodnutím č. 1/2020. V súlade s týmto rozhodnutím spoločný výbor požiada švajčiarskeho správcu registra a ústredného správcu registra Únie, aby vypracovali ďalšie technické usmernenia s cieľom sfunkčniť prepojenie a zabezpečiť, aby sa tieto usmernenia neustále prispôsobovali technickému pokroku a novým požiadavkám týkajúcim sa bezpečnosti a zabezpečenia prepojenia, ako aj jeho účinného a efektívneho fungovania.

2.1. Rozsah pôsobnosti

Tento dokument predstavuje všeobecnú zhodu zmluvných strán dohody týkajúcu sa vytvorenia procesných základov prepojenia medzi registrami EU ETS a ETS Švajčiarska. I keď sa v ňom uvádzajú celkové procedurálne požiadavky z hľadiska fungovania, na sfunkčnenie prepojenia budú potrebné ďalšie technické usmernenia.

Pokiaľ ide o riadne fungovanie, prepojenie si bude vyžadovať technické špecifikácie slúžiace na zabezpečenie jeho ďalšieho sfunkčnenia. Podľa článku 3 ods. 7 dohody sa tieto záležitosti podrobne uvádzajú v dokumente týkajúcom sa prepájacích technických noriem, ktorý sa má prijať samostatne, a to rozhodnutím spoločného výboru.

Cieľom spoločných operačných postupov je zabezpečiť, aby boli IT služby súvisiace s fungovaním prepojenia medzi registrami EU ETS a ETS Švajčiarska vykonávané efektívne a účinne, najmä pokiaľ ide o vybavovanie žiadostí o službu, riešenie zlyhania služby, odstraňovanie problémov, ako aj vykonávanie bežných prevádzkových úloh podľa medzinárodných noriem pre riadenie IT služieb.

V prípade odsúhlaseného predbežného riešenia budú potrebné iba tieto spoločné operačné postupy, ktoré sú súčasťou tohto dokumentu:

- Riadenie incidentov
- Riadenie problémov
- Vybavovanie žiadosti

- Riadenie zmien
- Riadenie vydaní
- Riadenie bezpečnostných incidentov
- Riadenie bezpečnosti informácií

Pri neskoršom zavedení trvalého prepojenia registrov sa musia spoločné operačné postupy v prípade potreby prispôsobiť a doplniť.

2.2. Adresáti

Cieľovou skupinou týchto spoločných operačných postupov sú podporné tímy registrov EÚ a Švajčiarska.

3. PRÍSTUP A NORMY

Na všetky spoločné operačné postupy sa vzťahuje táto zásada:

- EÚ a Švajčiarsko sa dohodli na vymedzení spoločných operačných postupov na základe ITIL (knižnica pre infraštruktúru informačných technológií, verzia 3). Uplatňujú sa postupy uvedené v tejto norme, ktoré sú prispôsobené osobitným potrebám súvisiacim s dočasným riešením.
- Komunikácia a koordinácia potrebná na spracovanie spoločných operačných postupov medzi obidvoma zmluvnými stranami sa uskutočňuje prostredníctvom centier podpory registrov Švajčiarska a EÚ. Úlohy sa vždy prideľujú v rámci jednej zmluvnej strany.
- Ak nedôjde k dohode o spôsobe pristupovania k spoločným operačným postupom, obidve centrá zanalyzujú a medzi sebou vyriešia túto otázku. Ak dohodu nie je možné dosiahnuť, nájdenie spoločného riešenia sa postúpi o úroveň vyššie.

Úrovne postúpenia	**EÚ**	**CH**
1. úroveň	Centrum podpory EÚ	Centrum podpory Švajčiarska
2. úroveň	Manažér operačných postupov EÚ	Švajčiarsky manažér pre aplikáciu registra
3. úroveň	Spoločný výbor (ktorý by mohol delegovať túto zodpovednosť podľa článku 12 ods. 5 dohody)	
4. úroveň	Spoločný výbor, ak je delegovaná 3. úroveň	

- Každá zmluvná strana môže určiť postupy fungovania svojho vlastného registračného systému, pričom zohľadní požiadavky a rozhrania týkajúce sa týchto spoločných operačných postupov.
- Nástroj riadenia IT služieb (ITSM) sa používa na podporu spoločných operačných postupov, najmä riadenie incidentov, riešenie problémov a vybavovanie žiadostí a komunikáciu medzi obidvoma zmluvnými stranami.
- Okrem toho je povolená výmena informácií e-mailom.
- Obidve zmluvné strany zabezpečia, aby boli požiadavky na informačnú bezpečnosť splnené v súlade s pokynmi pre zaobchádzanie s informáciami.

4. RIADENIE INCIDENTOV

Cieľom procesu riadenia incidentov je čo najrýchlejšie a s minimálnym narušením prevádzky vrátiť IT služby na prevádzkovú úroveň.

