Security™
Standards Council

Maksājumu karšu industrijas (PCI)
Datu drošības standarta (DSS)

Pašnovērtējuma anketa (SAQ) C
un atbilstības apliecinājums

Maksājumu lietojumprogramma pieslēgta internetam, kartes lietotāju dati netiek glabāti elektroniski

2.0 versija

2010. gada oktobris

Pārmaiņas dokumentā

Datums	Versija	Apraksts
2008. gada oktobrī	1.2	Lai pielāgotu saturu jaunajām PCI DSS versijas 1.2 prasībām un ieviestu nelielas pārmaiņas, kas nepieciešamas salīdzinājumā ar versiju 1.1.
2010. gada 28. oktobrī	2.0	Lai pielāgotu saturu jaunajām PCI DSS versijas 2.0 prasībām un pārbaudes procedūrām.

Saturs

PCI datu drošības standarts: saistītie dokumenti

Lai palīdzētu komersantiem un pakalpojumu sniedzējiem izprast PCI DSS un PCI DSS SAQ (Pašnovērtējuma anketu), tika izstrādāti šādi dokumenti.

Dokuments	**Mērķauditorija**
PCI datu drošības standarta prasības un drošības novērtējuma procedūras	Visi komersanti un pakalpojumu sniedzēji
Kā orientēties PCI DSS: Izpratne par prasību mērķiem	Visi komersanti un pakalpojumu sniedzēji
PCI datu drošības standarts: Pašnovērtējuma vadlīnijas un instrukcijas	Visi komersanti un pakalpojumu sniedzēji
PCI datu drošības standarts: Pašnovērtējuma anketa A un apliecinājums	Atbilstošie komersanti[1]
PCI datu drošības standarts: Pašnovērtējuma anketa B un apliecinājums	Atbilstošie komersanti[1]
PCI datu drošības standarts: Pašnovērtējuma anketa C un apliecinājums	Atbilstošie komersanti[1]
PCI datu drošības standarts: Pašnovērtējuma anketa D un apliecinājums	Atbilstošie komersanti un visi pakalpojumu sniedzēji
PCI datu drošības standarta un maksājumu programmatūras datu drošības standarta termini, saīsinājumi un akronīmi	Visi komersanti un pakalpojumu sniedzēji

[1] Lai noteiktu piemēroto pašnovērtējuma anketu, sk. PCI datu drošības standartu: Pašnovērtējuma vadlīnijas un instrukcijas, "Kā izvēlēties Pašnovērtējuma anketu un apliecinājumu, kas vislabāk atbilst jūsu organizācijai."

Pirms jūs sākat

Pašnovērtējuma anketas aizpildīšana

SAQ **C** izstrādāta, lai aplūkotu prasības, kas piemērojamas komersantiem, kuri apstrādā maksājumu karšu lietotāju datus, izmantojot maksājumu lietojumprogrammas (piemēram, POS sistēmas), kas pieslēgtas internetam (ar ātrgaitas savienojumu, DSL, kabeļu modemu u.c.), bet neuzglabā karšu lietotāju datus datorsistēmās

Šīs maksājumu lietojumprogrammas tiek uzskatītas par pieslēgtām Internetam, ja :

1. maksājumu lietojumprogramma atrodas personālajā datorā, kurš pieslēgts internetam, vai
2. maksājumu lietojumprogramm lieto internetu, lai nosūtītu kartes lietotāja datus.

PCI DSS Pašnovērtējuma anketu instrukcijās un vadlīnijās SAQ C aizpildīšanai piemērotie komersanti tiek klasificēti kā Validācijas tipa 4 komersanti, ja tie apstrādā karšu lietotāju datus, izmantojot POS terminālus vai citas maksājumu lietojumprogrammas, kas pieslēgtas internetam, neuzglabā karšu lietotāju datus datorsistēmās. Tie var būt gan komersanti, kuriem ir reālas tirdzniecības vietas (ar kartes klātbūtni), vai arī komersanti, kas nodarbojas ar e-tirdzniecību vai pieņem pasūtījumus pa pastu vai tālruni (bez kartes klātbūtnes). Šādiem komersantiem ir jāpārbauda atbilstība, aizpildot SAQ C un ar to saistīto atbilstības apliecinājumu, apstiprinot, ka:

- Komersanta uzņēmumam ir maksājumu lietojumprogrammas sistēmas / (ierīces) interneta

pieslēgums, izmantojot to pašu ierīci un/vai lokālo tīklu (LAN);

- maksājumu lietojumprogramma/(ierīce) nav savienota ar citu sistēmu Komersanta vidē (uzņēmumā) (to var panākt, tīklu segmentējot, lai izolētu maksājumu lietojumprogrammas sistēmu/ ierīci no visām citām sistēmām);
- Komersanta veikalam nav pieslēguma citu veikalu tīkliem, un katram veikalam ir individuāli lietojams lokālais tīkls (LAN *(Local Area Network)*
- Komersanta uzņēmums saglabā pārskatus papīra dokumenta veidā vai čeku (kvīšu) papīra kopijas;
- Komersanta uzņēmums nesaglabā karšu lietotāju datus elektroniskā veidā; un
- Komersanta uzņēmuma maksājumu lietojumprogrammas piegādātājs izmanto drošas metodes, lai nodrošinātu attālināto atbalstu jūsu maksājumu sistēmai.

Katra šīs anketas sadaļa pievēršas konkrētai drošības jomai, pamatojoties uz PCI DSS un drošības novērtēšanas procedūras prasībām. Šajā saīsinātajā SAQ (Pašnovērtējuma anketas) versijā ir iekļauti jautājumi, kas piemērojami konkrētiem mazajiem komersantiem, kuru darbības vide atbilst iepriekš minētajiem atbilstības kritērijiem.

Lai nodrošinātu jūsu uzņēmuma atbilstību PCI DSS, jums jāizpilda visas piemērojamās PCI DSS prasības. Ja jums zināmas PCI DSS prasības, kas ir piemērojamas jūsu uzņēmumam un kuras nav iekļautas šajā Pašnovērtējuma anketā, tas, iespējams, norāda, ka šī anketa nav piemērota jūsu uzņēmumam.

PCI DSS atbilstība – aizpildīšanas kārtība

1. Novērtēt jūsu datu apstrādes vides un pielietoto tehnoloģiju atbilstību PCI DSS.
2. Aizpildīt Pašnovērtējuma anketu (SAQ C) saskaņā ar Pašnovērtējuma anketas instrukcijām un vadlīnijām.
3. Veikt ievainojamību neesamības pārbaudes (skenēšanu) , izmantojot PCI SSC apstiprinātu ievainojamību pārbaužu pakalpojumu sniedzēju (ASV) pakalpojumus . Ievainojamību esamības gadījumos novērst tās un atkārtot pārbaudes tikmēr, kamēr ir iegūti apmierinoši pārbaužu rezultāti.
4. Pilnībā aizpildīt atbilstības apliecinājuma sagatavi.
5. Iesniegt SAQ, apmierinošu ievainojamību neesamības pārbaužu rezultātu apliecinājumu , atbilstības apliecinājumu, un citus pieprasītos dokumentus jūsu pieņēmējam (pieņēmējbankai).

