

Achiziționarea serviciilor de audit securitate cibernetică
Numărul lotului : a1c3e661-6747-11e9-8f69-ddf0ecccd6dd

SARCINA TEHNICĂ

SERVICII DE AUDIT DE SECURITATE CIBERNETICĂ

21 mai 2019

**Attn: Elena Adam, responsabil achiziții
IP” Agenția de Guvernare Electronică”**
Mun. Chișinău, MD 2012, str. Al. Pușkin nr. 42B
Tel: +373 22 82 00 21;
E-mail: elena.adam@egov.md
Pagina web: <http://egov.md/ro>

Cuprins

I. Despre companie	3
1. Descriere servicii, domenii	3
2. Experiență	4
III. Înțelegerea necesităților	7
1. Necesitățile beneficiarului(AGE)	7
2. Necesitățile entităților.....	7
IV. Rezultate și livrabile	8
V. Abordarea față de livrarea proiectului	9
1. Limitarea scopului	9
2. Termenii de livrare și structura activităților	9
3. Echipa de proiect de bază și extinsă.....	11
4. Guvernanță proiectului	12
5. Asigurarea calității	13
VI. ANEXE	14
ANEXA 1: CERTIFICĂRI	14
ANEXA 2: SCRISORI DE RECOMANDARE	14
ANEXA 3: CURRICULUM VITAE	14

I. Despre companie

1. Descriere servicii, domenii

BSD Management este specializată în audit și consultanță în domeniul securității și tehnologiilor informaționale. Experiența profesională cumulată a echipei depășește 50 ani. BSD Management posedă expertiză și experiență de realizare a proiectelor complexe guvernamentale, bancar dar și întreprinderi private.

BSD Management posedă cunoștințe tehnice necesare, personal și resurse pentru a realiza cu succes proiecte cu grad nivel de complexitate și a asigura:

- Înțelegerea și analiza detaliată a sistemelor informaționale, a infrastructurii de suport, a proceselor, contextului legal și altor cerințe;
- Evaluarea, evaluarea, implementarea și îmbunătățirea securității informaționale, în conformitate cu standardele internaționale, cele mai bune practici sau alte cadre de reglementare relevante;
- Planificare strategică și evaluare TI;
- Implementarea și managementul planului de sustenabilitate a afacerii;
- Evaluarea ciclului de viață al dezvoltării sistemului și punerea în aplicare a cadrului relevant;
- Continuitatea afacerii și planificarea implementării și gestionării.
- Transformarea businessului, reingineria proceselor, serviciilor și alte.

Experiența noastră, cunoștințele și angajamentul față de realizarea calitativă a serviciilor este conformată prin certificări relevante atât la nivel de companie cât și certificări individuale.

Certificările deținute de echipa noastră sunt următoarele:

- Certified Information Systems Auditor (CISA);
- Certified Management Consultant (CMC);
- Certified Information Systems Security Professional (CISSP);
- ISO 27001 Lead Auditor;
- Certified Information Security Manager (CISM);
- Certified in IT Infrastructure Library (ITIL Foundation);
- The Open Group Architecture Framework (TOGAF);
- Certified in Risk and Information Systems Control (CRISC).

BSD management a fost certificat conform standardelor IOS/IEC, în special:

- **ISO 9001:2015,**
- **ISO 27001:2013.**

Calitatea serviciilor noastre este confirmată de o serie de recomandări obținute de la beneficiari pentru care am prestat servicii de audit și consultanță.

Competențele noastre sunt extensive și acoperă arii precum:

- (1) Audit TI și al securității informaționale cibernetice.
- (2) Managementul securității informaționale.
- (3) Managementul continuității afacerii.
- (4) Guvernanța tehnologiilor informaționale.
- (5) Asigurarea calității la implementarea sistemelor.
- (6) Inovație și strategii în domeniul tehnologiilor Informaționale/securității informaționale.
- (7) Evaluare GDPR.
- (8) Alte arii.