Pri riadení incidentov by sa mali viesť aj záznamy o incidentoch na účely podávania správ a tento proces by mal byť integrovaný s inými procesmi s cieľom neustále ho zlepšovať.

- Z globálneho hľadiska riadenie incidentov zahŕňa tieto činnosti:
- zisťovanie a zaznamenávanie incidentov,
- klasifikácia a počiatočná podpora,
- vyšetrovanie a diagnostika,
- riešenie krízových situácií a obnova služby,
- uzavretie incidentu.

Počas celého trvania incidentu sa v rámci procesu riadenia incidentov neustále zabezpečuje zodpovednosť povolaných osôb, monitorovanie, sledovanie a komunikácia.

4.1. Zisťovanie a zaznamenávanie incidentov

Incident môže odhaliť podporná skupina, automatizované monitorovacie nástroje alebo technický personál vykonávajúci rutinný dohľad.

Po zistení sa incident musí zaznamenať a musí sa mu prideliť jednoznačný identifikátor umožňujúci jeho riadne sledovanie a monitorovanie. Jedinečný identifikátor incidentu je identifikátor, ktorý mu v spoločnom systéme tiketovania pridelí centrum podpory danej zmluvnej strany (EÚ alebo Švajčiarska), ktoré incident odhalilo, a musí sa používať v každej komunikácii týkajúcej sa tohto incidentu.

V prípade všetkých incidentov by kontaktným bodom malo byť to centrum podpory zmluvnej strany, ktoré daný tiket zaregistrovalo.

4.2. Klasifikácia a počiatočná podpora

Cieľom klasifikácie incidentov je zistiť a určiť, aký systém a/alebo služba sú zasiahnuté a do akej miery. Aby bola klasifikácia účinná, mala by nasmerovať incident k správnemu tímu na prvýkrát, aby sa urýchlilo jeho vyriešenie.

Klasifikačná fáza by mala kategorizovať incident a určiť jeho prioritu podľa jeho vplyvu a naliehavosti, aby mohol byť riešený podľa harmonogramu danej priority.

Ak má incident potenciálny vplyv na dôvernosť alebo integritu citlivých údajov a/alebo na dostupnosť systému, daný incident sa zároveň označí za bezpečnostný incident a následne sa rieši podľa postupu vymedzeného v kapitole „Správa incidentov v oblasti bezpečnosti“ tohto dokumentu.

Ak je to možné, centrum podpory, ktoré zaregistrovalo tento tiket, vykoná prvú diagnostiku. Centrum podpory pritom zistí, či v prípade daného incidentu ide o známu chybu. Ak áno, potom je postup riešenia alebo dočasné riešenie už známe a zdokumentované.

Ak centrum podpory tento incident úspešne vyrieši, potom ho v tomto okamihu uzavrie, keďže primárny účel riadenia incidentov (teda rýchle obnovenie služby pre koncového používateľa) bol splnený. Ak to tak nie je, centrum podpory tento incident postúpi príslušnej riešiteľskej skupine na ďalšie vyšetrovanie a diagnostiku.

4.3. Vyšetrovanie a diagnostika

Vyšetrovanie a diagnostika incidentov sa uplatňujú v prípade, že centrum podpory nemôže v rámci počiatočnej diagnostiky vyriešiť daný incident, a preto ho náležite postúpi ďalej. Postúpenie incidentov je plnohodnotnou súčasťou procesu vyšetrovania a diagnostiky.

Bežnou praxou vo fáze vyšetrovania a diagnostiky je pokus zopakovať incident za kontrolovaných podmienok. Pri vykonávaní vyšetrovania a diagnostiky incidentu je dôležité, aby sa zistilo správne poradie udalostí, ktoré k incidentu viedli.

Postúpenie je uznanie toho, že incident nemožno vyriešiť na úrovni daného centra podpory a musí sa postúpiť podpornej skupine na vyššej úrovni alebo druhej zmluvnej strane. Postúpenie môže prebiehať dvomi spôsobmi: horizontálne (funkčne) alebo vertikálne (hierarchicky).

Centrum podpory, ktoré incident zaznamenalo a začalo ho riešiť, je zodpovedné za postúpenie incidentu príslušnému tímu a za sledovanie celkového stavu a pridelenie incidentu.

Zmluvná strana, ktorej bol incident pridelený, je zodpovedná za zabezpečenie včasnej realizácie požadovaných opatrení a za poskytnutie spätnej väzby svojmu vlastnému centru podpory.

4.4. Riešenie krízových situácií a obnova služby

Keď sa incident úplne preskúma, dôjde k jeho riešeniu a obnove služby. Nájdenie riešenia incidentu znamená, že spôsob nápravy tohto problému bol identifikovaný. Realizácia riešenia je fázou obnovy služby.

Po tom, ako príslušné tímy vyriešia zlyhanie služby, incident je postúpený späť príslušnému centru podpory, ktoré incident zaregistrovalo, a u iniciátora incidentu sa potvrdí, že chyba bola odstránená a že incident možno uzavrieť. Zistenia zo spracovania incidentu sa zaznamenajú na budúce použitie.

