Насоки за дејствија по оценка и управување на ризикот

1. Органите се должни да спроведат проценка и оценка на ризиците по однос на безбедноста на информацискиот систем. Ваквата проценка треба да има стандардизиран и структуриран пристап во управувањето со ризиците.

2. Ризик претставува веројатност ранливоста/слабоста на информацискиот систем да биде искористена на начин што ќе доведе до спречување на нормалното функционирање на информацискиот систем.

3. Процесот за управување со ризиците треба да започне во раната фаза на планирање на било кој процес или проект.

4. Процесот за управување со ризиците треба да опфаќа оценка на нивната големина, избор и спроведување на ефективни и економски мерки за нивно намалување и оценка дали преостанатите (резидуалните) ризици се во прифатливи граници.

5. Управувањето со ризикот треба да се извршува преку постојана примена на два типа циклични повторувачки дејствија:
   а) оценка (преоценка) на ризикот;
   б) избор на ефективни и економски мерки за неговата неутрализација.

6. Идентификуваните ризици можат да се:
   а) ликвидираат;
   б) намалат;
   в) прифатат;
   г) пренесат.

7. Процесот за управување со ризиците треба да ги вклучи следниве фази:
   а) избор на објектите кои ќе бидат предмет на анализа;
   б) избор на методологија за оценка на ризикот;
   в) идентификација на информациските средства;
   г) откривање на слабостите/ранливоста на информацискиот систем / средства;
   д) анализа на заканите и можните последици од нив;
   ѓ) оценка на ризиците;
   е) избор на заштитни мерки;
   ж) реализација и проверка на ефикасноста и ефективноста на избраните мерки;
   з) оценка на преостанатиот (резидуалниот) ризик.

8. Заканите од безбедносните ризици по информацискиот систем се класифицираат согласно следниве критериуми:

а) елементите на сигурноста на информацискиот систем (достапност, интегритет и доверливост) кон кои се насочени;
б) елементите на информацискиот систем (хардвер, софтвер, податоци, инфраструктура) кон кои се насочени;
в) начинот на вршење (случајни/намерни, природен/технолошки карактер и др.);
г) изворот (внатре во/надвор од информацискиот систем).

9. Процесот за управување со ризиците треба да биде цикличен процес и да се спроведува:
а) кога преостанатиот (резидуалниот) ризик не се движи во прифатливите граници определени од страна на раководството на органот;
б) по истекот на определен рок, согласно со внатрешните интерни акти на органот.