Informacija o predlogu Akcionog plana za sprovođenje informacione bezbjednosti prema standardu ISO 27002 na nivou IPA okvira za period 2025-2027

Vlada Crne Gore je na sjednici održanoj 19. marta 2020. godine usvojila Predlog Akcionog plana ISO 27002 u vezi sa politikom bezbjednosti informacija. Zaključkom br. 07-2071 od 26. marta 2020. godine, Vlada Crne Gore je zadužila Ministarstvo javne uprave da formira Operativni tim i Odbor za praćenje realizacije Akcionog plana o upravljanju politikom informacione bezbjednosti na osnovu standarda ISO 27002 2020-2022, za institucije uključene u upravljanju fondovima pretpristupne pomoći (IPA).

U avgustu 2022. godine, Crna Gora je doživjela veliki sajber napad. Kao rezultat navedenog, svi organi u javnoj upravi i IPA strukturama bili su suočeni sa velikim problemima kao što su, između ostalog, gubitak pristupa svojim elektronskim podacima i mejlovima tokom perioda od tri mjeseca, ograničen ili onemogućen pristup dokumentima koji se čuvaju u elektronskoj verziji itd. U cilju podrške IPA strukturama, Delegacija Evropske unije u Crnoj Gori obezbijedila je e-mail adresu koja se koristila za aktivnosti javnih nabavki koje su bile u toku. Takođe, kako bi se pratilo stanje svih fajlova u fazi *ex-ante* odobrenja, stopa odobrenja/odbijanja i njihovi razlozi, DEU je predložila organima u IPA strukturama da koriste sigurnu aplikaciju pod nazivom IPA APP. Ova aplikacija evidentira gore navedene podatke i dostupna je i zemlji korisnici i Evropskoj komisiji.

S tim u vezi, a u skladu sa zahtjevima Evropske komisije, te izdatih nalaza i preporuka koji se odnose na ovo pitanje, a kako se u prethodnom periodu funkcionisanje Upravnog odbora za praćenje imlementacije i Operativnog tima pokazalo nefunkcionalnim, bilo je potrebno ažurirati i usvojiti inovirani Akcioni plan ISO 27002 u vezi sa politikom IT bezbjednosti. Definisan je drugačiji pristup kako bi se osiguralo praćenje sprovođenja Akcionog plana za IT ISO 27002 za sve institucije koje su uključene u implementaciju IPA III perspektive. Nacionalnim strukturama se, takođe, od strane Evropske komisije, preporučuje da nastave sa korišćenjem IPA aplikacije kako bi se pratila *ex-ante* odobrenja/odbijanja u okviru IPA II perspektive.

U vezi sa navedenim, ekspertska podrška je obezbijeđena kroz projekat tehničke podrške Direktoratu za upravljanje strukturama pretpristupne podrške EU (Upravljačka struktura u Ministarstvu finansija) u dijelu savjetovanja i pružanja pomoći koje za cilj ima rješavanje pitanja politike bezbjednosti informacija za institucije uključene u upravljanju sredstvima EU kroz Instrument pretpristupne pomoći – IPA. Imajući u vidu da je ovaj projekat finansiran od Evropske unije, definisano je da za 9 mjeseci trajanja projekta budu razvijene politike koje proizilaze iz usvojenog Akcionog plana. Za donošenje nacrta politika informacione bezbjednosti u IPA okviru, o temama orijentisanim na krajnjeg korisnika, neophodno je bilo spovesti određeni niz obuka što je i pruženo od strane eksperta angažovanog u sklopu projekta tehničke podrške Upravljačkoj strukturi. Pored toga, nacionalne vlasti i revizori Evropske komisije zajedničkog su stava, u odnosu na važeći Akcioni plan ISO 27002 koji je zastario da je na osnovu odrađenih analiza isti bilo neophodno revidirati. Revidirana verzija Akcionog plana pripremljena je u saradnji sa Ministarstvom javne uprave.

Donošenje Predloga akcionog plana se takođe, u vezi sa prethodno navedenim, kao jedna od aktivnosti, uvrstilo u Predlog rada Vlade za 2024. godinu, a kao period donošenja naznačen je III kvartal 2024. godine. Imajući u vidu da je ova aktivnost predviđena za III kvartal, Direktorat za upravljanje strukturama pretpristupne podrške EU je, tokom prve polovine 2024. godine, u saradnji sa pomenutim ekspertom, pripremio Predlog akcionog plana za sprovođenje informacione bezbjednosti prema standardu ISO 27002 na nivou IPA okvira, koji je dostavio relevantnim IPA tijelima na komentare.

Isti je dostavljen i Ministarstvu javne uprave koje je, shodno preporukama, bilo zaduženo za izdavanje komentara na Predlog akcionog plana u dijelu izrade politika, koje proizilaze iz razvijenog Predloga akcionog plana dostavljenog nadležnim službama Ministarstva javne uprave, čime bi bili definisani odgovori na pitanje koje usluge, koje pruža navedeno ministarstvo, mogu biti planirane da budu isporučene IPA institucijama. U vezi sa navedenim, Ministarstvo javne uprave/Direkcija za upravljanje projektima, analitiku i standardizaciju - Odsjek za standardizaciju informacionih sistema uprave je 25. oktobra 2024. godine, elektronskim putem, obavijestilo Direktorat za upravljanje strukturama pretpristupne podrške EU u Ministarstvu finansija da je saglasno sa Predlogom Akcionog plana koji je pripremljen uz podršku eksperta u ovoj oblasti, koji je održao niz sesija i obuka sa službenicima IPA strukture.

Struktura Predloga akcionog plana ISO 27002 na nivou IPA okvira sastoji se od definisanih oblasti, te 16 osnova, za jasno naznačenim ciljevima, mjerama, aktivnostima, odgovornostima i zaduženjima, rokovima za implementaciju mjera, neophodnim sredstvima i indikatorima.

Usvajanjem Akcionog plana ISO 27002 za IPA okvir, od strane Vlade Crne Gore, obezbjeđuju se konkretne mjere informacione bezbjednosti za postizanje najvišeg nivoa informacione bezbjednosti mrežnih i informacionih sistema IPA struktura, uključujući sajber bezbjednost, podizanje svijesti službenika na IPA poslovima o važnosti stanja povjerljivosti, cjelovitosti, dostupnosti i zaštite podatka, te ispunjava početni zahtjev Evropske komisije u odnosu na date preporuke u ovoj oblasti, kada je u pitanju upravljanje sredstvima Evropske unije kroz Instrument pretptristupne podrške (IPA).

Napomena: Kako su i sami standardi u oblasti informacione bezbjednosti pored engleskog usvojeni i prevedeni i na crnogorski jezik radi njihove važnosti i izražene potrebe za korišćenjem, tako se i ovaj Predlog akcionog plana o upravljanju politikom informacione bezbjednosti na osnovu standarda ISO 27002 na nivou IPA okvira za period 2025-2027 usvaja na dva jezika.

AKCIONI PLAN

ZA SPROVOĐENJE INFORMACIONE BEZBJEDNOSTI PREMA STANDARDU ISO 27002 NA NIVOU IPA OKVIRA

ZA PERIOD 2025-2027

Podgorica, decembar 2024.

OBLAST: USPOSTAVLJANJE OKVIRA ZA MONITORING I IMPLEMENTACIJU ISMS-a I AKCIONOG PLANA							
Implementacija i širenje Sistema za upravljanje bezbijednošću informacija (ISMS) uključuje uspostavljanje, upravljanje i kontinuirano poboljšanje okvira za bezbjednost informacija organizacije zasnovanog na standardu ISO/IEC 27002. ISMS je dizajniran da zaštiti povjerljivost, integritet i dostupnost informacija primjenom procesa upravljanja rizikom. Implementacija i širenje ISMS-a je strateški projekat koji zahtijeva posvećenost u cijeloj organizaciji, od najvišeg menadžmenta do svakog zaposlenog. Ovaj akcioni plan navodi ključne korake za uspostavljanje robusnog ISMS-a, sa ciljem da efektivno zaštiti informaciona sredstva uz obezbjeđivanje usklađenosti sa međunarodnim standardima i propisima. Instance za koje je ovaj Akcioni plan primjenljiv čine veoma složen ekosistem zbog njihove međuzavisnosti u realizaciji IPA projekata, različitih nivoa složenosti i različitog nivoa ovlašćenja koje imaju nad svojim odgovornostima za bezbjednost informacija. Ovo je razlog što ova oblast obuhvata sve procese koje treba da usmjerava, prati i ocjenjuje Direktorat za upravljačku strukturu. Kontrole iz standarda koji se primjenjuje na ovu oblast su 5, najviše rukovodstvo, posvećenost i politika, kao i 7, uloge i odgovornosti, kompetencije, komunikacija, svijest i dokumentovane informacije.							
Br.	**CILJEVI**	**MJERE**	**AKTIVNOSTI**	**ODGOVORNOSTI**	**ROKOVI**	**SREDSTVA I IZVOR FINANSIRANJA** **NOSILAC AKTIVNOSTI**	**INDIKATORI**
1.	**Formiranje projektnih timova i Upravnog odbora za praćenje implementacije Akcionog plana bezbjednosne politike u IPA institucijama na osnovu ISO standarda 27002**	Predstavnici ISMS-a i članovi projektnog tima treba da budu imenovani u svakom IPA tijelu/instituciji.	IPA tijela/institucije imenuju predstavnika ISMS-a i članove projektnog tima. Upravni odbor čine rukovodioci IPA tijela/institucija i Direktorata za upravljačku strukturu.	Predstavnici ISMS-a Projektni timovi IPA tijela Rukovodstvo IPA tijela	I kvartal 2025.	/	Odluka o imenovivanju predstavnika ISMS-a i Upravnog odbora
		Ključne ciljeve i odgovornosti ISMS predstavnika i članova projektnog tima treba definisati.	IPA tijela/institucije u komunikaciji sa kancelarijom NAO definišu ključne ciljeve i odgovornosti u okviru Odluke.				Ključni ciljevi i odgovornosti predstavnika ISMS-a, projektnog tima i Upravnog odbora definisani Odlukom
		Odgovarajuće rokove predviđene za sprovođenje mjera iz Akcionog plana bi trebalo definisati.	Upravni odbor na prvoj sjednici utvrđuje i usvaja predlog rokova predviđenih za sprovođenje mjera iz Akcionog plana.				Usvojen i potvrđen Predlog rokova za sprovođenje mjera iz Akcionog plana
2.	**Dostavljanje informacija o usvojenoj odluci Evropskoj komisiji**	Službenu bilješku treba dostaviti EK.	Priprema informacije i dostavljanje zvanične odluke iz Akcionog plana.	NAO	I kvartal 2025.	/	Informacija zvanično dostavljena EK
3.	**Uspostavljanje linije izvještavanja o realizaciji Akcionong plana**	Komunikaciju i izvještavanje o implementaciji Akcionog plana treba uspostaviti.	Rukovodioci IPA tijela definišu linije izvještavanja Upravnom odboru u okviru procesa. Revizija menadžmenta (definisana u 4.2 u ovom akcionom planu) jednom godišnje rezultat je ovog procesa.	Upravni odbor Predstavnici ISMS-a šef IPA tijela/institucija	I kvartal 2025.	/	Linije izvještavanja definisane zaključcima
4.	**Upoznavanje zvaničnika Upravnog odbora sa politikom IS**	Predložena politika bezbjednosti informacija treba da bude predstavljena Upravnom odboru	Upravni odbor utvrđuje usklađenost politike i potrebu za daljom operacionalizacijom.	Upravni odbor Predstavnik ISMS-a	II kvartal 2025.	/	Upravni odbor odobrava politiku