Obnovu služby môže vykonať personál IT podpory alebo sa koncovému používateľovi poskytne súbor pokynov, podľa ktorých má postupovať.

4.5. Uzavretie incidentu

Uzavretie je posledným krokom v procese riadenia incidentov a uskutoční sa krátko po vyriešení incidentu.

V rámci kontrolného zoznamu činností, ktoré je potrebné počas fázy uzavretia incidentu vykonať, treba zdôrazniť:

- overenie počiatočnej kategorizácie, ktorá bola priradená k incidentu,
- správne zachytenie všetkých informácií týkajúcich sa incidentu,
- riadne zdokumentovanie incidentu a aktualizáciu vedomostnej základne,
- primeranú komunikáciu s každou zainteresovanou stranou, ktorej sa incident priamo alebo nepriamo dotýka.

Incident sa formálne uzavrie vtedy, keď centrum podpory ukončí fázu uzavretia incidentu a oznámi to druhej zmluvnej strane.

Keď je incident uzavretý, znovu sa neotvára. Ak v krátkom čase dôjde k opätovnému výskytu incidentu, pôvodný incident sa znovu neotvára, namiesto toho sa musí zaregistrovať nový incident.

Ak incident sledujú centrá podpory EÚ a Švajčiarska, konečné uzavretie je zodpovednosťou toho centra podpory, ktoré tiket zaregistrovalo.

5. RIADENIE PROBLÉMOV

Tento postup by sa mal dodržať vždy, keď sa zistí problém, čím sa spúšťa proces riadenia problémov. Riadenie problémov sa zameriava na zvýšenie kvality a zníženie objemu výskytu incidentov. Problém môže byť príčinou jedného alebo viacerých incidentov. Ak sa podá správa o incidente, cieľom riadenia incidentov je obnoviť danú službu čo najrýchlejšie, aj pomocou dočasných riešení. Keď vznikne problém, cieľom je vyšetriť hlavnú príčinu problému, aby sa identifikovala zmena, ktorá zabezpečí, že problém a súvisiace incidenty sa už neobjavia.

5.1. Identifikácia a záznam problému

V závislosti od toho, ktorá zmluvná strana iniciovala tiket, kontaktným miestom pre otázky súvisiace s daným problémom bude centrum podpory EÚ alebo Švajčiarska.

Jedinečný identifikátor problému je identifikátor, ktorý mu pridelí riadenie IT služieb (ITSM). Musí sa používať pri každej komunikácii týkajúcej sa daného problému.

Problém môže spôsobiť incident alebo môže byť otvorený samostatne s cieľom odstrániť problémy zistené v systéme, a to v akejkoľvek fáze.

5.2. Priorizácia problému

Problémy sa môžu kategorizovať podľa ich závažnosti a priority rovnako ako incidenty s cieľom uľahčiť ich sledovanie, pričom sa zohľadní vplyv súvisiacich incidentov a frekvencia ich výskytu.

5.3. Vyšetrovanie a diagnostika problému

Každá zmluvná strana môže nastoliť problém a centrum podpory iniciujúcej zmluvnej strany bude zodpovedné za jeho zaregistrovanie, pridelenie príslušnému tímu a sledovanie jeho celkového stavu.

Riešiteľská skupina, ktorej bol problém postúpený, je zodpovedná za včasné riešenie problému a za komunikáciu s centrom podpory.

Obidve zmluvné strany sú na požiadanie zodpovedné za zabezpečenie vykonávania pridelených opatrení a za poskytnutie spätnej väzby svojmu vlastnému centru podpory.

5.4. Vyriešenie

Riešiteľská skupina, ktorej je problém pridelený, je zodpovedná za vyriešenie tohto problému a poskytnutie príslušných informácií svojmu vlastnému centru podpory.

Zistenia zo spracovania problému sa majú zaznamenať na budúce použitie.

5.5. Uzavretie problému

Problém sa formálne uzavrie, keď sa problém vyrieši vykonaním zmeny. Centrum podpory, ktoré zaregistrovalo problém, ukončí fázu uzavierania problému a informuje o tom centrum podpory druhej zmluvnej strany.

6. VYBAVOVANIE ŽIADOSTI

Proces vybavovania žiadosti je komplexné vybavovanie žiadosti o novú alebo existujúcu službu od okamihu jej zaregistrovania a schválenia až do momentu jej uzavretia. Žiadosti o

služby majú zvyčajne menší rozsah, sú vopred definované, opakovateľné, časté, vopred schválené a majú charakter procedurálnych žiadostí.

Hlavné kroky, ktoré sa musia dodržať, sú uvedené ďalej:

6.1. Iniciovanie žiadosti

Informácie súvisiace so žiadosťou o službu sa predkladajú centru podpory EÚ alebo Švajčiarska e-mailom, telefonicky alebo prostredníctvom nástroja riadenia IT služieb (ITSM) alebo akéhokoľvek iného dohodnutého komunikačného kanála.