Norādījumi par noteiktu un specifisku prasību nepiemērojamību

Izņēmums: ja jums jāatbild uz SAQ C, lai apstiprinātu savu atbilstību PCI DSS, var apsvērt sekojoša izņēmuma noteikšanu(atbilstošo SAQ atbildi sk. sadaļā "Nepiemērojamība"):

- Uz jautājumiem, kas ir specifiski bezvadu tīklam, jāatbild tikai tad, ja jūsu uzņēmuma tīkls paredz datu pāŗraidi, izmantojot bezvadu tīklu (piemēram, 2.1.1., 1.2.3. un 4.1.1. apakšpunktu prasības). Ņemiet vērā, ka atbilde uz 11.1. apakšpunktā noteikto prasību (par procedūras, kuras rezultātā tiek identificēti neatļauti bezvadu tīklu piekļuves punkti, esamību) jāsniedz pat tad, ja Jūsu uzņēmuma tīkls neparedz datu pārraidi bezvadu tīklos , jo ar šādu procesu Jums ir jāspēj konstatēt jebkuras nelikumīgas vai neatļautas ierīces, kas var būt pievienotas Jūsu uzņēmuma tīklam bez jūsu zināšanas.

Nepiemērojamība. Šo un citas prasības, kuras neattiecas uz jūsu vidi, jāatzīmē kā "N/A" SAQ Pašnovērtējuma anketas ailē "Speciāls". Par katru "N/A" ierakstu attiecīgi aizpildiet pielikumā doto darblapu "Nepiemērojamības skaidrojums".

Security™
Standards Council

Atbilstības apliecinājums, SAQ C

Iesniegšanas instrukcija

Komersantam jāaizpilda šī "Atbilstības apliecinājuma" sagatave, apliecinot komersanta atbilstību maksājumu karšu nozares datu drošības standarta (PCI DSS) prasībām un drošības novērtējuma procedūrām. Aizpildiet visas piemērojamās sadaļas un izmantojiet iesniegšanas instrukcijas atbilstoši šā dokumenta sadaļai "PCI DSS atbilstība – aizpildīšanas kārtība".

1. daļa. Komersanta un kvalificēta drošības vērtētāja informācija

1.a daļa. Komersanta informācija

Uzņēmuma nosaukums:		DBA(S):	
Kontaktpersona:		Amata nosaukums:	
Tālrunis:		E-pasts:	
Juridiskā adrese:		Pilsēta:	
Pagasts:		Valsts:	Pasta kods:
Interneta vietne:			

1.b daļa. Informācija par Kvalificēta drošības vērtētāja uzņēmumu (pēc vajadzības)

Uzņēmuma nosaukums:			
Vadošā QSA kontakti: Vārds/uzvārds:		Amata nosaukums:	
Tālrunis:		E-pasts:	
Juridiskā adrese:		Pilsēta:	
Pagasts:		Valsts:	Pasta kods:
Interneta vietne:			

2. daļa. Komersanta uzņēmējdarbības veids (atzīmēt visu atbilstošo)

Mazumtirgotājs	Telekomunikācijas	Pārtikas veikali un lielveikali	
Degviela	E-tirdzniecība	Pasūtījumi pa pastu vai tālruni	Citi (norādīt):
PCI DSS pārskatā iekļauto objektu un atrašanās vietu saraksts:			

2.a daļa. Sadarbība

Jautājums	Atbilde	
	Jā	Nē
Vai jūsu uzņēmumam ir sadarbība ar vienu vai vairākiem pakalpojumu sniedzējiem – trešām personām *(piemēram, Interneta pieslēgumu (vārtejas) pakalpojumu,Interneta servisu (tīmekļa izmitināšanas) pakalpojumu, aviobiļešu rezervēšanas uzņēmumiem, lojalitātes programmu aģentiem u.c.)*?		
Vai jūsu uzņēmumam ir sadarbība ar vairāk nekā vienu pieņēmēju/pieņēmējbanku?		

2.b daļa. Darījumu apstrāde

Kā un kādā statusā jūsu uzņēmums glabā, apstrādā un/vai pārraida maksājumu karšu lietotāju datus? Lūdzu, norādiet šādu informāciju par jūsu organizācijas izmantotajām maksājumu apstrādes *(Payment Application)* lietojumprogrammām.

Izmantotā maksājumu apstrādes lietojumprogramma	**Versijas numurs**	**Pēdējo reizi pārbaudīta saskaņā ar PABP/PA – DSS**

2.c daļa. Tiesības uz SAQ C aizpildīšanu

Komersants apliecina savu atbilstību aizpildīt šo saīsināto Pašnovērtējuma anketas versiju ar šādu pamatojumu.

	Komersanta maksājumu apstrādes lietojumprogrammas sistēma un piesļēgums internetam vai publiskajam tīklam izveidots tajā pašā ierīcē un/vai tajā pašā lokālajā tīklā.
	Maksājumu apstrādes lietojumprogrammas sistēma/interneta ierīce nav savienota ar jebkuru citu sistēmu komersanta vidē.
	Komersanta veikals nav saslēgts datortīklā ar citiem veikaliem, un katram veikalam ir savs lokālais tīkls.
	Komersants neuzglabā karšu lietotāju datus elektroniskā veidā.
	Ja Komersants elektroniski neuzglabā un nesaņem karšu lietotāju datus, un uzglabāšanas gadījumā šādi dati ir tikai papīra ziņojumu vai čeku/rēķinu papīra kopiju veidā **un**
	Komersanta maksājumu apstrādes lietojumprogrammas piegādātājs izmanto drošus paņēmienus, lai nodrošinātu attālinātu atbalstu komersanta maksājumu sistēmai.

3. daļa. PCI DSS apstiprinājums

Pamatojoties uz atbildēm, kuras atzīmējāt SAQ C, kas datēta *(pabeigšanas gads)*, *(komersanta uzņēmuma nosaukums)* apliecina šādu atbilstības statusu (atzīmējiet vienu).