5.	**Podizanje svijesti o značaju politike IS među učesnicima i drugim institucijama u procesu upravljanja i korišćenja sredstava iz IPA programa**	Predstavnike ISMS-a treba uvesti u institucije. Obuka o implementaciji neophodna je za predstavnike ISMS-a.	Neophodna mjera je sprovođenje obuke za predstavnike ISMS-a koji sprovode ISO 27002. Obuka se organizuje za sve predstavnike u dinamici koja odgovara broju i strukturi.	Predstavnik ISMS-a Izvođač	II kvartal 2025.	Budžet za obuku 5.000,00 € DUSPPEU	Kreiran plan obuke. Definisan program obuke. Zapisnici sa obuka.
6.	**Podizanje svijesti o značaju politike IS među učesnicima i drugim institucijama u procesu upravljanja i korišćenja sredstava iz IPA programa**	Nadogradnja ICT procedura koje koriste sva IPA tijela u odnosu na novousvojenu politiku o ISO 27002 i ponovno imenovanje ISMS predstavnika u relevantnim institucijama.	Na osnovu mjera iz Akcionog plana i ISO 27002 treba pripremiti i usvojiti novu verziju odgovarajućeg poglavlja Priručnika o procedurama. Predstavnike ISMS-a treba ponovo imenovati,, ako je potrebno, u okviru svih IPA institucija.	NAO	III kvartal 2025 – III kvartal 2026.	/	Usvojena nova verzija Priručnika procedura Predstavnik za ISMS ponovo imenovan
7.	**Operativne procedure**	Uspostavljene operativne procedure za procese rada	Odgovorni organ treba da dokumentuje procedure za operativne, sistemske i tehničke aktivnosti.	Predstavnici ISMS-a Rukovodstvo odjeljenja odgovornih za IPA tijela Rukovodstvo IPA tijela	IV kvartal 2025 – IV kvartal 2026.	Budžet za implementaciju ISMS-a je 10.000,00 € za sve aktivnosti; Izvori iz projekata i konsultantskih usluga DUSPPEU	Operativne procedure su dokumentovane i dostavljene svim raspoloživim korisnicima – IPA osoblju

OBLAST: OSNOVA 1 – USPOSTAVLJANJE KONTEKSTA, UPRAVLJANJE RIZICIMA I CILJEVI

Kreiranje akcionog plana za „Uspostavljanje konteksta, upravljanje rizicima i ciljevi "uključuje strukturirani pristup razumijevanju okruženja u kojem IPA tijela rade, identifikovanje i upravljanje rizicima kao i postavljanje jasnih ciljeva. Nacrt opsega je predložen kao „Usluge i informacije u vezi sa IPA fondovima "i treba ga dalje izvoditi za svako IPA tijelo.
Razvoj akcionog plana za upravljanje rizicima u kontekstu informacione bezbjednosti je od suštinskog značaja za efektivnu zaštitu informacionih sredstava organizacije. Ovaj plan opisuje sistematski pristup identifikovanju, procjeni, tretiranju i praćenju rizika sigurnosti informacija, obezbjeđujući povjerljivost, integritet i dostupnost informacija. Za mala IPA tijela Metodologija rizika mogla bi da bude jednostavan registar rizika sa dvije osnovne komponente odnosno vjerovatnoće i uticaja, koji bi bio usklađen sa opštom metodologijom rizika, dok bi za IPA agenciju trebalo da sadrži dodatne komponente kao što su prijetnje, slabosti, kontrolu, imovinu. Kontrole iz standarda obuhvaćene u ovoj oblasti su 4, 6, 8.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROKOVI	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
1.1	**Definisati kontekst, obuhvat i ciljeve ISMS sistema**	Kontekst, obuhvat i ciljevi IPA tijela treba da su dokumentovani.	Pripremiti nacrt dokumenta o kontekstu, obuhvatu i ciljevima. Saopštiti i prilagoditi nacrt dokumenta na osnovu određenog	Predstavnici ISMS-a Projektni timovi IPA tijela Rukovodioci IPA tijela	I kvartal 2025.	/	Nacrt dokumenta je pripremljen i prilagođen. Kontekst, obuhvat i ciljevi su odobreni.

			IPA tijela. Odobren kontekst, obuhvat i ciljevi.				
1.2	**Uspostavljanje metodologije za analizu, evaluaciju, praćenje i izvještavanje o rizicima**	Metodologiju za upravljanje rizicima IS-a treba razviti. Priručnik o procedurama za IPA tijela, u vezi sa politikom upravljanja rizicima, treba ažurirati.	Kreiranje usklađene metodologije za upravljanje rizicima koja obuhvata analizu, evaluaciju, praćenje, izvještavanje i tretman rizika za mala IPA tijela i agenciju za platni promet.	Izvođač Predstavnici ISMS-a Odbor za rizike Koordinatori rizika NAO	II kvartal 2025.	Budžet za implementaciju ISMS-a 5.000,00 €, iz projekata i konsultantskih usluga DUSPPEU	Metodologija upravljanja rizicima je razvijena. Priručnik o Procedurama je ažuriran.
1.3	**Uspostavljanje komunikacije između predstavnika ISMS-a, koordinatora rizika za IPA aktivnosti i predstavnika Panela za rizike**	Metodologiju i modalitet upravljanja rizicima IS treba dostaviti koordinatoru za rizike u IPA aktivnostima i predstaviti ih na posebnom sastanku Panela za rizike.	Model utvrđivanja, upravljanja i izvještavanja o rizicima u skladu sa preporukama ISO 27002 predstavljen je Koordinatoru rizika za IPA aktivnosti i Panelu za rizike	Predstavnici ISMS-a Koordinatori rizika Panel za rizike NAO	III kvartal 2025.	/	Smjernice za upravljanje rizicima prema preporukama ISO 27002 prepoznate su i uključene u opšti monitoring koordinatora rizika za IPA aktivnosti. IPA panel rizika za upravljanje rizicima, koji se održava na osnovu rizika identifikovanih implementacijom ISO27002. Informacije o ključnim rizicima dostavljene MJU i ministarstvima.
1.4	**Analiza rizika IS i priprema i usvajanje Plana tretmana rizika**	Identifikacija relevantnih rizika u okviru IPA struktura na osnovu zahtjeva ISO 27002 i definisana metodologija su neophodne.	Registar rizika visokog nivoa treba pripremiti na nivou svih IPA tijela na osnovu zahtjeva ISO 27002.	Predstavnici ISMS-a Koordinatori ICT-a Rukovodioci odjeljenja IPA tijela Rukovodioci IPA tijela Vlasnici rizika Izvođač NAO	III kvartal 2025.	Budžet za implementaciju ISMS-a 5.000,00 € iz projekata i konsultantskih usluga	Registar rizika pripremljen na nivou svih IPA tijela na osnovu metodologije upravljanja rizicima. Registar rizika predstavljen i ispraćen na sastancima Koordinacionog tijela. NAO je obavijestio o svim otkrivenim rizicima i o pripremljenim mjerama za njihovo pravilno praćenje.

		Izvršiti Procjenu rizika	Sva IPA tijela treba odvojeno da urade Procjenu rizika na osnovu zahtjeva ISO 27002				Procjena rizika izvršena i dostavljena kancelariji NAO na dalju razradu
		Procjena rizika i kriterijumi prihvatanja treba da se prilagode prema profilu rizika određenog IPA tijela. Plan tretmana rizika treba razraditi i pripremiti za svako IPA tijelo.	Procjenu rizika i kriterijume prihvatanja rizika treba primijeniti tokom analize. Treba odlučiti o opcijama tretmana rizika. Kontrole za tretmane rizika treba razviti za određenu IPA instituciju			DUSPPEU	Svi identifikovani rizici se procjenjuju Opcije tretmana rizika su odlučene Plan tretmana rizika razvijen Vlasnici rizika za pravilno ublažavanje rizika prepoznati Rezidualni rizik prihvata svako IPA tijelo Registar rizika ažuriran o trenutnom napretku
1.5	**Sprovođenje kontrola na osnovu Plana tretmana rizika**	Sve predložene akcije plana tretmana rizika treba blagovremeno da sprovedu definisani organi	Sprovode plan tretmana rizika sve IPA institucije	Predstavnici ISMS-a Koordinatori ICT-a Šefovi odjeljenja IPA tijela	Kontinuirano do IV kvartala 2026.	Budžet je raspoređen na određene kontrole u okviru Akcionog plana	IPA tijela kontinuirano sprovode aktivnosti na smanjenju rizika
1.6	**Uspostavljeno praćenje rizika i dalje praćenje**	NAO treba da obezbijedi da svi neprihvatljivi rizici budu efektivno ublaženi ili ako nisu, da se korektivne mjere sprovedu na vrijeme Proces procjene rizika dokumentuje se zajedno sa rezultatima sprovođenja plana tretmana rizika Rizici se procjenjuju na kontinuiranoj osnovi	NAO bi trebao da pažljivo prati sprovođenje kontrola za neprihvatljive rizike. Korektivne mjere treba sprovesti na vrijeme	Predstavnici ISMS-a Odbor za rizike NAO	Kontinuirano do IV kvartala 2026.	/	Praćenje plana tretmana rizika kontinuirano se predstavlja kancelariji NAO i na Panelu za rizike Korektivne mjere su identifikovane s ciljem poboljšanja sprovođenja plana tretmana rizika

OBLAST: OSNOVA 2 – POLITIKA BEZBJEDNOSTI INFORMACIJAMA

Politika postavlja osnovu za snažan program informacione bezbjednosti, naglašavajući principe i odgovornosti koje regulišu zaštitu informacionih sredstava. Za većinu IPA tijela politika bi trebalo da obuhvati kontrole koje se odnose na zaposlene, informacije kojima barataju i organizacione aspekte njihovih procesa. IPARD Agencija za plaćanja je poseban slučaj gdje politiku treba široko razvijati, kako bi pokrila druge aspekte njihovog djelovanja. Kontrole iz standarda obuhvaćenih u ovoj oblasti su 5.2, A5.1.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROKOVI	SREDSTVA I IZVOR FINANSIRANJA	INDIKATORI

						NOSILAC AKTIVNOSTI	
2.1	**Razvoj i sprovođenje politike informacione bezbjednosti – Uspostavljanje seta politika za bezbjednost informacija**	Razviti politiku informacione bezbjednosti koja se bavi svim kritičnim oblastima informacione bezbjednosti.	Nadležni organ treba da definiše skup politika bezbjednosti informacija, koje sadrže smjernice za uspostavljanje minimuma zahtjeva za bezbjedno pružanje IPA usluga	Predstavnici ISMS-a Koordinatori ICT-a Projektni timovi IPA tijela Rukovodioci IPA tijela Rukovodioci odjeljenja IPA tijela Konsultant	I kvartal 2025.	/	Razvijen nacrt politike
		Politiku bezbjednosti podataka treba da odobri nacionalno IPA tijelo, pa da se objavi i saopšti zaposlenima i relevantnim stranama.	Bezbjednost podataka se objavljuje i saopštava zaposlenima i relevantnim licima.	Predstavnici ISMS-a Koordinatori ICT-a Projektni timovi IPA tijela Rukovodioci IPA tijela Rukovodioci odjeljenja IPA tijela Zaposleni u IPA tijelima	II kvartal 2025.		Usvojen set politika za informacionu bezbjednost na adekvatnom nivou.
		Dokumentovani kontekst nacionalne IPA bezbjednosti informacija treba definisati i uspostaviti i dodatno održavati	Nadležni organ treba da sprovede set politika bezbjednosti podataka, da ih objavi, odobri i saopšti zaposlenima i relevantnim eksternim licima u obliku koji je relevantan, dostupan i razumljiv čitaocu kome je namijenjen.		II kvartal 2025.		Politike bezbjednosti informacija sprovode, objavljuju i koriste nacionalno IPA strukture i druge institucije.
		Obuku za politike informacione bezbjednosti treba sprovesti	Obučiti odgovorne zaposlene u IPA tijelima za politiku informacione bezbjednosti.	Zaposleni u IPA tijelima Konsultant	II kvartal 2025.		Odgovorni zaposleni su obučeni.
		Politike za informacionu bezbjednost, koje su usvojene, treba da su revidirane.	Tretman i ažuriranje politike bezbjednosti informacija na godišnjem nivou.	Predstavnici ISMS-a Rukovodioci IPA tijela	II kvartal 2025.		Politike bezbjednosti informacija pregledaju i ažuriraju IPA tijela.