6.2. Registrovanie a analýza žiadostí

Pre všetky žiadosti o službu by kontaktným miestom malo byť centrum podpory EÚ alebo Švajčiarska, v závislosti od toho, ktorá zmluvná strana žiadosť o službu predložila. Toto centrum podpory bude zodpovedné za riadnu registráciu a analýzu žiadosti o službu.

6.3. Schválenie žiadosti

Pracovník centra podpory zmluvnej strany, ktorá žiadosť o službu podala, skontroluje, či je potrebné schválenie druhej zmluvnej strany, a ak áno, tak si ho vyžiada. Ak žiadosť o službu nie je schválená, centrum podpory tiket aktualizuje a uzavrie ho.

6.4. Vybavovanie žiadosti

Tento krok slúži na účinné a efektívne spracovanie žiadostí o služby. Treba rozlišovať medzi týmito prípadmi:

- Vybavovanie žiadosti o službu sa týka len jednej zmluvnej strany. V tomto prípade táto zmluvná strana vydá pracovné príkazy a koordinuje vykonanie.
- Realizácia žiadosti o službu má vplyv na systém EÚ aj Švajčiarska. V tomto prípade vydávajú centrá podpory pracovné príkazy vo svojej oblasti zodpovednosti. Spracovanie vybavovania žiadosti sa koordinuje medzi obidvoma centrami podpory. Celkovú zodpovednosť nesie to centrum podpory, ktoré dostalo a iniciovalo žiadosť o službu.

Keď bola žiadosť o službu vyriešená, musí sa umiestniť do stavu „vyriešené“.

6.5. Postúpenie žiadosti

Centrum podpory môže v prípade potreby postúpiť nevybavenú žiadosť o službu príslušnému tímu (tretia strana).

Žiadosť sa postupuje príslušným tretím stranám, t. j. centrum podpory EÚ bude musieť postupovať cez centrum podpory Švajčiarska, ak má byť žiadosť postúpená švajčiarskej tretej strane a naopak.

Tretia strana, ktorej bola postúpená žiadosť o službu, je zodpovedná za včasné riešenie žiadosti o službu a za komunikáciu s centrom podpory, ktorá jej žiadosť o službu postúpila.

Centrum podpory, ktoré zaregistrovalo žiadosť o službu, je zodpovedné za sledovanie jej celkového stavu a jej pridelenie.

6.6. Kontrola vybavovania žiadostí

Pred uzavretím žiadosti predkladá príslušné centrum podpory správu o žiadosti o službu na účely konečnej kontroly kvality. Cieľom je zabezpečiť, aby sa daná žiadosť o službu skutočne spracovala a aby sa dostatočne podrobne uviedli všetky informácie potrebné na opis

životného cyklu žiadosti. Okrem toho sa zistenia zo spracovania žiadosti majú zaznamenať pre budúce použitie.

6.7. Uzavretie žiadosti

Ak sa zmluvné strany, ktorým bola žiadosť o službu pridelená, dohodnú, že daná žiadosť bola vybavená, a žiadateľ sa domnieva, že daný prípad je vyriešený, nastaví sa stav „uzavreté“.

Žiadosť o službu sa formálne uzavrie vtedy, keď centrum podpory, ktoré danú žiadosť o službu zaregistrovalo, ukončí fázu uzavretia žiadosti a informuje o tom centrum podpory druhej zmluvnej strany.

7. RIADENIE ZMIEN

Cieľom je zabezpečiť, aby sa používali štandardizované metódy a postupy na efektívne a rýchle spracovanie všetkých zmien týkajúcich sa kontroly IT infraštruktúry s cieľom minimalizovať počet akýchkoľvek súvisiacich incidentov a ich vplyv na službu. Zmeny v IT infraštruktúre môžu vzniknúť v reakcii na problémy alebo externe vznesené požiadavky, napr. legislatívne zmeny, alebo proaktívne na účely zlepšenia efektívnosti a účinnosti alebo s cieľom umožniť obchodné iniciatívy alebo ich zohľadniť.

Proces riadenia zmien zahŕňa rôzne kroky, ktoré zachytávajú všetky podrobnosti týkajúce sa žiadosti o zmenu na účely budúceho sledovania. Týmito procesmi sa zabezpečuje, aby sa zmena pred zavedením validovala a otestovala. Úspešné zavedenie zmeny sa realizuje prostredníctvom procesu riadenia vydaní.

7.1. Žiadosť o zmenu

Žiadosť o zmenu (RFC) sa predkladá tímu pre riadenie zmien na validáciu a schválenie. V prípade všetkých žiadostí o zmenu by kontaktným bodom malo byť centrum podpory EÚ alebo Švajčiarska, v závislosti od toho, ktorá zmluvná strana žiadosť predložila. Toto centrum podpory bude zodpovedné za riadnu registráciu a analýzu žiadosti.

