C. N. S. C.

# CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR

Str. Stavropoleos, nr. 6, sector 3, ... România, CIF 20329980, CP 030084
Tel. +4 021 3104641 Fax. +4 021 3104642 ; +4 021 8900745 www.cnsc.ro

**În conformitate cu prevederile art.266 alin.2) din OUG nr.34/ 2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, aprobată prin Legea nr. 337/2006, cu modificările şi completările ulterioare, Consiliul adoptă următoarea:**

## DECIZIE
**Nr. ...**
**Data: ...**

Pe rolul CNSC au fost înregistrate, sub nr. ... şi nr. ... contestaţiile formulate de ... şi ... referitoare la procedura de achiziţie, prin „licitaţie deschisă”, a contractului de achiziţie publică de servicii având ca obiect: „Servicii de consultanţă privind sistemele informatice în cadrul proiectului – ...– întărirea capacităţii instituţionale a ... în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale, prin implementarea de instrumente inovatoare – cod SMIS 36675”, cod CPV 72220000-3, 72611000-6, 72810000-1, sursa de finanţare: *„FSE – Programul Operaţional Dezvoltarea Capacităţii Administrative, Axa prioritară 2 – Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor publice, cu accentul pus pe procesul de descentralizare, Domeniul major de intervenţie: 2.2 Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor Operaţiunea: Implementarea iniţiativelor de reducere a duratei de livrare a serviciilor publice prin folosirea sistemelor informatice de management, respectiv semnătură electronică, arhivare electronică şi flux informatic unitar de raportare şi monitorizare*”, organizată de autoritatea contractantă ... cu sediul în ... ...

Prin contestaţia nr. 7/... înregistrată la CNSC cu nr...., formulată de ..., cu sediul în Municipiul ... ... având CUI: ... înregistrată la Oficiul Registrului Comerţului sub nr. ... reprezentată legal de ... împotriva documentaţiei de atribuire, s-a solicitat: „obligarea autorităţii contractante la adoptarea de măsuri corective cu privire la documentaţia de atribuire; în subsidiar, anularea procedurii".

Prin contestaţia nr. ... înregistrată la CNSC cu nr. ... formulată de către ... cu sediul în ... ... având CUI ... înregistrată la Oficiul Registrului Comerţului sub nr. ... reprezentată legal de ... împotriva documentaţiei de atribuire, s-a solicitat: „suspendarea procedurii de atribuire în cauză; în principal, modificarea cerinţelor de calificare şi selecţie de la pct. III.2.3.a din fişa de date a achiziţiei; în subsidiar, anularea procedurii."

Conform prevederilor art. 273, alin. (1) din OUG nr. 34/2006, aprobată prin Legea nr. 337/2006, cu modificările şi completările ulterioare, contestaţiile care fac obiectul dosarelor nr. ... şi nr. ... au fost conexate pentru a se pronunţa o soluţie unitară, deoarece acestea sunt formulate în cadrul aceleiaşi proceduri de atribuire.

În baza documentelor depuse de părţi,
CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR

**DECIDE:**

Admite, în parte, contestaţia formulată de ... în contradictoriu cu autoritatea contractantă ... astfel:

- dispune eliminarea de la cap. III.2.3.a) din fişa de date a achiziţiei, a cerinţei privind *„Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager – CISM;*

- respinge, ca nefondate, solicitările vizând eliminarea, din fişa de date a achiziţiei, a celorlalte cerinţe de calificare.

Respinge ca nefondată contestaţia formulată de ... în contradictoriu cu autoritatea contractantă ...

Respinge solicitările de anulare a procedurii de atribuire în cauză, remedierea documentaţiei de atribuire fiind posibilă fără încălcarea principiilor prevăzute la art. 2 alin. (2) lit. a) – f) din OUG nr. 34/2006, cu modificările şi completările ulterioare.

Obligă autoritatea contractantă la stabilirea unui nou termen limită pentru depunerea ofertelor, în conformitate cu dispoziţiile art. 72 din OUG nr. 34/2006, cu modificările şi completările ulterioare.

Dispune continuarea procedurii de atribuire în cauză prin aplicarea celor anterior dispuse, în termen de 10 zile de la comunicarea prezentei.

Prezenta decizie este obligatorie pentru părţi, în conformitate cu prevederile art. 280 alin. (1) şi (3) din OUG nr. 34/2006, cu modificările şi completările ulterioare.

Împotriva prezentei decizii se poate formula plângere în termen de 10 zile de la comunicare.

## MOTIVARE

În luarea deciziei s-au avut în vedere următoarele:

Prin contestaţia nr. 7/... înregistrată la CNSC cu nr...., formulată de ..., împotriva documentaţiei de atribuire, s-a solicitat: „obligarea autorităţii contractante la adoptarea de măsuri corective cu privire la documentaţia de atribuire; în subsidiar, anularea procedurii”.

Contestatorul precizează că autoritatea contractantă a încălcat prevederile art. 179 alin. (1) din OUG nr. 34/2006, solicitând prezentarea unor certificări numeroase, fără legătură cu obiectul contractului, vădit disproporţionate faţă de cerinţele generice ale caietului de sarcini, restricţionând accesul la procedura de achiziţie publică.

Pentru edificarea celor criticate, contestatorul face referire la obiectul contractului, aşa cum este acesta definit în caietul de sarcini, la punctul 3, arătând că cerinţele se referă strict la servicii de auditare, studiu de fezabilitate, proiect tehnic, derulare proces de achiziţie şi monitorizare pe durata implementării sistemului de semnătura digitală şi arhivare electronică şi nu la procesul efectiv de dezvoltare software de semnătură digitală şi arhivare electronică; practic, în caietul de sarcini sunt descrise numai activităţile de management de proiect şi nu activităţi privind realizarea efectivă a software-ului de semnătura digitală şi arhivare electronică.

Astfel, la pct III.2.3 a) - Capacitatea tehnică şi/sau profesională din anunţul de participare şi din fişa de date a achiziţiei, în vederea demonstrării capacităţii tehnice, autoritatea contractantă solicită prezentarea unei echipe de experţi formată din cel puţin 5 membri, din care 3 sunt lectori şi 2 sunt experţi IT, fiind omişi experţii cu atribuţii importante în derularea contractului, cum ar fi project managerul,

arhitectul de sistem, expertul în achiziţii etc. În susţinerea celor de mai sus, contestatorul prezintă cerinţele impuse de autoritatea contractantă pentru cei doi experţi IT, după cum urmează:
- *„Expert în securitatea informaţiei - 1 expert: Diploma de absolvire a studiilor universitare; minim 3 ani experienţă în domeniul Securităţii Informatice; capabilităţi şi certificări recunoscute internaţional în domeniul securităţii informatice: Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent); Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional- CSSLP) sau echivalent, Certificare independentă privind auditarea sistemelor informatice (Certified Information Systems Auditor (CISA) sau echivalent, Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager -CISM) sau echivalent*";
- certificările solicitate sunt disproporţionate faţă de cerinţele din caietul de sarcini, acestea suprapunându-se sau fiind chiar nejustificate în contextul caietului de sarcini.

