ALFA
ASSET MANAGEMENT

ПРАВИЛА ЗА УПРАВЛЕНИЕ НА РИСКА НА УД "АЛФА АСЕТ МЕНИДЖМЪНТ" ЕАД

(Изменена с Решение на Съвета на директорите от 24.09.2019г.)

С настоящите правила се уреждат организационната структура, нивата на отговорност и политиките по установяване, наблюдение, оценяване и управление на рисковете, свързани с дейностите, процедурите и системите по предоставяни от УД "Алфа Асет Мениджмънт" ЕАД (по-долу "Управляващото дружество" или само "УД") услуги.

I. ОСНОВНИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила за управление на риска съдържат:

1. Организационна структура, нива на отговорност и отчетност, по управлението на рисковете в УД.

2. Политика за управление на риска на УД, която включва:

а) процедури за установяване на рисковете, свързани с дейностите, процедурите и системите на управляващото дружество и за определяне на допускано ниво на риск, ако такова може да бъде установено;

б) процедури и мерки за управление на рисковете, свързани с дейностите, процедурите и системите на управляващото дружество;

в) механизми за осъществяване на наблюдение върху адекватността и ефективността на политиката и процедурите по т. а) и върху спазването от управляващото дружество и лицата, които работят по договор за управляващото дружество, на процедурите и мерките по т. б);

г) механизми за наблюдение върху адекватността и ефективността на предприетите мерки за отстраняване на констатирани непълноти и несъответствия в политиката и процедурите по т. 1 и процедурите и мерките по т. 2, вкл. невъзможност за спазването им от лицата;

д) счетоводни и административни процедури по управление на риска

3. Основни положения и рамка на план за действие при възникване на кризисни ситуации.

II. ОРГАНИЗАЦИОННА СТРУКТУРА

Чл. 2. (1) Организационната структура в управляващото дружество, свързана с управлението на риска включва:

1. Съвет на директорите.

2. Изпълнителен директор.

3. Служители, работещи по договор в управляващото дружество, а именно:
   3.1. Отдел „Контрол и управление на риска“
   3.2. Отдел „Управление на портфейли“
   3.3. Отдел „Счетоводство и административно обслужване“
   3.4. Отдел “Нормативно съответствие и вътрешен контрол”
   3.5. Отдел "Връзки с клиенти и маркетинг"
4. Комитет по управление на риска

(2) Когато организационната структура, определената в ал.1, е друга или се промени, следва да се гарантира спазването на основния принцип за разделянето на отговорностите между служителите с цел предотвратяване конфликти на интереси.

Чл. 3. Съветът на директорите има следните отговорности по управление на риска:

1. Приема правила за управление на риска както и последващите им актуализации.
2. Определя рисковата политика на договорните фондове при създаването им.
3. Взема решения за кадрово, софтуерно и друго осигуряване на дейностите по управление на риска.
4. Наред с отдела „Контрол и управление на риска“ на управляващото дружество, следи текущо за спазването на тези правила и издава заповеди за съобразяване с тях до служителите на Управляващото дружество в случай, че това се налага, като участва активно в процеса по управление на риска.
5. Компетентен е да взема решения относно намаляване на позиции, заемани по решение на инвестиционния консултант и за промяна в диверсификацията на активите на договорните фондове в рамките на инвестиционната политика, залегнала в проспектите на фондовете.

(2) Най-малко веднъж годишно преглежда и оценява правилата, като при непълноти и/или необходимост от подобряване на управлението на риска приема изменения и допълнения в правилата. Въз основа на извършената проверка и при необходимост от внасяне на промени в Правилата за управление на риска, Съветът на директорите на УД приема промени в Правилата, които се внасят в КФН в срок не по-късно от 7 дни след датата на приемането им.

Чл. 4. Изпълнителният директор има следните отговорности по управлението на риска:

1. Организира работата по правилно провеждане на приетата от Съвета на директорите политика по управление на риска.
2. Създава организация на работа, която осигурява контрол и спазването на определените лимити и нива на риск на договорните фондове управлявани от УД.
3. Следи за съответствие на използваните от съответните служители процедури по измерване, наблюдение и оценка на риска с приетите вътрешно-дружествени документи от Съвета на директорите.
4. Взема решения за кадрово, материално-техническо и методическо осигуряване на дейностите по управление на риска.

Чл. 5. (1) Отдел “Контрол и управление на риска” функционира независимо от останалите отдели и звена и се отчита пряко пред СД.

(2) Основните функции на отдела включват:

1. Разработване и внедряване на системата за управление на риска на база на Правилата за управление на риска на УД и на всяка КИС;

2. Изпълнение на правилата и процедурите по управление на риска;

3. Извършване на първоначална и текуща проверка на методите за оценка на риска и предложения за тяхната корекция; събиране, изготвяне и анализиране на ежедневната информация с цел оценка на риска на всяка позиция и на портфейла като цяло и предприемане на мерки за ограничаване на рисковите експозиции;

4.Контрол на входящите данни, необходими за оценка на риска;

5.Консултиране на Съвета на Директорите на УД относно определянето на рисковия профил на всяка колективна инвестиционна схема;

6.Докладване редовно пред Съвета на директорите на УД и отдел „Нормативно съответствие и вътрешен контрол" за:

a) Съответствието между текущото ниво на риск, на което е изложена всяка управлявана колективна инвестиционна схема и одобрените рискови профили на тази схема;
b) Съответствието на всяка колективна инвестиционна схема с вътрешната й система за ограничаване на риска;
c) Адекватността и ефективността на процеса за управление на риска и по-специално показващ дали са предприети подходящи коригиращи мерки в случаите, когато са констатирани недостатъци;
d) Докладване редовно пред Съвета на директорите на УД, представяйки текущото ниво на риск, на което е изложена всяка колективна инвестиционна схема и за текущите или предвиждани нарушения на ограниченията, като по този начин се осигурява предприемането на навременни и подходящи действия;

7.Участие в ежедневните процеси по планиране, наблюдение, управление и контрол на рисковете;

8. Контрол на спазването на установените лимити и сигнализиране на Съвета на директорите при достигане на утвърдените лимити или надвишаването им;

9.Гарантиране на съответствието с одобрената вътрешна система за ограничаване на риска на КИС, включително с нормативно определените лимити за стойността на общата рискова експозиция и риска на насрещната страна по чл. 46 – 48 от Наредба 44;

10. Извършване на преглед и подпомагане на организацията и процедурите за оценка на извънборсовите деривативи по чл. 49 от Наредба № 44;

11.Проверка и оценка на адекватността и ефективността на приетите от УД мерки, политики и процедури за установяване на всеки риск от неспазване на законовите задължения, както и свързаните това последици;

12.Следене за своевременно разкриване и предотвратяване на рисковете от използване на вътрешна информация и търговията на база вътрешна информация включително чрез поддържане на списък с вътрешните лица;

13. Осъществяване на контрол за изпълнение от членовете на Съвета на директорите и лицата, работещи по договор за УД на всички изисквания на законодателството, както и на правилата на УД и управляваните от него КИС и на поетите задължения към лицата, чиято дейност или портфейл дружеството управлява, съгласно сключените с тях договори;

14.Подпомага лицата, отговорни за извършваните от дружеството услуги и дейности, с цел гарантиране на осъществяването им в съответствие с изискванията на закона.