OBLAST: OSNOVA 3 – ULOGE I ODGOVORNOSTI BEZBJEDNOSTI INFORMACIJA

Definisanje i saopštavanje uloga i odgovornosti u oblasti bezbjednosti informacija ključno je za uspostavljanje jasne strukture upravljanja, koja podržava strategiju bezbjednosti informacija organizacije. Ovo osigurava da svaki član organizacije razumije svoju ulogu u zaštiti informacionih sredstava. Trenutno, osim u Agenciji za plaćanja u kojoj je imenovan CISO, ne postoji uloga predstavnika za ISMS, koja je ključna za implementaciju politike IS. Kontrole iz standarda obuhvaćenih u ovoj oblasti su 5.3, 7.1, 7.2, A5.2, A5.3, A5.4, A5.5, A5.6.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI

3.1	**Imenovati predstavnika za ISMS**	Potencijalni kandidati treba da budu zaposleni u IPA tijelima kao Menadžeri rizika, zaposleni na obezbjeđenju kvaliteta ili koordinatori za IT.	Na osnovu interne politike u svakom IPA tijelu imenovati ISMS predstavnika.	Predstavnici ISMS-a Rukovodioci IPA tijela	IV kvartal 2024.	/	Predstavnik ISMS-a imenovan za svako IPA tijelo
3.2	**Uspostavljanje upravljačkog okvira za iniciranje i kontrolu implementacije i rada informacione bezbjednosti unutar organizacije i na nivou koordinacije**	Uloge i odgovornosti kod bezbjednosti informacija treba da budu mapirane i pokrivene funkcijama u skladu sa politikom bezbjednosti informacija, a u vezi sa razgraničenjem dužnosti.	Uloge i odgovornosti kod bezbjednosti informacija u institucijama koje priznaju IPA tijela.	Predstavnici ISMS-a Rukovodioci IPA tijela Projektni timovi IPA tijela Vlasnici i čuvari sredstava Vlasnici rizika	I kvartal 2025.	/	Uloge i odgovornosti prepoznaju i razvijaju IPA tijela kroz Pravilnik o unutrašnjoj organizaciji i sistematizaciji resorne institucije.
			Razviti odgovornosti kod bezbjednosti informacija u skladu sa politikama bezbjednosti informacija.				
			Implementirane su kontrole za podjelu dužnosti.				Osigurano adekvatno praćenje implementacije IS
			Primjenjuju se i kontrole za rješavanje aspekata informacione bezbjednosti u upravljanju projektima i kontaktima sa posebnim interesnim grupama ili drugim specijalizovanim bezbjednosnim forumima i profesionalnim udruženjima.				Uspostavljene komunikacione linije sa eksternim zainteresovanim stranama
			Definisane komunikacione linije sa posebnim eksternim zainteresovanim stranama				

OBLAST: OSNOVA 4 – EVALUACIJA I POBOLJŠANJE PERFORMANSI

Procjena učinka i poboljšanje informacione bezbjednosti je od ključnog značaja da se osigura da su bezbjednosne mjere efektivne i da se razvijaju kako bi odgovorile na nove prijetnje i organizacione promjene. Ova oblast bi postala aktuelna nakon uspostavljanja Sistema upravljanja bezbjednošću podataka, a to je najranije do kraja 2024. godine. Postoje tri oblika evaluacije i poboljšanja rada koji bi trebali da se uspostave i održavaju u kontinuitetu, tj. interna revizija, mjerenje i ocjena upravljanja kao i njihova primjena, kako je i opisano u ovom Akcionom planu. Za mala IPA tijela ovo bi trebalo da se sprovodi na nivou ministarstava, ali bi se za aspekte IPA to radilo na nivou DMS-a. Za više detalja pogledajte kontrole 9 i 10 iz standarda.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA	INDIKATORI
4.1	**Uspostaviti funkciju interne revizije**	Odlučite koja strategija će se koristiti, tj.	Odlučite o strategiji i imenujte ovu funkciju izabranim revizorima.	Predstavnici ISMS-a Rukovodioci IPA tijela Interni revizori	II kvartal 2025.	Budžet za obuku 5.000,00 €, € iz projekata i	Imenovana je funkcija revizije. Izrađuje se plan interne revizije.

		- obučite interno osoblje za međusobnu reviziju, - koristite neku državnu funkciju koja bi vršila internu reviziju ili - dogovorite podugovarača kao eksterno osoblje za pružanje ove usluge.				konsultantskih usluga	Izvještaj za internu reviziju je dostavljen.
		Izradite plan za internu reviziju baziran na rizicima.	Izradite plan za obavljanje interne revizije.		II kvartal 2025. i svake naredne godine	DUSPPEU	
		Izvještaj interne revizije treba dostaviti.	Izvršite internu reviziju i dostavite izvještaj.		III kvartal 2025. i svake naredne godine		
4.2	**Izvršiti pregled rada uprave**	Ocjenu uprave treba planirati sa relevantnim inputima kao što su interne revizije, upravljanje ririzicima,...	Ocijenite upravljanje planom sa svim relevantnim inputima.	Predstavnici ISMS-a Rukovodioci IPA tijela Rukovodioci odjeljenja IPA tijela	IV kvartal 2025. i svake naredne godine	/	Plan je razvijen. Odluke o ocjeni rada uprave su dokumentovane.
		Ocjenu rada uprave treba sagledati kroz relevantne rezultate tj. resurse za stalno unaprjeđenje ISMS-a	Izvršite ocjenu rada uprave kroz postignute rezultate		I kvartal 2026. i svake naredne godine		
4.3	**Izvršiti mjerenje**	Indikatori za mjerenje trebaju se razvijati u razdobljima mjerenja	Razvijte indikatore	Predstavnici ISMS-a Šefovi IPA tijela	II kvartal 2025. i svake naredne godine	/	Tabela indikatora je izrađena Indikatori su prijavljeni
		O indikatorima treba periodično izvještavati u odnosu na trendove i pragove	Izvještavajte o rezultatima indikatora		IV kvartal 2025. i svake naredne godine		

OBLAST: OSNOVA 5 – PODIZANJE SVIJESTI, EDUKACIJA I OBUKA O BEZBJEDNOSTI PODATAKA

Kreiranje akcionog plana za podizanje svijesti, edukacija i obuku o bezbjednosti informacija je od suštinskog značaja da bi se svi članovi organizacije opremili znanjem i vještinama potrebnim za zaštitu informacionih sredstava. Ova inicijativa ima za cilj da podstakne kulturu bezbjednosti, smanji vjerovatnoću bezbijednosnih incidenata i obezbijedi da zaposleni mogu da reaguju na prijetnju na odgovarajući način. U prvoj godini program obuke treba da bude više koncentrisan na teme svijesti i komunikacije, a u sljedećoj godini na kompetencije i učenje iz incidenata. Kontrole iz standarda su 7.2, 7.3, 7.4, A5.27, A6.3.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI

5.1	**Podizanje kolektivne svijesti o značaju politike bezbjednosti podataka i bezbijednosnih kontrola, kao i dobre bezbijednosne prakse**	Odrediti učesnike obuka	Odredite učesnike obuka sa prioritetima baziranim na procjeni potreba	Predstavnici ISMS-a Kadrovsko odjeljenje u institucijama Zaposleni u IPA tijelima ICT koordinatori Treneri za obuke	II kvartal 2025. i svake godine	Budžet za obuku 5.000,00 € svake godine, € iz projekata i konsultantskih usluga	Izrađena lista učesnika
		Izraditi program obuka za tekuću godinu	Razvijte program obuke sa odgovarajućim temama				Program obuke razvijen
		Trebalo bi angažovati predavače za obuke, i izraditi materijale za obuke	Razvijte materijal za obuku ili angažujte trenere obuka			DUSPPEU	Razvijeni materijali za obuku ili ugovoreni treneri za obuke
		Obuke treba održati	Organizujte obuke, vodite evidenciju i ocjenjujte rezultate				Dokumentovana lista učesnika i evaluacija obuke

OBLAST: OSNOVA 6 – KONTROLA LJUDI

Primjena kontrole ljudi u informacionoj bezbjednosti uključuje uspostavljanje politika, procedura i praksi koje se fokusiraju na ljudske elemente informacione bezbjednosti. Ove kontrole su dizajnirane da smanje rizik od narušavanja bezbjednosti uzrokovanih ljudskom greškom ili zlonamjernim radnjama. Skup politika i procedura koje treba razviti obuhvataju odnose sa zaposlenima prije, tokom i nakon zapošljavanja, uključujući rad na daljinu i izvještavanje o događajima. Za mala IPA tijela, većina ovih politika treba da se razvije na nivou ministarstava. Za više detalja pogledajte kontrole iz standarda A6.1, A6.2, A6.4, A6.5, A6.6, A6.7, A6.8.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
6.1	**Razviti politike i procedure koje zaposleni kao ljudski faktor treba da poštuju.**	Politike i procedure koje poboljšavaju budnost bezbjednosti podataka treba da se izrade.	Na osnovu analize nedostataka odlučite koje politike i procedure na osnovu životnog ciklusa zaposlenja (uključujući rad na daljinu i izvještavanje o događajima) i izradite nacrtnu verziju.	Predstavnici ISMS-a Rukovodstvo IPA tijela Kadrovsko odjeljenje u institucijama Pravne službe u institucijama Zaposleni u IPA tijelima	II kvartal 2025.	/	Izvršena analiza nedostataka Izrađen nacrt politika i procedura
		Razvijene politike i procedure o životnom ciklusu zapošljavanja trebalo bi odobriti.	Odobrite razvijene politike i procedure i sprovodi ih.		II kvartal 2025.		Politike i procedure su odobrene
		Diseminacija treba da se vrši kroz obuku.	Organizujte obuku i vodite evidenciju da su svi zaposleni u tom obuhvatu razumjeli i prihvatili politike i procedure.		II kvartal 2025.		Održana obuka Vođena evidencija o obuci

OBLAST: OSNOVA 7 – UPRAVLJANJE SREDSTVIMA

Upravljanje imovinom je kritična komponenta bezbjednosti informacija, fokusirajući se na identifikaciju, klasifikaciju i zaštitu sredstava organizacije. Efikasno upravljanje imovinom osigurava da su vrijedne informacije i fizička sredstva na odgovarajući način zaštićeni od prijetnji. Za mala IPA tijela upravljanje sredstvima bi se bavilo podacima vezano za IPA usluge i njihova lična sredstva, dok se sredstva vezana za servere i mrežu evidentiraju na nivou ministarstava. Više detalja o ovim kontrolama može se naći u standardu pod A5.9,A5.10, A5.11, A5.12, A5.13, A8.10, A8.11.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
7.1	**Napraviti inventar sredstava, klasifikaciju i politiku prihvatljivog korišćenja.**	Inventar sredstava treba napraviti	Kreirajte i popunite inventar sredstava sa svim potrebnim atributima.	Predstavnici ISMS-a Koordinatori ICT-a Vlasnici i čuvari sredstava	I kvartal 2025.	/	Inventari sredstava popunjeni
		Sredstava treba klasifikovati	Na osnovu politike klasifikacije, sredstva treba klasifikovati prema povjerljivosti, integritetu i dostupnosti.		I kvartal 2025.		Sredstva su klasifikovana
		Politika prihvatljivog korišćenja treba da se razvije za životni ciklus sredstava.	Razvite politiku prihvatljivog korišćenja i primijenite je na osnovu klasifikacije sredstava.		II kvartal 2025.		Politika prihvatljivog korišćenja je razvijena i odobrena.
		Politika klasifikacije i prihvatljive upotrebe treba da se propagira na obuci	Održite sesije obuke koje bi pokrivale politiku inventara sredstava i klasifikaciju, politiku prihvatljivog korišćenja uključujući vraćanje sredstava, brisanje podataka i maskiranje podataka, ako je primjenljivo.		II kvartal 2025.		Obuka obavljena.