În continuare, contestatorul prezintă într-un tabel comparativ, certificările solicitate şi care se suprapun – CISSP cu CSSLP, astfel:

| Certificarea **CSSLP** acoperă, conform documentației oficiale (vezi Anexa nr.l_CSSLP-Brochure.pdf), următoarele domenii: | Certificarea **CISSP** acoperă, conform documentației oficiale (Anexa nr.2_CISSP-WEB.pdf, certificare oferita de acelaşi furnizor ca si CSSLP), următoarele domenii: |
|---|---|
| ■ Secure Software Concepts<br>■ Secure Software Requirements<br>■ Secure Software Design<br>■ Secure Software Implementation/Coding<br>■ Secure Software Testing<br>■ Software Acceptance<br>■ Software Deployment, Operations, Maintenance and Disposal | ■ Access Control<br>■ Telecommunications and Network Security<br>■ Information Security Governance and Risk Management<br>■ Software Development Security<br>■ Cryptography<br>■ Security Architecture and Design<br>■ Operations Security<br>■ Business Continuity and Disaster Recovery Planning<br>■ Legal, Regulations, Investigations and Compliance<br>■ Physical (Environmental) Security |

În plus, arată contestatorul, potrivit specificaţiilor privind certificarea CISSP din Anexa nr.2_CISSP-WEB.pdf, în cadrul Software

Development Security, unul din subiectele tratate este Systems Development Life Cycle (SDLC). Ciclul de dezvoltare al sistemelor, conform definiţiei acceptate pe piaţa, acoperă următoarele faze: *„Preliminary Analysis; Systems analysis, requirements definition; Systems design; Development;Integration and testing; Acceptance, installation, deployment; Maintenance*", fiind astfel, evidentă suprapunerea aproape de identificare între domeniile CSSLP-ului şi cele acoperite în cadrul domeniului Software Development Security din CISSP.

Ţinând cont de cele anterior menţionate, contestatorul consideră că CSSLP este o certificare care permite o viziune mult mai detaliată a securităţii ciclului de dezvoltare software, dar acoperind în general, aceleaşi subiecte care sunt prezentate şi în cadrul certificării CISSP; acest nivel de detaliu este nejustificat pentru îndeplinirea reglementară a contractului, fiind în fapt o cerinţă disproporţionată faţă de obiectul acestuia. În plus, trebuie ţinut cont şi de numărul limitat de persoane certificate din punct de vedere al certificării CSSLP propriu-zise, în România existând o singură persoană certificată (confrom site-ului oficial al furnizoriului certificărilor CSSLP şi CISSP), în timp ce, la nivelul Europei, există mai puţin de 150 persoane certificate.

În ceea ce priveşte alte două certificări solicitate şi care se suprapun - CISSP cu CISM, contestatorul prezintă un tabel comparativ pentru cele două certificări, din care rezultă o suprapunere a domeniilor security governance, risk management, compliance, acestea fiind prezentate în ambele certificări:

| | |
|---|---|
| Certificarea CISSP (certificare oferita de acelaşi furnizor ca si CSSLP, conform Anexei nr.2_CISSP-WEB.pdf,), acopera urmatoarele domenii: | Certificarea CISM ( conform site-ului oficial al furnizorului http://www.isaca.org/Certification/CISM-Certified- Information-Security-Manager/Prepare-for-the-Exam/Job- Practice-Areas/Pages/default.aspx), domeniile acoperite sunt: |

| | |
|---|---|
| ▪ Access Control<br>▪ Telecommunications and Network Security<br>▪ Information Security Governance and Risk Management<br>▪ Software Development Security<br>▪ Cryptography<br>▪ Security Architecture and Design<br>▪ Operations Security<br>▪ Business Continuity and Disaster Recovery Planning<br>▪ Legal, Regulations, Investigations and Compliance<br>▪ Physical (Environmental) Security | ▪ Information Security Governance<br>▪ Information Risk Management and Compliance<br>▪ Information Security Program Development and Management<br>▪ Information Security Incident Management |

De asemenea, potrivit documentaţiei de atribuire certificarea CISM este considerată echivalentă cu specializarea de management a certificării CISSP, mai precis CISSP – ISSP, motiv pentru care solicitarea prezentării certificării CISM - Certified Information Security Manager - este disproporţionată faţă de cerinţele din caietul de sarcini, nivelul de cunoştinţe oferit de certificarea CISSP în domeniul managementului fiind mai mult decât acoperitoare pentru îndeplinirea reglementară a contractului.

Referitor la Expert în Servicii IT - 1 expert, pentru care se solicită următoarele: *„diploma de absolvire a studiilor universitare; minim 3 ani experienţa în domeniul IT&C; Certificat ITIL Expert v3 sau echivalent; Cunoaşterea metodologiei Six Sigma demonstrată prin participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metologii echivalente*", ţinând cont de cerinţele caietului de sarcini, contestatorul susţine că este imposibil a fi identificată vreo relaţie între scopul proiectului, serviciile de urmează a fi prestate de către expertul în servicii IT şi solicitările referitoare la cunoaşterea metodologiei Six Sigma.

În susţinerea afirmaţiilor de mai sus, contestatorul menţionează că:

- din documentaţia publica *Six Sigma* rezulta că aceasta reprezintă un set de instrumente şi bune practici în vederea îmbunătăţirii proceselor, creşterea calităţii şi minimizarea defectelor rezultate asociate, în cele mai multe cazuri cu zona de producţie, ceea ce defineşte maturitate la care a ajuns un proces. Maturitatea unui proces

de producţie poate fi descris printr-o rată sigma, care indică procentul de defecte pe care le generează;

- din cele de mai sus rezultă că aceste tehnici şi metodologia Six Sigma nu au nicio legătură cu caietul de sarcini sau cu scopul proiectului - descris în capitolul 3 - fiind acela de auditare, studiu de fezabilitate, proiect tehnic, documentaţie de atribuire, derulare proces de achiziţie şi monitorizare în implementarea sistemului de semnătură digitală şi arhivare electronică.

În ceea ce priveşte cerinţa prezentării ISO 27001, contestatorul precizează că în fişa de date a achiziţiei, se solicita, la Secţiunea - informaţii privind capacitatea tehnică, *„prezentarea documentelor emise de organisme naţionale sau internaţionale acreditate care confirmă respectarea standardelor de securitatea informaţiei, respectiv ISO 27001 sau echivalent*"; aceasta solicitare încălcând în mod flagrant prevederile art. 176 din OUG nr. 34/2006, cu modificările şi completările ulterioare, prin care legiuitorul dă posibilitatea autorităţii contractante de a aplica criterii de calificare şi selecţie referitoare numai la: *„a) situaţia personală a candidatului sau ofertantului; b) capacitatea de exercitare a activităţii profesionale; c) situaţia economică şi financiară; d) capacitatea tehnică şi/sau profesională; e) standarde de asigurare a calităţii; f)standarde de protecţie a mediului, în cazurile prevăzute la art. 188 alin. (2) lit. f) şi alin. (3) lit. e*)".

Având în vedere următoarele aspecte: caietul de sarcini se referă preponderent la activităţi de management de proiect decât la monitorizare tehnică din punct de vedere al securităţii informaţiei; ISO 27001 nu este un standard referitor la asigurarea calităţii şi nici referitor la protecţia mediului, contestatorul solicită eliminarea cerinţei în cauză.

Prin contestaţia nr. ... înregistrată la CNSC cu nr. ... formulată de către ... împotriva documentaţiei de atribuire, s-a solicitat: „suspendarea procedurii de atribuire în cauză; în principal, modificarea cerinţelor de calificare şi selecţie de la pct. III.2.3.a din fişa de date a achiziţiei; în subsidiar, anularea procedurii.".