(3). Ръководителят и служителите в отдел "Контрол и управление на риска" не могат да бъдат лица, които участват във вземането на инвестиционни решения, на които е възложено оперативното управление на дружеството или които участват в извършването на дейности или отделни действия, спрямо които осъществяват контрол.
(4). Служителите в отдела следва да имат подходяща квалификация и професионален опит, които да съответстват на изпълняваните от тях дейности и функции да отговарят на нормативните изисквания.
(5). Ръководителят на Отдел "Контрол и управление на риска" се назначава от Изпълнителния директор на УД и се освобождава от длъжност при системно нарушаване на нормативната уредба и вътрешните правила, както и на основания, предвидени в сключения трудов договор.
(6). Отдел „Контрол и управление на риска" осъществява функции по управление на риска и във връзка с извършваните от УД допълнителни услуги по чл. 86, ал. 2 от Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране (ЗДКИСДПКИ), включително изготвя и представя на Съвета на директорите на Управляващото дружество, веднъж годишно доклад за дейността на отдела, в който посочва констатираните непълноти и несъответствия в политиката и процедурите, както и предприетите мерки за отстраняването им.
(7). Отдел „Контрол и управление на риска" е постоянно действащ отдел на УД, функциониращ отделно и независимо от другите отдели в УД. Включително чрез приемане и изпълнение на настоящите Правила, Съветът на директорите на УД осигурява дейността на отдела и гарантира неговата йерархическа и функционална независимост от останалите, включително оперативни, отдели в УД.
(8). Отдел „Контрол и управление на риска" изготвя и представя на Съвета на директорите на Управляващото дружество, до 10-то число на всеки месец, доклад по чл. 42, ал.1 т.6 от Наредба № 44 за предходния месец.
(9). Отдел „Контрол и управление на риска" представя писмен доклад на Съвета на директорите на УД по чл.121, ал. 1 от Наредба № 44.
(10). Отдел „Контрол и управление на риска" разкрива веднъж годишно публично информацията по чл. 43, ал. 1 от Наредба № 44 по отношение на изтеклата календарна година в срок до 31-во число на месец март, следващ календарната година.

Чл. 6. Служители, работещи по договор в управляващото дружество извън лицата по чл. 3, 4 и 5 са задължени да се запознаят и да спазват процедурите, описани в настоящите правила по Управление на риска.

Чл. 6а Комитетът по управление на риска подпомага дейността по контрол и управление на риска, като следи за спазването на правилата за управление на риска на управляваните договорни фондове и участва активно в управлението на риска. В него освен Ръководителя отдел „Контрол и управление на риска", изпълнителния директор и портфолио мениджъра, могат да бъдат включени и външни консултанти.

III. ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА РИСКА НА УД

Чл. 7. (1) Политиката по управление на риска е част от вътрешноорганизационната структура на УД действа и се прилага интегрирано с всички вътрешно-нормативни документи на дружеството.
(2) Целта на настоящата политика е да се документират процедурите по установяване, управление, наблюдение и оценка на рисковете, свързани с дейността на УД по реда

на Наредба № 44 от 20.11.2011 г. за изискванията към дейността на колективните инвестиционни схеми, националните инвестиционни фондове и лицата, управляващи алтернативни инвестиционни фондове.
(3) Детайлна категоризация на всички видове рискове се съдържа в Приложение 1, неразделна част от настоящите правила.

Чл. 8. Управляващото дружество разграничава следните видове оперативни рискове:

а. Вътрешни – свързани с организацията на работата на управляващото дружество и във връзка с управлението на колективните инвестиционни схеми.

б. Външни – свързани с макроикономически, политически и други фактори, които оказват и/или могат да окажат влияние върху дейността на управляващото дружество във връзка с управлението на колективните инвестиционни схеми.

(1) Вътрешните оперативни рискове се състоят без да се ограничават до:

а. Рискове свързани с персонал;

б. Технологичен риск;

В. Рискове свързани с накърняване интереса на клиента.

(2) Външните оперативни рискове се състоят без да се ограничават до:

а. Риск на обкръжаващата среда;

б. Риск от физическо вмешателство.

Чл.9 (1) Оценката на оперативните рискове се извършва от Отдел "Контрол и управление на риска".

(2).Служителите, работещи в управляващото дружество оказват пълно съдействие на Отдел "Контрол и управление на риска".

(3). Оперативните рисковете се оценяват с една от следните оценки:

1. нисък – когато всички рискове са покрити с адекватни контролни процедури с висока ефективност и липсват или са налице незначителни отклонения;

2. среден – когато всички рискове са покрити в известна степен с контролни процедури с недостатъчна ефективност;

3. висок – когато не всички рискове са покрити с контролни процедури и/или процедурите на предварителния контрол липсват или не действат ефективно, в резултат на което е нарушено спазването на принципите за добро управление и прозрачност.

(2) Оценката на рисковете се отчита от отдела по управление на риска, въз основа на резултатите от описаната по-долу „Процедура по идентификация, оценка и контрол на риска", прилагана от всички функционални звена на УД.

(3) Въз основа на отчетените резултати, съгласно процедурата, УД установява допустимо ниво на риск за организацията и осигурява извършването на дейността да бъде в рамките на определеното допустимо ниво.

Чл. 10. (1) Рискове, свързани с персонала, са рискове, свързани със загуби от:

1. Измами и кражби на лица, работещи по договор за УД;

2. Грешки и недобросъвестно поведение от страна на служителите на УД, както и некоректно отношение на ръководния персонал към служителите;

3. Недостатъчна квалификация и липса на подготовка на лицата, работещи по договор за УД;

4. Неблагоприятни изменения в трудовото законодателство;

5. Неосигурена безопасност на трудовата среда;

6. Текучество.

