Wymagania dotyczące audytu bezpieczeństwa

1. Audyt bezpieczeństwa może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5) Certified Information Security Manager (CISM);
6) Certified in Risk and Information Systems Control (CRISC);
7) Certified in the Governance of Enterprise IT (CGEIT);
8) Certified Information Systems Security Professional (CISSP);
9) Systems Security Certified Practitioner (SSCP);
10) Certified Reliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

3. Celem audytu jest wykazanie przez Świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności zgodnie z niniejszym zarządzeniem oraz w obszarach wskazanych w poniższej tabeli w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u Świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Świadczeniodawców.

Nazwa obszaru	**Opis działań skutkujących podniesieniem poziomu bezpieczeństwa teleinformatycznego u Świadczeniodawców.**
Skuteczność działania infrastruktury	-Urządzenia i konfiguracja w zakresie systemów serwerowych. -Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa.
Procesy zarządzania bezpieczeństwem informacji.	-Nośniki wymienne - udokumentowany sposób postępowania.

Zarządzanie ciągłością działania.	-Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa. -Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa. -Procedury wykonywania i przechowywania kopii zapasowych. -Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP). -Procedury utrzymaniowe.
Weryfikacja podniesienia poziomu bezpieczeństwa.	Przeprowadzony audyt wykazał podniesienie poziomu bezpieczeństwa teleinformatycznego w stosunku do stanu sprzed przystąpienia do działań mających na celu podniesienie poziomu bezpieczeństwa teleinformatycznego finansowanych w ramach zarządzenia.