OBLAST: OSNOVA 8 – KONTROLA PRISTUPA

Kontrola pristupa je ključna u zaštiti informacionih sredstava organizacije. Kontrola pristupa osigurava da samo ovlašćeni pojedinci imaju pristup određenim resursima, štiteći na taj način osjetljive informacije od neovlašćenog pristupa, otkrivanja i izmjene. Za mala IPA tijela primjenjiva je kontrola pristupa aplikacijama i strukturama datoteka, dok pristupom servisima imenika i fizičkim perimetrima upravljaju ministarstva. Takođe u domenu nadležnosti ministarstava su privilegovana prava pristupa, sigurna autentifikacija i pristup izvornom kodu. Kontrole povezane sa standardom u ovom domenu su A5.15, A5.16, A5.17, A5.18, A8.2, A8.3, A8.4, A8.5.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
8.1	**Sprovođenje kontrola koje ograničavaju pristup zaposlenima u IPA strukturi i drugim institucijama ka**	Politiku kontrole pristupa treba razviti	Razvijte politiku kontrole pristupa (treba znati, treba imati) na odgovarajućem nivou na osnovu trenutnog vlasništva sredstava.	Predstavnici ISMS-a Koordinatori ICT-a Vlasnici sredstava i administratori	I kvartal 2025.	/	Razvijena politika kontrole pristupa

	određenim podacima i informacionim sredstvima	Politiku kontrole pristupa treba primijeniti	Na osnovu politike razvijte matricu kontrole pristupa, koju administratori treba da koriste da bi je primijenili na sredstva u okviru obuhvata.	Kadrovsko odjeljenje u institucijama Rukovodioci IPA tijela Zaposleni u IPA tijelima	III kvartal 2025.		Implementirana matrica kontrole pristupa
		Obuku vezano za kontrolu pristupa treba održati	Održite obuku koja uključuje politiku kontrole pristupa, odgovornost, prava pristupa, informacije o autentifikaciji…		II kvartal 2025.		Održana obuka
		Politiku kontrole pristupa treba ocijeniti	Najmanje jednom godišnje vlasnici i administratori sredstava treba da pregledaju politiku i saglase se da li su potrebne neke promjene.		I kvartal 2026. i svake godine		Vođenje evidencije o ocjenama

OBLAST: OSNOVA 9 – FIZIČKA BEZBJEDNOST

Kreiranje akcionog plana za fizičku bezbjednost je od suštinskog značaja za zaštitu fizičke sredstava organizacije, uključujući zgrade, hardver i osoblje, od potencijalnih prijetnji kao što su neovlašćeni pristup, krađa, vandalizam i prirodne katastrofe. Ovaj plan navodi korake potrebne da bi se obezbijedilo sigurno fizičko okruženje. Mala IPA tijela su odgovorna za zaštitu svojih fizičkih podataka, opreme (lični i mobilni računari, uređaji za skladištenje) i svojih sjedišta, kancelarija, stolova i monitora. Relevantne kontrole iz standarda za ovu oblast su A7.1, A7.2, A7.3, A7.4, A7.5, A7.6, A7.7, A7.8, A7.9, A7.10, A7 .11, A7.12, A7.13, A7.14.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
9.1	**Fizička bezbjednost**	Obezbjeđenje perimetra treba da bude projektovano i sprovedeno.	Dizajnirajte fizičke perimetre uključujući kancelarije i sobe, te ih zaštitite fizički ulazom i dodatnim kontrolama na osnovu nivoa klasifikacije.	Predstavnici ISMS-a Koordinatori ICT-a Fizičko obezbjeđenje u institucijama Zaposleni u IPA tijelima	I kvartal 2025.	/	Informacije o fizičkim perimetrima i zaštiti.
		Politiku fizičke bezbjednosti treba uspostaviti.	Razvijte i uvedite politiku o svakom sjedištu, bez ostavljenih papira na stolu, zaštiti zapisa, korišćenju i odlaganju opreme za sjedenje i skladištenje. Od ministarstava obezbijedite informacije o nadzoru objekata i radu u zaštićenim područjima.		II kvartal 2025.		Politika fizičke bezbjednosti
		Fizička i ekološka bezbjednost treba da se dokumentuju.	Pribavite informacije od ministarstava o zaštiti od fizičkih i ekoloških prijetnji, pomoćnim komunalnim uslugama, održavanju opreme i bezbjednosti kablova.		III kvartal 2025.		Informacije o zaštiti od fizičkih i ekoloških prijetnji, pratećim komunalnim uslugama, održavanju opreme i bezbjednosti kablova.

		Za sve zaposlene treba organizovati obuku o fizičkoj sigurnosti.	Sprovodite redovne obuke za zaposlene na temu svijesti o fizičkoj bezbjednosti, kontroli pristupa njihovim kancelarijskim arhivama, zaštiti evidencije.		II kvartal 2025.		Materijali sa obuke i evidencija sa obuke
		I za fizičku sigurnost treba uraditi reviziju.	Uključite fizičku bezbjednost kao temu za internu reviziju i izradite integralni godišnji revizorski izvještaj.		I kvartal 2026.		Integralni izvještaj interne revizije.
OBLAST: OSNOVA 10 – UPRAVLJANJE INCIDENTIMA BEZBJEDNOSTI INFORMACIJA							
Upravljanje incidentima kod bezbjednosti informacija podrazumijeva skiciranje strukturisanog pristupa identifikovanju, reagovanju na bezbijednosne incidente i oporavku od njih, kako bi se njihov uticaj minimizirao i spriječile se takve buduće pojave. Postoji jedan interfejs ovog procesa sa kontinuitetom poslovanja i oporavkom ako se incident kategoriše kao poremećaj. Drugi interfejs se odnosi na praćenje, otkrivanje i reagovanje, što je aktivnost kojom upravljaju ministarstva, odgovorna za mala IPA tijela koja su uglavnom odgovorna za prijavljivanje incidenata i slabosti u svom radnom okruženju, uključujući usluge koje koriste. Kontrole iz standarda obuhvaćenih u ovoj oblasti su A5.24, A5.25, A5.26, A5.28.							
Br.	**CILJEVI**	**MJERE**	**AKTIVNOSTI**	**ODGOVORNOSTI**	**ROK**	**SREDSTVA I IZVOR FINANSIRANJA** **NOSILAC AKTIVNOSTI**	**INDIKATORI**
10.1	**Omogućavanje brzog i urednog upravljanja incidentima bezbjednosti informacija**	Upravljanje kod informativnog incidenta treba da je isplanirano	Kreirajte politike i procedure za planiranje odgovora na incidente, procjenu i donošenje odluka o incidentima bezbjednosti informacija.	Predstavnici ISMS-a Koordinatori ICT-a Rukovodstvo odjeljenja IPA tijela Zaposleni u IPA tijelima	I kvartal 2025.	/	Kreirane su politike i procedure za upravljanje incidentima bezbjednosti informacijama
		Treba uspostaviti proces reagovanja na incidente bezbjednosti informacija.	Razvijte proces odgovora na incidente kod bezbjednosti informacija sa kontaktnim tačkama i interfejsima za druge procese.		II kvartal 2025.		Proces reagovanja na incident je dokumentovan.
		Zaposleni treba da budu obučeni za upravljanje incidentima u oblasti bezbjednosti informacija	Obučite zaposlene o važnosti i odgovornostima kod incidenata u oblasti bezbjednosti informacija.		II kvartal 2025.		Obuke se izvode i vode se evidencije.
		Prikupljanje dokaza treba da bude zakonito	Za incidente koji mogu imati pravni postupak treba garantovati prikupljanje dokaza i lanac nadzora		III kvartal 2025.		Dokaz o incidentu sa pravnim postupkom je zaštićen.

		Incidente treba analizirati, mjeriti i izvući lekcije.	U redovnim periodima izvještavajte o mjerenju učinka u vezi sa incidentima. Za veće incidente treba izvršiti ocjenu nakon incidenta.		II kvartal 2025.		Izvještaji o učinku i evidencije o pregledu nakon incidenta.

OBLAST: OSNOVA 11 – ODNOS SA DOBAVLJAČIMA

Uspostavljanje i održavanje sigurnih i efektivnih odnosa sa dobavljačima je od ključnog značaja. Rizik u kontekstu IPA tijela osim Agencije za platni promet više je povezan sa uslugama koje se pružaju ka internim „kupcima" od ministarstava ili MJU. Što se tiče odgovornosti za bezbjednost informacija, one se dijele tamo gdje ministarstva imaju odgovornost da dijele informacije i da se pridržavaju zahtijevanih standarda bezbjednosti informacija dok pružaju usluge IPA tijelima. Kontrole iz standarda koji se odnose na ovu oblast su A5.19, A5.20, A5.21, A5.22, A5.23.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
11.1	**Uspostaviti odnos sa dobavljačima**	Servisni katalog za usluge informacione bezbjednosti treba definisati	Definisati sve usluge informacione bezbjednosti koje treba da se isporuče IPA tijelima kao "insource" ili "outsource".	Predstavnik ISMS-a Koordinatori ICT-a Ministarstva Ministarstvo javne uprave Javne nabavke u instituciji	I kvartal 2025.	U zavisnosti od kataloga usluga i komercijalno ugovorenih usluga	Definisan katalog usluga
		Zahtjevi informacione bezbjednosti i standardi usluga treba da su dokumentovani	Dokumentovati izvještaje koje zahtijeva standard, kako bi IPA tijela mogla da pribave dokaze o isporučenim uslugama.		II kvartal 2025.		Definisani servisni izvještaji
		Usluge informacione bezbjednosti treba da su isporučene	Pružene i isporučene usluge IPA tijelima. Ako je usluga dobijena komercijalno, potpisati ugovor sa navedenim svim zahtjevima.		III kvartal 2025. do IV kvartala 2026.		Usluge se pružaju i isporučene su
		Isporuka usluga treba da se pregleda i izmjeri	Vršite periodične preglede, mjerite dogovoreni učinak i izvršite izmjene ako je potrebno.		I kvartal 2026. i svake godine		Zapisnik o pregledu i mjerenju učinka

OBLAST: OSNOVA 12 – PRAĆENJE, DETEKCIJA I REAGOVANJE

Kreiranje akcionog plana za praćenje, otkrivanje i reagovanje je ključno za zaštitu organizacije od sajber prijetnji. Ovaj sveobuhvatni pristup uključuje prikupljanje obavještajnih podataka o prijetnjama, obezbjeđenje krajnjih uređaja, upravljanje kapacitetima sistema i sprovođenje mjera protiv malvera, između ostalih radnji. Oblast je primjenljiva na sve IPA institucije, ali osim Agencije za plaćanje, sve druge, uključujući CFCU, bi obezbijedile* usluge. MJU i ministarstva kojima pripadaju IPA tijela odlučiće ko će pružati uslugu. Sve kontrole definisane u odnosima sa dobavljačima treba da se koriste u ovoj oblasti za upravljanje uslugama. Kontrole iz standarda obuhvaćenih uslugama u ovoj oblasti su A5.7, A.8.1, A8.6, A8.7, A8.8, A8.9, A8.12, A8.15, A8.16, A8.17 , A8.18, A8.23 integrisane u projekte ispod.
* Izraz nabavka u ovoj oblasti se koristi za definisanje usluge koja se traži od MJU ili ministarstva kome pripada IPA tijelo.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA	INDIKATORI