... critică cerinţele autorităţii contractante cu privire la „Expert în securitatea informaţiei – 1 expert" şi la „Expert în Servicii IT – 1 expert", respectiv, toate cerinţele care fac referire la certificările Certified Information Systems Security Professional (CISSP) sau echivalent, Certified Secure Software Cycle Professional- CSSLP sau echivalent, Certified Information Systems Auditor (CISA) sau chivalent, Certified Information Security Manager -CISM sau echivalent, ITIL Expert v3 sau echivalent, cunoaşterea metodologiei Six Sigma demonstrată prin participarea la cel puţin un curs de instruire pentru

nivelul Green Belt sau a unei metodologii echivalente, cerinţe considerate a fi ilegale, întrucât niciuna dintre certificările solicitate nu este emisă de vreo autoritate publică competentă şi nici de vreun organism de drept public, astfel:
- certificarea ITIL este emisă de APM Group Ltd din Marea Britanie http://www.itil- officialsite.com, entitate care utilizează propria schemă de certificare şi propriile reguli de creditare a certificărilor, specific unei activităţi comerciale şi nu unei instituţii publice; nu există autorităţi publice sau organisme de drept public sau privat în sensul prevăzut de art. 177 alin. (1) din OUG nr. 34/2006, care să ofere certificări în domeniul managementului serviciilor IT, astfel încât, în speţa de faţă nu se poate impune obligativitatea prezentării certificărilor specifice, deoarece respectivele calificări nu sunt titluri de calificare oficială, fiind doar o formă de promovare a specialiştilor care doresc să fie cunoscuţi pentru experienţa şi cunoştinţele în domeniu;
- certificările Certified Information Systems Security Professional (CISSP) şi Certified Secure Dftware Lifecycle Professional (CSSLP) sunt emise de International Information Systems Security Certification Consortium, (ISC)2, https://www.isc2.org/CISSP, entitate care utilizează propria schemă de certificare şi propriile reguli de acreditare a certificărilor, specific unei activităţi comerciale şi nu unei instituţii publice; nu există autorităţi publice sau organisme de drept public sau privat în sensul prevăzut de art. 177 alin. (1) din OUG nr. 34/2006, care să ofere certificări strict în domeniul securităţii sistemelor informatice, astfel încât, în speţa de faţă nu se poate impune obligativitatea prezentării certificărilor specifice, deoarece respectivele calificări nu sunt titluri de calificare oficială, fiind doar o formă de promovare a specialiştilor care doresc să fie recunoscuţi pentru experienţa şi cunoştinţele în domeniu;
- certificările Certified Information Security Auditor (CISA) şi Certified Information Security Manager (CISM) ISACA sunt emise de ISACA, https://www.isaca.org, o fundaţie educaţională care promovează profesioniştii care doresc să fie recunoscuţi pentru experienţa şi cunoştinţele lor în domeniul guvernanţei IT şi a securităţii IT, fiind de asemenea o entitate care utilizează propria schema de certificare şi propriile reguli de acreditare a certificărilor, specific unei activităţi comerciale şi nu unei instituţii publice;
- Six Sigma este *„un set de unelte şi strategii pentru eficientizarea proceselor, dezvoltată iniţial de firma Motorola în anul 1985*" (informaţii extrase de la http://en.wikipedia.org/wiki/Six Sigma). Obiectivul Six Sigma este acela de a *„îmbunătăţi calitatea rezultatelor unui proces prin*

*dentificarea şi eliminarea cauzei defectelor (erorilor) şi prin minimizarea variaţiilor în cadrul proceselor de afaceri şi de producţie*"; nu există o standardizare a acestei netodologii, ea fiind adaptată de către fiecare organizaţie pornind de la nişte concepte de bază; de asemenea, nu există programe de formare sau de certificare standardizate, fiecare organizaţie care a dezvoltat cursuri în acest domeniu sau care a implementat conceptele Six Sigma utilizând propriile criterii de certificare.

De asemenea, contestatorul precizează că în cuprinsul caietului de sarcini, nu se regăseşte nici un fel de descriere a rolurilor şi a atribuţiilor experţilor solicitaţi, din care să reiasă eventuala relevanţă a certificărilor solicitate pentru aceşti experţi, astfel încât alegerea acestor certificări şi mai ales gruparea mai multor astfel de certificări în cadrul unui singur rol apare ca arbitrară, din perspectiva relevanţei, construită pentru a corespunde unei anumite persoane şi nu pentru a corespunde unei nevoi justificate a autorităţii contractante.

Totodată, contestatorul critică următoarele:

- solicitarea unor „Capabilităţi şi certificări recunoscute internaţional", în condiţiile în care acest proiect se va desfasura în România, iar recunoaşterea internaţională a unei anumite certificări nu poate fi o condiţie necesară pentru participarea unui expert la procedură, fiind suficientă o certificare naţională (dacă o astfel de certificare este prevăzută de legislaţia naţională ca fiind necesară pentru desfaşurarea unei anumite activităţi);
- cerinţele formulate pentru Expertul Infrastructură Hardware cu privire la dovedirea cunoaşterii unor anumite tehnologii (tehnologie de stocare a datelor de tip SAN, tehnologie de back-up a datelor, soluţie de virtualizare şi sistem de operare) printr-o certificare tehnică sau respectiv „certificare de specializare", deoarece nu există autorităţi publice sau organisme de drept public sau privat în sensul prevăzut de art. 177 alin. (1) din OUG nr. 34/2006 care să ofere certificări pentru anumite produse sau tehnologii IT, astfel încât, autoritatea contractantă nu poate impune obligativitatea prezentării certificărilor specifice, deoarece respectivele calificări nu sunt titluri de calificare oficială, motiv pentru care, contestatorul solicită înlocuirea cerinţelor de certificare cu cerinţe de experienţa teoretică (participarea la cursuri de specializare în domeniul tehnologiilor de stocare a datelor de tip SAN, în domeniul tehnologiilor de back-up al datelor, în domeniul tehnologiilor de virtualizare şi al sistemelor de operare) SAU de experienţă practică privind utilizarea respectivelor tehnologii.

Ca soluţie de remediere a aspectelor criticate anterior, contestatorul solicită eliminarea din fişa de date a tuturor cerinţelor cu privire la certificările solicitate şi reformularea cerinţelor astfel:

1. Expert în securitatea informaţiei - 1 expert: Diplomă de absolvire a studiilor universitare; Minim 3 ani experienţă în domeniul Securităţii Informatice
2. Expert în Servicii IT- 1 expert: Diplomă de absolvire a studiilor universitare; Minim 3 ani experienţă în domeniul IT&C.
3. Expert Infrastructură Hardware - 1 expert; Diploma de absolvire a studiilor universitare; Minim 3 ani experienţa in domeniul IT&C Capabilităţi şi cunoştinţe: Cunoaşterea a cel puţin 1 tehnologie de stocare a datelor de tip SAN (Storage Area Network) sau echivalent dovedita prin existenta unei experienţe similare anterioare de lucru cu astfel de tehnologii sau prin participarea la cursuri de instruire in domeniul tehnologiilor de stocare a datelor de tip SAN; Cunoaşterea a cel puţin 1 tehnologie de back-up a datelor, dovedite prin existenta unei experienţe similare anterioare de lucru cu astfel de tehnologii sau prin participarea la cursuri de instruire in domeniul tehnologiilor de back-up al datelor ISO 9001 REGISTERED c.2689.1 IS0 14001 REGISTERED m.1262.1;Cunoaşterea a cel puţin unei soluţii de virtualizare, dovedite prin existenta unei experienţe similare anterioare de lucru cu astfel de tehnologii sau prin participarea la cursuri de instruire in domeniul tehnologiilor de virtualizare; Cunoaşterea unui sistem de operare, dovedite prin existenţa unei experienţe similare anterioare de lucru cu astfel de tehnologii sau prin participarea la cursuri de instruire în domeniul sistemelor de operare.