BSD Management a realizat un număr semnificativ de proiecte în domeniul de audit și consultanță ca Auditului securității informaționale, Planificarea continuității afacerii, Evaluări de securitate/Audit complex al sistemelor, evaluarea calității și performanței sistemelor.

Dintre clienții noștri în domeniul public putem menționa: Ministerul Economiei și Infrastructurii, Comisia Electorală Centrală, Parlamentul Republicii Moldova, CNAȘ, USM, BNM, etc. Pe lângă aceștia, BSD Management a oferit servicii pentru un număr de instituții financiare și bancare.

2. Experiență

Proiecte relevante realizate de membrii echipei noastre:

No.	Numele companie	Perioada	Proiect
1	Bănci Moldova	2018 2019	<p>Elaborare și implementare cadru reglementare gestiune riscuri în baza standardelor internaționale, cerințelor BNM și recomandărilor EBA (The European Banking Authority).</p> <p>Realizare analiză riscuri.</p> <p>Elaborare și completare instrumente de evidență și analiză a riscurilor.</p>
2	Bancă Moldova	2018	<p>Elaborare și implementare cadru reglementare gestiune riscuri în baza standardelor internaționale, cerințelor BNM și recomandărilor EBA (The European</p>

			Banking Authority). Elaborare instrumente de evidență și analiză a riscurilor.
3	Banca Națională a Moldovei	2017- 2018	Evaluare riscuri de securitate pentru sistem de tip CRM (soluție pentru eficientizarea procesului de licențiere și autorizare, notificare) – servicii subcontractate.
4	Bănci Moldova	2016-2018	Auditul complex privind organizarea și funcționarea domeniului TCI, sistemului de management de securitate a informației și funcțiilor de control intern.
5	Bănci Moldova	2016-2018	Implementarea sistemului de management al continuității afacerii.
6	Bancă Moldova	2018	Actualizarea cadrului de reglementare în domeniul sistemului de management al continuității afacerii și a documentelor de punere în aplicare a acestuia. Realizarea activităților de testare și de instruire în domeniu.
7	Bancă Moldova	2018	Auditul sistemului de management al securității informației.
8	Bancă Moldova	2018	Audit sistem de deservire bancară la distanță.
9	Bancă Moldova	2017	Studiu de fezabilitate pentru selectarea Data Centru. Elaborare plan de tranziție și viziuni asupra arhitecturii țintă.
10	Întreprindere de Stat	2016	Suport în pregătirea caietului de sarcini pentru achiziția unei platforme integrate de gestiune a activității.
11	Întreprindere financiară	2018	Externalizarea responsabilităților Ofițer de Securitate a Informației.
13	Bancă Moldova	2016	Auditul strategiei tehnologiei informaționale cu obiectivele de afacere stabilite, evaluarea capacității IT de realizarea a

			acestei strategii, argumentarea bugetului IT și eficiența alocării resurselor.
14	Grup companii Romania	2016	Suport la selectarea sistemului de tip ERP.
15	Parlamentul RM	2017	Evaluare calitate și securitate sistem informatic. Inventariere și analiză capacități tehnice în raport cu cerințele de funcționare.
16	Proiect Banca Mondială (UIPAC, Ministerul Economiei și Infrastructurii)	2018 - 2019	Evaluare calitate sistem informațional, realizare activități complexe de testare funcțională și non-funcțională. Evaluare securitate sistem și corespundere cu cerințele Beneficiarului.
17	CEC	2018 - 2019	Evaluare performanță și securitate sisteme informaționale prin realizarea testărilor specifice.
18	Bancă Moldova	2018-2019	Suport în ajustarea și elaborarea cadrului de reglementare în domeniul securității informației.
19	Bănci Moldova	2016 - 2019	Suport în realizarea auditelor financiare prin auditarea și furnizarea opiniei privind eficiența și eficacitatea controalelor generale TI. Realizarea activităților complexe de evaluare a controalelor de aplicație pentru procesele critice.
20	Operatori de monedă electronică	2017 - 2018	Realizare misiuni audit complex TIC în baza cerințelor BNM. Furnizarea recomandărilor necesare conformării cerințelor minime și înlăturării neajunsurilor. Suport în implementarea recomandărilor și depunere dosar documente pentru evaluare de către BNM.