K predloženiu žiadostí o zmenu môže dôjsť z dôvodu:

- incidentu, ktorý zmenu spôsobí,
- existujúceho problému, v dôsledku ktorého dôjde k zmene,
- požiadavky na novú zmenu zo zmluvnej strany koncového používateľa,
- zmeny v dôsledku prebiehajúcej údržby,
- legislatívnej zmeny.

7.2. Hodnotenie a plánovanie zmien

Táto etapa sa týka posudzovania zmien a činností plánovania. Zahŕňa činnosti priorizácie a plánovania s cieľom minimalizovať riziko a vplyv.

Ak má vykonávanie RFC vplyv tak na EÚ, ako aj na Švajčiarsko, zmluvná strana, ktorá RFC zaregistrovala, v spolupráci s druhou stranou overí hodnotenie a plánovanie danej zmeny.

7.3. Schválenia zmien

Každá zaregistrovaná žiadosť o zmenu sa musí schváliť na príslušnej úrovni postúpenia.

7.4. Vykonanie zmeny

Vykonanie zmeny sa vykonáva formou riadenia vydaní. Tímy obidvoch zmluvných strán pre riadenie vydaní postupujú podľa vlastných postupov, ktoré zahŕňajú plánovanie a testovanie.

Po dokončení vykonania zmeny sa uskutoční kontrola zmeny. V záujme postupu podľa plánu sa existujúci proces riadenia zmien neustále prehodnocuje a v prípade potreby aktualizuje.

8. RIADENIE VYDANÍ

Vydanie predstavuje jednu alebo viacero zmien IT služieb súhrnne uvedených v pláne vydaní, ktoré budú musieť byť povolené, pripravené, vytvorené, otestované a zavedené. Jedno vydanie môže predstavovať opravu chyby, zmenu hardvéru alebo iných komponentov, zmeny softvéru, aktualizáciu verzií aplikácií, zmeny dokumentácie a/alebo procesov. Obsah každého vydania sa riadi, testuje a zavádza ako jeden celok.

Cieľom riadenia vydaní je naplánovať, vytvoriť, otestovať a validovať a pritom zabezpečiť schopnosť poskytovať navrhované služby, prostredníctvom ktorých sa budú plniť požiadavky zainteresovaných strán a dosahovať plánované ciele. Počas koordinácie návrhu sa zadefinujú a zdokumentujú kritériá prijateľnosti týkajúce sa všetkých zmeny danej služby a poskytnú sa tímom zodpovedným za riadenie vydaní.

Vydanie zvyčajne pozostáva z viacerých opráv problémov a vylepšení služby. Obsahuje požadovaný nový alebo zmenený softvér a akýkoľvek nový alebo zmenený hardvér potrebný na vykonanie schválených zmien.

8.1. Plánovanie vydania

Prvým krokom v tomto procese je priradenie schválených zmien do balíkov vydaní a definovanie rozsahu a obsahu vydaní. Na základe týchto informácií sa v rámci čiastkového procesu plánovania vydaní vypracuje harmonogram vytvorenia, testovania a zavedenia vydania.

V rámci plánovania by sa mal zadefinovať:

- rozsah a obsah vydania,
- posúdenie rizika a rizikový profil vydania,
- klient/používatelia, ktorých sa vydanie dotkne,
- tím zodpovedný za vydanie,
- stratégia realizácie a zavedenia,
- zdroje pre dodanie a zavedenie.

Obidve zmluvné strany sa navzájom informujú o plánovaní svojich vydaní a časoch údržby. Ak sa vydanie týka tak EÚ, ako aj Švajčiarska, koordinujú plánovanie a určujú spoločný čas údržby.

8.2. Vytvorenie a otestovanie balíka vydaní

Pri vytváraní a testovaní procesu riadenia vydaní sa stanoví prístup realizácie vydania alebo balíka vydaní a údržby kontrolovaného prostredia pred zmenou produkcie, ako aj testovanie všetkých zmien vo všetkých zavedených prostrediach.

Ak sa vydanie týka EÚ, ako aj Švajčiarska, koordinujú plány dodania a testovanie. Patria sem tieto aspekty:

- spôsob a čas dodania jednotiek vydania a komponentov služby,
- aké sú obvyklé časy realizácie; čo sa stane, ak dôjde k oneskoreniu,
- ako sledovať napredovanie dodávky a získať potvrdenie,

- kritériá na monitorovanie a určenie úspešnosti zavádzania vydania,
- spoločné testovacie prípady pre príslušné funkcie a zmeny.

Na konci tohto čiastkového procesu sú všetky požadované komponenty vydania pripravené na vstup do fázy spustenia reálnej prevádzky.

8.3. Príprava na zavedenie

Prípravný čiastkový proces zabezpečuje, aby boli komunikačné plány definované správne a oznámenia pripravené na odoslanie všetkým dotknutým zainteresovaným stranám a konečným používateľom a aby sa dané vydanie začlenilo do procesu riadenia zmien s cieľom zabezpečiť kontrolované vykonanie všetkých zmien a ich schválenie požadovanými subjektmi.