	Prasībām atbilstošs: visas PCI SAQ sadaļas ir aizpildītas un uz visiem jautājumiem atbildējāt "jā", tādējādi iegūstot vispārēju **ATBILSTĪBAS** vērtējumu, **un** PCI SSC apstiprināts ievainojamību neesamības pārbaužu pakalpojumu sniedzējs ir veicis *(komersanta uzņēmuma nosaukums)* pārbaudes , pierādot pilnīgu atbilstību PCI DSS.
	Prasībām neatbilstošs: ne visas PCI SAQ sadaļas ir aizpildītas vai uz dažiem jautājumiem atbildējāt "nē", tādējādi iegūstot vispārēju **NEATBILSTOŠU** vērtējumu, **vai arī** PCI SSC apstiprināts ievainojamību neesamības pārbaužu pakalpojumu sniedzējs nav veicis pārbaudes s, tādējādi *(komersanta uzņēmuma nosaukums*) *nav* pierādījis pilnīgu atbilstību PCI DSS. **Termiņš** atbilstības nodrošināšanai: Komersantam, kas iesniedz šo veidlapu ar statusu **Prasībām neatbilstošs** , var tikt noteikta prasība iesniegt rīcības plānu atbilstoši šā dokumenta 4. daļai. *Sazinieties ar savu pieņēmējbanku vai maksājumu karšu organizāciju, pirms pildāt 4. daļu, jo ne visas maksājumu karšu organizācijas pieprasa šo daļu.*

3.a daļa. Atbilstības statusa apstiprinājums

Komersants apstiprina:

	PCI DSS Pašnovērtējuma anketa C (SAQ C) tika aizpildīta saskaņā ar tajā dotajām instrukcijām.
	Visa informācija iepriekš minētajā SAQ un šajā apliecinājumā godīgi atspoguļo mana vērtējuma rezultātus visos būtiskajos aspektos.
	Esmu saņēmis savu maksājumu apstrādes lietojumprogrammas pārdevēja apstiprinājumu, ka mana maksājumu sistēma nesaglabā sensitīvus autentifikācijas datus pēc maksājumu autorizācijas.
	Esmu iepazinies ar PCI DSS un atzīstu, ka man vienmēr jānodrošina pilna atbilstība PCI DSS.
	Nav pierādījumu par magnētisko joslu (t.i., celiņu) datu[2], CAV2, CVC2, CID vai CVV2 datu[3], vai PIN datu[4] uzglabāšanu pēc tam, kad darījums ticis autorizēts, nevienā sistēmā, kas šeit tika novērtēta.

[2] Magnētiskajā joslā iekodēti dati vai līdzvērtīgi dati mikroshēmā, ko izmanto fizisko karšu darījumu autorizācijai. Uzņēmumi nedrīkst saglabāt visus magnētiskās joslas datus pēc darījuma autorizācijas. Vienīgie celiņa datu elementi, kurus drīkst saglabāt, ir konta numurs, derīguma termiņš un kartes lietotāja vārds.

[3] Trīsciparu vai četrciparu skaitļi, kas uzdrukāti uz vai pa labi no paraksta paneļa vai uz maksājumu kartes priekšpuses, kurus lieto karšu darījumu pārbaudei bez kartes klātbūtnes (piemēram, internetā – šā oriģinālā nav).

[4] Personiskais identifikācijas numurs, kuru kartes lietotājs norāda kartes darījuma laikā, un/vai šifrēts PIN bloks ir daļa no karšu maksājuma ziņojuma.

3.b daļa. Komersanta apstiprinājums

Komersanta izpilddirektora paraksts	*Datums*
Komersanta izpilddirektora vārds, uzvārds	*Amata nosaukums:*
Komersanta pārstāvētais uzņēmums	

4. daļa. Rīcības plāns neatbilstoša statusa gadījumā

Lūdzu, izvēlieties atbilstošu "Atbilstības statusu" katrai prasībai. Ja atbildat "NĒ" uz kādu no prasībām, jums jāmin termiņš, kurā uzņēmums nodrošinās prasības izpildi, un īss apraksts par veiktajiem pasākumiem, lai izpildītu prasības.

Pirms 4. daļas aizpildīšanas sazinieties ar savu pieņēmējbanku vai maksājumu karšu organizāciju, jo ne visas maksājumu karšu organizācijas pieprasa šo daļu.

PCI DSS prasība	Prasības apraksts	Atbilstības statuss (atzīmējiet vienu) JĀ	Atbilstības statuss (atzīmējiet vienu) NĒ	Uzlabošanas pasākumu datums un rīcība (Ja atbilstības statuss ir "NĒ")
1.	Uzstādīt un uzturēt ugunsmūra konfigurāciju, lai aizsargātu kartes lietotāja datus.			
2.	Nelietot pārdevēja piegādātās sistēmas standartizētās paroles un citus drošības parametrus.			
3.	Aizsargāt uzglabātos kartes lietotāja datus.			
4.	Šifrēt kartes lietotāja datu pārraidi atklātos publiskajos tīklos.			
5.	Izmantot un regulāri atjaunināt pretvīrusu programmatūras.			
6.	Izstrādāt un uzturēt drošas sistēmas un lietojumprogrammas .			
7.	Atļaut piekļuvi kartes lietotāja datiem t tikai tām personām, kurām tas nepieciešams darba pienākumu izpildei.			
8.	Piešķirt unikālu ID katrai personai, kurai ir datorpiekļuve.			
9.	Ierobežot fizisku piekļuvi kartes lietotāja datiem.			
11.	Regulāri pārbaudīt drošības sistēmas un procesus.			
12.	Nodrošināt un īstenot politiku , kas nodrošina visa personāla iesaisti informācijas drošībā.			

Pašnovērtējuma anketa C

Piezīme. Turpmākie jautājumi numurēti saskaņā ar PCI DSS prasībām un pārbaudes procedūrām, kā noteikts PCI DSS prasību un drošības novērtējuma procedūru dokumentā (PCI DSS *Requirements and Security Assessment Procedures*).

Aizpildīšanas datums:

Veidot un uzturēt drošu tīklu

1. prasība. Uzstādīt un uzturēt ugunsmūra konfigurāciju, lai aizsargātu kartes lietotāja datus

1.2. Vai ugunsmūra un maršrutētāja konfigurācija sekojoši ierobežo sakarus starp neuzticamiem tīkliem un jebkurām kartes lietotāja datu apstrādes infrastruktūras sistēmām. *Piezīme. "Neuzticams tīkls" ir jebkurš tīkls, kas ir ārpus tīkliem, kuri pieder pārbaudāmajam uzņēmumam un/vai kurš neatrodas uzņēmuma kontrolē vai pārvaldībā*			
1.2.1. a) Vai ienākošā un izejošā datplūsma ir kontrolēti ierobežoti atļauta tikai atbilstoši kartes lietotāju datu apstrādes infrastruktūru sistēmu vajadzībām un vai šie ierobežojumi ir dokumentēti?			
1.2.1. b) Vai visa cita ienākošā un izejošā datplūsma tiek atteikta (piemēram, lietojot ugunsmūra/maršrutētāja precīzi vai netieši formulētus atteikumu nosacījumus (piemēram explicit "deny all" or an implicit deny after nosacījumi)?			
1.2.3. Vai starp jebkuru bezvadu tīkliu un kartes lietotāja datu apstrādes infrastruktūru ir instalēt perimetra ugunsmūri un vai tie ir konfigurēti tā, lai neatļautu vai kontrolētu (ja šāda datplūsma nepieciešama darbības nodrošināšanai) jebkādu datplūsmu no bezvadu vides uz kartes lietotāja datu apstrādes infrastruktūru?			
1.3. Vai ugunsmūra konfigurācija sekojoši aizliedz tiešu publisku piekļuvi no interneta uz jebkuru *v* kartes lietotāja datu apstrādes infrastruktūras sistēmu?			
1.3.3. Vai ir aizliegtas tiešas saslēgšanās (*ienākošā vai izejošā datplūsma) starp internetu un maksājumu karšu lietotāju datu apstrādes infrastruktūras sistēmām?*			
1.3.5. Vai *izejošā datplūsma no maksājumu karšu lietotāju datu apstrādes infrastruktūras sistēmām uz internetu notiek pēc nepārprotamas autorizācijas (atļaujas)?*			
1.3.6. Vai ir ieviesta dinamisko pakešu filtrēšana *(stateful inspection)*, lai nodrošinātu, ka tīklā tiek atļauti tikai iau izveidotas datu plūsmas / savienojumi (connections)?			