						NOSILAC AKTIVNOSTI	
12.1	**Definišite zahtjeve i obuhvat usluga praćenja, otkrivanja i reagovanja.**	Usluge i obuhvat treba definisati	Na osnovu zahtjeva u ovoj oblasti definisati usluge, njihov obim i kanale komunikacije interno sa zaposlenima u instituciji (Ministarstvu ili MJU). IPARD Agencija za plaćanja treba da odluči koje usluge će se razvijati interno, a za koje će biti angažovano MJU ili eksterno.	Predstavnici ISMS-a Koordinatori ICT-a Rukovodioci pružalaca usluga MJU Izvođači	I kvartal 2025.	Za IPARD agenciju budžet treba biti 300.000,00 EUR i finansiran iz sopstvenog budžeta.	Zahtjevi usluga i obima definisani.
12.2	**Postignite dogovor (ili definišite ugovor ako je usluga ugovorena sa eksternom firmom) za pružanje usluga.**	Sporazum/ugovor treba postići/potpisati	Na osnovu strategije o kibernetičkoj bezbjednosti i Zakona o informacionoj bezbjednosti, treba postići dogovor MJU sa IPA institucijama ili ugovore sa eksternim dobavljačima o isporučenim uslugama.		II kvartal 2025.		Ugovor pripremljen i dogovor postignut.
12.3	**Obezbjeđivanje usluga sajber bezbjednosti kako su dostupne.**	Pružanje usluga treba obezbijediti	Na osnovu sporazuma/ugovora usluge treba da budu obezbijeđene i isporučene onako kako su dostupne.		III kvartal 2025 – IV kvartal 2026.		Dogovor postignut ili potpisan ugovor.
12.4	**Usluga rizične pozicije**	Uslugu rizične pozicije treba pružiti	Usluga rizične pozicije uključuje: - otkrivanje ranjivosti - otkrivanje prijetnji koje su stvarne i mogle bi da zloupotrijebe postojeće ranjivosti infrastrukture IPA tijela - otkrivanje pogrešnih konfiguracija Konačni isporučen rezultat je da IPA tijela treba da budu svjesna rizika njihove osnovne infrastrukture.		III kvartal 2025.	IPARD agencija	Izvještaji o stavu rizika dostavljeni
12.5	**Usluga evidentiranja i praćenja**	Uslugu evidentiranja i praćenja trebalo bi obezbijediti	Usluge evidentiranja i praćenja uključuju: - evidentiranje relevantnih događaja, - posmatranje mrežnog saobraćaja, - evidencija sistema i aplikacija,		I kvartal 2026.		Izveštaji o događajima koji potiču od evidentiranja i praćenja su isporučeni

			- korišćenje privilegovanih komunalnih usluga - drugi relevantni izvori podataka - praćenje dostupnosti da otkrije neobično ponašanje ili potencijalne prijetnje.				
12.6	**Usluga multivektorske detekcije i reakcije**	Usluga multivektorske detekcije i reakcije trebala bi biti isporučena	Usluga multivektorske detekcije i reakcije uključuje: - detekciju krajnje tačke i reakciju - detekciju mreže i reakciju - zaštitu od malvera - sprječavanje curenja podataka - web filtriranje Konačni rezultat je da ove usluge treba da odgovore na napad koji je u toku.		IV kvartal 2026.		Izvještaji o incidentima koji dolaze od otkrivanja i reagovanja su dostavljeni

OBLAST: OSNOVA 13 – OPORAVAK I PRAVLJENJE REZERVNE KOPIJE

Izrada akcionog plana za oporavak i rezervnu kopiju je ključna za obezbjeđivanje otpornosti organizacije u slučaju poremećaja, održavanje bezbjednosti informacija i obezbjeđivanje ICT spremnosti. Ovaj plan pokriva ključne oblasti kao što su održavanje informacione bezbjednosti tokom prekida, ICT spremnost, rezervne kopije informacija i strategije viška. Mala IPA tijela u potpunosti zavise od ministarstava i treba da slijede njihovu strategiju za kontinuitet poslovanja. Obaveze malih IPA tijela za rezervne kopije vezane su za proceduru koja ih obavezuje da svu dokumentaciju čuvaju u odgovarajućem skladištu koje definišu ministarstva. Kontrole iz standarda koje pokriva ovu oblast su A5.29, A5.30, A8.13, A8.14.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
13.1	**Politika upravljanja kontinuitetom poslovanja**	Informaciona bezbjednost, ICT spremnost i suvišnost tokom prekida treba da se kontrolišu.	Na osnovu BIA odredite uslove za informacionu bezbjednost i kontinuitet poslovanja tokom prekida.	Predstavnici ISMS-a Koordinatori ICT-a Ministarstva Ministarstvo javne uprave Izvođač	II kvartal 2025.	Budžet za implementaciju ISMS-a 5.000,00 €, kroz projekte i konsultantske usluge	BIA obavljen
			Razvijte politiku koja bi definisala glavne ciljeve kontinuiteta poslovanja kao RTO, RPO i SDO.		II kvartal 2025.		Politika sa odobrenim ciljevima
			Razvijte i implementirajte planove kontinuiteta poslovanja koji bi ispunili definisane ciljeve.		IV kvartal 2025.	DUSPPEU	Planovi za kontinuitet poslovanja izrađeni

			Održavajte, testirajte i ažurirajte planove kontinuiteta poslovanja.		II kvartal 2026. i svake godine		Proizvedene evidencije i ažuriranje testova
13.2	**Politika pravljenja rezervnih kopija je primijenjena**	Rezervnu kopiju i blagovremeni oporavak informacija treba uspostaviti	Politika pravljenja rezervnih kopija je razvijena da definiše zahtjeve za pravljenje rezervnih kopija informacija.	Predstavnici ISMS-a Koordinatori ICT-a Ministarstva Ministarstvo javne uprave	II kvartal 2025.	/	Politika rezervne kopije je odobrena
			Dokumentovana procedura pravljenja rezervnih kopija i oporavka je razvijena i odobrena		II kvartal 2025.		Procedura rezervne kopije je odobrena
			Rezervna kopija se redovno testira		II kvartal 2025. kontinuirano		Postoje zapisi o testiranju rezervnih kopija

OBLAST: OSNOVA 14 – ŽIVOTNI CIKLUS RAZVOJA SISTEMA (SDLC) I POLITIKA UPRAVLJANJA PROMJENAMA

Životni ciklus razvoja sistema (SDLC) i upravljanje promjenama podrazumijevaju uspostavljanje praksi koje obezbjeđuju sigurnost i integritet informacionih sistema tokom njihovog razvoja, primjene i operativnih faza. To je strukturirani pristup ugrađivanja bezbjednosti u SDLC i efektivnom upravljanju promjenama, obezbjeđujući da se informacioni sistemi razvijaju, održavaju i bezbjedno rade. Mala IPA tijela su uključena u testiranje na osnovu Zahtjeva za promjenu kao krajnji korisnici. Kontrole iz standarda koje se odnose na ovu oblast su A5.8, A8.19, A8.25, A8.26, A8.27, A8.28, A8.29, A8.30, A8.31, A8.32, A8 .33, A8.34.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
14.1	**Politika upravljanja promjenama**	Politiku upravljanja promjenama treba razviti	Politika upravljanja promjenama treba da je odobrena i primijenjena	Predstavnici ISMS-a Koordinatori ICT-a Rukovodstvo IPA tijela Pojedinci koji upravljaju promjenama	II kvartal 2025.	Budžet za implementaciju ISMS-a 5.000,00 €, € iz projekata i	Odobrena politika upravljanja promjenama

14.2	**Procedura upravljanja kontrolama**	Promjene treba kontrolisati procedurom	Razvijte proceduru kontrole promjena koja bi upravljala promjenama u: - Bezbjednosnom testiranju tokom razvoja - Instalaciji softvera na operativnim sistemima Razvoj uz angažovanje eksternih dobavljača i dodatna kontrola kao: - Razdvajanje razvojnog, testnog i operativnog okruženja - Zaštita informacionih sistema tokom revizije i testiranja - Zaštita testnih podataka		III kvartal 2025.	konsultantskih usluga	Procedura upravljanja promjenama je odobrena
14.3	**Zahtjevi bezbjednosti u SDLC-u**	Bezbjednosne zahtjeve u SDLC-u treba definisati	Na osnovu procedure razvoja politike koja bi zahtijevala rano definisanje i implementaciju bezbjednosnih karakteristika i karakteristika u životnom ciklusu razvoja sistema, počevši od upravljanja projektima, bezbjednosti aplikacija, arhitekture sistema i kodiranja.		III kvartal 2025.	DUSPPEU	SDLC procedura odobrena
14.4	**Pregled procesa upravljanja promjenama**	Pregled promjena treba izvršiti	Izvršite pregled svih glavnih promjena i izradite izvještaj sa indikatorima.		I kvartal 2026. kontinuirano		Izvještaj sa indikatorima

OBLAST: OSNOVA 15 – SIGURNOST MREŽE

Bezbjednost mreže uključuje uspostavljanje strategija i mjera za zaštitu integriteta, povjerljivosti i dostupnosti informacija dok se prenose kroz mreže. Ovaj plan se bavi ključnim aspektima kao što su prenos informacija, bezbjednost mreže, bezbjednost mrežnih usluga, segregacija mreža i upotreba kriptografije. Mala IPA tijela imaju veoma ograničene odgovornosti u ovoj oblasti i sve ove usluge su zadužene za ministarstva. Kontrole iz standarda koje pokriva ova oblast su A5.14, A8.20, A8.21, A8.22, A8.24.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI

15.1	**Mrežne bezbjednosne kontrole**	Prenos informacija treba da bude zaštićen	Razvijte i implementirajte politike i procedure za bezbijedan prenos podataka, uključujući korišćenje bezbjednih protokola za prenos datoteka i šifrovanja.	Predstavnici ISMS-a Koordinatori ICT-a Ministarstva Ministarstvo javne uprave	III kvartal 2025.	/	Politike i procedure odobrene
		Mrežu treba procijeniti i ojačati	Redovno sprovodite procjene ranjivosti mreže i testirajte penetraciju da biste identifikovali i otklonili bezbijednosne nedostatke. Primijenite mjere za jačanje bezbjednosti na mrežne usluge i opremu, kao što su IDS/IPS, zaštitni zid, šifrovanje.				Evidencija o procjeni ugroženosti i otvrdnjavanju
		Segmentiranje i pristup kontroli	Dizajnirajte i primijenite segmentaciju mreže da biste odvojili kritična sredstva i usluge od opšte mreže. Sprovedite strogu kontrolu pristupa za mrežne usluge, zasnovanu na principu najmanje privilegija.				Informacije o segmentaciji mreže ACL

OBLAST: OSNOVA 16 – USKLAĐENOST SA ZAKONSKIM ZAHTJEVIMA

Pruža strukturirani pristup rješavanju i održavanju usaglašenosti sa složenom mrežom zakonskih, statutarnih, regulatornih i ugovornih zahtjeva u oblasti bezbjednosti informacija, obezbjeđujući zaštitu intelektualne svojine, organizacionih zapisa i informacija koje mogu da identifikuju, i podstičući kulturu stalnog poštovanja i poboljšanja. Za mala IPA tijela, kontrole u vezi sa pravima intelektualne svojine, zaštitom zapisa i privatnošću, kao i zaštitom ličnih podataka primjenljive su u okviru zapisa i skupova podataka koje obrađuju. Kontrole iz standarda koji se primjenjuje za ovu oblast su A5.31, A5.32, A5.33, A5.34, A5.35, A5.36.

Br.	CILJEVI	MJERE	AKTIVNOSTI	ODGOVORNOSTI	ROK	SREDSTVA I IZVOR FINANSIRANJA NOSILAC AKTIVNOSTI	INDIKATORI
16.1	**Obezbjeđivanje obrade informacija u skladu sa zakonskim, statutarnim, regulatornim politikama, pravilima i standardima za bezbjednost informacija.**	Politike zaštite, evidencije, prava intelektualne svojine i privatnosti treba da budu razvijene i sprovedene.	Definišite, dokumentujte i vodite evidenciju o zakonskim, statutarnim, regulatornim i ugovornim zahtjevima.	Predstavnici ISMS-a Koordinatori ICT-a Pravna služba u okviru institucija Izvođač	I kvartal 2025.	/	Dokument o pravnim, zakonskim, regulatornim i ugovornim zahtjevima.
			Razvijte i dajte na odobrenje politike o zaštiti evidencija, prava intelektualne svojine i privatnosti.		II kvartal 2025.		Politika razvijena i odobrena.

