АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ІШКІ АУДИТІН ЖҮРГІЗУ ҚАҒИДАЛАРЫ

Астана
2023 ж.

1. Мақсаты және қолдану саласы

Осы ұйымның ақпараттық жүйесінің ақпараттық қауіпсіздігіне ішкі аудит жүргізу қағидалары (бұдан әрі – қағидалар) ҚР СТ ИСО 9001:2016, ҚР СТ ИСО/МЭК 27001:2015 8.2.2, 6-бөлімдерінің талаптарына сәйкес әзірленді.

1. Осы қағидалардың талаптары «Qazaq Green» ЖЭК қауымдастығы ЗТБ барлық қызметкерлеріне қолданылады.
2. Осы қағидалар ақпараттық қауіпсіздік жөніндегі ішкі аудит процесіне қатысатын басшылық пен қызметкерлердің іс-әрекеттерін реттейді.
3. Осы қағидаларды қайта қарау және оларға өзгерістер енгізу іс жүргізуге сәйкес жүзеге асырылады.
4. Осы қағидалар бекітілген сәттен бастап күшіне енеді.

2. Нормативтік сілтемелер

5. Осы қағидаларды әзірлеу кезінде келесі нормативтік құжаттар мен сапа нысандары пайдаланылды:

- ҚР СТ ИСО 9001-2016 Сапа менеджменті жүйесі. Талаптар.
- ҚР СТ ИСО/МЭК 27001:2015 Ақпараттық қауіпсіздікті басқару жүйесінің қауіпсіздігін қамтамасыз ету әдістері мен құралдары.

3. Терминдер мен қысқартулар

Ұйым – «Qazaq Green» ЖЭК қауымдастығы ЗТБ;

АЖ – 2.0 «Қазақстанның тауар және шикізат биржаларына арналған сауда платформасы» ақпараттық жүйесі;

Аудит өлшемшарттары – саясаттар, рәсімдер мен талаптардың жиынтығы;

Аудит куәлігі – аудит өлшемшарттарымен байланысты және тексерілуі мүмкін жазбалар, фактілер туралы мәлімдемелер немесе басқа ақпарат;

Аудит – аудиттің келісілген өлшемшарттарының орындалу дәрежесін анықтау мақсатында аудит куәліктерін алудың және оларды объективті бағалаудың жүйелі тәуелсіз және құжатталған процесі;

Аудитор – бірінші басшының бұйрығымен тағайындалған және ішкі аудитті жүргізуге уәкілетті ұйым қызметкері;

Ішкі аудит – ақпараттық қауіпсіздікті басқару жүйесінің ішкі аудиті;

СМЖ – сапа менеджменті жүйесі;

АҚБЖ – ақпараттық қауіпсіздікті басқару жүйесі;

Ақпараттық қауіпсіздік жөніндегі маман – ақпараттық қауіпсіздікке жауапты ұйым қызметкері;

Сәйкессіздік – бекітілген регламенттеуші құжаттың талаптарын орындамау;

Түзету – анықталған сәйкессіздікті жою;

Түзету әрекеттері – анықталған сәйкессіздіктің немесе басқа ықтимал жағымсыз жағдайдың себебін жою үшін жасалған әрекет;

Ескерту әрекеттері – ықтимал сәйкессіздіктің немесе басқа ықтимал жағымсыз жағдайдың себебін жою үшін жасалған әрекет;

4. Жалпы ережелер

6. Процестің иесі ақпараттық қауіпсіздік жөніндегі маман болып табылады.

7. Ішкі аудит мына мақсатта жүргізіледі:

1) АҚБЖ-ның ҚР СТ ИСО/МЭК 27001:2015 стандартының талаптарына сәйкестігін тексеру;

2) ұйымда АҚБЖ енгізілетінін немесе енгізілгенін және жұмыс жағдайында сақталғанын растау;

3) АҚБЖ рәсімдерінде анықталған қағидаларға қаншалықты жақын екендігін, ұйымдағы жұмыстардың орындалатындығын және нақты жұмыс пен АҚБЖ құжаттамасында анықталғандардың арасында айырмашылығының болуын көрсету.