Ja uzņēmums nav ieviesis nepieciešamās drošības prasības (N/A) vai lieto citu kompensējošu kontroles mehānismu, atbilstoši nepieciešams aizpildīt pielikumā sniegto "Kompensējošās kontroles darblapu" vai "Nepiemērojamības skaidrojuma lapu".

2. prasība. Nelietojiet pārdevēja piegādātās sistēmas standarta (iepriekš uzstādītās noklusētās) paroles un citus drošības parametrus

2.1. Vai piegādātāja noklusējumi vienmēr ir nomainīti pirms sistēmas instalēšanas tīklā? *Piegādātāja noklusējumi ir, piemēram, paroles, vienkāršā tīkla pārvaldības protokola (SNMP) lietotāju identifikatori , kā arī darbībām nevajadzīgi lietotāju konti .*			
2.1.1. Vai Bezvadu videi, kas pieslēgta kartes lietotāja datu apstrādes infrastuktūrai un tiek izmantota kartes lietotāja datu pārraidei, noklusējumi ir šādi mainīti ?			
a) Vai noklusētās šifrēšanas atslēgas tiek nomainītas instalācijas laikā? Vai šifrēšanas atslēgas vienmēr tiek nomainītas, ja persona, kas atbildīga par šifrēšanas atslēgām, pārtrauc darba attiecības vai maina amatu?			
b) Vai SNMP savienojumu noklusējuma iestatījumi tiek mainīti?			
c) Vai pieejas punktu noklusējuma paroles/ paroļu frāzestiek mainītas?			
d) Vai bezvadu ierīces aparātprogrammatūra ir atjaunināta, lai nodrošinātu bezvadu tīklos stipru šifrēšanu autentifikācijai un datu pārraidei?			
e) Vai ir mainīti citi piegādātāja noklusējuma iestatījumi, kas saistīti ar drošību bezvadu tīklos?			
2.2.2. a) Vai atļauti tikai tie servisi, protokoli, fona programmas vai palīgprogrammas u.c., kas nepieciešamas sistēmas darbības nodrošināšanai (citi servisi un protokoli, kas nav tieši nepieciešami ierīcei noteiktās funkcijas veikšanai, tiek atspējoti)?			
2.3. Vai visa attālinātā administratīvā piekļuve tiek šifrēta šādi? *Izmanto attālinātās piekļuves tehnoloģijas, kā SSH, VPN vai SSL/TLS attālinātai pārvaldībai un ne-konsoles administratīvajai piekļuvei.*			
a) Vai visām administratīvajām darbībām nekonsoles pieejas laikā tiek piemērota stiprā šifrēšana , kā arī vai stiprās šifrēšanas metode tiek izmantota, pirms tiek pieprasīta administratora parole?			
b) Vai sistēmas servisi un parametru faili ir konfigurēti, lai izslēgtu *Telnet* lietošanu un citas nedrošas attālinātās pieslēgšanās iespējas vadības komandu ievadīšanai?			
c) Vai administratora attālinātās pieslēgšanās administrēšanas saskarnēm ir aizsargāta, ar stipro šifrēšanu?			

"Neattiecas" (N/A) vai "Izmantota kompensējoša kontrole". Organizācijām, kuras izmanto šo iedaļu, jāaizpilda attiecīgi pielikumā sniegtā Kompensējošās kontroles darblapa vai Nepiemērojamības skaidrojuma darblapa.

Aizsargāt kartes lietotāja datus

3. prasība. Aizsargāt uzglabātos kartes lietotāja datus

3.2. b) Ja tiek saņemti un dzēsti sensitīvi autentifikācijas dati, vai ir izveidoti procesi drošai datu dzēšanai, lai nodrošinātu to, ka datus nav iespējams atgūt?

c) Vai visas sistēmas ievēro šādas prasības attiecībā uz sensitīvu autentifikācijas datu neglabāšanu pēc autorizācijas (pat ja tie ir šifrēti)?

3.2.1. Neviena magnētiskās joslas celiņa pilns saturs (atrodas kartes aizmugurē, līdzvērtīgi dati mikroshēmā vai citur) netiek saglabāts nekādos apstākļos.
Šos datus sauc arī par pilnu celiņu ierakstu, celiņu ierakstu, 1-ā celiņa ierakstu, 2-ā celiņa ierakstu vai magnētiskās joslas datiem.
Parasti var būt pieļaujama šādu magnētiskās joslas datu elementu saglabāšana:
– kartes lietotāja vārds,
– maksājumu kartes numurs (PAN - primārā konta numurs–),
– derīguma termiņš un
– pakalpojuma kods.
Lai samazinātu risku, glabājiet tikai tos datu elementus, kas vajadzīgi uzņēmējdarbībai.

3.2.2. Kartes drošības kodi vai vērtības (trīsciparu vai četrciparu numuri, kas iedrukāti maksājumu kartes priekšpusē vai aizmugurē) netiek saglabāti nekādos apstākļos.

3.2.3. Personiskie identifikācijas numuri (PIN) vai šifrētie PIN bloki netiek saglabāti nekādos apstākļos.

3.3. Vai PAN tiek daļēji slēpts, to uzrādot (atļauts uzrādīt tikai pirmos sešus un pēdējos četrus ciparus)?
Piezīmes.
– Šī prasība neattiecas uz darbiniekiem un citām personām, kurām ir noteikta nepieciešamība redzēt pilnu PAN.
– Šī prasība neaizstāj ieviestas stingrākas prasības attiecībā uz karšu lietotāju datu uzrādīšanu, piemēram, POS čekos.