			Odlučite o strategiji zaštite zapisa i zaštitite ih od gubitka, uništenja, falsifikovanja, neovlašćenog pristupa i otkrivanja u skladu sa zakonskim, regulatornim i statutarnim zahtjevima.		II kvartal 2026.		IPA evidencije su zaštićene u skladu sa zakonskim, regulatornim, i statutarnim zahtjevima.
16.2	**Usklađenost sa politikom, pravilima i standardima za bezbjednost podataka**	Tehničku usklađenost treba sprovesti	Ispitivanje informacionog sistema za usaglašenost tehničke kontrole.	Predstavnik ISMS-a Koordinatori ICT-a Ministarstvo javne uprave Izvođač	III kvartal 2025.	Budžet tehničke kontrole 6.000,00 €, € iz projekata i konsultantskih usluga DUSPPEU	Izvještaj o tehničkoj usklađenosti
16.3	**Osigurati da se ISMS implementira i radi u skladu sa nacionalnim politikama i procedurama strukture IPA**	Procjenu sistema upravljanja bezbjednošću informacija treba obezbijediti	Nezavisna revizija kako bi se osigurala stalna podobnost, adekvatnost i efektivnost pristupa nacionalnoj IPA strukturi za upravljanje ISMS-om.	Predstavnik ISMS-a Koordinatori ICT-a Ministarstvo javne uprave Izvođač	I kvartal 2026.	Nezavisna revizija 5.000,00 €€, iz projekata i konsultantskih usluga	Izvještaj revizije o usklađenosti sa zahtjevima strukture IPA
16.4	**Nezavisna revizija o bezbjednosti informacija**	Nezavisnu reviziju bezbjednosti informacija treba obezbijediti	Izvršite nezavisnu reviziju tehničkih aspekata bezbjednosti informacija.			DUSPPEU	Nezavisni izvještaj revizije bezbjednosti informacija

ACTION PLAN

FOR THE IMPLEMENTATION OF THE INFORMATION SECURITY ON THE BASIS OF ISO 27002 STANDARD AT THE LEVEL OF IPA FRAMEWORK FOR THE PERIOD 2025-2027

Podgorica, December 2024

AREA: ESTABLISHMENT OF THE FRAMEWORK FOR THE MONITORING AND IMPLEMENTATION OF THE ISMS AND ACTION PLAN

Implementing and disseminating an Information Security Management System (ISMS) involves establishing, managing, and continuously improving the organization's information security framework based on the ISO/IEC 27002 standard. An ISMS is designed to protect the confidentiality, integrity, and availability of information by applying a risk management process. Implementing and disseminating an ISMS is a strategic project that requires commitment across the organization, from top management to every employee. This action plan outlines the key steps to establish a robust ISMS, aiming to protect information assets effectively while ensuring compliance with international standards and regulations. Instances for which this Action Plan is applicable form very complex ecosystem because of their interdependency in realizing IPA projects, different levels of complexity and various level of authority they have over their information security responsibilities. This a reason that these areas is overarching all processes that should be directed, monitored and evaluated by the Directorate Management Structure. Controls from the standard applicable to this area are 5 i.e. top leadership, commitment and policy and 7 i.e.roles and responsibilities, competencies, communication, awareness and documented information.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
1.	**Establishment of the Project teams and Steering Committee for the monitoring of the Action Plan on Security Policy implemented in IPA institutions based on ISO standard 27002**	ISMS representatives and project team members should be appointed at each IPA body/ institution.	IPA bodies/institutions appoint ISMS representative and project team members. Committee is consisted of Heads of IPA bodies/institutions and DMS.	ISMS Representatives IPA bodies Project teams IPA Bodies Heads	IQ 2025	/	Decision on appointment of the ISMS Representative and the Steering Committee
		Key goals and responsibilities of the ISMS Representatives and project team members should be defined.	IPA bodies/institutions in communication with NAO defines key goals and responsibilities within Decision.				Key goals and responsibilities of the ISMS Representative, project team and Steering Committee and defined within Decision
		Respective deadlines predicted for implementation of the measures from the AP should be defined.	Steering committee, on its first session, defines and adopts proposal of deadlines predicted for implementation of the measures from the AP				Proposal of the deadlines for implementation of the measures from the AP adopted and confirmed
2.	**Submission of the Information on adopted Decision to the European Commission**	Official note to the EC should be submitted.	Preparation of the Information and submission of official decision of the AP.	NAO	IQ 2025	/	Information officially submitted to the EC
3.	**Reporting lines on the implementation of the AP established**	Communication and reporting on the implementation of the Action Plan should be established.	Heads of IPA bodies define reporting lines to Steering Committee within process. Management review (defined in baseline 4.2 in this action plan) once per year is the output of this process.	Steering committee ISMS Representatives Head of IPA bodies/institutions	I Q 2025	/	Reporting lines defined by Conclusions

4.	**Introducing Steering Committee officials to the IS policy**	Proposed information security policy should be presented to Steering Committee	Steering Committee determines the compliance of the policy and need for further operationalization	Steering Committee ISMS Representative	II Q 2025	/	Steering Committee approval of the policy
5.	**Raising awareness about the importance of IS policy among the participants and other institutions in the process of management and use of funds from the IPA programs**	ISMS Representatives should be introduced within institutions. Training regarding implementation should be delivered to ISMS Representatives.	Necessary measure is to conduct training for ISMS representatives for ISO 27002 Implementer. Training is carried out for all representatives in dynamics corresponding the number and structure.	ISMS Representatives Contractor	IIQ 2025	Training Budget 5.000,00 € from DMS consulting budget DMS	Training plan created. Defined Program for training. Records from the trainings prepared
6.	**Raising awareness about the importance of IS policy among the participants and other institutions in the process of management and use of funds from the IPA programs**	Upgrade of the ICT procedures used by all IPA bodies in respect to newly adopted policy on ISO 27002 and re-appointment of ISMS Representatives within relevant institutions.	New version of the relevant chapter of the Manual of Procedures should be prepared and adopted on the basis of the measures from the AP and ISO 27002. ISMS Representatives should be re-appointed if needed within all IPA institutions	NAO	III Q 2025 – III Q 2026	/	New MoP version adopted ISMS Representative re-appointed
7.	**Operating procedures**	Operational procedures for work processes established	Responsible authority should document procedures for operational, system and technical activities	ISMS Representatives IPA bodies Department Heads IPA Bodies Heads	IV Q 2025 – IV Q 2026	ISMS Implementation budget 10.000,00 € for all activities from DMS consulting budget DMS	Operating procedures are documented and made to all available users – IPA staff

AREA: BASELINE 1 – CONTEXT ESTABLISHEMENT, RISK MANAGEMENT AND OBJECTIVES

Creating an action plan for "Context Establishment, Risk Management, and Objectives" involves a structured approach to understanding the environment in which an IPA bodies operates, identifying and managing risks, and setting clear objectives. Draft scope is proposed as " Services and information related with IPA funds." and it should be derived further for each IPA body.
Developing an action plan for risk management within the context of information security is essential to safeguard an organization's information assets effectively. This plan outlines a systematic approach to identifying, assessing, treating, and monitoring information security risks, ensuring the confidentiality, integrity, and availability of information. For small IPA bodies Risk methodology could be simple risk register with two basic components i.e. probability and impact that would be aligned with general risk methodology while for IPA agency it should consist additional components as threats, weaknesses, controls, assets,… Controls from the standard covered within this area are 4, 6, 8.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS	INDICATORS

						RESPONSIBLE BODY FOR BUDGETING	
1.1	**Define context, scope and objectives of ISMS system**	Context, scope and objectives for IPA Bodies should be documented.	Prepare draft document for context, scope and objectives. Communicate and adjust draft document based on specific IPA Body. Approve context, scope and objectives.	ISMS Representatives IPA bodies Project teams IPA Bodies Heads	I Q 2025	/	Draft document is prepared and adjusted. Context, scope and objectives are approved.
1.2	**Establishing methodology for analysis, evaluation, monitoring and reporting on risks**	Methodology for IS risk management should be Developed. Manual of Procedures for IPA bodies regarding risk management policy should be updated.	Creating aligned methodology for risk management which covers analysis, evaluation, monitoring, reporting and treatment of the risks for small IPA bodies and payment agency.	Contractor ISMS Representatives Risk Panel Risk Coordinators NAO	II Q 2025	ISMS implementation budget 5.000,00 € from DMS consulting budget DMS	Methodology for risk management developed. Manual of Procedures updated.
1.3	**Establishing communication between ISMS Representative, Risk Coordinators on IPA activities and Risk Panel representatives**	Methodology and modality of IS risk management should be submitted to the Risk Coordinator on IPA activities and presented on the separate Risk Panel meeting	Model of determination, management and reporting on risks in accordance with the recommendations of ISO 27002 is presented to Risk Coordinator for IPA activities and Risk Panel	ISMS Representatives Risk coordinators Risk Panel NAO	III Q 2025	/	Guidelines for risk management according the recommendations of the ISO 27002 are recognised and included in the general monitoring of the Risk Coordinator for IPA activities IPA risk panel for risk management held on the basis of risks identified through implementation of the ISO27002 Information on key risks delivered to MPA and Ministries
1.4	**Analysis of the IS risks and preparation and adoption of the Risk treatment plan**	Risk identification of relevant risks within the IPA structures on the basis of the ISO 27002 requirements and defined methodology should be performed.	High level risk register should be prepared on the level of all IPA bodies on the basis of ISO 27002 requirements	ISMS Representative ICT coordinators IPA bodies Department Heads IPA Bodies Heads Risk Owners	III Q 2025	ISMS Implementation budget 5.000,00 € from DMS consulting budget	Risk register prepared on the level of all IPA bodies based on risk management methodology.

				Contractor NAO			Risk register presented and monitored on the meetings of the Coordination body. NAO informed on all risks detected and on measures prepared for their proper follow-up.
		Risk Assessment should be performed.	All IPA bodies should separately perform Risk Assessment based on ISO 27002 requirements				Risk Assessment performed and delivered to NAO for further elaboration
		Risk estimation and acceptance criteria should be adjusted according to the risk profile of specific IPA body. Risk treatment plan should be elaborated and prepared for each IPA Body	Risk evaluation and risk acceptance criteria should be applied during analysis. Risk treatment options should be decided. Controls for risk treatments should be developed for a specific IPA institution			DMS	All identified risks are evaluated Risk treatment options decided Risk treatment plan developed Risk owners for the proper risk mitigation recognised Residual Risk accepted by each IPA body Risk register updated with the current progress
1.5	**Implementation of the controls based on the Risk Treatment Plan**	All proposed risk treatment plan actions should be timely implemented by the defined authorities	Implementation of risk treatment plan by each IPA institution	ISMS Representatives ICT coordinators IPA bodies Department Heads	Continuously up to IVQ 2026	Budget is distributed across specific controls within the Action Plan	IPA bodies are continuously performing activities in respect to risk mitigation
1.6	**Risk monitoring and follow-up established**	NAO should ensure that all unacceptable risks are effectively mitigated and if not corrective actions have been implemented timely The risk assessment process is documented together with the results	Implementation of the controls for unacceptable risks should be closely monitored by the NAO Corrective actions should be timely implemented	ISMS Representatives Risk Panel NAO	Continuously up to IV Q 2026	/	Follow-up on the Risk Treatment plan continuously presented to NAO and Risk Panel Corrective measures are identified to improve implementation of Risk treatment plan

		of the risk treatment plan implementation Risks are evaluated on a continuous basis					

AREA: BASELINE 2 – INFORMATION SECURITY POLICY

Policy sets the foundation for a robust information security program, outlining the principles and responsibilities that govern the protection of information assets. For most of IPA bodies policy should cover controls related with employees, information they are handling and organizational aspects of their processes. IPARD Payment Agency is special case where policy should be developed widely to cover other aspects of their operations. Controls from the standard covered within this area are 5.2, A5.1.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
2.1	**Development and Implemenatation of Information Security Policy – Establishing set of policies for information security**	Develop Information security policy that addresses all critical areas of information security.	Responsible authority should define a set of information security policies which contains guidelines to establish minimum of requirements for secure delivery of IPA services	ISMS Representatives ICT Coordinators IPA Bodies Project Teams IPA bodies Heads IPA bodies Department Heads Consultant	I Q 2025	/	Draft polices developed.
		Information security Policy should be approved by national IPA management, published and communicated to employees and relevant parties	Information security is published and communicated to employees and relavant parties.	ISMS Representatives ICT Coordinators IPA Bodies Project Teams IPA bodies Heads IPA bodies Department Heads IPA bodies Employees	II Q 2025		A set of policies for information security are adopted on the adequate level.
		Documented national IPA information security context should be defined and established and additionally maintained	Responsible authority have to implement a set of information security policies, publish, approve and announce it to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader.		II Q 2025		Information security policies are implemented, published and used by national IPA management and other institutions
		Training for Information security policies should be delivered	Train responsible employees within IPA Bodies for Information Security policy.	IPA bodies Employees Consultant	II Q 2025		Responsible employees are trained.