(2) Методи за управление на рисковете, свързани с персонала включват:

1. Ясно дефиниране на вътрешни правила относно правата и задълженията на служителите, както и изготвяне и запознаване на служителите с индивидуални длъжностни характеристики;

2. Ясно дефинирани нива за достъп до информационните системи и бази данни на Управляващото Дружество;

3. Регулярни обучения на персонала по теми, свързани с финансова теория и практика, управление на риска, нормативната база, имаща отношение към дейността на УД, информационни технологии и сигурност и други;

4. Регулярни срещи между отделните звена на Управляващото Дружество за обмяна на опит, впечатления и препоръки, по отношение на източниците на риск и търсене на решения за управлението и минимизирането им;

5. Ежегодни събеседвания и оценка на персонала;

6. Поддържане на отворени, открити комуникации между различните звена в Управляващото Дружество;

7. Извършване на начален и периодичен инструктаж, свързан с безопасните условия на труд.

Чл. 11. (1)Технологичните рискове могат да се разделят в 4 основни групи:

1. **Сигурност на използваните технологии** – информацията може да бъде променяна, достъпна или използвана от неоторизирани лица. Източници на този риск са: външни атаки, злонамерени хакерски атаки, физическо унищожение, неодобрен достъп, недоволни служители, разнообразни системи за злонамерен достъп, имперсониране и автоматизация на усилията за придобиване на нерегламентиран достъп до привилегирована информация.
   Последствията от подобрен тип риск са: промяна на информацията, външна измама, кражба на идентичност, кражба на активи управлявани и под пряк контрол от системите, уронване на репутацията и унищожаване на активи.
2. **Достъп/наличност до използваните технологии** – информация или приложения, до които няма да има достъп поради срив в системата/ите или природно бедствие и периодът по възстановяване. Източници на подобен риск са: срив в хардуерни устройства, сривове на мрежи, сривове в дейта центрове, форс мажорни обстоятелства.
   Последствията от подобен тип риск са: незавършени транзакции, неосъществени продажби, накърнено доверие в клиенти, партньори и служители, забавяне или прекъсване на важни бизнес процеси, драстично намалена ИТ производителност на екипа.
3. **Оперативен технологичен риск** – намалена функционалност и/или производителност на системите, несъвършенство на използваните технологии, грешки на софтуерни продукти, приложенията или служителите, което намалява като цяло бизнес производителността или стойността. Източници на този риск са: неправилно оразмерени сървърни и мрежови ресурси, неефективен код, софтуерни архитектури, които не съответстват на системните и/или приложни нужди.
   Последствията от подобен риск са: намалена удовлетвореност на клиентите и лоялност, прекъсване или забавяне на критични бизнес процеси, загуба на ИТ продуктивност.

4. **Риск свързан с нормативното съответствие** – обработването и съхранението на информацията не отговаря на регулаторните, ИТ или бизнес изисквания. Обикновено включва административни нарушения, глоби или уронване на репутацията от нарушаване на съответствието със закони, наредби и ИТ политики. Източници на подобен риск са: регулации, които са уникални за всяка юрисдикция, правни действия, неадекватни стандарти за нормативно съответствие на 3ти страни.
Последствията от подобен риск са: уронване на репутацията, нарушаване на клиентската тайна, съдебни процеси и др.

(2) Методите за управлението на технологичните рискове включват:

1. Сигурност на използваните технологии

- Политика по архивиране данните, включително потребителски акаунти, бази данни с клиентска информация, изходен код на системите, оперативна документация в различните ѝ форми;
- Употребата и/или имплементацията на системи и код позволяващи RBAC (Role-Based Access Control);
- Организация и управление на достъпа на потребителите до информационната система на колективните инвестиционни схеми;
- Дефиниране на различни класове информация съхранявана в УД;
- Дефиниране на нива на достъп на служителите на управляващото дружество според длъжностната им характеристика;
- Употребата на последни версии на инфраструктурни системи и код;
- Процедура по възстановяване на работоспособността на информационната система;
- УД разработва и разполага с план за действие в кризисни ситуации, който осигурява продължаването и поддържането за достатъчно дълъг период нормалната работа на дружеството при спазване на законоустановените норми за дейността.

2. Достъп/наличност до използваните технологии

- Употребата на мониторинг системи за нападения (IDS, Intrusion Detection Systems);
- Употребата на системи за агрегиране и анализ на логове;
- Използването на HA (highly-available) доставчици и на инфраструктура, софтуерни архитектури и алтернативни комуникационни канали и технологии;
- Процедура за възстановяване на работоспособността на информационната система на УД и колективните инвестиционни схеми.

3. Оперативен технологичен риск

- Употреба на системи за мониторинг в реално време както и за анализ на исторически данни за производителността на системите;
- Интегрирани процеси и системи за оценка и тестване на производителността на системите и използваният софтуер.

Чл. 12. (1) Рискове, възникващи от накърняване интереса на клиента в резултат на:

1. Действия в нарушение на определената инвестиционна стратегия;
2. Неправилна преценка за рисковия профил на клиента и избор на неподходяща и неуместна за клиента инвестиционна стратегия;
3. Виновно причинени вреди, които са в пряка причинна връзка с предоставяне на неверни, неточни или непълни анализи и прогнози в конкретна инвестиционна консултация;

4. Извършване на транзакции с инструменти, с които Клиентът няма право да търгува;
5. Недобросъвестно използване на поверителна информация, предоставена от клиента (неупълномощен достъп до поверителна информация на клиента), нарушаване на търговска тайна;
6. Злоупотреба с поверителна информация;
7. Конфликт на интереси;
8. Грешки при събиране, въвеждане и осчетоводяване на данни;
9. Действие в нарушение на политиката за най-добро изпълнение и дължима грижа към клиента;
10. Грешки при подаване на информация към клиента;
11. Грешки при преоценка на клиентски активи;
12. Неправилна отчетност и съхранение на клиентски активи.

(2) Методи за управление на рисковете, свързани с накърняване на интереса на клиентите, включват:

1. Изчерпателно и максимално точно уговаряне в договорните отношения с клиента обхватът на управлението и конкретните сделки и действия, които УД е овластено да извършва.

2. С цел коректната оценка на рисковия профил на клиента УД класифицира клиентите, които се ползват от допълнителните услуги по чл. 86, ал. 2 от ЗДКИСДПКИ, предоставяни от УД си съгласно Правилата за категоризация на клиентите като професионални, непрофесионални или приемлива насрещна страна.

3. Изискване към клиентите и потенциалните клиенти в писмена форма информация за установяване на съществени факти относно финансовите им възможности, инвестиционните цели, знания, опит относно услугите по управление на портфейл и предоставяне на инвестиционни консултации и за готовността им да рискуват. При промяна на горепосочените факти Клиентът се задължава своевременно да уведоми УД.

4. Поддържане на системи и процедури, които осигуряват трайното и конфиденциално съхранение на получената от клиентите информация за техните финансови възможности, инвестиционни цели, знания, опит и готовност да рискуват, както и за дадените им съвети и препоръки.

5. Предварително подробно запознаване на клиентите с вида и характеристиките на конкретния вид финансов инструмент и на конкретните рискове, свързани с него.