Ak sa vydanie týka EÚ, ako aj Švajčiarska, obidve zmluvné strany koordinujú tieto činnosti:

- záznam žiadosti o zmenu v súvislosti s plánovaním a prípravou zavedenia do produkčného prostredia,
- vytvorenie plánu vykonávania,
- spôsob návratu, aby bolo v prípade zlyhania zavedenia možné vrátiť predchádzajúci stav,
- oznámenia zaslané všetkým stranám,
- žiadosť o schválenie realizácie vydania na príslušnej úrovni postúpenia.

8.4. Návrat do pôvodného stavu

Ak sa zavedenie nepodarilo zrealizovať alebo z testovania vyplynulo, že zavedenie nebolo úspešné alebo nezodpovedalo dohodnutým kritériám prijateľnosti/kvality, tímy obidvoch zmluvných strán, ktoré sú zodpovedné za riadenie vydaní, budú musieť vrátiť systém do pôvodného stavu. Bude potrebné informovať všetky potrebné zainteresované strany vrátane dotknutých koncových používateľov. Až do schválenia sa proces môže znovu začať v ktorejkoľvek z predchádzajúcich etáp.

8.5. Preskúmanie a uzavretie vydania

Pri kontrole zavedenia by sa mali vykonať tieto činnosti:

- získať spätnú väzbu o spokojnosti zákazníkov a používateľov s dodaním a zavedením služby (zhromaždiť spätnú väzbu a zohľadniť ju pri neustálom zlepšovaní služby),
- preskúmať všetky kritériá kvality, ktoré neboli splnené,
- skontrolovať, či sú všetky opatrenia, potrebné opravy a zmeny kompletné,
- zabezpečiť, aby po dokončení zavedenia nezostali nevyriešené žiadne otázky týkajúce sa funkčnosti, zdrojov, kapacity alebo výkonnosti,
- skontrolovať, či sú všetky problémy, známe chyby a dočasné riešenia zdokumentované a akceptované zákazníkom, koncovými používateľmi, prevádzkovou podporou a inými dotknutými stranami,
- monitorovať incidenty a problémy spôsobené zavedením (poskytnúť podporu operačným tímom v začiatočnej fáze v prípade, že vydanie spôsobilo zvýšenie objemu práce),

- aktualizovať podpornú dokumentáciu (t. j. technické informačné dokumenty),
- formálne odovzdať zavedenie vydania do prevádzkových operácií,
- zdokumentovať získané poznatky,
- zhromaždiť od realizačných tímov súhrnnú dokumentáciu o vydaní,
- formálne uzavrieť vydanie po overení záznamu týkajúceho sa žiadosti o zmenu.

9. RIADENIE BEZPEČNOSTNÝCH INCIDENTOV

Riadenie bezpečnostných incidentov je proces riešenia bezpečnostných incidentov, s cieľom informovať potenciálne ovplyvnené zainteresované strany o incidente; hodnotenie incidentu a priorizácia a reakcia na incident v záujme vyriešenia všetkých skutočných alebo potenciálnych narušení dôvernosti, dostupnosti alebo integrity citlivých informačných aktív alebo podozrení na takéto narušenie.

9.1. Kategorizácia incidentov informačnej bezpečnosti

Všetky incidenty, ktoré majú vplyv na prepojenie medzi registrom Únie a švajčiarskym registrom, sa analyzujú s cieľom určiť možné narušenie dôvernosti, integrity alebo dostupnosti akýchkoľvek citlivých informácií zaznamenaných v zozname citlivých informácií (SIL).

V kladnom prípade sa incident charakterizuje ako incident informačnej bezpečnosti, ktorý sa okamžite zaregistruje v nástroji riadenia IT služieb (ITSM) a ako taký sa riadi.

9.2. Riešenie incidentov informačnej bezpečnosti

Bezpečnostné incidenty sa riešia na 3. úroveň postúpenia, pričom riešením incidentov sa bude zaoberať osobitný tím pre riadenie incidentov (IMT).

IMT je zodpovedný za:

- vykonanie prvej analýzy, kategorizovanie a stanovenie závažnosti incidentu,
- koordináciu činností všetkých zainteresovaných strán vrátane úplného zdokumentovania analýzy konkrétneho incidentu, rozhodnutí prijatých na riešenie daného incidentu a možných zistených nedostatkov,
- v závislosti od závažnosti bezpečnostného incidentu za včasné postúpenie na príslušnú úroveň na účely informovania a/alebo rozhodnutia.

V procese riadenia bezpečnosti informácií sú všetky informácie týkajúce sa udalostí klasifikované na najvyššej úrovni citlivosti informácií, v každom prípade však minimálne ako ETS SENSITIVE.

V prípade prebiehajúceho vyšetrovania a/alebo nedostatku, ktorý by sa mohol zneužiť, až pokým nedôjde k odstráneniu predmetného problému, sa informácie klasifikujú ako ETS CRITICAL.

