

Informace o hodnocení rizik, kontrolních a bezpečnostních opatřeních a o informačních a komunikačních systémech

Těmito informacemi jsou alespoň:

- a) podrobné hodnocení rizik souvisejících s platebními službami, které žadatel poskytuje nebo hodlá poskytovat, včetně hodnocení rizika podvodného jednání, zahrnující bezpečnostní a kontrolní opatření a postupy ke zmírnění identifikovaných rizik a k ochraně držitelů elektronických peněz nebo uživatelů platebních služeb před těmito riziky,
- b) popis informačních a komunikačních systémů (dále jen „IKT systémy“), který zahrnuje
 1. popis architektury IKT systémů a jejich síťových prvků,
 2. popis IKT systémů sloužících k podpoře podnikatelské činnosti,
 3. popis podpůrných IKT systémů používaných pro organizaci a správu,
 4. informaci, zda žadatel, nebo skupina, jejíž je součástí, tyto systémy již používá, případně předpokládaný termín jejich zavedení do používání,
- c) informace o druzích oprávněných připojení ze strany smluvních partnerů, osob ze skupiny, jejíž je žadatel součástí, pracovníků s dálkovým výkonem práce a dalších osob, včetně odůvodnění těchto připojení,
- d) u každého druhu připojení podle písmene c) popis zavedených logických bezpečnostních opatření a upřesnění kontrol prováděných v této oblasti žadatelem,
- e) popis opatření týkajících se logické bezpečnosti a mechanismů, jimiž se řídí vnitřní přístup do IKT systémů, a která zahrnují opatření technické a organizační povahy, četnost každého opatření, zda je vykonáváno v reálném čase a jak je řešena otázka oddělení prostředí držitelů elektronických peněz nebo uživatelů platebních služeb v případech sdílení IKT systémů,
- f) popis opatření týkajících se fyzické bezpečnosti a mechanismů obchodních prostor a datového centra žadatele, jako jsou kontroly přístupu a zabezpečení prostor,
- g) popis zabezpečení platebních procesů zahrnujících procedury ověřování držitelů elektronických peněz nebo uživatelů platebních služeb a všech souvisejících platebních nástrojů používaných pro náhled a transakční přístup,
- h) popis, jak je zajištěno bezpečné doručování informací oprávněnému držiteli elektronických peněz nebo uživateli platebních služeb a integrity ověřovacích faktorů v okamžiku prvního i dalších přihlášení,
- i) popis postupů, které žadatel uplatňuje za účelem analyzování transakcí a odhalování podezřelých nebo neobvyklých transakcí,
- j) podrobné hodnocení prokazující, že systém řízení rizik je ucelený, rizika byla řádně identifikována a vyhodnocena a bezpečnostní a kontrolní opatření a postupy ke zmírnění rizik, zahrnuté v hodnocení rizik podle písmene a), identifikovaná rizika náležitě řeší a
- k) seznam hlavních písemných postupů týkajících se IKT systémů žadatele.