III. Înțelegerea necesităților

1. Necesitățile beneficiarului (AGE)

Reieșind din inițiativele strategice de e-Transformare a guvernării și în scopul îmbunătățirii actului de guvernare și a calității serviciilor publice, în baza Statutului său, Agenția de Guvernare Electronică a inițiat prezentul proiect. Înțelegând exact contextul desfășurării prezentei licitații, precum și deținând experiență vastă în domeniile vizate, avem certitudinea de a echivala înțelegerea noastră a necesităților Agenției de Guvernare Electronică cu abordare optimă în raport cu rezultatele așteptate.

Considerăm că perspectiva derulării proiectului include nu numai prevederile Statutul Agenției, aprobat prin Hotărârea Guvernului nr.760/2010, pct.11 subpct. 11-13, dar trebuie să țină cont de obiectivele e-Transformării Guvernului per ansamblu și necesitățile specifice ale instituțiilor vizate. Un interes separat considerăm că trebuie acordat așteptărilor și necesităților beneficiarilor finali ai serviciilor publice, în special cetățenii Republicii Moldova.

Astfel, vedem drept obiectiv principal al angajamentului pentru proiectul dat acordarea suportului profesionist, imparțial și obiectiv Agenției de Guvernare Electronică în exercitarea eficientă a următoarelor funcții:

- efectuare a auditului de securitate cibernetică a infrastructurilor de tehnologie a informației și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetică de interes național, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora;
- efectuarea și evaluarea conformității auditului de securitate cibernetică efectuate în autoritățile publice cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern, și informarea autorităților interesate conform domeniilor de competență;
- monitorizarea implementării rezultatelor auditului de securitate cibernetică efectuate în autoritățile publice în conformitate cu cerințele minime obligatorii de securitate cibernetică, aprobate de Guvern.

În contextul proiectului dat, salutăm inițiativa includerii unui număr semnificativ de instituții în scop, fapt ce va permite obținerea unor date importante și actuale per întreg Guvernul, precum și va permite utilizarea unei abordări adaptate fiecărei instituții în parte.

2. Necesitățile entităților

Subiectul asigurării securității informației este unul actual și critic atât în sectorul public, cât și în sectorul privat. Calitatea, performanța și competitivitatea serviciilor sunt direct dependente de utilizare tehnologiilor și tehnicilor moderne. În acest context, inițiativele în domeniul e-Guvernării prezintă atât oportunități pentru instituțiile Statului, cât și implică

riscuri, rezultând în responsabilități în domeniul securității informației, protecției datelor cu caracter personal, asigurarea continuității, gestiunea proiectelor, etc.

În baza obiectivului stabilit în documentația de licitație, dar și considerând prevederile altor acte legislative, aplicând standardele internaționale și cele mai relevante bune practici în domeniu, vom evalua în mod independent și imparțial gradul de conformare al sistemului de management al securității cibernetice/informației la cerințele Hotărârii de Guvern nr.201 din 28.03.2017.

Evaluarea sistemului de management al securității cibernetice/informației este un exercițiu standard bine cunoscut experților propuși pentru angajament. Deținem competențe și experiență vastă atât în evaluare cât și în implementarea sistemelor de management al securității informației în cadrul instituțiilor de variată dimensiune și diferit nivel de maturitate al domeniului. Astfel, în baza experienței vaste vom putea selecta cele mai eficiente și relevante metode și instrumente de lucru, încât fiecare instituție în parte să fie tratată maxim de atent și echidistant, iar concluziile generale să fie reprezentative pentru toate entitățile evaluate (inclusiv și cele din subordine).