9.3. Identifikácia bezpečnostných incidentov

Na základe typu bezpečnostného incidentu určí pracovník pre bezpečnosť informácií príslušné organizácie, ktoré majú byť zapojené do činností IMT a ktoré majú byť súčasťou tohto tímu.

9.4. Analýza bezpečnostných incidentov

Pri skúmaní incidentu spolupracuje IMT so všetkými zainteresovanými organizáciami a podľa potreby s príslušnými členmi ich tímov. Počas analýzy sa určí rozsah dôvernosti, integrity alebo straty dostupnosti aktív a posúdia sa dôsledky pre všetky dotknuté organizácie. Ďalej sa vymedzia počiatočné a následné opatrenia na vyriešenie incidentu a na riadenie jeho vplyvu vrátane vplyvu týchto opatrení na zdroje.

9.5. Posudzovanie závažnosti bezpečnostných incidentov, postúpenie a podávanie správ

IMT posúdi závažnosť každého nového bezpečnostného incidentu po jeho charakterizácii a okamžite začne s realizáciou potrebného opatrenia podľa závažnosti incidentu.

9.6. Podávanie správ o reakcii na bezpečnostný incident

IMT uvedie informácie o obmedzení dôsledkov incidentu a výsledky obnovy služby v správe o reakcii na incident informačnej bezpečnosti. Správa sa predkladá na 3. úrovni postúpenia pomocou zabezpečeného e-mailu alebo iných vzájomne akceptovaných prostriedkov bezpečnej komunikácie.

Zodpovedná zmluvná strana preskúma obmedzenia dôsledkov a výsledky obnovy služby a:

- opäť pripojí register v prípade, že bol predtým odpojený,
- zabezpečí komunikáciu o incidente s tímami zodpovednými za správu registra,
- uzavrie incident.

IMT by mal zabezpečeným spôsobom v správe o reakcii na incident informačnej bezpečnosti uviesť relevantné podrobnosti s cieľom zabezpečiť konzistentné zaznamenávanie a komunikáciu a umožniť okamžité a náležité opatrenia na obmedzenie dôsledkov incidentu. Po jeho dokončení predloží IMT v príslušnej lehote záverečnú správu o reakcii na incident informačnej bezpečnosti.

9.7. Monitorovanie, budovanie kapacít a kontinuálne zlepšovanie

IMT poskytne správy o všetkých bezpečnostných incidentoch 3. úrovni postúpenia. Správy budú použité na tejto úrovni postúpenia, aby bolo možné určiť:

- slabé miesta v bezpečnostných kontrolách alebo operačnom postupe, ktoré treba posilniť,
- prípadné potreby zdokonaliť tento postup s cieľom zlepšiť jeho účinnosť pri reakcii na incidenty,
- možnosti školenia a budovania kapacít v záujme ďalšieho posilnenia odolnosti registračných systémov v oblasti bezpečnosti informácií, znižovania rizika budúcich incidentov a minimalizovania ich vplyvu.

10. RIADENIE BEZPEČNOSTI INFORMÁCIÍ

Cieľom riadenia informačnej bezpečnosti je zabezpečiť dôvernosť, integritu a dostupnosť utajovaných skutočností, údajov a IT služieb organizácie. Okrem technických komponentov vrátane ich návrhu a testovania (pozri LTS) sú na splnenie bezpečnostných požiadaviek pre predbežné riešenie potrebné tieto spoločné operačné postupy.

10.1. Identifikácia citlivých informácií

Citlivosť informácií sa posudzuje stanovením, aký vplyv na podnik by mohlo mať narušenie bezpečnosti v prípade tejto informácie (napr. finančné straty, poškodenie povesti, porušenie právnych predpisov...).

Citlivé informačné aktíva sa identifikujú na základe ich vplyvu na prepojenie.

Úroveň citlivosti týchto informácií sa posudzuje podľa škály citlivosti, ktorá sa uplatňuje na toto prepojenie a je podrobne opísaná v oddiele tohto dokumentu „Riešenie incidentov informačnej bezpečnosti“.

10.2. Úrovne citlivosti informačných aktív

Informačné aktívum sa pri svojej identifikácii klasifikuje podľa týchto pravidiel:

- pri identifikácii aspoň jednej VYSOKEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako ETS CRITICAL,
- pri identifikácii aspoň jednej STREDNEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako ETS SENSITIVE,
- pri identifikácii iba NÍZKEJ úrovne dôvernosti, integrity alebo dostupnosti sa aktívum klasifikuje ako ETS LIMITED.