6. Разработване на система за отчитане пред клиента в съответствие с профила на клиента и законоустановените изисквания, която да гарантира навременното и точно подаване на изискуемата информация. При предоставяне на информация до клиента, УД се стреми да предоставя максимално релевантна такава, която да осигури на клиента възможност да направи преценка за обекта инвестициите.

7. УД създава вътрешна организация и условия за установяване на потенциалните конфликти на интереси.

8. УД приема ефективни процедури и мерки за третиране на конфликт на интереси, съгласно чл. 127 и чл. 148 от Наредба 44 от 01.11.2011 г. за изискванията към дейността на колективните инвестиционни схеми,

инвестиционните дружества от затворен тип и управляващите дружества, както и в съответствие с действащото законодателство и добрите международни практики.

9. УД прилага подходящи мерки за съхраняване на финансовите инструменти и паричните средства на клиентите и за отделяне на собствения портфейл от финансови инструменти от този на инвеститорите, да отчита отделно паричните средства на клиентите от сделки с финансови инструменти.

10. УД приема и прилага политика, която да осигурява постигането на най-добър резултат за клиента отчитайки факторите по чл. 30, ал. 1 ЗПФИ, като политиката определя по отношение на всеки клас финансови инструменти лицата, до които УД подава нарежданията или на които предава нарежданията за изпълнение.

11. УД организира права и нива на достъп до клиентска информация, които осигуряват превенция на лицата, работещи по договор за УД да разгласяват, и да ползват за облагодетелстване на себе си или на други лица факти и обстоятелства, засягащи наличностите и операциите по паричните сметки и по сметките за финансови инструменти на клиенти на УД, както и всички други факти и обстоятелства, представляващи търговска тайна, които са узнали при изпълнение на служебните и професионалните си задължения.

Чл. 13. (1) Като риск на обкръжаващата среда се класифицират рисковете свързани с възможните загуби, свързани с изменения в средата, в която оперира УД:

1. Неблагоприятни промени в нормативната уредба;
2. Риск, свързан с финансови средства с незаконен произход;
3. Рискове, свързани с прехвърлянето на важни дейности на трета страна изпълнител;
4. Политически изменения;
5. Изменения в данъчната уредба.

(2) Методите за управление на рисковете свързани с обкръжаващата среда включват:

1. УД поддържа актуална база данни с нормативната регламентация, имаща отношение към дейността на УД, организира мерки за следене на съответствието на прилаганите политики с изискванията на законодателството и използва външни консултанти и юридически кантори в случай на необходимост за привеждане на дейността на Управляващото Дружество в съответствие с нормативните изисквания и промените в тях;

2. При встъпване в трайни отношения (сключване на договор), УД извършва идентификация на клиентите в съответствие с изискванията на Закона за мерките срещу изпирането на пари и Закона за финансиране на тероризма, както и актовете по прилагането им. УД изисква от клиентите декларация за произход на средствата и съхранява събраните по идентификация на клиента данни и документи по начин, който позволява да бъдат достъпни при поискването им по законоустановения ред;

3. УД взема активно участие в публичните обсъждания по отношение планирани промени в нормативната уредба, касаеща дейността на Управляващото Дружество;

4. При възлагане за изпълнение на съществени функции, УД постоянно следи за ефективността и качеството на изпълнение от страна на лицата, до които УД

подава или предава нареждания за изпълнение, и когато е необходимо взема мерки за отстраняване на установени нередности.

Чл. 14. (1) Риск от физическо вмешателство:

1. Природни бедствия;
2. Пожар;
3. Външни измами и кражби;
4. Терористични актове;
5. Непозволено проникване в информационните системи.

(2).Методи за управление на риска от физическо вмешателство:

1. Осигуряване на подходящ начин на наблюдение и контрол на помещенията, в които се намират технологичните средства и архивите на Управляващото Дружество;
2. Профилактика на регулярна база на въведените системи за наблюдение и контрол;
3. Процедура за докладване на инциденти.

Чл. 15. (1) УД прилага краткосрочна и дългосрочна стратегия за управление на оперативните рискове, свързани с осъществяването на дейността на УД и управляваните договорни фондове.

(2). Дългосрочната стратегия предвижда следните принципи при развитието на управлението на оперативните рискове:

1. Идентифициране на основните рискови идентификатори и представянето им пред Съвета на директорите на УД.
2. Създаване на карта на процесите в УД, както и правила за разпределението на задачите и отговорностите на отделите при всеки един от процесите.
3. Измерване статистически на точките, в които са концентрирани най-много събития.
4. Усъвършенстване на организацията, създавайки ясни правила и инструкции за всеки един от процесите.
5. Изготвяне на стратегия за редуциране на риска, чрез сключване на застраховки и други механизми за прехвърляне на риска.

(3). Краткосрочната стратегия за управлението на оперативните рискове включва:

1. Основната цел на краткосрочната стратегия е определяне на насоките, които трябва да бъдат следвани за идентифициране, оценка, наблюдение, контрол и намаляване на оперативния риск, свързан с дейностите на Фонда, както и определяне на организационната структура в УД, заета със създаването и практическото прилагане на системата за управление на оперативен риск.

2. Идентифициране на оперативния риск - за откриване и разграничаване на оперативния риск от другите видове риск, УД използва подробен анализ на бизнес процесите в дружеството, както и вътрешно за всеки отдел изследване, което представлява дейност по установяване на факти, спомагащи за разкриването, определянето и локализирането на източниците и концентрация на оперативен риск в

дейността на Фонда. Допуска се определени (малко на брой) рискове да не бъдат проследени (неидентифицирани). Поради тази причина се цели да се подобри своевременното установяване на неидентифицираните рискове във всеки отдел.

2.1. С цел по-точно разпределяне на операционните събития по рискови класове в зависимост от първопричината за тяхното възникване, в дейността на УД са идентифицирани, като потенциални четири основни рискови категории:

2.1.1. Рискове свързани с персонал - *Например:* грешки, недобронамереност, недостатъчна квалификация.

2.1.2.Технологичен риск - *Например:* неадекватност на провежданите операции, липса на прецизност на методите на обработка на данните, ниско качество на използваните данни.

2.1.3. Рискове, възникващи от накърняване интереса на клиента – *Например: з*лоупотреба с поверителна информация; Конфликт на интереси;

2.1.4.Риск на обкръжаващата среда *Например:* изменения в законодателството, политически изменения, изменения в данъчната система.

2.1.5. Риск от физическо вмешателство – *Например:* грабеж, терористичен акт, непозволено проникване в информационната система, природни бедствия, пожар.