\

4. prasība. Šifrēt kartes lietotāja datu pārraidi atklātos publiskajos tīklos

4.1. Vai tiek izmantoti stiprās šifrēšanas un drošības protokoli (piemēram, SSLTLS, SSH vai IPSEC), lai aizsargātu sensitīvus kartes lietotāja datus pārraides laikā atklātos publiskajos tīklos? *Piemēram, atklāti publiskie tīkli PCI DSS izpratnē ir internets, bezvadu tehnoloģijas, Globālā mobilo sakaru sistēma (GSM) un Vispārējais pakešu radio pakalpojums (GPRS).*			
b) Vai tiek pieņemtas tikai uzticamas šifrēšanas atslēgas un/vai sertifikāti?			

c) Vai ir ieviesti drošības protokoli tikai drošu konfigurāciju lietošanai un tie neatbalsta nepārbaudītas versijas vai konfigurācijas?			
d) Vai šifrēšanai tiek lietots atbilstošais šifrēšanas stiprums (atbilstoši piegādātāja ieteikumiem un/vai labajai praksei)?			
e) SSL/TLS lietošana – Vai URL *(Universal RecordLocator)* pārlūkprogramma tiek izmantota HTTPS režīmā ? – Vai maksājumu karšu lietotāju dati tiek pieprasīti tikai tad, kad HTTPS parādās pieprasījuma URL?			
4.1.1. Vai stiprajai šifrēšanai , kas tiek pielietota autentifikācijai un datu pārraidei bezvadu tīklā, pārraidot maksājumu kartes lietotāju datus , vai pieslēdzoties pie maksājumu kartes lietotāju datu apstrādes infrastruktūras sistēmām, tiek piemērota atbilstoši labās prakses standartiem (piemēram, IEEE 802.11i) ? *Piezīme. WEP protokola lietošana drošības kontrolei ir aizliegta kopš 2010. gada 30. jūnija.*			
4.2. Vai ir izveidota politika, lai nepieļautu nešifrēta PAN nosūtīšanu ar galalietotāja ziņojumapmaiņas tehnoloģijām (piemēram, e-pastu, tūlītēju ziņojumapmaiņu, čatu)?			

Uzturēt ievainojamības kontroles programmu

5. prasība. Izmantot un regulāri atjaunināt pretvīrusu programmatūras

Atbilde			
	Jā	Nē	Cita atbilde
5.1. Vai pretvīrusu programmatūra ir uzstādīta visās sistēmās,, kuras parasti skar ļaunprogrammatūra?			
5.1.1. Vai visas pretvīrusu programmas spēj atklāt, novērst un aizsargāt pret visiem zināmajiem ļaunprogrammatūras veidiem (piemēram, vīrusiem, Trojas zirgiem, tārpiem, spiegprogrammatūru, reklāmprogrammatūru un sistēmlaužņiem)?			
5.2. Vai visas pretvīrusu programmatūras pašlaik aktīvi darbojas un nodrošina auditācijas pierakstus šādā veidā?			
a) Vai pretvīrusu politika paredz pretvīrusu programmatūras un definīciju atjaunināšanu?			
b) Vai programmatūras pamatinstalācijā iespējota automātiskās atjaunināšanas un skenēšanas iespēja?			
c) Vai automātiskā atjaunināšana un periodiska skenēšana ir iespējota?			
d) Vai visi pretvīrusu mehānismi nodrošina auditācijas pierakstus un tiek saglabāti saskaņā ar PCI DSS 10.7. prasību?			

6. prasība. Izstrādāt un uzturēt drošas sistēmas un lietojumprogrammas

PCI DSS jautājums	Atbilde		
	Jā	Nē	Cita atbilde
6.1. a) Vai visās sistēmas sastāvdaļās un programmatūrās ir instalēti jaunākie sistēmas izstrādātāja piegādātie drošības ielāpi, lai novērstu zināmos trūkumus?			
b) Vai svarīgi drošības ielāpi tiek uzstādīti viena mēneša laikā pēc to izlaišanas?			

Īstenot stingrus piekļuves kontroles pasākumus

7. prasība. Atļaut piekļuvi kartes lietotāja datiem tikai tiem, kam tas nepieciešams darba vajadzībām

PCI DSS jautājums	Atbilde		
	Jā	Nē	Cita atbilde
7.1. a) Vai piekļuve sistēmas komponentēm un kartes lietotāja datiem ir atļauta tikai tām personām, kuru darba pienākumi to prasa?			
7.1.2. Vai privileģētu lietotāju ID piekļuves tiesības tiek noteiktas, nepārsniedzot privilēģiju minimumu, kas nepieciešams darba pienākumu veikšanai? 7.1.2. Vai privilēģijas personām tiek piešķirtas, pamatojoties uz amata klasifikāciju un veicamajām funkcijām (sauc arī par piekļuves kontroles pielāgošanu atbilstoši lomām vai RBAC (”role based Access control”))?			

8. prasība. Piešķirt unikālu ID katrai personai ar datorpiekļuvi

PCI DSS jautājums	Atbilde		
	Jā	Nē	Cita atbilde
8.3. Vai, nodrošinot darbinieku, administratoru un trešo pušu attālināto piekļuvi tīklam pieejai no ārējā tīkla, tiek izmantota divu faktoru autentifikācija ? *(Piemēram, attālinātās autentifikācijas un iezvanpieejas serviss (RADIUS), izmantojot identitātes nesējierīces (tokens)**;** vai termināļa piekļuves kontroliera piekļuves kontroles sistēma (TACACS), izmantojot izmantojot identitātes nesējierīces**;** vai citas tehnoloģijas, kas paredz divu faktoru autentifikāciju).* ***Piezīme**. Divu faktoru autentifikācija paredz, ka autentifikācijai izmanto divas no trim autentifikācijas metodēm (autentifikācijas metožu aprakstus sk. PCI DSS 8.2. apakšpunkta prasības aprakstā). Viena faktora divreizēja vai atkārtota izmantošana nav uzskatāma par divu faktoru autentifikāciju (piemēram, divas dažādas paroles).*			
8.5.6. Vai lietotāju konti, ko programmatūras izstrādātāji vai uzturētāji izmanto attālinātai piekļuvei apkalpošanas un uzturēšanas vajadzībām, ir iespējoti tikai tajā laika posmā, kad tas ir nepieciešams?			
b) Vai izmantošanas laikā programmatūras izstrādātāju un uzturētāju attālinātās pieejas konti tiek uzraudzīti?			

9. prasība. Ierobežot fizisku piekļuvi kartes lietotāja datiem

Jautājums	Atbilde:	Jā	Nē	Cita atbilde
9.6. Vai visi datu nesēji (t.sk. datori, noņemami elektroniskie datu nesēji, čeki/kvītis, ziņojumi un faksi papīra formātā) ir fiziskā drošībā? 9. prasības izpratnē "datu nesēji" ir visi papīra un elektroniskā formāta datu nesēji, kas satur kartes lietotāja datus.				
9.7. a) Vai tiek stingri nodrošināta kontrole jebkura veida datu nesēju iekšējai vai ārējai izplatīšanai?				
b) Vai kontrole ietver šādas pārbaudes?				
9.7.1. Vai datu nesēji tiek klasificēti tā, ka iespējams noteikt datu sensitivitātes pakāpi?				
9.7.2. Ja datu nesējus nosūta, izmantojot kurjerus vai citas piegādes metodes, tās var precīzi izsekot?				
9.8. Vai tiek veikti pieraksti, lai būtu iespējams izsekot visiem datu nesējiem, kas tiek pārvietoti no drošās vides, un vai pirms datu nesēju pārvietošanas tiek saņemts vadības apstiprinājums (īpaši, ja datu nesēji tiek nodoti fiziskām personām)?				
9.9. Vai tiek nodrošināta stingra datu nesēju glabāšanas un pieejamības kontrole?				
9.10. Vai visi datu nesēji tiek iznīcināti, kad tie vairs nav nepieciešami darba vai juridisku iemeslu dēļ?				
Vai iznīcināšana tiek veikta šādi?				
9.10.1. a) Vai papīra formāta datu nesēji tiek sasmalcināti, sadedzināti vai pārstrādāti celulozē tā, lai kartes lietotāja datus nevar rekonstruēt?				
b) Vai konteineri, kuros tiek glabāta iznīcināmā informācija, ir nodrošināti, lai iznīcināšanas procesā neļautu piekļūt to saturam? (Piemēram, konteineram, kurā atrodas sasmalcināšanai domātie materiāli, ir atslēga vai uzstādīta parole, kas neļauj piekļūt tā saturam.)				