Estimăm furnizarea unor concluzii individuale pentru fiecare instituție, care vor fi aplicabile și relevante obiectivului de conformare. Acestea vor fi coordonate corespunzător cu toate părțile interesate, încât să fie pasibile implementării printr-o abordare relevantă și eficientă. Rezultatele planificate și livrabilele furnizate, precum și abordarea aplicată față de livrarea proiectului sunt prezentate în continuare, acestea fiind bazate și însoțite de probe și dovezi concludente cu obiectivele angajamentului și concluziile formulate.

IV. Rezultate și livrabile

Angajamentul dat va include 13 instituții de stat, care de fapt reprezintă toate ministerele din componența Guvernului, Cancelaria de Stat și alte trei instituții specializate, responsabile de furnizare unui număr mare de servicii publice.

În conformitate cu scopul definit în documentația de licitație, vom realiza evaluarea sistemului de management al securității cibernetice/informației atât la nivel de ministere, cât și la nivel de instituții subordonate, specializate și teritoriale. În acest scop vor fi utilizate instrumente standarde aplicabile pentru evaluarea sistemelor de management. În rezultat vor fi obținute rapoarte detaliate în raport cu criteriul de evaluare (Hotărârea de Guvern nr.201 din 28.03.2017) atât pentru cele 13 instituții nominalizate în documentația de licitație, cât și pentru alte instituții relevante obiectivului care intră în componența acestora sau sunt subordonate.

Rezultatele așteptate vor reprezenta o viziune independentă asupra gradului de conformare a sistemului de management al securității cibernetice/informației în instituțiile respective la cerințele Hotărârii de Guvern Nr. 201 din 28.03.2017. Vor fi livrate rapoarte de audit separate pentru fiecare entitate auditată. Rapoartele elaborate vor oferi constatările, opinia și recomandările auditorului privind implementarea Hotărârii de Guvern Nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică. Fiecare raport va fi coordonat cu instituția evaluată (auditată) și

cu Agenția de Guvernare Electronică, încât livrabilele furnizate să fie obiective și relevante atât la nivel de instituție, cât și Guvern.

Suplementar ne propunem să livrăm un raport generalizator în baza tuturor rezultatelor obținute, cu formularea unor concluzii și recomandări specifice, relevante și reprezentative.

V. Abordarea față de livrarea proiectului

1. Limitarea scopului

- Se va realiza o evaluare generalizată, de tip diagnostic, fapt ce presupune ca auditorul nu va merge în detalii pentru a verifica respectarea HG 201 pentru fiecare sistem în parte, ci va nota excepțiile identificate.
- eGov va oferi suportul necesar organizării ședințelor și obținerii informației relevante, solicitate întemeiat.
- Auditul și procedurile analitice se vor baza pe informația obținută în mod oficial (în baza chestionarelor tipizate), fără a fi realizate inventarii sau interviuri cu toate persoanele responsabile (excepție cazurile când vor fi necesare concretizări sau va fi informație critică).
- Scopul angajamentului nu va include abordarea pentru entități de nivel jos, atât la obținerea și analiza informației, cât și nici la furnizarea rapoartelor. Nivelul de divizare și detaliere a entităților subordonate celor de bază incluse în documentația de licitație va depinde de capacitatea acelor 13 instituții de a furniza informația necesară în mod centralizat.
- Depășirea termenelor de organizare a ședințelor / prezentare a informației va asigura prelungirea termenului general al proiectului cu aceeași perioadă.
- Comunicarea și coordonarea rezultatelor (constatări, recomandări) va fi realizată pe verticală numai în interacțiune cu instituțiile incluse în documentația de licitație.
- Dovezile de audit vor fi documentate și referențiate doar pentru și în conexiune cu constatările identificate.
- Cadrul legal aplicabil (cu excepția celui indicat expres în documentația de licitație), precum și actele, acordurile sau alte tipuri de documente interdepartamentale nu vor fi evaluate și nici utilizate drept reper de evaluare.
- Adițional cadrului de reglementare inclus în documentația de licitație vor fi utilizate standardele internaționale și bunele practici recunoscute (dacă va fi necesar acestea vor fi coordonate cu AGE).