8. Аудит екі түрлі болуы мүмкін:

1) жоспарлы аудит;

2) жоспардан тыс аудит.

9. Аудит нәтижелері басшылыққа түзету және/немесе ескерту әрекеттерін әзірлеу үшін беріледі.

10. Аудит бойынша жазбаларға мыналар жатады:

1) жылдық ішкі аудит жоспары;

2) ішкі аудит жүргізу бағдарламасы;

3) чек-парақ;

4) ішкі аудит нәтижелері бойынша есеп.

11. Осы нұсқаулыққа қосымшаларда келтірілген аудит бойынша жазбалардың нысандары ұсынымдық сипатқа ие және ұйымның бизнес-процесінің ерекшелігіне қарай өзгертілуі мүмкін.

5. Ішкі аудитті жүргізу тәртібі

5.1. Ішкі аудитті жоспарлау

12. Ішкі аудитті аудиторлар осы қағидаларға **1-қосымшаға** сәйкес бекітілген жылдық ішкі аудит жоспарына сәйкес жүзеге асырады.

13. Ішкі аудиттің жылдық жоспарын ақпараттық қауіпсіздік жөніндегі маман әзірлейді, жүйелік әкімшімен келісіледі және ағымдағы жылдың 15 желтоқсанынан кешіктірмей ұйымның бірінші басшысы бекітеді.

14. Бекітілген жылдық ішкі аудит жоспарының көшірмелері әрбір тексерілетін қызметкерге ағымдағы жылдың 20 желтоқсанынан кешіктірілмей жіберіледі.

15. Жоспардан тыс ішкі аудиттерді жүргізу жазбаша хабарламаны және аудит жоспарын ресімдемей, бірақ осы қағидаларға сәйкес аудит нәтижелерін міндетті түрде ресімдей отырып, оңайлатылған тәртіппен жүргізілуі мүмкін.

5.2. Ішкі аудиторлар тобын дайындау

16. Аудиторлар келесі қағидат бойынша таңдалады: Аудитор өзінің тікелей басшысын тексермеуі тиіс.

17. Ақпараттық қауіпсіздік жөніндегі маман аудиттің барлық кезеңдеріне жауап береді.

18. Ұйым басшылығы аудиторлардың біліктілігін арттыруға ықпал етуі тиіс.

19. АҚ ішкі аудитін жүргізу үшін топтың саны мен құрамын айқындау кезінде оның қатысушыларының біліктілік деңгейіне негізделген тексеруші топтың құзыреттілігі ескеріледі.

20. Ұйымның ішкі аудитін жүргізу бойынша рөлдер мен міндеттерді аудиторлық топ мүшелері арасында бөлу жүргізіледі. Қызметкерлердің білімін аудитпен (тексерумен) және олардың нормативтік құжаттардың талаптарын, АҚ-ға қатысты ұйым ережелерін орындауымен және ұйымның ақпараттық қауіпсіздігін анықтайтын нормативтік құжаттардың тікелей аудитімен тікелей айналысатын негізгі топтар құрылады.

21. Аудиторлар тобы жұмыс орындарымен, барлық қажетті нормативтік-техникалық құжаттамамен (саясат, актілер, хаттамалар, шарттар және т.б.) қамтамасыз етіледі.

22. АҚ ішкі аудитін жүргізу кезінде тиісті аспаптық қамтамасыз ету қолданылады. АҚ аудитінде қолданылатын аспаптық қамтамасыз ету АҚ талаптарының орындалуын талдауды автоматтандыру құралдарын қамтуы мүмкін.