		Policies for information security that are adopted should be reviewed.	Treatment and updating of information security policy on the annual basis.	ISMS Representatives IPA bodies Heads	II Q 2025		Information security policies are reviewed and updated by IPA bodies
AREA : BASELINE 3 – INFORMATION SECURITY ROLES AND RESPONSIBILITIES							
Defining and communicating information security roles and responsibilities is crucial for establishing a clear governance structure that supports the organization's information security strategy. This ensures that every member of the organization understands their part in protecting information assets. Currently, except in the Payment Agency where CISO is appointed, there is no role of ISMS Representative that is crucial for IS Policy implementation. Controls from the standard covered within this area are 5.3, 7.1, 7.2, A5.2, A5.3, A5.4, A5.5, A5.6.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
3.1	**Appoint ISMS Representative**	Potential candidates should be employees within the IPA bodies as Risk Managers, QA staff or IT Coordinators.	Based on internal policy at each IPA body appoint ISMS Representative	ISMS Representatives IPA bodies Heads	I Q 2025	/	ISMS Representative appointed for each IPA Body
3.2	**Establishing a management framework to initiate and control the implementation and operation of information security within the organisation and on the level of coordination**	Roles and responsibilities for information security should be mapped and covered with functions in accordance with information security policy in relation with segregation of duties.	Roles and responsibilities for information security in institutions recognized by IPA bodies.	ISMS Representatives IPA bodies Heads IPA bodies Project teams Asset owners and custodians Risk Owners	I Q 2025	/	Roles and responsibilities are recognized and developed by IPA bodies through Rulebook of Internal organization and systematization of the line institution.
			Develop information security responsibilities in accordance with the information security policies.				
			Controls for segregation of duties are implemented				Adequate monitoring of the implementation of the IS ensured
			Controls for addressing information security aspects in project management and contacts with special interest groups or other specialist security forums and professional associations are also implemented				
			Communication lines with special external interested parties defined				Communication lines with external stakeholders established
AREA: BASELINE 4 – PERFORMANCE EVALUATION AND IMPROVEMENT							

Performance evaluation and improvement in information security is crucial to ensure that the security measures in place are effective and evolve to meet emerging threats and organizational changes. This area would be become actual after the establishment of Information Security Management System and earliest by the end of 2024. There are three forms of performance evaluation and improvement that should be established and maintained continuously i.e. Internal Audit, Management Review and measurements and their implementation would be described in this action plan. For small IPA Bodies this should be performed on the level of Ministries but for IPA aspects it would be performed on the level of DMS. For more details refer to controls 9 and 10 from the standard.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
4.1	**Establish Internal Audit function**	Decide on what strategy would be used i.e. - train internal staff for cross auditing, - use some government function that would perform internal audit or - subcontract external staff to deliver this service.	Decide on strategy and appoint this function to auditors chosen.	ISMS Representatives IPA bodies Heads Internal Auditors	II Q 2025	Training Budget 5.000,00 € from DMS consulting budget	Audit function is appointed Internal audit plan is developed. Report for Internal Audit is delivered.
		Risk based plan for internal audit should be developed.	Develop plan for performing internal audit.		II Q 2025 and Each year subsequently	DMS	
		Internal audit report should be delivered.	Perform internal audit and deliver report.		III Q 2025 and Each year subsequently		
4.2	**Perform Management Review**	Management Review should be planned with relevant inputs as internal audits, risk management,	Plan Management Review with all relevant inputs.	ISMS Representative IPA Bodies Heads IPA bodies Department Heads	IV Q 2025 and Each year subsequently	/	Plan is developed Management review decisions are documented
		Management Review should be performed with relevant outputs i.e. resources for continual improvement of ISMS	Perform Management Review by producing outputs		I Q 2026 and Each year subsequently		
4.3	**Perform measurement**	Indicators for measurement should be developed with recording periods	Develop indicators	ISMS Representatives IPA Bodies Heads	II Q 2025 and Each year subsequently	/	Table of indicators is developed Indicators are reported
		Indicators should be periodically reported with trends and thresholds	Report indicator results		IV Q 2025 and Each year subsequently		
AREA : BASELINE 5 – INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING							

Creating an action plan for Information Security Awareness, Education, and Training is essential to equip all members of an organization with the knowledge and skills needed to protect information assets. This initiative aims to foster a culture of security, reduce the likelihood of security incidents, and ensure employees can respond appropriately to threat. In the first year training program should be more concentrated on awareness and communication topics and in the subsequent on competencies and learning from the incidents. Controls from the standard related are 7.2, 7.3, 7.4, A5.27, A6.3.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
5.1	**Raising the collective awareness of the importance information security policy and security controls as well as good security practices**	Training participants should be determined	Determine training participants with prioritization based on needs assessment	ISMS Representatives HR within the institutions IPA bodies Employees ICT coordinators Training provider	II Q 2025 and Each Year	Training budget 5.000,00 € per year from DMS consulting budget	List of participants developed
		Training programme for the current year should be developed	Develop training program with appropriate topics				Training program developed
		Training provider should be engaged, and training materials developed	Develop training materials or engage training provider			DMS	Training materials developed or provider contracted
		Training should be delivered	Perform trainings, acquire recors and evaluate results				List of participants and training evaluation documented

AREA: BASELINE 6 – PEOPLE CONTROLS

Implementing people controls in information security involves establishing policies, procedures, and practices that focus on the human elements of information security. These controls are designed to reduce the risk of security breaches caused by human error or malicious actions. Set of policies and procedures that should be developed include relations with the employees before, during and after the employment including remore working and event reporting. For small bodies most of these policies should be already be developed on a level of Ministries. For more details refer to controls from the standard A6.1, A6.2, A6.4, A6.5, A6.6, A6.7, A6.8.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
6.1	**Develop policies and procedures that employees as human factor should follow.**	Policies and procedures that improve information security vigilance should be drafted.	Based on gap analysis decide on which policies and procedures based on employment lifecycle (including remote working and event reporting) and develop draft versions.	ISMS Representatives IPA Bodies Heads HR within the institutions Legal departments within the institutions Employees within IPA bodies	II Q 2025	/	Gap analysis performed Policies and procedures drafted
		Developed policies and procedures on employment life cycle should be approved.	Approve developed policies and procedures and implement them.		II Q 2025		Policies and procedures approved
		Dissemination should be performed by delivering training.	Deliver training and acquire records that all employees within the scope have understood and accepted policies and procedures.		II Q 2025		Training delivered Records of training completed.

AREA: BASELINE 7 – ASSET MANAGEMENT							
Asset management is a critical component of information security, focusing on the identification, classification, and protection of an organization's assets. Effective asset management ensures that valuable information and physical assets are appropriately safeguarded against threats. For small IPA bodies asset management would address data related with IPA services and their personal assets while assets related with servers and network are recorded at the level of Ministries. More details about these controls could be found in standard under A5.9,A5.10, A5.11, A5.12, A5.13, A8.10, A8.11,							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
7.1	**Create inventory of assets, classification, and acceptable use policy.**	Inventory of assets should be developed	Create and populate asset inventory with all required attributes.	ISMS Representatives ICT coordinators Asset owners and custodians	I Q 2025	/	Asset inventories populated
		Assets should be classified	Based on classification policy assets should be classified for Confidentiality, Integrity, and Availability.		I Q 2025		Assets are classified
		Acceptable use policy should be developed for the asset lifecycle.	Develop acceptable use policy and implement it based on asset classification.		II Q 2025		Acceptable use policy developed and approved
		Policies on classification and acceptable use should be disseminated by training	Deliver training sessions that would cover asset inventory and classification policy, acceptable use policy including return of assets, information deletion and data masking if applicable.		II Q 2025		Trainings delivered.
AREA : BASELINE 8 – ACCESS CONTROL							
Access control is pivotal in safeguarding an organization's information assets. Access control ensures that only authorized individuals have access to specific resources, thereby protecting sensitive information from unauthorized access, disclosure, and alteration. For small IPA Bodies access control to applications and file structures is applicable while access to directory services and physical perimeters is managed by the Ministries. Also in the domain of responsibilities of Ministries are privileged assess rights, secure authentication and access to source code. Controls related with the standard in this domain are A5.15, A5.16, A5.17, A5.18, A8.2, A8.3, A8.4, A8.5.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
8.1	**Implementation of the controls that restrict access to IPA structure employees and other institutions to specific**	Access control policy should be developed	Develop acces control policy (need to know, need to have) at appropriate level based on current asset ownership.	ISMS Representatives ICT Coordinators Asset owners and Administrators HR within the institutions	I Q 2025	/	Access control policy developed

	information and information assets	Access control policy should be implemented	Based on the policy develop access control matrix, that should be used by the administrators to implement it on the assets within the scope.	IPA bodies Heads IPA bodies Employees	III Q 2025		Access control matrix implemented
		Training related with access control should be delivered	Deliver training that includes access control policy, accountability, access rights, authentication information...		II Q 2025		Training delivered
		Access control policy should be reviewed	At least once per year asset owners and administrators should review the policy and agree if some changes are needed.		I Q 2026 and Each Year		Review record created

AREA : BASELINE 9 – PHYSICAL SECURITY

Creating an action plan for physical security is essential to safeguard an organization's physical assets, including buildings, hardware, and personnel, from potential threats such as unauthorized access, theft, vandalism, and natural disasters. This plan outlines the steps needed to ensure a secure physical environment. Small IPA Bodies are responsible for protection of their physical records, equipment (personal and mobile computers, storage devices) and their seating, offices, desks and screens. Relevant controls from the standard for this are A7.1, A7.2, A7.3, A7.4, A7.5, A7.6, A7.7, A7.8, A7.9, A7.10, A7.11, A7.12, A7.13, A7.14.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
9.1	**Physical security**	Perimeter security should be designed and implemented.	Design physical perimeters including offices and rooms and protect them with physical entry and additional controls based on classification levels,	ISMS Representatives ICT Coordinators Physical security within the institutions IPA bodies Employees	I Q 2025	/	Information abouth physical perimeters and protection.
		Policy on physical security should be established.	Develop and introduce policy on equipment seating, clear desk, records protection, equipment seating and storage use and disposal. Obtain information about monitoring of facilities and work in secure areas from Ministries.		II Q 2025		Physical security policy
		Physical and environmental security should be documented.	Obtain information from Ministries about protection against physical and environmental threats, supporting utilities, equipment maintenance and cabling security.		III Q 2025		Information about protection against physical and environmental threats, supporting utilities, equipment maintenance and cabling security

		Training to all employees for physical security should be delivered.	Conduct regular training sessions for employees on physical security awareness, access control to their office archives, protection of records.		II Q 2025		Training materials and records
		Physical security should be audited.	Include physical security as topic for internal audit and produce integral yearly audit report.		I Q 2026		Integral internal audit report.
AREA: BASELINE 10 – INFORMATION SECURITY INCIDENT MANAGEMENT							
Information security incident management involves outlining a structured approach to identifying, responding to, and recovering from security incidents to minimize their impact and prevent future occurrences. There is one interface of this process with business continuity and recovery if the incident is categorized as a disruption. Other interface is related with monitoring, detection and response that is activity managed by Ministries for small IPA bodies that are mainly responsible for reporting incidents and weaknesses within their working environment including services they are using. Controls from the standard covered within this area are A5.24, A5.25, A5.26, A5.28.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
10.1	**Enabling quick and orderly management of information security incidents**	Information incident management should be planned	Create policies and procedures for incident response planning, assessment, and decision on information security incidents.	ISMS Representatives ICT Coordinators IPA bodies Department Heads IPA bodies Employees	I Q 2025	/	Policies and procedures for information security incident management are created
		Process for response to information security incidents should be established.	Develop process for response to information's security incidents with contact points and interfaces to other processes.		II Q 2025		Process for incident response is documented
		Employees should be trained on information security incident management	Train employees for information security incident importance and responsibilities.		II Q 2025		Trainings are performed and records are created
		Collection of evidence should be lawful	For incidents that may have legal proceeding collection of evidence and chain of custody should be guaranteed		III Q 2025		Evidence for incidents with legal proceeding is protected
		Incidents should be analysed, measured and lesons learned.	On regular periods report on performance measurement related with incidents. For major incidents post incident review should be performed.		II Q 2025		Performance reports and post incident review records.
AREA: BASELINE 11 – SUPPLIER RELATIONSHIP							
Establishing and maintaining secure and effective supplier relationships is critical. Risk in the context of IPA Bodies except for the IPARD Payment Agency is more related with services obtained to internal "customers" from Ministries or MPA. Regarding the information security responsibilities, they are shared where Ministries have responsibilities to share information and adhere to required information security standards while delivering services to IPA Bodies. Controls from the standard related with this area are A5.19, A5.20, A5.21, A5.22, A5.23.							