2. Termenii de livrare și structura activităților

Conform Cap.3 al Hotărârii de Guvern nr.201 din 28.03.2017 Cancelaria de Stat, ministerele și alte autorități administrative centrale subordonate Guvernului și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, instituțiile publice în care

Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), autoritățile administrative autonome și unitățile cu autonomie financiară, în termen de până la 31 decembrie 2017, vor asigura implementarea Cerințelor minime obligatorii de securitate cibernetică.

Agenția de Guvernare Electronică a inițiat prezentul proiect pentru a obține date veridice și actuale, în baza activităților stipulate în Capitolul 5 al Anexei 1 la invitația de participare la licitație „Caiet de sarcini achiziție de servicii de audit securitate cibernetică”, după cum urmează:

- Va analiza implementarea cerințelor minime de securitate cibernetică – 6 domenii ce corespund Anexei la Hotărârea Guvernului nr.201 din 28.03.2017;
- Va analiza implementarea sistemului de control intern al instituției din punct de vedere al asigurării implementării cerințelor minime de securitate cibernetică;
- Va analiza nivelul de documentare a modalității de implementare a cerințelor minime de securitate cibernetică;
- Va analiza modalitatea de identificare, precum și nivelul de asigurare, inclusiv bugetare, a resursele necesare pentru implementarea cerințelor minime de securitate cibernetică;
- Va obține și prezenta dovezi suficiente în suportul opiniei de audit privind:
- Statutului implementării cerințelor minime de securitate cibernetică;
- Asigurarea cu resursele necesare pentru implementarea cerințelor minime de securitate cibernetică;
- Organizarea controlului intern privind implementarea cerințelor minime de securitate cibernetică;
- Calitate și nivelul de documentare a modalității de implementare a cerințelor minime de securitate cibernetică.

Pentru atingerea obiectivelor ne propunem să structurăm proiectul după cum urmează:

1. Delimitarea inițială a scopului: entități subordonate, specializate, teritoriale, etc.
2. Stabilirea sponsorilor și managerilor de proiect pentru fiecare entitate din cele 13 incluse în listă (fără a coborî la nivel de instituții subordonate). Elaborarea și aprobarea cartei de proiect.
3. Clasificarea entităților în scop conform art.2, Capitol 1 în funcție de tipul modul de utilizare TIC (utilizare in-house, prestare servicii către alte entități și cetățeni).
4. Elaborarea programului de lucru pentru entitățile clasificate ca fiind de nivel 1.
5. Elaborarea programului de lucru pentru entitățile clasificate ca fiind de nivel 2.
6. Elaborarea și agrearea structurii de raport.
7. Organizarea unei sedinte (workshop), cu participarea reprezentanților tuturor entităților în scop pentru a oferi informație privind abordarea și instrumentele de audit ce vor fi aplicate de către membrii echipei de audit.

Activitățile nemijlocite realizate de către echipele de audit se vor încadra în structura misiunilor de audit realizate în baza cerintelor HG 201 și cuprinde:

a) Planificarea auditului.

- b) Realizarea procedurilor de audit la distanta (analiza regulamente, proceduri, ghiduri, structuri organizaționale, etc.).
- c) Finalizarea delimitării scopului: sisteme, infrastructură, Data Centre, procese.
- d) Executarea procedurilor de audit la fata locului (pentru fiecare entitate inclusă în scop în parte).
- e) Definirea constatărilor.
- f) Elaborarea recomandărilor și coordonarea acestora cu entitățile.
- g) Sistematizarea dovezilor de audit.
- h) Elaborarea Raportului final de audit.
- i) Prezentarea rezultatelor către AGE și entitatea în cauză.
- j) Realizarea activităților analitice și totalizatoare și prezentarea rezultatelor către sponsorii proiectului.