În vederea soluţionării contestaţiei susmenţionate, Consiliul a solicitat autorităţii contractante, prin adresa nr. 6556/... 09.04.2013 şi adresa nr. 6580/... transmiterea dosarului achiziţiei publice în copie, întocmit conform precizărilor art. 213 din OUG nr. 34/2006, cu modificările şi completările ulterioare, precum şi punctul de vedere cu privire la contestaţia în cauză, potrivit dispoziţiilor art. 274 alin. (1) din acelaşi act normativ.

Prin adresa nr. 13128/... înregistrată la CNSC sub nr. 11663/11.04.2013, autoritatea contractantă transmite documentele solicitate, precum şi punctul de vedere cu privire la cele două contestaţii.

Prin punctul de vedere nr. 13127/... înregistrat la CNSC sub nr. 11664/11.04.2013, autoritatea contractantă solicită Consiliului respingerea ca nefondată a contestaţiei formulată de ..., din considerentele ce vor fi expuse mai jos.

În preambul, autoritatea contractantă precizează următoarele aspecte de ordin procedural: Proiectul *„e - ... - întărirea capacităţii instituţionale a ... în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale prin implementarea de instrumente inovatoare*”, Cod SMIS 36675 este derulat de ... în perioada 25.09.2012 - 25.09.2014, în conformitate cu ordinul de finaţare OMAI nr. 341 din 25.09.2012;

- Proiectul este finanţat din Fondul Social European prin Programul Operaţional - Dezvoltarea Capacităţii Administrative - Axa prioritară 2 îmbunătăţirea calităţii şi eficienţei furnizării serviciilor publice, cu accentul pus pe procesul de descentralizare, Domeniul major de intervenţie: 2.2 Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor Operaţiunea: Implementarea iniţiativelor de reducere a duratei de livrare a serviciilor publice prin folosirea sistemelor informatice de management, respectiv semnătură electronică, arhivare electronică şi flux informatic unitar de raportare şi monitorizare;

- scopul acestui proiect este dezvoltarea de instrumente inovatoare referitoare la utilizarea semnăturii electronice la nivelul administraţiei publice centrale şi locale şi arhivarea electronică a documentaţiei existente în arhiva ...;

- importanţa proiectului, în contextul descentralizării administrative, a îmbunătăţirii calităţii şi eficienţei furnizării serviciilor publice, necesitatea adaptării continue a administraţiei publice la progresul tehnologic, valoarea acestuia, precum şi obiectivele şi rezultatele aşteptate de autoritatea contractantă, pe de o parte, şi cerinţele caietului de sarcini, pe de altă parte, impun stabilirea şi aplicarea unor criterii de calificare multiple şi adecvate care să demonstreze potenţialul fiecărui operator economic participant la procedură, respectiv posibilitatea concretă de a îndeplini acest contract şi de a rezolva eventualele dificultăţi legate de îndeplinirea acestuia.

Referitor la documentaţia de atribuire pentru *„Servicii de consultanţă privind sistemele informatice în cadrul proiectului "e - ... - întărirea capacităţii instituţionale a ... în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale prin implementarea de instrumente inovatoare*”, Cod SMIS 36675, autoritatea contractantă menţionează ca aceasta a fost publicată iniţial în SEAP sub nr. ..., în vederea verificării de către ANRMAP în data de

06.03.2013; ANRMAP, exercitându-şi atribuţiile de verificare a documentaţiilor postate în SEAP, a decis respingerea acestuia şi modificarea cerinţelor de calificare şi selecţie în conformitate cu prevederile legale. Astfel, luând în considerare observaţiile reprezentanţilor ANRMAP, s-au realizat modificările solicitate iar Documentaţia de atribuire a fost repostată, aceasta fiind acceptată decis acceptarea ei sub nr. 84750/20.03.2013. Ca urmare a acceptării documentaţiei, a fost publicat anunţul de participare nr. ... şi publicat în SEAP în data de 26.03.2013; de asemenea, anunţul de participare a fost publicat în JOUE sub nr.....

Referitor la cerinţele minime obligatorii privind experienţa profesională a experţilor cheie – *„Expert în securitatea informaţiei: a) Diplomă de absolvire a studiilor universitare; b) Minim 3 ani experienţă în domeniul Securităţii Informatice. Capabilităţi şi certificări recunoscute internaţional în domeniul securităţii informatice: c) Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent); d) Certificare independentă privind securitatea aplicata la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professiona l- CSSLP) sau echivalent; e) Certificare independenta privind auditarea sistemelor informatice (Certified Information Systems Auditor (CISA) sau echivalent; f) Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager -CISM) sau echivalent*”, autoritatea contractantă precizează că îndeplinirea cumulativă a cerinţelor este necesară deoarece expertul în securitatea informaţiei va coordona activitatea de audit a sistemului informatic solicitată în proiect, atât din punct de vedere al infrastructurii hardware şi de comunicaţii, al aplicaţiilor informatice, precum şi al politicilor şi procedurilor de lucru, realizarea unui studiu privind serverele disponibile precum şi întocmirea documentaţiei în vederea achiziţiei echipamentelor software şi hardware şi a licenţelor aferente pentru buna implementare a proiectului, inclusiv cerinţe pentru: amenajarea unui DataCenter la nivel ... cu dotările corespunzătoare; amenajarea unei camere securizată şi ingnifugă pentru depozitarea suporturilor electronice de stocare rezultate în urma arhivării electronice; analiza fluxurilor informatice existente în cadrul ...; propuneri privind remodelarea/actualizarea fluxurilor informatice prin raportare la cadrul legal existent, respectiv structura organizaţională, cadrul legal de funcţionare, atribuţii şi competenţe instituţionale; specificaţiile tehnice pentru echipamentele IT; implementarea semnăturii electronice şi a

mărcii temporale la nivelul ...; implementarea arhivei electronice la nivelul ...; instruirea personalului propriu ...; realizarea de manuale de utilizare a semnăturii electronice şi a arhivei electronice.