Regulāri kontrolēt un pārbaudīt tīklus

11. prasība. Regulāri pārbaudīt drošības sistēmas un procesus

PCI DSS jautājums	Atbilde		
	Jā	Nē	Cita atbilde
11.1. a) Vai ir ieviests dokumentēts process bezvadu piekļuves punktu atklāšanai un identificēšanai? Piezīme. Metodes, kuras var tikt izmantotas šajā procesā, ietver tai skaitā bezvadu tīklu skenēšanu, sistēmas komponenšu un tīkla infrastruktūras, tīkla piekļuves kontroļu (NAC) vai bezvadu IDS/IPS fiziskās/loģiskās pārbaudes, Lai kura metode arī tiktu lietota, tai jābūt pietiekamai, lai atrastu un identificētu			

jebkuru neatļautu ierīci.			
b) Vai šīs metodes atklāj un identificē jebkuru neatļautu bezvadu piekļuves punktu, kā minimums, ietverot: – WLAN kartes, kas ievietotas datu apstrādes infrastruktūras sistēmu iekārtās; – pārvietojamas bezvadu iekārtas, kas pieslēgtas datu apstrādes infrastruktūras sistēmu iekārtām (piemēram, izmantojot USB pieslēgvietas); – bezvadu iekārtas, kas pieslēgtas tīkla portiem vai tīkla iekārtām?			
c) Vai process, kas identificē neatļautus bezvadu piekļuves punktus, tiek veikts vismaz reizi ceturksnī?			
d) Ja tiek lietotas automātiskas monitoringa kontroles (piemēram, bezvadu IDS/IPS, NAC u.c.), vai monitoringa kontroļu konfigurācija iekļauj brīdinājumu ziņojumu veidošanu personālam?			
e) Vai incidentu novēršanas plāns (12.9. prasība) paredz atbildes reakciju gadījumos, kad tiek atklātas neatļautas bezvadu iekārtas?			
11.2. Vai iekšējo un ārējo tīkla ievainojamību neesamību pārbaude (skenēšana) tiek veikta vismaz reizi ceturksnī, kā arī ikreiz pēc būtiskām pārmaiņām tīklā (piemēram, jaunu sistēmas komponentu uzstādīšana, pārmaiņas tīkla topoloģijā, ugunsmūra noteikumu pārmaiņas, produktu atjauninājumi) šādā veidā. *Piezīme. Netiek noteikta prasība, lai sākotnējās PSI DSS atbilstības noteikšanai ar apmierinošiem rezultātiem būtu veiktas četras ik ceturkšņa skenēšanas, ja: 1) pēdējās skenēšanas rezultāts bija apmierinošs, 2) uzņēmums ir dokumentējis politiku un procedūras, kas nosaka ceturkšņa skenēšanas veikšanu, un 3) skenēšanas rezultātos uzrādītie trūkumi ir izlaboti, par ko liecina atkārtotās skenēšanas rezultāti. Nākamajos gados pēc sākotnējās PCI DSS pārbaudes gadā jābūt veiktām četrām skenēšanām ar apmierinošiem rezultātiem.*			
11.2.1. a) Vai reizi ceturksnī notiek tīkla iekšējo ievainojamību skenēšana?			
b) Vai ceturkšņa iekšējās skenēšanas process ietver atkārtotu skenēšanu, līdz tiek sasniegti apmierinoši rezultāti vai arī līdz tiek novērsti visi trūkumi, kuru nopietnības pakāpe ir "Augsta", kā norādīts PCI DSS 6.2. prasībā?			
c) Vai iekšējo ceturkšņa skenēšanu veic kvalificēts iekšējais resurs(i) vai arī kvalificēts trešās puses resurss un pēc vajadzības tiek nodrošināta pārbaudītāja organizatoriskā neatkarība (var nebūt QSA vai ASV)?			
11.2.2. a) Vai reizi ceturksnī tiek veikta ārējā ievainojamības skenēšana?			
b) Vai ārējās ceturkšņa skenēšanas rezultāti ir saskaņā ar ASV Programmas gida prasībām (piemēram, nav ievainojamību, kas novērtētas augstāk par 4.0 saskaņā ar CVSS un nav notikušas automātikas kļūdas)?			
c) Vai ārējo ceturkšņa ievainojamības skenēšanu veic ASV *(Approved Scanning Vendor)*, kuru sertificējusi PCI SSC *(Payment Card Industry Security Standards Council*; Maksājumu karšu nozares Drošības standartu padome)?			
11.2.3. a) Vai iekšējā un ārējā skenēšana tiek veikta pēc jebkuru būtisku pārmaiņu ieviešanas (piemēram, jaunu sistēmas komponentu instalēšanas, tīkla topoloģijas pārmaiņām, ugunsmūra noteikumu pārmaiņām, produktu atjauninājumiem)? Piezīme. Skenēšanu pēc tīkla pārmaiņām var veikt uzņēmuma iekšējie darbinieku resursi.			

b) Vai skenēšanas process ietver atkārtotu skenēšanu, līdz: – ārējās skenēšanas gadījumā – visi atlikušie esošie trūkumi netiek vērtēti augstāk par 4.0 saskaņā ar CVSS; – iekšējās skenēšanas gadījumā – tiek iegūts apmierinošs rezultāts vai visi trūkumi ar nozīmības pakāpi "Augsta", (atbilstoši PCI DSS 6.2. apakšpunkta definējumam) , ir novērsti?			
c) Vai skenēšanu veic atbilstoši kvalificēts iekšējais resurss(-i) vai atbilstoši kvalificēta ārējā trešā organizācija un, ja nepieciešams, ir nodrošināta testētājas organizācijas neatkarība (var nebūt QSA vai ASV kvalifikācija)?			