Durata activităților specifice, dar și a perioadei de evaluare vor varia considerabil pentru fiecare entitate, în dependență de dimensiunile acesteia, nivelul de maturitate în gestiunea TIC, dimensiunea și complexitatea acestora, termenii de livrare a informației și coordonare a constatărilor, etc. Luând în considerație cerințele înaintate în documentația de licitație vom respecta termenii și condițiile de livrare/prestare/executare solicitate: din data semnării contractului până la 30 decembrie 2019.

3. Echipa de proiect de bază și extinsă

Pentru realizarea proiectului și pentru a asigura o governanță eficientă a derulării misiunii de audit de securitate cibernetică am stabilit două echipe de bază cu doi auditori principali care vor gestiona membrii echipelor de audit.

Noi am propus așa abordare pentru a reuși derularea misiunilor de audit în timpul prestabilit de AGE luând în considerare numărului mare de entități care au intrat în scop și diversitatea nivelului de complexitate și maturitate.

Echipele create vor conține specialiști cu competențe în domenii specifice pentru a atinge obiectivele misiunii de audit stabilite. Aceasta abordare ne va permite să înțelegem și să acoperim tehnologiile utilizate de către instituțiile publice.

Experții cheie (auditorii principali) propuși pentru realizarea misiunii de audit sunt cei mai calificați specialiști în domeniul auditului, iar CV sunt atașate la ofertă. Membrii echipei de proiect vor constitui dintr-o serie de specialiști înalt calificați în domeniul securității cibernetice, securității informaționale, managementul tehnologiilor informaționale cu experiență confirmată, skill-uri tehnice și gestiunea proiectelor (de variată dimensiune și complexitate).

În concordanță cu achiziția publică inițiată noi am stabilit persoanele cheie ale proiectului conform pozițiilor cerute:

Poziție	Persoana
Audit Team Leader 1/Project Manager	Valeriu Cernei
Audit Team Leader 2	Dorin Carmanovici

Noi avem suficiente resurse și cunoștințe necesare să realizăm activitățile planificate. Abordarea dată ne va permite de a fi mai flexibili și a asigura livrarea livrabilelor în condiții de eficiență maximă și un nivel de calitate înalt.