23. АҚ талаптарының орындалуын талдауды автоматтандырудың аспаптық құралдары (АҚ аудитінің өлшемшарттары) мыналарға мүмкіндік беруі тиіс:

- АҚ талаптарының орындалу дәрежесін бағалау процесін олардың маңыздылығын ескере отырып автоматтандыру;
- қорғаныс шараларының әр түрлі нұсқаларының тиімділігін бағалау;
- пайдаланушылардың анықталған және тіркелген штаттан тыс әрекеттері мен АҚ инциденттерін талдау процестерін автоматтандыру;
- әр түрлі рәсімдердің нәтижелерімен құжаттық есептеулер жүргізу.

5.3 АҚ аспаптық аудиті.

24. Аспаптық аудит – автоматтандырылған тексеру әдістерімен бағдарламалық-аппараттық құралдардың осалдығын анықтау.

25. Аспаптық аудитті жүргізудің негізгі кезеңі барлық ақпараттық активтер туралы барлық қажетті деректерді жинау болып табылады:

– серверлердің, жұмыс станцияларының және коммуникациялық жабдықтардың тізбесі;
– шеткі жабдық туралы ақпарат;
– жұмыс станциялары мен серверлерде орнатылған операциялық жүйелер туралы ақпарат;
– АҚБЖ туралы деректер;
– қолданбалы БҚ тізбесі;
– қорғау құралдарын өндіруші туралы ақпарат;
– қорғау құралдарын конфигурациялық баптау;
– қорғаныс құралын орнату схемасы;
– байланыс арналарының түрлері туралы ақпарат;
– пайдаланылатын желілік хаттамалар, IP-мекенжайлар туралы ақпарат;
– ақпараттық ағындардың схемасы

26. Қауіпсіздікті аспаптық талдау АЖ бағдарламалық-аппараттық қамтамасыз етудегі технологиялық осалдықтарды анықтау үшін жүргізіледі.

27. Аспаптық аудит процесінде мамандандырылған бағдарламалық құралдар қолданылады. Желілік сканерлеу екі негізгі кезеңде жүзеге асырылады. Бірінші кезеңде хост туралы бастапқы ақпарат жиналады, оған ашық порттардың тізімі, хостта жұмыс істейтін желілік қызметтердің түрі туралы ақпарат және т.б. кіреді.

28. Екінші кезеңде осалдықтарды іздеу осы сервердің жұмысындағы

негізгі болып табылатын желілік қызметте жүзеге асырылады (мысалы – web-сервер).

29. Аспаптық аудит шеңберінде жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз етудің конфигурациялық баптауларына талдау жүргізіледі. Бұл аудит бағдарламалық қамтамасыз етуді немесе аппараттық құралдарды баптаудағы қателерді қамтитын операциялық осалдықтарды анықтауға бағытталған.

30. Қорытынды кезеңде қауіпсіздіктің аспаптық аудитінің нәтижелері туралы есеп және АҚ қамтамасыз ету процестерінде анықталған кемшіліктерді жою бойынша жалпы ұсынымдар жасалады.

5.4. Аудит жүргізу

31. Ақпараттық қауіпсіздік жөніндегі маман 7 жұмыс күні ішінде тексерілушіге кез келген қолжетімді нысанда ішкі аудит жүргізілгені туралы хабарлауға және **2-қосымшаға** сәйкес ресімделген аудит бағдарламасымен таныстыруға тиіс.

32. Аудиттің мақсаты ретінде мыналар көрсетілуі мүмкін:

- бекітілген регламенттеуші құжат талаптарының орындалуын тексеру;
- қызметтің бекітілген регламенттеуші құжаттардың талаптарына сәйкестігін тексеру.

33. Аудит бағдарламасының түпнұсқасы ақпараттық қауіпсіздік жөніндегі маманда сақталады.

34. Тексерілетіндер, өз кезегінде, мүдделі тұлғалардың назарына алдағы аудит туралы ақпаратты жеткізуге міндетті.