10.3. Priradenie vlastníka informačných aktív

Všetky informačné aktíva by mali mať priradeného vlastníka. Informačné aktíva ETS, ktoré patria k prepojeniu medzi EUTL a SSTL alebo sú s ním spojené, by sa mali uviesť v spoločnom inventúrnom súpise aktív vedenom obidvomi zmluvnými stranami. Informačné aktíva ETS mimo prepojenia medzi EUTL a SSTL by sa mali zahrnúť do inventúrneho súpisu aktív, ktorý vedie príslušná zmluvná strana.

zmluvné strany sa majú dohodnúť na vlastníctve každého informačného aktíva, ktoré patrí k prepojeniu medzi EUTL a SSTL, alebo je s ním spojené. Vlastník informačného aktíva je zodpovedný za posúdenie jeho citlivosti.

Vlastník by mal mať pracovníkov s funkciami a skúsenosťami zodpovedajúcimi hodnote prideleného aktíva, resp. aktív. Mala by sa dohodnúť a formalizovať zodpovednosť vlastníka za aktívum, resp. aktíva, ako aj za povinnosť zachovávať požadovanú úroveň dôvernosti, integrity a dostupnosti.

10.4. Registrácia citlivých informácií

Všetky citlivé informácie sa registrujú v zozname citlivých informácií.

V relevantných prípadoch sa zohľadní a v zozname citlivých informácií zaregistruje súhrn citlivých informácií, ktorý by mohol mať väčší vplyv, ako je vplyv jedinej informácie (napr. súbor informácií uložených v databáze systému).

Zoznam citlivých informácií nemá stály charakter. Charakter hrozieb, zraniteľných miest či pravdepodobnosť alebo dôsledky bezpečnostných incidentov súvisiacich s aktívami sa môžu bez akéhokoľvek upozornenia meniť, pričom sa do prevádzky registračných systémov môžu zavádzať nové aktíva.

Zoznam citlivých informácií sa preto pravidelne preskúmava a akékoľvek nové informácie, ktoré sú označené za citlivé, sa do neho okamžite zaregistrujú.

Zoznam citlivých informácií návrh obsahuje v prípade každého zápisu aspoň tieto informácie:

- opis informácie,
- vlastníka informácie,
- úroveň citlivosti,
- upozornenie o tom, či informácie zahŕňajú osobné údaje,
- dodatočné informácie, ak sú potrebné.

10.5. Zaobchádzanie s citlivými informáciami

Ak sa citlivé informácie spracúvajú mimo prepojenia medzi registrom Únie a švajčiarskym registrom, spracúvajú sa v súlade s pokynmi pre zaobchádzanie.

Citlivé informácie spracúvané v prepojení medzi registrom Únie a švajčiarskym registrom sa spracúvajú v súlade s bezpečnostnými požiadavkami zmluvných strán.

10.6. Riadenie prístupu

Cieľom riadenia prístupu je udeliť oprávneným používateľom právo na využívanie služby a zároveň zabrániť prístupu neoprávnených používateľov. Riadenie prístupu sa niekedy označuje aj ako „riadenie práv“ alebo „riadenie totožnosti“.

V prípade predbežného riešenia a jeho fungovania potrebujú obidve zmluvné strany prístup k týmto komponentom:

- Wiki: prostredie pre spoluprácu na výmenu spoločných informácií, ako je plánovanie vydaní,
- nástroj riadenia IT služieb (ITSM) na riadenie incidentov a problémov (pozri kapitolu „Prístup a normy“),
- systém výmeny správ: každá zmluvná strana zabezpečuje bezpečný systém výmeny správ na účely prenosu správ obsahujúcich údaje o transakciách.

Švajčiarsky správca registra a ústredný správca registra Únie zabezpečujú, aby pre ich zmluvné strany boli prístupy aktuálne a fungovali ako kontaktné miesta, pokiaľ ide o činnosti súvisiace s riadením prístupu. Žiadosti o prístup sa riešia v súlade s postupmi vybavovania žiadosti.

10.7. Správa certifikátov/kľúčov

Každá zmluvná strana je zodpovedná za správu svojich vlastných certifikátov/kľúčov (generovanie, registrácia, ukladanie, inštalácia, používanie, predĺženie platnosti, zrušenie, zálohovanie a obnova platnosti certifikátov/kľúčov). Ako sa uvádza v prepájacích technických normách (LTS), musia sa používať len digitálne certifikáty vydané certifikačným orgánom (CA), ktorému obidve zmluvné strany dôverujú. Zaobchádzanie s certifikátmi/kľúčmi a ich uchovávanie musí byť v súlade s ustanoveniami uvedenými v pokynoch pre zaobchádzanie.

Každé zrušenie a/alebo predĺženie platnosti certifikátu a kľúča sa musí koordinovať obidvoma zmluvnými stranami. Tieto procesy prebiehajú v súlade s postupmi vybavovania žiadosti.

Švajčiarsky správca registra a ústredný správca registra Únie si vymenia certifikáty/kľúče cez zabezpečené komunikačné prostriedky podľa ustanovení uvedených v pokynoch pre zaobchádzanie.

Akékoľvek overovanie certifikátov/kľúčov medzi zmluvnými stranami sa uskutoční mimo IP sieť.