2.2 Бизнес процес - Една или няколко свързани помежду си процедури или операции, които съвместно реализират определена бизнес задача и реализирането им води до конкретни резултати. С оглед постигането на по-точни резултати в оценка на оперативния риск са идентифицирани някои от следните бизнес процеси:

2.2.1 Управление на портфейли;
2.2.2 Оценка на НСА.
2.2.3 Координация и комуникация;
2.2.4 Организация и управление на продажбите и обслужване на клиенти;
2.2.5 Управление на риска;
2.2.6 Счетоводство на ДФ;
2.2.7 Счетоводство на УД;
2.2.8 Управление на УД;
2.2.9.Процес на регулативно и вътрешно групово отчитане, управленска информация;

3. Оценка на рисковете - чрез съпоставянето на идентифицираните рискове срещу бизнес процесите в една плоскост се отчита и влиянието им върху всеки вид осъществявана дейност в УД. По този начин се определя и така наречената рискова зона, която е пресечната точка на риска с конкретната дейност. Там е съсредоточен оперативния риск, който най-често подлежи на количествено измерване. Рискът се оценява от гледна точка на характеристиките - честота на възникване и степен на въздействие.

4. Наблюдение на рисковете - всички операционни събития, които носят ефективна загуба, както и такива с потенциална такава, надвишаваща 500 лв. следва да се

докладват на отдела по „Контрол и управление на риска" от съответните отдели и да се регистрират в базата данни.

5. Управление/Редуциране на риска – стратегията включва прилагането на правила уреждащи организационната структура и нивата на отговорност, както и политики по управление на рисковете, конкретизирани във вътрешните за УД документи. Отдел „Контрол и управление на риска" може да извършва по-задълбочени анализи на рисковите фактори, както и да определя нови методи за управлението/редуцирането им.

IV. СЧЕТОВОДНИ ПРОЦЕДУРИ ПО УПРАВЛЕНИЕ НА РИСКА

Чл. 16. Основна цел на счетоводните процедури е адекватното събиране, обработване и представяне на достоверна, систематизирана и навременна информация за степента на риск, на която са изложени УД, клиентските портфейли или колективни инвестиционни схеми, управлявани от управляващото дружество.

Чл. 17. Своевременното и вярно представяне на информацията за степента на изложеност на риск пред Съвета на директорите е предпоставка за недопускане на концентрация на рисковете и понасяне на финансови загуби.

Чл. 18. Счетоводните процедури трябва да осигуряват всеобхватност на стопанските процеси, като по този начин се минимизира рискът от загуба и изкривяване на информацията за моментното състояние на клиентските портфейли или колективни инвестиционни схеми, управлявани от управляващото дружество.

Чл.19 Счетоводните процедури трябва да осигуряват подходящо структуриране на финансово-счетоводната информация за целите на управление на рисковете от управляващото дружество. Това се постига чрез детайлизиране адекватно групиране на информацията от първичните счетоводни документи, на базата на индивидуалния сметкоплан и специализирано програмно осигуряване.

Чл. 20. За осъществяване на целите, стоящи пред счетоводните процедури за управление на рисковете е необходимо съгласуваност с всички отдели в управляващото дружество.

Чл. 21. Предпоставките за правилното функциониране на счетоводните процедури са следните:

1. Спазване на одобрената от Съвета на директорите счетоводна политика, изработена в съответствие с Международните стандарти за финансови отчети;
2. Вярно, точно и своевременно осчетоводяване на стопанските процеси;
3. Осигуряване на необходимия информационен поток към счетоводния отдел;
4. Навременност на подаваната към счетоводния отдел информация;
5. Структуриране на индивидуалния сметкоплан за целите на получаване на необходимата счетоводна информация;
6. Активно взаимодействие с отдел „Контрол и управление на риска" и другите отдели на управляващото дружество за получаване на вярна и навременна информация за степента на изложеност на риск;

7. Наличие на програмни продукти, целящи автоматизиране на процесите, систематизиране на информацията, улесняване достъпа на данните от първичните документи и източници и надеждното им архивиране;
8. Организационна структура на счетоводния отдел в съответствие с нуждите на управляващото дружество, при ясно определени права, отговорности и нива на достъп до информацията;
9. Ежедневно осчетоводяване на всички операции, както и преоценка на ценните книжа в портфейлите на клиентите и колективни инвестиционни схеми, управлявани от управляващото дружество, съобразно нормативните изисквания и възприетата счетоводна политика;
10. Ежедневно извличане и предоставяне на информация на други отдели и на ръководството на управляващото дружество, както и анализ на същата за оценка на рисковете. Ежедневно изготвяне на баланс и аналитична оборотна ведомост и активно участие при изготвяне на ежедневните справки;
11. Предвиждане на коригиращи действия при допускане на грешки от различно естество в счетоводния отдел;
12. Възможност за контрол на дейността от отдел „Контрол и управление на риска" и Съвета на директорите на управляващото дружество;

Чл. 22. Управляващото дружество определя източниците на ценова информация, данните от които ще се ползват за ежедневна и/или ежемесечна преоценка на позициите в портфейла на клиенти или колективни инвестиционни схеми, управлявани от управляващото дружество, както и отговорните за това служители.

V. АДМИНИСТРАТИВНИ ПРОЦЕДУРИ ПО УПРАВЛЕНИЕ НА РИСКА

Чл. 23. Правилата, уреждащи вътрешната организация и отговорностите, трябва да осигуряват и съдържат:

а) идентифициране, събиране и разпространяване в подходяща форма и срокове на надеждна и достоверна информация, която позволява на всяко лице в управляващото дружество да поеме определена отговорност;

б) ефективна комуникация по хоризонтална и вертикална линия и на всички йерархични нива на дружеството;

в) политики и процедури за разрешаване и одобряване;

г) политики и процедури за разделяне на отговорностите по начин, който не позволява един служител едновременно да носи отговорност по одобряване, изпълнение, осчетоводяване и контрол на сделките;

д) политики и процедури за достъп до информацията;

е) правила за управление на човешките ресурси.

Чл. 24. Административни процедури, необходими за осъществяване да дейността на управляващото дружество са:

1. Процедура за одобряване или коригиране на вътрешните правила;
2. Наличие на система за осъществяване на контрол, съгласно вътрешната организация на УД;
3. Поредица от действия на служители, във връзка с осъществяване на дейността на управляващото дружество, съобразно издадения му лиценз;
4. Упълномощаване на служители за потвърждаване и подписване на документи в рамките на дейността на управляващото дружество;

5. Процедура за създаване, функциониране и управление на данните и документите в управляващото дружество, включително и тяхното архивиране;

6. Администриране и управление на информационната система;

7. Правила и отговорни служители за уведомяване на Комисията за финансов надзор относно дейността на управляващото дружество.