35. Аудит жоспарында белгіленген уақытта аудит жүргізу мүмкін болмаған жағдайда, осы аудит мерзімін ауыстыру туралы шешім қабылдайтын адам ауыстыру себебін көрсете отырып, ішкі аудиторға электрондық нысанда хабарлау қажет. Ауыстыру мерзімі бір айдан аспауы керек.

36. Ішкі аудит жүргізу процесінде аудиторлар ұйым қызметкерлерінен сұрау, құжаттарды зерделеу және бақылаулар жүргізу арқылы процестердің бекітілген регламенттеуші құжаттарға сәйкестігінің объективті куәліктерін жинайды.

37. Ішкі аудит барысында алынған деректерді аудитор осы қағидаларға **3-қосымшаға** сәйкес чек-парақтарда тіркеуі тиіс. 2-бағандағы сұрақтар аудит бағдарламасында көзделген талаптарға сәйкестік дәлелдемелерінің болуын немесе жоқтығын растайтын дұрыс және толық ақпарат алуды қамтамасыз етуі тиіс.

38. Ішкі аудиттің қорытындылары бойынша аудитор осы қағидаларға **4-қосымшаға** сәйкес ішкі аудиттің нәтижелері бойынша есеп құрастырады және оның көшірмесін тексерілушіге жібереді.

39. Әрбір сәйкессіздік туралы есепті аудитор сәйкессіздік туралы есептерді тіркеу журналына тіркейді және тексерілушіге береді.

40. Тексерілетін адам сәйкессіздік туралы есепті алғаннан кейін күнтізбелік 3 күн ішінде түзету/ескерту әрекеттерін әзірлейді және оны ақпараттық қауіпсіздік жөніндегі маманға жібереді. Сәйкессіздіктерді жою кезеңін тексерілуші анықтайды, бірақ 1 айдан аспауы тиіс.

41. Сәйкессіздіктерді жою мерзімі аяқталғаннан кейін ақпараттық қауіпсіздік маманы жоспардан тыс аудит жүргізеді және сәйкессіздік туралы есепте және сәйкессіздік туралы есептерді тіркеу журналында белгі қояды.

42. Аудит жазбалары жұмыс күйінде сақталуы тиіс және ақпараттық қауіпсіздік жөніндегі маманда сақталады.

43. Ішкі аудиттің жылдық жоспарының орындалуын бақылауды жүйелік әкімші және ақпараттық қауіпсіздік жөніндегі маман өз қызмет саласына сәйкес жүзеге асырады.

44. Ішкі аудит нәтижелері бойынша түзету/алдын алу іс-әрекеттерінің орындалуын бақылауды ақпараттық қауіпсіздік жөніндегі маман жүргізеді.

6. Жауапкершілік

45. Ақпараттық қауіпсіздік жөніндегі маман ішкі аудит жүргізуді ұйымдастыруға жауапты болып табылады.

46. Ақпараттық қауіпсіздік жөніндегі маман ішкі аудит бойынша жазбаларды сақтауға жауапты.

47. Ақпараттық қауіпсіздік жөніндегі маман осы қағидаларды әзірлеуге және өзектендіруге жауапты болады.

48. Аудиторлар ішкі аудиттер барысында алынған құпия ақпаратты жария етпегені үшін жауапкершілік алады.

49. Жүйелік әкімші осы қағидалардың талаптарының орындалуын тексеруге жауапты болады.

50. Тексерілушілер ішкі аудит нәтижелері бойынша түзету/алдын алу іс-әрекеттерін әзірлеуге және уақтылы орындауға жауапты болады.

51. Тексерілетіндер осы қағидаларда баяндалған АҚБЖ талаптарын орындамағаны/тиісінше орындамағаны үшін жауапкершілік алады.