În susţinerea afirmaţiilor de mai sus, autoritatea contractantă aduce următoarele argumente:

- dinamica de dezvoltare a tehnologiilor, sistemelor si aplicaţiilor specifice IT este foarte mare, astfel încât evoluţia acestora, de-a lungul a 3-5 ani, este substanţială şi profundă;
- progresul tehnologic extrem de alert din industria IT, impune experţilor din domeniu, ca în permanenţă să îşi actualizeze cunoştinţele şi, prin participare la realizarea de proiecte, să-şi dezvolte abilităţile. Complexitatea tot mai mare a instrumentelor IT şi diversitatea soluţiilor posibile, fac ca timpul necesar pentru a le cunoaşte foarte bine şi a le putea implementa cu succes în proiecte de anvergură, să fie de cel puţin 3 ani. Această perioadă de implicare directă, de experienţa efectivă, este de natură să diminueze riscul alocarii, de către ofertant, a unei persoane inadecvate gradului de complexitate a proiectului;
- pentru realizarea auditului sistemului informatic certificările CISA sau echivalent, care atestă capacitatea de realizare a auditurilor asupra sistemelor informatice, şi CSSLP sau echivalent care atestă capacitatea de evaluare a aplicaţiilor software, a ciclului de dezvoltare şi implementare în sistem, sunt absolut necesare;
- pentru a se obţine o imagine obiectivă asupra sistemului, a aplicaţiilor şi proiectelor viitoare, precum şi pentru evaluarea infrastructurii hardware şi elaborarea documentaţiei de atribuire, este necesar ca expertul în securitatea informaţiei să deţină experienţa şi expertiza dovedite, care să demonstreze capabilităţile sale de a avea o viziune globală asupra tuturor aspectelor şi elementelor necesare realizării sistemului;
- pentru a demonstra acest lucru, este necesar ca ofertantul să nominalizeze pentru acest rol o persoană calificată corespunzător, respectiv certificată CISSP sau echivalent; această certificare presupune deţinerea unei expertize tehnice recunoscute la nivel internaţional;
- expertul în securitatea informaţiei va coordona, de asemenea, întreaga derulare a proiectului informatic, inclusiv activitatea Coordonatorului de formare;
- pentru asigurarea unei viziuni globale privind realizarea proiectului, este necesar ca ofertantul să nominalizeze pentru acest rol, o persoană calificată corespunzător, respectiv certificată CISM (Certified Information Security Manager) sau echivalent;

- aceasta certificare presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în coordonarea tehnică, construirea şi gestionarea sistemelor informatice complexe, de mari dimensiuni.

Referitor la cerinţele minime obligatorii privind experrienţa profesională a experţilor cheie – *„Expert în Servicii IT: a) Diplomă de absolvire a studiilor universitare; b) Minim 3 ani experienţă în domeniul IT&C; c) Certificat ITIL Expert v3 sau echivalent; d) Cunoasterea metodologiei Six Sigma demonstrată prin participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metodologii echivalente*", autoritatea contractantă precizează că îndeplinirea cumulativă a cerinţelor este necesară deoarece expertul în servicii IT va fi direct implicat atât în evaluarea sistemului informatic existent şi a fluxurilor informatice din ..., realizarea de propuneri privind remodelarea/actualizarea fluxurilor informatice, prin raportare la cadrul legal existent, respectiv structura organizatională, cadrul legal de funcţionare, atribuţii şi competenţe instituţionale; cât şi în realizarea documentaţiei de atribuire.

Totodată, în susţinerea celor de mai sus, autoritatea contractantă precizează următoarele:

- dinamica de dezvoltare a tehnologiilor, sistemelor şi aplicaţiilor specifice IT este foarte mare, astfel încât evoluţia acestora, de-a lungul a 3-5 ani, este substanţială şi profundă; progresul tehnologic extrem de alert din industria IT, impune experţilor din domeniu, ca în permanenţă să îşi actualizeze cunoştinţele şi, prin participare la realizarea de proiecte, să-şi dezvolte abilităţile;
- complexitatea tot mai mare a instrumentelor IT şi diversitatea soluţiilor posibile, fac ca timpul necesar pentru a le cunoaşte foarte bine şi a le putea implementa cu succes în proiecte de anvergură, să fie de cel puţin 3 ani; această perioadă de implicare directă, de experienţă efectivă, este de natură să diminueze riscul alocării, de către ofertant, a unei persoane inadecvate gradului de complexitate a proiectului;
- pentru obţinerea unei evaluări profesioniste a serviciilor oferite de sistemul informatic al ..., a fluxurilor de lucru existente şi pentru realizarea de propuneri de îmbunătăţire, remodelare şi actualizare a fluxurilor de lucru este necesar ca ofertantul să nominalizeze pentru acest rol o persoana calificată corespunzător, respectiv certificată ITIL Expert v3 sau echivalent; această certificare presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în utilizarea standardelor şi a bunelor practici recunoscute în ceea ce priveşte managementul serviciilor IT;

- remodelarea fluxurilor de lucru din cadrul ... necesită expertiză în ceea ce priveşte evaluarea proceselor de afaceri şi îmbunătăţirea calităţii acestora; astfel, este necesar ca ofertantul să nominalizeze pentru acest rol o persoană calificată corespunzător, care să cunoască o metodologie de lucru recunoscută internaţional, aşa cum este metodologia Six Sigma, sau o metodologie echivalentă. Pentru a demonstra cunoaşterea metodologiei este necesar ca expertul să fi participat la cel puţin un curs de instruire pentru nivelul Green Belt al metodologiei Six Sigma, sau un nivel corespunzător metodologiei echivalente propuse.

Faţă de solicitările constestatorului, autoritatea contractantă precizează următoarele :

- îndeplinirea cerinţelor acoperă aria de expertiză necesară pentru execuţia corespunzătoare a tuturor activităţilor contractului, pornind de la necesitatea realizării unei evaluări profesioniste a serviciilor oferite de sistemul informatic al ..., a fluxurilor de lucru existente, pentru realizarea unei analize diagnostic corecte ce va sta la baza propunerilor de îmbunătăţire, remodelare şi actualizare a fluxurilor de lucru, a spaţiilor de lucru şi a instrumentelor/echipamentelor hardware şi software astfel încât să se poată implementa sistemul de semnătură digitală la nivelul ... şi a 1.930 de autorităţi şi instituţii publice şi arhivare electronică a documentelor;
- faptul că proiectul se implementează la nivelul a 1.930 de autorităţi şi instituţii publice, parte din totalul autorităţilor şi instituţiilor publice cu care ... relaţionează în gestionarea, la nivel de ţară, a funcţiei publice şi a funcţionarilor publici implică o securitate ridicată şi o procesare complexă a datelor şi informaţiilor care intră în posesia Agenţiei;
- complexitatea şi unicitatea proiectului, necesitatea utilizării eficiente a fondurilor publice, inclusiv nerambursabile, importanţa strategică a acestuia prin raportare la numărul mare de autorităţi şi instituţii publice pe care le va gestiona, inclusiv prin operarea datelor cu caracter personal, faptul că sistemul de management al funcţiei publice este infrastructură critică au impus solicitarea unor certificări adecvate, dar care au fost lăsate deschise posibilităţii de echivalare;
- privitor la afirmaţia contestatorului „*solicitarea a numeroase certificări, cerinţe sunt disproporţionate în raport cu natura şi complexitatea contractului*”, aceasta este nejustificată, întrucât se poate dovedi complexitatea contractului prin prezentarea de date statistice, conform Raportului managementului funcţieipublice, care atestă cantitatea şi complexitatea datelor şi informaţiilor pe care Agenţia le gestionează;