(2) Административните процедури по ал. 1 се съдържат в нормативен акт, вътрешни правила на УД или се разработват в отделен вътрешен документ.

Чл. 25. Във вътрешните правила управляващото дружество регламентира случаите на конфиденциалност при работа с вътрешна информация, както и нормите за поведение на служителите по отношение на клиентите на управляващото дружество, в случаи, когато услугата, искана от клиент, се отнася до инвестиция, информацията за която не е публично достояние.

VI. ПРОЦЕДУРА ПО ИДЕНТИФИКАЦИЯ, ОЦЕНКА И КОНТОЛ НА РИСКА

Чл. 26. Процедурата по идентификация, оценка и контрол на риск обхваща следните 4 фази:

1. Идентификация на рисковете – риск и контрол самооценка, идентификация на рисковете, които не са обект на контрол;

2. Оценка на риска – оценка на честота на настъпване и степента на въздействие на рисковете, както и промяна в нивата на риск:

а) отчитане на Съществени Рискови Показатели;

б) отчитане за настъпили инциденти.

3. Наблюдение на риска – наблюдение на неприемливите рискове, промяна в рисковете/рисковите нива и процеси за управление на риска:

а) отдел „Контрол и управление на риска“;

б) Съвет на директорите;

4. Намаляване на риска – управление за намаляване на риска, съобразно допустимото ниво на риск:

а) проследяване на открития риск при извършване на проверки от регистрирани одитори;

б) установяване на контролни стандарти.

Чл. 27. (1) Идентификация на риска – в тази фаза се идентифицират основните рискове. Допуска се определени (малко на брой) рискове да не бъдат проследени (неидентифицирани). По дефиниция това са рискове, които не могат да бъдат разпознати. Идентификацията на риска започва с вътрешно за всяко звено изследване, което представлява дейност по установяване на факти. За целта, всеки отдел се задължава да информира по подходящ начин ръководителя на отдел „Контрол и управление на риска” относно броя на засечените инциденти, както и информация за размера на понесените щети, в случаите когато е налична информация за това.

(1) Резултатът от фазата “Оценка” е набор от приемливи и неприемливи рискове.

(2) По време на фазата “Ограничаване на риска” се прилагат подходящи мерки (контрол, прехвърляне или избягване) за ограничаване на неприемливите рискове.

Чл. 28. (1) Риск и Контрол Самооценка. Целта на процеса по Риск и Контрол Самооценката е:

1. Да се подобри навременното установяване на неидентифицирани рискове;
2. Да се подобри преценката за приемливостта на нивото на идентифицираните рискове;
3. Да се доразвият и подобрят алтернативни механизми за контролиране на неприемливите рискове;
4. Да се улесни прилагането на навременни и адекватни действия за ограничаване на риска;
5. Да се ангажират отделните функционални звена в УД в процеса по установяване и оценка на риска, като по този начин се постига по-голяма отговорност на служителите на дружеството за управлението на рисковете.

2) Процесът по Риск и Контрол Самооценка е периодичен. Всеки последващ цикъл е свързан с предходните особено във фазата "Идентификация". Наборът от вече идентифицираните рискове служи като отправна точка, като в хода на процеса се проверява доколко те са актуални, междувременно ограничени или невалидни.

3) Резултатите от процеса по Риск и Контрол Самооценка се използват за определянето на Съществени Рискови Показатели за отделните бизнес функции. Крайните резултати се свеждат до знанието на съответно отговорните лица.

Чл. 29. (1) Оценка на риска - действията, които се предприемат в тази фаза се предопределят от резултатите получени във фазата идентификация. Оценката се определя съвместно от съответния отдел, който идентифицира риска и отдела по контрол и управление на риска.

(2) Идентифицираните рискове се анализират от гледна точка на следните 2 характеристики:

1. честота на възникване;
2. степен на въздействие.

(3) Съгласно тази оценка, рисковете се категоризират на приемливи и неприемливи, съобразно определеното за допустимо ниво на риск в дружеството.

Чл. 30. (1) Ограничаване на риска - въз основа на резултатите от оценката на риск се определят възможни мерки за ограничаването му. Необходимо е да се оцени и остатъчният риск, след предприемане на ограничителните мерки.

(2) Ограничаването на риска се налага в случаите когато, идентифицираните нива на риск надхвърлят приетите за допустими. Ограничаването може да бъде осъществено по няколко начина:

1. избягване на риска чрез прекратяване на дейността, която го поражда или заменянето и с алтернативна;
2. намаляване на възможността на проява на риска – чрез внедряването на контролни процеси, подобряване на надзора върху дейността, обучения;
3. намаляване ефекта от проявяването на риска – чрез застраховане;

4. прехвърляне на риска към трети страни, които по същество са обект на същия тип риск;

5. предварително установяване и приемане на част от ефекта на риска, като присъща за решението на управителните органи за продължаване на съответната дейност.

(3) Ограничителните мерки се одобряват от отдел „Контрол и управление на риска“

(4) Последната стъпка е извършване на действия съобразно одобрените ограничителни мерки.

Чл. 31. Наблюдение на риска - предприемането на конкретни действия по ограничаването на риска е отговорност на упълномощените лица в съответните звена. Отделът по “Контрол и управление на риска” подпомага внедряването на контролните механизми и установяването на вътрешни контролни стандарти. Отговорните лица се отчитат пред отдела за контрол и управление на риска.

Чл. 32. (1) Отчитане на настъпили инциденти – отчитането на настъпили инциденти цели:

1. да спомага за формирането на информационна база за загуби, предизвикани от операционни инциденти;

2. да спомага за увеличаване на риск културата, съответно подобряване на процеса по управление на риска и възможностите за ограничаване чрез подобряване на информацията за действителната цена на операционния риск;

3. периодично да измерва стойността на възникващите следствие операционен риск инциденти, осигурявайки по-добра възможност на мениджмънта за ограничаване на разходите;

4. да подобри възможността за реагиране при значителни операционни инциденти;

5. да приведе в съответствия изискванията на нормативната уредба на ниво функционална единица;

6. да създаде изцяло синхронизирана процедура за събиране на данни и отчитане, както и избягване на дублиране на информация и празноти.

(2) Политиката по управление на риска изисква незабавно отчитане инциденти, които са: значими; имат заплашителен характер; имат отношение към репутацията на дружеството; имат незаконно или осквернително действие.

Чл. 33. Отчитане на Съществените Рискови Показатели:

1. Съществените Рискови Показатели дават информация на ръководния персонал дали специфичните рискове са в предварително определените граници и дали е необходимо предприемането на действия за ограничаването им до допустимото ниво за дружеството;

2. Наличието на Съществените Рискови Показатели се определя на базата на резултати от процеса по Риск и Контрол Самооценка;

3. Отделите сами идентифицират Съществените Рискови Показатели, свързани с тяхната дейност с помощта на отдела „Контрол и управление на риска“;

4. След оценката на Съществените Рискови Показатели отдел „Контрол и управление на риска“ и функционалните единици определят реалистични нива на рискова поносимост;

5. Съветът на директорите се уведомява при възникването/констатирането на Съществени рискови показатели.