Uzturēt informācijas drošības politiku

12. prasība. Uzturēt politiku, kas nodrošina visa personāla iesaisti informācijas drošībā

Jautājums	Atbilde:	Jā	Nē	Cita atbilde*
12.1. Vai ir izveidota, publicēta, uzturēta drošības politika, un vai tā ir darīta zināma visam attiecīgajam personālam? *12. prasības izpratnē termins "personāls" attiecināms uz pilna laika, nepilnas slodzes darbiniekiem, pagaidu darbiniekiem un personālu, kā arī līgumstrādniekiem un konsultantiem, kas izvietoti uzņēmuma telpās vai kam ir citāda pieeja uzņēmuma karšu lietotāju datu apstrādes infrastruktūrai .*				
12.1.3. Vai informācijas drošības politika tiek pārskatīta un pēc vajadzības atjaunināta vismaz reizi gadā, lai atspoguļotu uzņēmuma mērķu vai riska vides pārmaiņas?				
12.3. Vai ir izstrādāti lietošanas noteikumi kritiskām tehnoloģijām (piemēram, attālinātas pieejas tehnoloģijas, bezvadu tehnoloģijas, noņemamie elektroniskie datu nesēji, portatīvie datori, planšetdatori, plaukstdatori, e-pasts, internets), lai definētu šo tehnoloģiju pareizu lietošanu visam personālam un vai tie paredz:				
12.3.1. skaidru pilnvaroto personu atļauju izmantot konkrētās tehnoloģijas;				
12.3.2. autentifikāciju tehnoloģijas izmantošanai;				
12.3.3. visu šāda veida ierīču un darbinieku ar piekļuves tiesībām sarakstu;				
12.3.5. pieņemamus tehnoloģijas lietošanas veidu aprakstus;				
12.3.6. pieņemamas tehnoloģiju atrašanās vietas tīklā;				
12.3.8. automātisku sesiju pārtraukšanu pēc noteikta bezdarbības laika attālinātās pieejas tehnoloģijām;				
12.3.9. attālinātas pieejas tehnoloģiju pieejamības aktivizēšanu izplatītājiem un biznesa partneriem tikai, kad tas tiem nepieciešams, un tūlītēju deaktivizāciju pēc lietošanas?				
12.4. Vai drošības politika un procedūras skaidri definē informācijas drošības pienākumus un atbildības visam personālam?				
12.5. Vai atsevišķām personām vai personāla grupām ir oficiāli noteikti šādi informācijas drošības vadības pienākumi?				

12.5.3. Izveidot, dokumentēt un izplatīt drošības incidentu novēršanas un darbības atjaunošanas procedūras, lai nodrošinātu savlaicīgu un efektīvu rīcību visās situācijās.

12.6. Vai eksistē oficiāla informētības paaugstināšanas programma par drošību, lai viss personāls apzinātos, cik svarīga ir kartes lietotāja datu drošība?

12.8. Ja kartes lietotāja dati tiek koplietoti ar pakalpojumu sniedzējiem, vai ir izveidota un īstenota politika un procedūras pakalpojumu sniedzēju kontrolei, t.sk. šādas darbības.

12.8.1. Tiek uzturēts pakalpojumu sniedzēju saraksts.

12.8.2. Tiek uzturēta rakstiska vienošanās, kas ietver apstiprinājumu, ka pakalpojumu sniedzēji atbild par to rīcībā esošo kartes lietotāja datu drošību.

12.8.3. Ir izveidots process sadarbībai ar pakalpojumu sniedzējiem, t.sk. ietverot padziļinātu izpēti pirms sadarbības sākuma.

12.8.4. Tiek uzturēta programma, lai vismaz reizi gadā kontrolētu pakalpojumu sniedzēju PCI DSS atbilstības statusu.

A pielikums (netiek izmantots)

Šī lapa atstāta tukša ar nodomu

B pielikums. Kompensējošās kontroles

Kompensējošās kontroles var izmantot, lai aizstātu lielāko daļu PCI DSS prasību, ja uzņēmums nespēj izpildīt prasības tieši tā, kā norādīts, sakarā ar likumīgiem tehniskiem vai dokumentētiem darbības ierobežojumiem, bet ir pietiekami mazinājis risku, kas saistīts ar prasībām, īstenojot citas vai kompensējošas kontroles.

Kompensējošām kontrolēm jāatbilst šādiem kritērijiem.

1. Jāatbilst sākotnējo PCI DSS prasību mērķiem un nopietnības pakāpei.
2. Jānodrošina līdzīga līmeņa aizsardzība, kā to paveic sākotnējās PCI DSS prasības, tā lai kompensējošā kontrole pietiekami mazinātu risku, kuru bija paredzēts novērst ar sākotnējās PCI DSS prasības palīdzību. (Katra PCI DSS mērķus sk. sadaļā *"Kā orientēties PCI DSS".)*
3. Jāpārsniedz pārējo PCI DSS prasību darbības apjoms. (Vienkārša atbilstība pārējām PCI DSS prasībām nav uzskatāma par kompensējošu kontroli.)

   Vērtējot līmeni, kādā kompensējošās kontroles pārsniedz prasību darbības apjomu, apsverami šādi faktori.

   Piezīme: a)–c) apakšpunktā minētais ir tikai piemērs. PCI DSS novērtētājam jāpārskata visas kompensējošās kontroles un jāapstiprina, ka tās ir pietiekamas. Kompensējošās kontroles efektivitāte ir atkarīga no vides specifikas, kurā kontrole īstenota, apkārtējām drošības kontrolēm, kā arī kontroles konfigurācijas. Uzņēmumiem jāapzinās, ka konkrēta kompensējošā kontrole nebūs efektīva visās vidēs.

   a) Esošās PCI DSS prasības NEVAR uzskatīt par kompensējošām kontrolēm, ja tās jau ir noteiktas pārbaudāmajai pozīcijai. Piemēram, paroles administratora piekļuvei, neizmantojot konsoli, jānosūta šifrētas, lai mazinātu atklāta teksta administratora paroles pārtveršanas risku. Uzņēmums nevar izmantot citas PCI DSS paroļu prasības (ielaušanās bloķēšanu, sarežģītas paroles utt.), lai kompensētu šifrētas paroles trūkumu, jo šīs citas paroles prasības nemazinās atklāta teksta paroles pārtveršanas risku. Turklāt citas paroles kontroles jau ir ietvertas PCI DSS prasībās attiecībā uz pārbaudāmo pozīciju (paroles).

   b) Esošās PCI DSS prasības VAR uzskatīt par kompensējošām kontrolēm, ja tās noteiktas citā jomā, bet netiek prasītas pārbaudāmajai pozīcijai. Piemēram, divu faktoru autentificēšana ir PCI DSS prasība attiecībā uz attālināto piekļuvi. Divu faktoru autentificēšanu *iekšējā tīklā* var uzskatīt par kompensējošo kontroli administratora piekļuvei, neizmantojot konsoli, ja nav iespējams nodrošināt šifrētas paroles pārraidi. Divu faktoru autentifikācija varētu būt pieņemama kompensējošā kontrole, ja: 1) tā atbilstu sākotnējās prasības mērķim, novēršot atklāta teksta administratora paroles pārtveršanas risku, un 2) tā izveidota pareizi un drošā vidē.

   c) Esošās PCI DSS prasības var papildināt ar jaunām kontrolēm, lai izveidotu kompensējošo kontroli. Piemēram, ja uzņēmums nespēj nodrošināt kartes lietotāja datu nelasāmību saskaņā ar prasību 3.4. apakšpunktu (piemēram, šifrējot), kompensējošo kontroli var veidot ierīce vai ierīces, lietojumprogrammas un kontroles, kas ietver visus šādus elementus: 1) iekšējo tīklu segmentācija, 2) IP adrešu vai MAC adrešu filtrēšana un 3) divu faktoru autentifikācija iekšējā tīklā.
4. Jābūt samērīgām salīdzinājumā ar papildu risku, ko rada PCI DSS prasības neievērošana.