- ... (...) este principala instituţie responsabilă pentru managementul funcţiei publice şi al funcţionarilor publici, având ca principală misiune *„crearea şi dezvoltarea unui corp de funcţionari publici profesionist, stabil şi imparţial*" şi *„aplicarea strategiilor şi a Programului de guvernare în domeniul managementului funcţiei publice şi al funcţionarilor publici, cât şi în domeniul formării profesionale a personalului din administraţia publică*";
- în anul 2012, conform Raportului anual de activitate, http://www.....gov.ro/PaginaContinut.aspx?Id=254, activitatea Agenţiei în domeniului managementului funcţiilor publice şi al funcţionarilor publici s-a axat pe realizarea evidenţei naţionale a funcţiilor publice şi a funcţionarilor publici prin intermediul sistemului informaţional integrat existent la nivelul Agenţiei precum şi pe implementarea sistemului privind semnătura electronică, în relaţia cu instituţiile publice, pentru facilitarea proceselor de transmitere a datelor;
- de asemenea, s-a realizat accesul la portalul de management al tuturor autorităţilor şi instituţiilor publice ale căror structuri sunt gestionate prin intermediul sistemului;
- numărul total al funcţionarilor publici la sfârşitul anului 2012 este 132.417 şi reprezintă 1.41% din populaţia ocupată a României (9,36 milioane, conform datelor publicate de Institutul Naţional de Statistică pentru trimestrul II al anului 2012); numărul total de funcţii publice (161.583) şi ponderea acestora pe niveluri administrativ-teritoriale cu defalcare pe funcţii publice ocupate şi vacante pentru anul 2012; la sfârşitul lunii decembrie 2010 erau înregistrate în baza de date 4.270 de instituţii; la momentul februarie 2013 sunt înregistrate în bază 4.430 instituţii; pe parcursul anului 2012, numărul autorităţilor şi instituţiilor publice ale căror structuri de funcţii publice sunt gestionate prin intermediul sistemului informaţional integrat a crescut de la 4.423 la 4.485, reprezentând peste 99 % din autorităţile şi instituţiile publice din România care deţin în acest moment astfel de structuri;
- în anul 2012 au fost extinse funcţiile ..., cu implicaţii pentru proiectarea şi dezvoltarea modulului de generare şi gestiune a cazierelor administrative, dezvoltarea de noi facilităţi în cadrul modulului de gestiune a concursurilor şi implementare semnăturii electronice, care facilitează transmiterea documentelor semnate electronic între ... şi alte instituţii publice;
- în perioada de referinţă, au fost efectuate un număr de 229.641 de operaţiuni pentru actualizarea bazei de date (inclusiv validarea acestora), în urma transmiterii datelor de către autorităţile şi instituţiile publice; în urma operaţionalizării portalului de management al funcţiilor

publice şi funcţionarilor publici, până la sfârşitul anului 2012, toate autorităţile şi instituţiile publice ce deţin structuri de funcţii publice au primit acces pentru vizualizarea propriilor structuri înregistrate în sistemul informaţional integrat;
- de asemenea, fluxul de transmitere şi recepţionare a datelor privind evidenţa funcţiilor publice se efectuează prin intermediul portalului; astfel, în această perioadă, numărul de operaţiuni de transfer de date desfăşurate între ... şi instituţiile publice prin intermediul portalului de management al funcţiilor publice şi funcţionarilor publici a fost de 33.604 fişiere transmise de către instituţiile publice către Agenţie prin portal, respectiv 3.053 mesaje preluate de la instituţiile publice prin intermediul acestuia; în perioada 3 ianuarie - 28 decembrie 2012 au fost operate un număr de 152.597 de operaţiuni (inclusiv cele prin intermediul portalului, şi fară a fi numărate aici şi validările operaţiunilor);
- astfel, în anul 2012, se poate concluziona că în vederea realizării unui sistem unitar din punct de vedere al tehnologiei informaţiei şi comunicaţiilor, la nivelul Agenţiei au fost elaborate Procedurile Operaţionale de Securitate specifice sistemelor informatice ce vehiculează informaţii clasificate;
- în ceea ce priveşte activitatea de implementare a soluţiilor software, care să sprijine activitatea Agenţiei, accentul a fost pus pe extinderea funcţionalităţilor ... cât şi pe extinderea funcţionalităţilor Portalului de management al ... (https://www.....gov.ro).

În ceea ce priveşte solicitarea contestatorului de eliminare a cerinţei privind prezentarea Certificatului ISO 27001 sau echivalent, autoritatea contractantă precizează următoarele:
- auditul de securitate este definit ca fiind multitudinea de teste de audit realizate de către auditor asupra unui sistem sau componente IT&C şi care vizează identificarea conformităţii măsurilor implementate cu măsurile de securitate contractate de către achizitor şi cu standardele internaţionale în vigoare;
- în cadrul auditului, se vor lua în considerare normele de securitate fizică şi logică, conforme standardelor ISO 27001 sau echivalente;
- auditul de securitate va certifica starea la momentul realizării acestuia, a unui sistem sau componente IT&C, din punct de vedere al securităţii IT;
- auditul de securitate nu este destinat, şi nu va lua locul unui plan de securitate informaţională a organizaţiei, ci îşi propune să reflecte în mod cât mai detaliat climatul general de securitate, inclusiv analiza planului şi politicilor de securitate;

- procedura de atribuire în cauză, are ca obiective: achiziţionarea de servicii de audit informatic, consultanţă în vederea elaborării documentaţiei tehnice de proiectare pentru implementarea sistemului de semnătura digitală şi arhivarea electronică, servicii de formare şi nu de consultanţă pentru management de proiect.

În consecinţă, autoritatea contractantă solicită Consiliului respingerea ca nefondată şi lipsită de obiect a contestaţiei.

Prin punctul de vedere nr. 13018/... înregistrat la CNSC sub nr. 11665/11.04.2013, autoritatea contractantă solicită respingerea contestaţiei formulată de ... din considerentele ce vor fi expuse mai jos.

Referitor la solicitarea contestatorului privind obligarea luării măsurilor de remediere cu referire la modificarea cerinţelor de calificare şi selecţie de la punctul. III. 2.3 a) - Capacitatea tehnică şi sau profesională din fişa de date a achiziţiei, autoritatea contractantă o consideră ca fiind nefondată.

Privitor la cerinţele minime obligatorii privind experienţa profesională a experţilor cheie – *„Expert în securitatea informaţiei: a) Diplomă de absolvire a studiilor universitare; b) Minim 3 ani experienţă în domeniul Securităţii Informatice. Capabilitati şi certificări recunoscute internaţional în domeniul securitatii informatice; c) Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent); d) Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional- CSSLP) sau echivalent; e) Certificare independentă privind auditarea sistemelor informatice (Certified Information Systems Auditor (CISA) sau echivalent; f) Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager -CISM) sau echivalent*”, autoritatea contractantă precizează că îndeplinirea cumulativă a cerinţelor este necesară deoarece expertul în securitatea informaţiei va coordona activitatea de audit a sistemului informatic solicitată în proiect, atât din punct de vedere al infrastructurii hardware şi de comunicaţii, al aplicaţiilor informatice, precum şi al politicilor şi procedurilor de lucru, realizarea unui studiu privind serverele disponibile precum şi întocmirea documentaţiei în vederea achiziţiei echipamentelor software şi hardware şi a licenţelor aferente pentru buna implementare a proiectului, inclusiv cerinţe pentru:

- amenajarea unui DataCenter la nivel ... cu dotările corespunzătoare;

- amenajarea unei camere securizată şi ignifugă pentru depozitarea suporturilor electronice de stocare rezultate în urma arhivării electronice;
- analiza fluxurilor informatice existente în cadrul ...;
- propuneri privind remodelarea/actualizarea fluxurilor informatice prin raportare la cadrul legal existent, respectiv structura organizaţională, cadrul legal de funcţionare, atribuţii şi competenţe instituţionale;
- specificaţiile tehnice pentru echipamentele IT;
- implementarea semnăturii electronice şi a mărcii temporale la nivelul ...;
- implementarea arhivei electronice la nivelul ...;
- instruirea personalului propriu ...;
- realizarea de manuale de utilizare a semnăturii electronice şi a arhivei electronice.