VII. ПЛАН ЗА ДЕЙСТВИЕ ПРИ ВЪЗНИКВАНЕ НА КРИЗИСНИ СИТУАЦИИ

Чл. 34. (1) Основни положения: Планът за действие при кризисни ситуации установява процедурите по възстановяване работоспособността на информационните и комуникационни системи на УД и на организацията като цяло в случаите на възникване на извънредни неблагоприятни обстоятелства.

1. Планът за действие в кризисни ситуации е неразделна част от политиката по управление на риска и непосредствен резултат от процедурите по установяване, оценка, наблюдение и управление на рисковете в УД.

2. Планът има за цел да сведе до минимум времето на прекъсване на обичайните бизнес процеси и да предпази критичните за дейността на организацията функционални/информационни центрове от отрицателните въздействия на възникнали кризисни ситуации.

(2) Дефиниране на кризисни ситуации. Като кризисни ситуации се определя тези, които имат за резултат прекъсване бизнес-процесите в УД, загуба/нанасяне на щети върху съоръжения, функционален/информационен център на УД, загуба на персонал и др. Без да се изчерпват, кризисните ситуации се свеждат до:

- Пожари, земетресения, наводнения и други природни бедствия;
- Спиране на тока, прекъсване на комуникациите, срив на хардуерни системи, срив на софтуерни системи, нарушаване на конфиденциалността, интегритета и достъпа до фирмените бази данни и др.;
- Терористични атаки, заплахи.

(3) Конструктивни елементи на Плана за действие в кризисни ситуации:

1. Основна цел на плана: кратко описание на целите на плана.

- в случай на срив в телекомуникационните системи това може да бъде: “Поддържане на дейностите по управление на клиентски портфейли и предоставяне на инвестиционни консултации за периода на времетраене на срива в телекомуникационните системи.”
- в случай на природно бедствие – запазване, доколкото е възможно, на работоспособността на информационните и комуникационни системи на УД и на информацията и последващото им възстановяване в случай на загуби;
- в случай на срив на хардуерните или софтуерните системи – възстановяване на изгубената информация;
- в случай на нарушаване на конфиденциалността и изтичане на информация - минимизиране на възможните загуби за клиентите и за самото УД и предотвратяване на последващо неоторизирано разкриване на информация;
- в случай на терористична заплаха и/или атака – своевременна евакуация на персонала на УД, прехвърляне на информацията, съхранявана от управляващото дружество, на носители, които не са

застрашени от атаката/заплахата, с цел предотвратяване на изгубването/унищожаването й.

2. Запознати лица: списък на лицата (вътрешни или външни за организацията), които са запознати с процедурите за действие в настоящия план и техните координати за връзка (Приложение № 3).

3. Лица, отговорни за изпълнение на плана:

а) Определяне на лицето/лицата, които разполагат с правомощия за разпореждане със системата в случай на кризисна ситуация, както и лицето/лицата, които ще ръководят дейностите по преодоляване на възникналата ситуация – обикновено това е изпълнителния директор на УД.
б) Определяне на лицето/лицата, които ще следят за това описаните в плана процедури и действия да се изпълняват от достатъчно квалифициран персонал: това може също да е изпълнителният директор на УД или мениджър от по-висок ранг.

4. Определяне на причините/факторите, които могат да доведат до възникване на кризисна ситуация. Това могат да бъдат, но не само:

а) Срив на телефонните линии/ интернет
достъп;

б) Прекъсвания на електрозахранването: пълно или
частично;

в) Физически повреди по телекомуникационните линии;

г) Земетресение, пожар, наводнение или друго природно бедствие;

д) Грешки в софтуерните системи;

е) Кражби/подправяне на информация от персонала на УД или от външни лица, разкриване на конфиденциална информация на неоторизирани лица;
ж) Нападение на помещенията и/или персонала на УД, отправяне на заплаха за извършване на терористичен атентат.

5. Определяне на показателите, които сигнализират за възникване на кризисна ситуация. Това могат да бъдат, но не само:

а) Спад в броя на входящи обаждания;
б) Трудности или невъзможност за извършване на изходящо обаждане;
в) Невъзможност за отпечатване на справки/отчети;
г) Невъзможност на модемите да установят връзка.
д) По-слаби или по-силни земни трусове, проникване на вода или течове в помещенията на УД или възникване на пожар;
е) Установяване наличието на информация, която е конфиденциална, в пресата или възпроизвеждане на такава информация от други средства за масово осведомяване; установяване знанието на конфиденциална информация от неоторизирани лица;
ж) Установяване на пробиви в информационните системи на УД;
з) Получаване на заплахи за атаки/атентати срещу УД и/или негови служители.

6. Определяне на засегнатите функционални звена, процеси, съоръжения. В зависимост от характера и вида на възникналата кризисна ситуация, могат да бъдат засегнати следните звена, процеси и съоръжения:

- в случай на природно бедствие – всички звена и системи на УД, както и материалната база; в случай на срив на телекомуникационните системи - комуникациите вътре в организацията, както и комуникациите с клиенти и/или доставчици на УД;

- в случай на срив на хардуерните или софтуерните системи – събирането, въвеждането и осчетоводяването на данни; подаването на информация към или от клиентите и/или генерирането на информация;

- в случай на нарушаване на конфиденциалността и изтичане на информация – базите данни на УД и процесът по съхранение на информация;

- в случай на терористична заплаха и/или атака всички звена на УД и неговата материална база, както и цялата извършвана от УД дейност.

7. Определяне на целеви времеви интервал за възстановяване на системата: това е времевият интервал, в който системата се наблюдава и след изтичането на който се пристъпва към изпълнението на настоящия план с цел избягване на сериозни смущения в бизнес процесите.

8. Известяване: изискване на съдействие и уведомяване на отговорните лица. Тази част от плана съдържа лицата (вътрешни или външни за организацията), които следва да бъдат уведомени в случай на възникване на кризисна ситуация и след изтичане на времевия интервал за възстановяване на системата. Това могат да бъдат: пряк ръководител, изпълнителен директор на УД, IT специалист.

9. Изброяване на средствата за известяване: това могат да бъдат мобилни телефони, вътрешни телефонни линии и др.

10. Проверка на резервни ресурси/съоръжения: генератори, UPS системи, хранилища за документи и др. В тази фаза се извършва проверка на състоянието на резервните ресурси съоръжения и при необходимост възстановяване на тяхната функционалност.