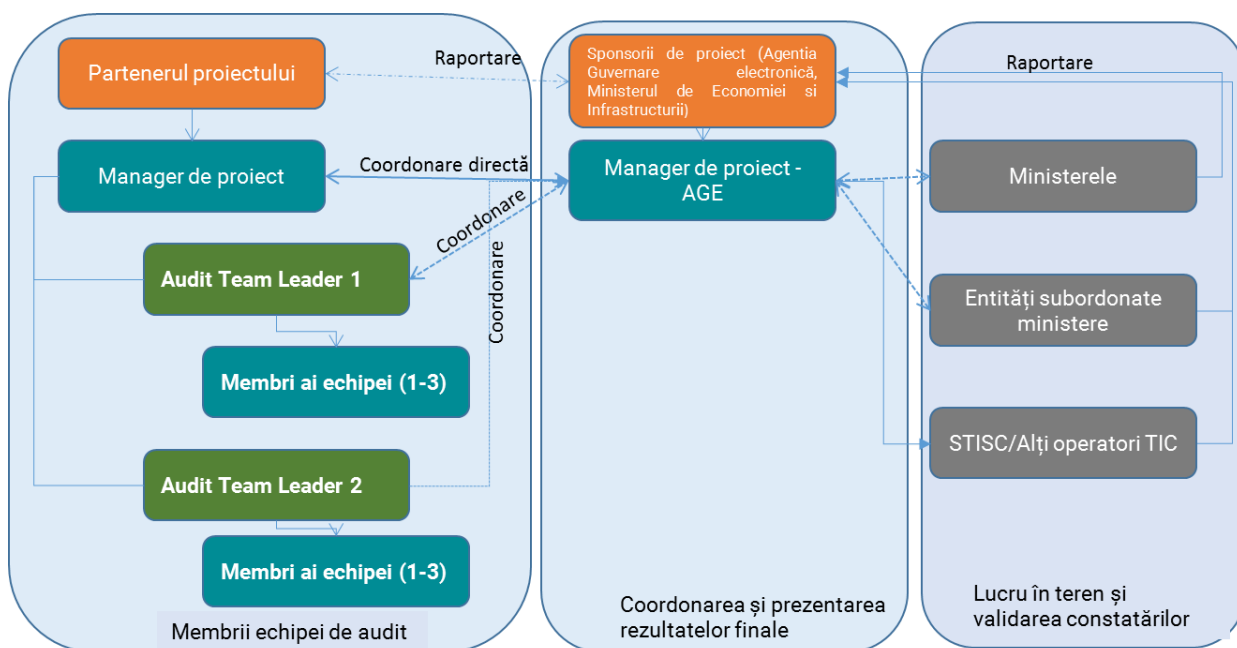
4. Guvernanță proiectului

Pentru a putea gestiona eficient proiectul, luând în considerare numărul mare de părți implicate este important de a stabili o structură de guvernanță pentru fiecare aspect/arie a proiectului.

Noi suntem flexibili de a ajusta guvernanța proiectului pentru a include toate părțile interesate în cadrul misiunii de audit.

O astfel de guvernanță va necesita coordonarea unei game largi de echipe din partea Sponsorilor de Proiect, Agenția de Guvernare Electronică, Ministere, Entități subordonate, etc.

Diagrama prezentată mai jos reprezintă o viziune de nivel înalt a interacțiunii dintre părțile implicate în audit, un nivel detaliat stabilit de rolurilor și modalitățile de interacțiune va fi realizat în etapa de Planificare a proiectului.



Persoana ce mai importantă în cadrul proiectului va fi Managerul de proiect din partea AGE (Șef Serviciu Calitatea și Securitatea Informației) ce va coordona toate activitățile și va fi un facilitator în organizarea interacțiunii cu toate instituțiile implicate în scopul de audit. Suplimentar, Managerul de proiect din partea AGE, împreună cu Managerul de proiect din partea BSD va fi persoana cheie de contact cu Sponsorii proiectului.

Luând în considerare numărul mare de ministere/entități subordonate noi am divizat echipa în două echipe de bază gestionare respectiv Audit Team Leader 1 și Audit Team Leader 2.

Managerul de proiect din partea BSD se va concentra pe gestiunea taskurilor pentru a se asigura că activitățile derulează conform activităților planificate. PM precum și Audit Team

Leaderii vor asigura liniile de comunicare cu echipa și responsabili din partea beneficiarului.

Numărul de persoane necesare pentru fiecare audit îl va stabili Audit Team Leader și vor comunica cu experții relevanți de la beneficiarii auditelor sau alți operatori TIC implicați.

5. Asigurarea calității

Procesul de asigurare a calității reprezintă o activitate integrată în cadrul proiectelor companiei noastre per ansamblu și pentru fiecare etapă separat. Aplicăm standardele internaționale și bunele practici aplicabile, implementând și aplicând cele mai relevante tehnici și metodologii în conformitate cu specificul proiectelor.

În cadrul companiei BSD Management este implementat și se aplică asupra întregului spectru de activități, un sistem integrat de management, bazat pe standardele ISO 9001:2015 și ISO 27001:2013 (copiile certificatelor sun incluse în ofertă).

Pentru proiectul prezent vom adapta metodologia de gestiune a proiectelor, încât să putem furniza un nivel maxim de calitate a rezultatelor. Structura și componența echipelor de proiect vor fi ajustat în acest scop, pentru fiecare domeniu specific în parte fiind furnizate resurse competente și performante.

VI. ANEXE

ANEXA 1: CERTIFICĂRI

Copiile certificatelor *ISO 9001:2015* și *ISO/IEC 27001:2013*

Copiile certificărilor individuale ale experților cheie.

ANEXA 2: SCRISORI DE RECOMANDARE

Copiile scrisorilor de recomandare prezentate separat și atașate la ofertă.

ANEXA 3: CURRICULUM VITAE

Curriculum Vitae a membrilor cheie sunt prezentate separat, pentru fiecare membru separat.