# ПРИЛОГ 2

# САДРЖАЈ ПРОЦЕНЕ РИЗИКА ОД СТРАНЕ ДОБАВЉАЧА 5G ОПРЕМЕ

Основни елементи процене ризика од стране добављача 5G опреме обухватају:

# Идентификација и процена ризика и рањивости који укључују:

* + процену технолошких ризика који су повезани са новим и напредним технологијама, као што су нови протоколи, архитектуре и стандарди који се користе у 5G мрежама. Ово укључује и процену потенцијалних рањивости у дизајну, кодирању и интеграцији опреме.
  + процену безбедносних ризика који обухватају анализу потенцијалних утицаја на безбедност, као што су рањивости у опреми, напади на мрежну инфраструктуру и могући утицај злоупотребе података, постојање претходних инцидената добављача у области информационе безбедности у Републици Србији.
  + процену оперативних ризика који се могу јавити током инсталације, конфигурације, тестирања и одржавања 5G опреме.
  + процену ризика у вези са снабдевањем и ланцем снабдевања који се односе на кашњења у снабдевању, неиспуњавање стандарда или други проблеми са добављачима.

Добављачи 5G опреме могу да идентификују и друге ризике и рањивости.

Квантификација ризика помоћу матрице ризика омогућава систематски приступ у процени ризика и рањивости, чиме се добија јаснија слика о тежини и вероватноћи одређених ризика.

Матрица ризика треба да комбинује два параметра:

1. Вероватноћа појаве ризика (висока, средња, ниска).
2. Утицај ризика (високи, средњи, ниски).

Поред наведеног добављачи могу користити и стандардизоване методологије као што су NIST SP 800-30 и/или ISO/IEC 27005 за идентификовање и процену ризика и рањивости и предлог одговарајућих мера за њихово елиминисање или ублажавање.

# Техничка процена безбедности опреме и софтвера добављача:

Подразумева процену техничких аспеката безбедности опреме и софтвера добављача, узимајући у обзир потенцијалне рањивости у дизајну, кодирању, интеграцији и управљању опремом кроз:

* + процену да ли опрема користи сигурне методологије у дизајну, као што су примена принципа "Security by Design" или "Privacy by Design", као и техничке контроле за спречавање неовлашћеног приступа;
  + процену безбедности софтвера са фокусом на познате рањивости и примена најбољих пракси за безбедно кодирање;
  + примену процедура тестирања безбедности и укључивање независних тела за проверу интегритета система;
  + примену процедура за јачање интегритета софтвера, ажурирање и управљање ажурирањем софтвера током животног века компоненте;
  + оцењивање способности опреме да ради у сложеним мрежним окружењима без угрожавања других делова мреже;
  + процену доступности транспарентних и сигурних функција за управљање и надзор, укључујући спречавање неовлашћеног приступа.

# Предложене мере за елиминисање или ублажавање идентификованих ризика и рањивости:

* + анализа усклађености са стандардима која осигурава да опрема буде у складу са релевантним стандардима;
  + процена утицаја на инфраструктуру која омогућава процену како нова опрема може утицати на постојеће мреже и инфраструктуру, што је кључно за идентификацију и минимизирање ризика који се односе на интеграцију нових технологија и одржавање стабилности и сигурности постојећих мрежа;
  + стратегија за осигурање квалитета и планови за тестирање и верификацију како би се омогућило откривање потенцијалних проблема у раним фазама и смањиле могућности дефеката и грешака у опреми;
  + стратегије за праћење и идентификовање нових ризика које подразумевају стратешко опредељење за праћење током читавог животног века опреме;
  + сарадња са операторима 5G мреже у спровођењу пенетрацијских тестова и/или спровођење пенетрацијских тестова у тестном окружењу и транспарентна подела информација са операторима о рањивостима које су откривене у пенетрацијским тестовима спроведеним у другим државама;
  + стратегије за минимизацију ризика у ланцу снабдевања која обухвата управљање ризицима који се јављају у ланцу снабдевања, као што су кашњења, неиспуњавање стандарда или поремећаји у снабдевању.

Добављачи могу да предложе и друге мере за елиминисање или ублажавање идентификованих ризика и рањивости.

За све предложене мере добављачи 5G опреме достављају и план за спровођење.

Сви подаци и анализе који се користе у процени ризика морају бити образложени и документовани.