11. Първоначални действия по справяне с кризисната ситуация:

а) При възможност оценка на очакваната продължителност на действие на съответната ситуация (А) и сравняване с определения целеви интервал за възстановяване на системата (Б). Ако (А) < (Б), премини към дейностите по мониторинг на кризисната ситуация. Ако (А) > (Б), премини към първоначални дейностите по справяне с кризисната ситуация.

б) Дейности по мониторинг на кризисната ситуация: определяне на процедури за нормално провеждане на бизнес операциите до отминаване на кризисната ситуация. Определяне на лицата и отговорностите по извършване на процедурите.

в) Първоначални дейности по справяне с кризисната ситуация: определяне на алтернативни дейности за провеждане на бизнес операциите. Определяне на лицата и отговорностите по извършване на алтернативните дейности.

12. Поддържащи дейности по преодоляване на кризисната ситуация: мониторинг на ситуацията и периодична оценка на определен интервал от

време (например: оценка на ситуацията на всеки кръгъл час. На 6-ия час премини към изпълнение на поддържащите мерки).

а) Поддържащи дейности: организиране на работни станции за извършване на рутинните дейности, изготвяне на график за работа на смени и при необходимост - възлагане на дейности на външни изпълнители до отминаване на кризисната ситуация.

б) Определяне на лицата и отговорностите им по извършване на поддържащи дейности.

13. Фаза на възстановяване на работоспособността на системите/функционалността на съоръженията. При потвърждение, че кризисната ситуация е отминала, следва да се започнат дейности по възстановяване нормалния ход на бизнес операциите. Лицата отговорни за изпълнението на плана следва да се уверят, че са налице всички предпоставки за безпрепятствено функциониране на системите и звената/отделите в УД. Посочват се лицата, от които да се изисква необходимата информация, както и нивата на нейното докладване.

(4) Оценка на възникналата рискова ситуация и на адекватността и ефективността на предприетите мерки: с цел повишаване културата по управление на рискови ситуации и оценка на адекватността и ефективността на предприеманите мерки УД следва да изготвя Дневник на регистрирани инциденти (Приложение № 2).

Настоящите Правила са приети на заседание на Съвета на директорите на „Алфа Асет мениджмънт" ЕАД, проведено на 04.03.2016г. и са изменени с решение на Съвета на директорите от 24.09.2019г.

за УД „Алфа Асет Мениджмънт" ЕАД

Иван Ненков – изпълнителен директор

Приложение № 1 към чл. 7, ал. 3

Ниво 1	Ниво 2	Ниво 3
Неупълномощени действия	Неупълномощени действия	Неупълномощени одобрения
		Незаконни сделки
		Неотчетени сделки
		Погрешно отчетени сделки
		Неоторизирана търговия
		Прехвърляне на пълномощия
Вътрешни криминални действия	Кражби и измами от страна на персонала	Нарушение на задължения по договор
		Нарушение на дължима грижа при изпълнение на договор за доверително управление
		Нарушаване на патент
		Дискриминация при предоставяне на услуги на клиенти
		Нарушение на законодателството
		Злоупотреба, незаконно присвояване
		Фалшифициране и подправяне на документи от страна на персонала
		Кражба от страна на персонала
		Изнудване
		Отвличане за откуп от страна на персонала
		Избягване или заобикаляне на данъчни задължения
		Подкуп
		Злоупотреба с вътрешна информация
		Други вътрешни криминални действия
Срив на системите за информационна сигурност	Вътрешни системи за сигурност	Непозволен достъп в системата от страна на персонала
		Компютърна измама от външни лица
		Манипулиране на вътрешните системи от страна на персонала
		Компютърна измама от страна на персонала
		Непозволен достъп в системата от външни лица
		Манипулиране на системите от външни лица
		Злонамерени хакерски атаки
		Грешки на софтуерни продукти и приложения
		Намалена функционалност и производителност
Криминални действия на външни лица	Кражби и измами на външни лица	Фалшифициране и подправяне на документи от външни лица
		Неоповестяване на задължителна информация от страна на клиента
		Кражба от външни лица

		Изнудване от външни лица
		Отвличане и искане за откуп – от външни лица
		Подкуп – от външни лица
		Палеж – от външни лица
		Заплахи
		Терористични действия
		Вандализъм
		Индустриален шпионаж от външни лица
		Други криминални действия на външни лица
Отношения с персонала и работна среда	Отношения с персонала	Стачни действия от страна на служителите
		Неправомерно прекратяване на трудов договор
		Конфликти между служители
		Неправомерни действия срещу служители
	Безопасност на трудовата среда	Безопасност на работната среда
	Различия и дискриминация	Сексуален тормоз
		Дискриминация
Клиенти, продукти, услуги и търговска практика	Подходящи услуги, разкриване на информация и доверително управление	Конфликт с клиенти
		Неправомерни действия срещу клиенти
		Подвеждащи търговски практики и прикриване на съществена информация
		Регулаторни отношения
		Нарушение на установени правила
		Неправилно тълкуване на информация
		Нарушение на инвестиционна стратегия
		Неправилна преценка на рисковия профил на клиента и неуместна инвестиционна стратегия
		Други
	Неподходящи бизнес и пазарни практики	Злоупотреба с вътрешна информация
		Извършване на транзакции с инструменти, с които клиентът няма право да търгува
		Пазарна манипулация
		Пране на пари
		Антитръст
		Други
	Грешки на продукти/услуги	Неразкриване на съществена информация

		Неуместен продукт
		Погрешен модел
		Грешка при преоценка на клиентски активи
		Неправилна отчетност и съхранение на активи
	Подбор и експозиция към клиенти	Пропуски в интерпретирането на информация за клиента
		Нарушение на лимит към клиент
	Консултантски услуги	Конфликт при предоставяне на консултация
Нарушения на дейността	Природни бедствия и други сътресения	Земетресение
		Наводнение
		Свличане
		Светкавица
		Буря
		Торнадо
		Други природни бедствия
		Стълкновения
		Експлозия
		Пожар
		Терористични актове
Срив на системите	Системи	Системна инфраструктура
		Мрежи
		Морално остарели системи
		Срив на хардуерните системи
		Грешки в софтуерните системи
		Развитие на системите
		Износен хардуер
		Нарушения във връзките
		Проблеми в инфраструктурата

Приложение № 2 към чл. 34, ал. 4

Дневник на настъпили инциденти

Описание на събитието:			
Местоположение:			
Дата	Час	Лице регистрирано инцидента	Отговорно лице/Изпълнени задачи

Приложение №3 към чл. 34, ал. 3, т. 2

Имена на лицата, запознати с процедурите за действие в плана за действие при възникване на кризисни ситуации.

- Име, с ЕГН , на длъжност