De asemenea, subliniază că:

- dinamica de dezvoltare a tehnologiilor, sistemelor şi aplicaţiilor specifice IT este foarte mare, astfel încât evoluţia acestora, de-a lungul a 3-5 ani, este substanţială şi profundă;
- progresul tehnologic extrem de alert din industria IT, impune experţilor din domeniu, ca în permanenţă să îşi actualizeze cunoştinţele şi, prin participare la realizarea de proiecte, să-şi dezvolte abilităţile;
- complexitatea tot mai mare a instrumentelor IT şi diversitatea soluţiilor posibile, fac ca timpul necesar pentru a le cunoaşte foarte bine şi a le putea implementa cu succes în proiecte de anvergură, să fie de cel puţin 3 ani;
- această perioadă de implicare directă, de experienţa efectivă, este de natură să diminueze riscul alocarii, de către ofertant, a unei persoane inadecvate gradului de complexitate a proiectului;
- pentru realizarea auditului sistemului informatic certificările CISA sau echivalent, care atestă capacitatea de realizare a auditurilor asupra sistemelor informatice, şi CSSLP sau echivalent care atestă capacitatea de evaluare a aplicaţiilor software, a ciclului de dezvoltare şi implementare în sistem, sunt absolut necesare;
- pentru a se obţine o imagine obiectivă asupra sistemului, a aplicaţiilor şi proiectelor viitoare, precum şi pentru evaluarea infrastructurii hardware şi elaborarea documentaţiei de atribuire, este necesar ca expertul în securitatea informaţiei să deţină experienţa şi expertiza dovedite, care să demonstreze capabilităţile sale de a avea o viziune globală asupra tuturor aspectelor şi elementelor necesare realizării sistemului. Pentru a demonstra acest lucru, este necesar ca ofertantul să nominalizeze pentru acest rol o persoană calificată corespunzător,

respectiv certificată CISSP sau echivalent. Această certificare presupune deţinerea unei expertize tehnice recunoscute la nivel internaţional;
- expertul în securitatea informaţiei va coordona, de asemenea, întreaga derulare a proiectului informatic, inclusiv activitatea Coordonatorului de formare;
- pentru asigurarea unei viziuni globale privind realizarea proiectului, este necesar ca ofertantul să nominalizeze pentru acest rol, o persoană calificată corespunzător, respectiv certificată CISM (Certified Information Security Manager) sau echivalent. Aceasta certificare presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în coordonarea tehnică, construirea şi gestionarea sistemelor informatice complexe, de mari dimensiuni.

Privitor la cerinţele minime obligatorii pentru experienţa profesională a experţilor cheie *„Expert în Servicii IT: a) Diplomă de absolvire a studiilor universitare; b) Minim 3 ani experienţa în domeniul IT&C; c) Certificat ITIL Expert sau echivalent; d) Cunoasterea metodologiei Six Sigma demonstrată prin participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metodologii echivalente*", autoritatea contractantă menţionează că îndeplinirea cumulativă a cerinţelor este necesară deoarece expertul în servicii IT va fi direct implicat atât în evaluarea sistemului informatic existent şi a fluxurilor informatice din ..., realizarea de propuneri privind remodelarea/actualizarea fluxurilor informatice, prin raportare la cadrul legal existent, respectiv structura organizaţională, cadrul legal de funcţionare, atribuţii şi competenţe instituţionale; cât şi în realizarea documentaţiei de atribuire.

Totodată, subliniază că:
- dinamica de dezvoltare a tehnologiilor, sistemelor şi aplicaţiilor specifice IT este foarte mare, astfel încât evoluţia acestora, de-a lungul a 3-5 ani, este substanţială şi profundă;
- progresul tehnologic extrem de alert din industria IT, impune experţilor din domeniu, ca în permanenţă să îşi actualizeze cunoştinţele şi, prin participare la realizarea de proiecte, să-şi dezvolte abilităţile.;
- complexitatea tot mai mare a instrumentelor IT şi diversitatea soluţiilor posibile, fac ca timpul necesar pentru a le cunoaşte foarte bine şi a le putea implementa cu succes în proiecte de anvergură, să fie de cel puţin 3 ani. Această perioadă de implicare directă, de experienţă efectivă, este de natură să diminueze riscul alocării, de către ofertant, a unei persoane inadecvate gradului de complexitate a proiectului;

- pentru obţinerea unei evaluări profesioniste a serviciilor oferite de sistemul informatic al ..., a fluxurilor de lucru existente şi pentru realizarea de propuneri de îmbunătăţire, remodelare şi actualizare a fluxurilor de lucru este necesar ca ofertantul să nominalizeze pentru acest rol o persoana calificată corespunzător, respectiv certificată ITIL Expert v3 sau echivalent. Această certificare presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în utilizarea standardelor şi a bunelor practici recunoscute în ceea ce priveşte managementul serviciilor IT;
- remodelarea fluxurilor de lucru din cadrul ... necesită expertiză în ceea ce priveşte evaluarea proceselor de afaceri şi îmbunătăţirea calităţii acestora; astfel, este necesar ca ofertantul să nominalizeze pentru acest rol o persoană calificată corespunzător, care să cunoască o metodologie de lucru recunoscută internaţional, aşa cum este metodologia Six Sigma, sau o metodologie echivalentă;
- pentru a demonstra cunoaşterea metodologiei este necesar ca expertul să fi participat la cel puţin un curs de instruire pentru nivelul Green Belt al metodologiei Six Sigma, sau un nivel corespunzător metodologiei echivalente propuse.

Privitor la cerinţele minime obligatorii pentru „*Expert Infrastructura Hardware: a) Diploma de absolvire a studiilor universitare; b) Minim 3 ani experienţa în domeniul IT&C Capabilităţi şi certificări recunoscute internaţional; c) Certificat ITIL Foundation v3 sau echivalent; d) Cunoaşterea a cel puţin 1 tehnologie de stocare a datelor de tip SAN (Storage Area Network) sau echivalent dovedită prin deţinerea de certificări tehnice; e) Cunoaşterea a cel puţin 1 tehnologie de back-up a datelor, dovedite prin deţinerea de certificări tehnice; f) Cunoaşterea a cel puţin unei soluţii de virtualizare, dovedite prin deţinerea a cel puţin unei certificări tehnice; g) Certificare de specializare într-un sistem de operare*”, autoritatea contractantă menţionează că îndeplinirea cumulativă a cerinţelor este necesară, deoarece expertul în infrastructură hardware va fi direct implicat, atât în realizarea unui studiu privind serverele disponibile şi spaţiul special amenajat pentru acestea, cât şi în realizarea documentaţiei de licitaţie în vederea achiziţionării echipamentelor software şi hardware şi a licenţelor aferente pentru buna implementare a proiectului, inclusiv cerinţe pentru amenajarea unui DataCenter la nivel ... cu dotările corespunzătoare şi amenajarea unei camere securizată şi ingnifugă pentru depozitarea suporturilor electronice de stocare rezultate în urma arhivării electronice.