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
11.1	**Establish supplier relationship**	Service catalogue for information security services should be defined	Define all information security services that should be delivered to IPA bodies as insource or outsource.	ISMS Representative ICT Coordinators Ministries Ministry for Public Administration Procurement within the institution	I Q 2025	Depending of the service catalogue and services contracted commercially	Service catalogue defined
		Information security requirements and standards for services should be documented	Document reports required by the standard so that IPA bodies can obtain evidence of delivered services.		II Q 2025		Service reports defined
		Information security services should be delivered	Services to IPA bodies provisioned and delivered. If service is obtained commercially sign a contract with all requirements.		III Q 2025 to IV Q 2026		Services are provisioned delivered
		Service delivery should be reviewed and measured	Perform periodic reviews, measure agreed performance and make changes if required.		I Q 2026 and Each Year		Record of review and performance measurement

AREA: BASELINE 12 – MONITORING, DETECTION AND RESPONSE

Creating an action plan for monitoring, detection, and response is crucial to protect an organization from cyber threats. This comprehensive approach involves gathering threat intelligence, securing endpoint devices, managing system capacities, and implementing measures against malware, among other actions. Area is applicable to all IPA institutions but except Payment Agency all other including CFCU would insource* services. MPA and Ministries where the IPA Bodies belong will decide who will provide the service. All controls defined in supplier relationship should be used in this area to manage services. Controls from the standard covered with services within this area are A5.7, A.8.1, A8.6, A8.7, A8.8, A8.9, A8.12, A8.15, A8.16, A8.17, A8.18, A8.23 integrated within the projects below.

* Term insourcing in this area is used to define service that is required from MPA or Ministry where the IPA body belongs.

No.	GOALS	MEASURES	ACTIVITIES	RESPONSABILITIES	DEADLINE	FUNDS AND SOURCE OF FUNDS RESPONSIBLE BODY FOR BUDGETING	INDICATORS
12.1	**Define requirements and scope for monitoring, detection and response services.**	Services and scope should be defined	Based on the requirements in this area define the services, their scope and communication channels with insourcing institution (Ministry or MPA). IPARD Payment Agency should decide which services would be developed internally and what would be insourced to MPA or outsourced.	ISMS Representatives ICT Coordinators Heads of Service providers MPA Contractors	I Q 2025	For IPARD agency budget should be 300.000,00 EUR funded from their own budget.	Service requirements and scope defined.
12.2	**Achieve agreement (or define contract if the service is outsourced) for service delivery.**	Agreement/contract should be achieved/signed	Based on Cybersecurity strategy and Law on information security achieve agreement of MPA with		II Q 2025		Contract prepared and agreement achieved.

			IPA institutions or outsourcing contracts on services delivered				
12.3	**Cybersecurity service provisioning as they are available.**	Service delivery should be provisioned	Based on the agreement/contract's services should be provisioned and delivered as they are available.		III Q 2025 – IV Q 2026		Agreement achieved or contract signed.
12.4	**Risk Posture service**	Risk posture service should be delivered	Risk posture service include: - Detection of vulnerabilities - Detection of threats that are actual and could misuse existing vulnerabities of IPA body infrastructure - Detection of misconfigurations Final result delivered that IPA bodies should be aware what is the risk of their underlaying infrastructure.		III Q 2025	IPARD agency	Reports on risk posture delivered
12.5	**Loging and monitoring service**	Logging and monitoring service should be delivered	Logging and monitoring service include: - logging relevant events, - observation of network traffic, - system and application logs, - use of privileged utilities - other relevant data sources - availability monitoring to detect unusual behaviour or potential threats.		I Q 2026		Reports on events coming from logging and monitoring delivered
12.6	**Multi vector Detection and Response service**	Multi vector detection and response service should be delivered	Multivector detection and response service include: - end point detection and response - network detection and response - protection against malware - data leakage prevention - web filtering Final result is that these services should respond to an ongoing attack.		I Q 2027		Reports on incidents coming from detection and response delivered

AREA: BASELINE 13 – RECOVERY AND BACKUP							
Developing an action plan for Recovery and Backup is crucial to ensuring an organization's resilience in the face of disruptions, maintaining information security, and ensuring ICT readiness. This plan covers key areas such as maintaining information security during disruptions, ICT readiness, information backup, and redundancy strategies. Small IPA bodies are completely dependent on Ministries and they should follow their strategy for business continuity. Backup responsibilities of small IPA Bodies are related with the procedure that make them obliged to save all documents at appropriate storage defined by the Ministries. Controls from the standard covered with this area are A5.29, A5.30, A8.13, A8.14.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS / RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
13.1	**Business Continuity Management Policy**	Information security, ICT readiness and redundancy during disruption should be controlled.	Based on BIA determine requirements for information security and business continuity during disruptions.	ISMS Representatives ICT Coordinators Ministries Ministry of Public Administration Contractor	II Q 2025	ISMS Implementation budget 5.000,00 € from DMS consulting budget	BIA performed
			Develop policy that would define main business continuity objectives as RTO, RPO and SDO.		II Q 2025		Policy with objectives approved
			Develop and implement business continuity plans that would deliver defined objectives.		IV Q 2025	DMS	Business continuity plans developed
			Maintain, test and update Business continuity plans.		II Q 2026 and Each Year		Test records and updates produced
13.2	**Backup policy implemented**	Backup and timely recovery of information should be established	A backup policy is developed to define requirements for information backup.	ISMS Representatives ICT Coordinators Ministries Ministry of Public Administration	II Q 2025	/	Back-up policy is approved
			Documented backup and recovery procedure is developed and approved		II Q 2025		Back-up procedure is approved
			Backup is regularly tested		II Q 2025 Continuously		Records for Back-up testing exist
AREA: BASELINE 14 –SDLC AND CHANGE MANAGEMENT							
System Development Life Cycle (SDLC) and change management involves establishing practices that ensure the security and integrity of information systems throughout their development, deployment, and operational phases. It is a structured approach to embedding security throughout the SDLC and managing changes effectively, ensuring that information systems are developed, maintained, and operated							

securely. Small IPA Bodies are included in testing based on Requests for change as end users. Controls from the standard related with this area are A5.8, A8.19, A8.25, A8.26, A8.27, A8.28, A8.29, A8.30, A8.31, A8.32, A8.33, A8.34.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
14.1	**Change management policy**	Policy for change management should be established	Change management policy should be approved and implemented	ISMS Representatives ICT Coordinators IPA bodies Heads Change Owners	II Q 2025	ISMS Implementation budget 5.000,00 € from DMS consulting budget	Change management policy approved
14.2	**Change control procedures**	Changes should be controlled by procedure	Develop change control procedure that would manage changes in: - Security testing in development - Installation of software on operating systems - Outsourced development and additional controls as: - Separation of development, test and operations environments - Protecting Information systems during audit and testing - Protection of test data		III Q 2025		Change Management procedure approved
14.3	**Security requirements in SDLC**	Security requirements in SDLC should be defined	Based on policy develop procedure that would require early definition and implementation of security features and characteristics in System Development Lifecycle starting from Project management, application security, system architecture and coding.		III Q 2025	DMS	SDLC procedure approved

14.4	**Change management process review**	Review of changes should be performed	Perform review of all major changes and produce report with indicators.		I Q 2026 Continuously		Report with indicators
AREA: BASELINE 15 – NETWORK SECURITY							
Network security involves establishing strategies and measures to protect the integrity, confidentiality, and availability of information as it is transferred across networks. This plan addresses crucial aspects such as information transfer, network security, security of network services, segregation of networks, and the use of cryptography, Small IPA bodies have very limited responsibilities in this area and all these services are insourced to Ministries. Controls from the standard covered by this area are A5.14, A8.20, A8.21, A8.22, A8.24.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS** **RESPONSIBLE BODY FOR BUDGETING**	**INDICATORS**
15.1	**Network security controls**	Information transfer should be protected	Develop and implement policies and procedures for the secure transfer of information, including the use of secure file transfer protocols and encryption.	ISMS Representatives ICT Coordinators Ministries Ministry for Public Administration	III Q 2025	/	Policies and procedures approved
		Network should be assessed and hardened	Regularly conduct network vulnerability assessments and penetration testing to identify and remediate security gaps. Apply security hardening measures to network services and equipment as IDS/IPS, Firewall, encryption.				Records on vulnerability assessments and hardening
		Segmentation and access control	Design and implement network segmentation to separate critical assets and services from the general network Implement strict access controls for network services, based on the principle of least privilege.				Network segmentation information and ACL
AREA: BASELINE 16 – COMPLIANCE WITH THE LEGAL REQUIREMENTS							
Provides a structured approach to addressing and maintaining compliance with the complex web of legal, statutory, regulatory, and contractual requirements in information security, ensuring the protection of intellectual property, organizational records, and personally identifiable information, and fostering a culture of continuous compliance and improvement. For small IPA Bodies controls related with IP Rights, Protection of records and Privacy and protection of PII are applicable within the scope of records and datasets they process. Controls from the standard applicable for this area are A5.31, A5.32, A5.33, A5.34, A5.35, A5.36.							
No.	**GOALS**	**MEASURES**	**ACTIVITIES**	**RESPONSABILITIES**	**DEADLINE**	**FUNDS AND SOURCE OF FUNDS**	**INDICATORS**

						RESPONSIBLE BODY FOR BUDGETING	
16.1	**Ensuring that processing of information comply with legal, statutory, regulatory and policy, rules and standards for information security.**	Policies on protecting, records, intellectual property rights and privacy should be developed and implemented.	Define, document and maintain record of legal, statutory, regulatory and contractual requirements	ISMS Representatives ICT Coordinators Legal department within the institutions Contractor	I Q 2025	/	Document on legal, statutory, regulatory and contractual requirements.
			Develop and approve policies on protecting records, intellectual property rights and privacy.		II Q 2025		Policy developed and approved.
			Decide the strategy for records protection and protect them from loss, destruction, falsification, unauthorized access, and disclosure in accordance with legal, regulatory, and statutory requirements.		II Q 2026		IPA records protected in accordance with legal, regulatory, and statutory requirements.
16.2	**Compliance with policy, rules and standards for Information Security**	Technical compliance checking should be implemented	Testing information system for technical control compliance.	ISMS Representative ICT Coordinators MPA Contractor	Q III 2025	Technical controls budget 6.000,00 € from DMS consulting budget.	Technical compliance report
						DMS	
16.3	**Ensure that ISMS is implemented and operated in accordance with the national IPA structure policies and procedures.**	Assessment of information security management system should be provided	Independent review to ensure the continuing suitability, adequacy and effectiveness of the national IPA structure approach to managing ISMS	ISMS Representative ICT Coordinators MPA Contractor	Q I 2026	Independent Audit 5.000,00 € from DMS consulting budget	Audit report on compliance with IPA structure requirements
16.4	**Independent review on information security**	Independent audit for information security should be provided	Perform independent audit for information security technical aspects.			DMS	Independent information security audit report