7. АҚБЖ сапа өлшемшарттары

52. Басшылық тарапынан талдау үшін есепті қалыптастыру кезінде келесі сапа өлшемшарттары қолданылады:

№ р	Өлшемшарт атауы	Өлшем бірлігі	Формула
1.	Жылдық аудит жоспарын орындау	%	(жоспарланған аудиттер/жоспарланған аудиттер) * 100
2.	Анықталған сәйкессіздіктер саны	дана	

Ақпараттық қауіпсіздіктің ішкі аудитін жүргізу
қағидаларына **1-қосымша**
202_ жылғы «__» _____ № __

БЕКІТЕМІН
Директор _____
_____
«____» _____ 202_ ж.

202_ жылға арналған жылдық ішкі аудит жоспары.

Р/т №	Аудиттің мақсаты	Тексерілетін	Жылдың айлары												Ішкі аудитордың аты-жөні	Ескертпелер
			Қаңтар	Ақпан	Наурыз	Сәуір	Мамыр	Маусым	Шілде	Тамыз	Қыркүйек	Қазан	Қараша	Желтоқсан		
			Айдың күндері													
1	2	3	4												5	6

ДАЙЫНДАҒАН: _____ _____ _____
лауазымы *(қолы)* *(Т.А.Ә.)*

КЕЛІСІЛДІ: Жүйе әкімшісі _____ _____
(қолы) *(Т.А.Ә.)*

Ақпараттық қауіпсіздіктің
ішкі аудитін жүргізу қағидаларына
2-қосымша
202_ жылғы «__» _____ № __

Ішкі аудит жүргізу бағдарламасы

_____

Тексерілетін адамның лауазымы (немесе құрылымдық бөлімшенің атауы)

1. Аудиттің басталу уақыты мен күні _____ «____» _____ 20___ жыл
2. Аудиттің аяқталу уақыты мен күні _____ «____» _____ 20___ жыл
3. Аудиттің мақсаты:
_____
_____

Аудит өлшемшарттары:
_____
_____
_____

4. Аудит талаптарға сәйкес жүргізіледі

№	Регламенттеуші құжаттың тармағы	Сұрақтар

Ішкі аудитор _____ _____ _____
қолы *ТАӘ* *күні*

Аудитті өткізуге
жауапты (тексерілетін) _____ _____ _____
қолы *ТАӘ* *күні*

Ақпараттық қауіпсіздіктің
ішкі аудитін жүргізу қағидаларына
3-қосымша
202_ жылғы «__» _____ № __

Чек-парақ

_____

Тексерілетін адамның лауазымы (немесе құрылымдық бөлімшенің атауы)

«____» _____202_ ж.

ҚР СТ ИСО/МЭК 27001:2015 стандарттарының тармақтары	**Сұрақ**	**Аудитордың бақылауы**

Ішкі аудитор _____ _____ _____

қолы *ТАӘ* *күні*

Ақпараттық қауіпсіздіктің
ішкі аудитін жүргізудің қағидаларына
4-қосымша
202_ жылғы «__» _____ № __

Ішкі аудит нәтижелері бойынша № ___есеп

1-бөлім.
1. Тексерілетін (немесе құрылымдық бөлімше):
_____
_____
2. Аудитор:
_____
3. Аудит кезеңі _____ бастап _____ дейін
күні *күні*

2-бөлім.
Аудиттің мақсаты:
_____

3-бөлім.
Аудит өлшемшарттары:
_____
_____

4-бөлім.
Аудиттің нәтижелері:
1. Сәйкессіздік (маңызды/елеусіз):
_____
_____

2. Ішкі аудит нәтижелері бойынша ұсынымдар:
_____
_____

Тексерілетін _____ _____ _____
қолы *ТАӘ* *күні*

Ішкі аудитор _____ _____ _____
қолы *ТАӘ* *күні*

ТАНЫСУ ПАРАҒЫ

№	Тегі, аты, әкесінің аты	Лауазымы	Жеке қолы	Күні
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				