Novērtētājam nepieciešams rūpīgi novērtēt kompensējošās kontroles katrā gadskārtējā PCI DSS novērtējumā, lai pārliecinātos, ka katra kompensējošā kontrole atbilstoši novērš risku, kuru bija jānovērš sākotnējās PCI DSS prasības izpildei, kā minēts 1.–4. punktā. Lai uzturētu atbilstību, jābūt izveidotiem procesiem un kontrolēm, kas nodrošina kompensējošo kontroļu efektivitāti arī pēc novērtējuma pabeigšanas.

C pielikums. Kompensējošo kontroļu darblapa

Izmantojiet šo darblapu, lai definētu kompensējošās kontroles visām prasībām, kuras tika atzīmētas ar "JĀ" un kurām ailē "Cita atbilde" tika minēta kompensējoša kontrole.

Piezīme. *Tikai tie uzņēmumi, kas veikuši riska analīzi un kuriem pastāv likumīgi tehnoloģiski vai dokumentēti darbības ierobežojumi, var apsvērt iespēju izmantot kompensējošās kontroles, lai panāktu atbilstību.*

Prasības numurs un definēšana

	Nepieciešamā informācija	**Paskaidrojums**
1. Ierobežojumi	Uzskaitiet ierobežojumus, kuri nepieļauj atbilstību sākotnējām prasībām.	
2. Mērķi	Definējiet sākotnējās kontroles mērķus, nosakiet mērķus, kurus atbalsta kompensējošā kontrole.	
3. Identificētie riski	Identificējiet papildu riskus, kurus rada nepietiekama sākotnējā kontrole.	
4. Kompensējošo kontroļu definīcija	Definējiet kompensējošās kontroles un paskaidrojiet, kā tās nodrošina sākotnēji paredzētās kontroles mērķu sasniegšanu un vajadzības gadījumā novērš paaugstināto risku.	
5. Kompensējošo kontroļu apstiprināšana	Nosakiet, kādā veidā kompensējošās kontroles tika apstiprinātas un pārbaudītas.	
6. Uzturēšana	Nosakiet procesu un kontroles kompensējošo kontroļu uzturēšanai.	

Kompensējošo kontroļu darblapa – aizpildīts piemērs

Izmantojiet šo darblapu, lai definētu kompensācijas kontroli attiecībā uz jebkuru prasību, ja tika atzīmēts "JĀ" un kompensācijas kontrole tika minēta "speciālajā" ailē.

Prasības numurs: ***8.1. Vai visi lietotāji tiek identificēti ar unikālu lietotāja vārdu, pirms tiem atļauj piekļuvi sistēmas komponentēm vai kartes lietotāja datiem?***

	Nepieciešamā informācija	Paskaidrojums
1. Ierobežojumi	Uzskaitiet ierobežojumus, kuri nepieļauj atbilstību sākotnējām prasībām.	*Uzņēmums XYZ izmanto ārpus tīkla esošus Unix serverus, kuri neizmanto uzņēmuma LDAP protokolu. Katram no šiem serveriem nepieciešams "superlietotāja" pieteikumvārds. Uzņēmumam XYZ nav iespējas kontrolēt "superlietotāja" pieteikumvārda izmantošanu, kā arī nav iespējams reģistrēt visu lietotāju veiktās "superlietotāja" darbības.*
2. Mērķi	**Definējiet sākotnējās kontroles mērķus, nosakiet mērķus, kurus atbalsta kompensējošā kontrole.**	*Prasībai ievadīt unikālu pieteikumvārdu ir divējāds mērķis. Pirmkārt, no drošības viedokļa ir nepieņemami, ka vairākas personas izmanto vienus pieteikumvārda datus. Otrkārt, izmantojot kopīgus pieteikumvārdus, nav iespējas ar pārliecību konstatēt, vai konkrētā persona ir atbildīga par konkrēto darbību.*
3. Identificētie riski	Identificējiet papildu riskus, kurus rada nepietiekama sākotnējā kontrole.	*Piekļuves kontroles sistēmā rodas papildu risks, ja nenodrošina, ka visiem lietotājiem ir unikāli pieteikumvārdi (ID) un ka lietotāju darbības iespējams izsekot.*
4. Kompensējošo kontroļu definīcija	Definējiet kompensējošās kontroles un paskaidrojiet, kā tās nodrošina sākotnēji paredzētās kontroles mērķu sasniegšanu un vajadzības gadījumā novērš paaugstināto risku.	*Uzņēmums XYZ gatavojas pieprasīt, lai visi lietotāji pievienojas serverim no galddatoriem, izmantojot SU komandu. SU ļauj lietotājiem piekļūt "superlietotāja" kontiem un veikt darbības "superlietotāja" kontā, vienlaikus spējot pieslēgties SU žurnāla direktorijai. Šādā veidā katra lietotāja darbības var izsekot caur SU kontu.*
5. Kompensējošo kontroļu apstiprināšana	**Definējiet, kādā veidā kompensējošās kontroles tika apstiprinātas un pārbaudītas.**	*Uzņēmums XYZ pierāda novērtētājam, ka SU komandas tiek izpildītas un personas, kuras izmantojušas komandu, tiek reģistrētas žurnālā, lai konstatētu,*

		ka persona veic darbības saskaņā ar "superlietotāja" privilēģijām.
6. Uzturēšana	**Definējiet procesu un kontroles kompensējošo kontroļu uzturēšanai.**	*Uzņēmums XYZ dokumentē procesus un procedūras, lai nodrošinātu, ka SU konfigurācijas netiek mainītas, pārveidotas vai dzēstas, kas ļautu atsevišķiem lietotājiem izpildīt "superlietotāja" komandas bez iespējas to atsevišķi izsekot vai reģistrēt žurnālā.*

D pielikums. Nepiemērojamības skaidrojums

Ja ailē "Cita atbilde" tika ierakstīts "N/A" vai "Neattiecas", izmantojiet šo darblapu, lai paskaidrotu, kāpēc attiecīgā prasība neattiecas uz jūsu organizāciju.

Prasība	Iemesls, kāpēc prasība nav piemērojama
Piemērs, 12.8.	*Pakalpojumu sniedzējiem nekad nav pieejas karšu lietotāju datiem.*