De asemenea, autoritatea contractantă precizează că:

- pentru obţinerea unei evaluări profesioniste a infrastructurii hardware a ... şi a necesităţilor pentru amenajarea unui nou data center şi a unei camere securizată şi ignifugă, precum şi a cerinţelor privind migrarea în noul centru de date este necesar ca ofertantul să nominalizeze pentru acest rol o persoană calificată corespunzător, respectiv certificată ITIL Expert v3 sau echivalent;
- această certificare presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în utilizarea standardelor şi a bunelor practici recunoscute mondial în ceea ce priveşte managementul serviciilor IT şi în ceea ce priveşte infrastructura hardware;
- pentru a putea evalua corespunzător sistemele existente pe piaţă şi a propune cele mai bune soluţii privind noua infrastructură hardware, este necesar ca Expertul infrastructura hardware să poată realiza o evaluare obiectivă din punct de vedere tehnologic al celor mai noi soluţii de pe piaţă;
- ofertantul trebuie să nominalizeze pentru acest rol o persoană calificată corespunzător care să deţină expertiză în cel puţin 1 tehnologie diferită pentru următoarele domenii de interes: Tehnologii de stocare a datelor de tip SAN (Storage Area Network), dovedită prin deţinerea de certificări tehnice. Tehnologii de back-up a datelor, dovedite prin deţinerea de certificări tehnice;
- expertul infrastructură hardware trebuie să demonstreze cunoaşterea a cel puţin unei soluţii de virtualizare, dovedite prin deţinerea a cel puţin unei certificări tehnice. Acest lucru este necesar pentru a putea evalua şi propune, daca este cazul, ca noua infrastructură instalată în centrul de date să folosească resurse virtualizate în loc de a utiliza echipamente hardware dedicate pentru fiecare server;
- certificare de specializare într-un sistem de operare este necesară pentru a demonstra experienţa lucrului cu aceste sisteme de operare la nivel enterprise, posibilităţile de migrare în centre de date noi precum si realizarea de back-up şi restaurare a sistemului.

Faţă de propunerile de modificare a cerinţelor pentru experţii IT prezentate de contestator, autoritatea contractantă consideră că îndeplinirea cerinţelor propuse de acesta, nu acoperă aria de expertiză necesară pentru execuţia corespunzătoare a tuturor activităţilor contractului, pornind de la necesitatea realizării unei evaluări profesioniste a serviciilor oferite de sistemul informatic al ..., a fluxurilor de lucru existente, pentru realizarea unei analize diagnostic corecte ce va sta la baza propunerilor de îmbunătăţire, remodelare si actualizare a fluxurilor de lucru, a spaţiilor de lucru şi a

instrumentelor/echipamentelor hardware şi software astfel încât să se poată implementa sistemul de semnătură digitala la nivelul ... şi a 1.930 de autorităţi şi instituţii publice şi arhivare electronică a documentelor.

De asemenea, în susţinerea punctului său de vedere, autoritatea contractantă precizează următoarele aspecte:

- faptul ca proiectul se implementează la nivelul a 1.930 de autorităţi şi instituţii publice, parte din totalul autorităţilor şi instituţiilor publice cu care ... relaţionează în gestionarea, la nivel de ţară, a funcţiei publice şi a funcţionarilor publici implică o securitate ridicată şi o procesare complexă a datelor şi informaţiilor care intră în posesia Agenţiei;
- complexitatea şi unicitatea proiectului, necesitatea utilizării eficiente a fondurilor publice, inclusiv nerambursabile, importanţa strategică a acestuia prin raportare la numărul mare de autorităţi şi instituţii publice pe care le va gestiona, inclusiv prin operarea datelor cu caracter personal, faptul că sistemul de management al funcţiei publice este infrastructură critică, au impus solicitarea unor certificări adecvate, dar care au fost lăsate deschise posibilităţii de echivalare;
- astfel, menţiunea contestatorului *„solicitarea a numeroase certificări, cerinţe sunt disproporţionate in raport cu natura si complexitatea contractului*" este considerată a fi nejustificată, întrucât se poate dovedi complexitatea contractului prin prezentarea de date statistice, conform Raportului managementului funcţiei publice, care atestă cantitatea şi complexitatea datelor şi informaţiilor pe care Agenţia le gestionează;
- ... (...) este principala instituţie responsabilă pentru managementul funcţiei publice şi al funcţionarilor publici, având ca principală misiune „crearea şi dezvoltarea unui corp de funcţionari publici profesionist, stabil şi imparţial" şi „aplicarea strategiilor şi a Programului de guvernare în domeniul managementului funcţiei publice şi al funcţionarilor publici, cât şi în domeniul formării profesionale a personalului din administraţia publică";
- în anul 2012, conform Raportului anual de activitate, hUp://www....,uov.ro/Paii inaContinut.aspx?ld=254, activitatea Agenţiei în domeniului managementului funcţiilor publice şi al funcţionarilor publici s-a axat pe realizarea evidenţei naţionale a funcţiilor publice şi a funcţionarilor publici prin intermediul sistemului informaţional integrat existent la nivelul Agenţiei precum şi pe implementarea sistemului privind semnătura electronică, în relaţia cu instituţiile publice, pentru facilitarea proceselor de transmitere a datelor;

- de asemenea, s-a realizat accesul la portalul de management al tuturor autorităţilor şi instituţiilor publice ale căror structuri sunt gestionate prin intermediul sistemului;
- numărul total al funcţionarilor publici la sfârşitul anului 2012 este 132.417 şi reprezintă 1.41% din populaţia ocupată a României (9,36 milioane, conform datelor publicate de Institutul Naţional de Statistică pentru trimestrul II al anului 2012); numărul total de funcţii publice (161.583) şi ponderea acestora pe niveluri administrativ-teritoriale cu defalcare pe funcţii publice ocupate şi vacante pentru anul 2012;
- la sfârşitul lunii decembrie 2010 erau înregistrate în baza de date 4.270 de instituţii; la momentul februarie 2013 sunt înregistrate în bază 4.430 instituţii; pe parcursul anului 2012, numărul autorităţilor şi instituţiilor publice ale căror structuri de funcţii publice sunt gestionate prin intermediul sistemului informaţional integrat a crescut de la 4.423 la 4.485, reprezentând peste 99 % din autorităţile şi instituţiile publice din România care deţin în acest moment astfel de structuri; în anul 2012 au fost extinse funcţiile Sistemului Integrat pentru Gestionarea Funcţionarilor Publici şi a Funcţiei Publice şi ale Portalului de management al Funcţionarilor Publici şi a Funcţiei Publice, cu implicaţii pentru proiectarea si dezvoltarea modulului de generare şi gestiune a cazierelor administrative, dezvoltarea de noi facilităţi în cadrul modulului de gestiune a concursurilor şi implementare semnăturii electronice, care facilitează transmiterea documentelor semnate electronic între ... şi alte instituţii publice;
- în perioada de referinţă, au fost efectuate un număr de 229.641 de operaţiuni pentru actualizarea bazei de date (inclusiv validarea acestora), în urma transmiterii datelor de către autorităţile şi instituţiile publice; în urma operaţionalizării portalului de management al funcţiilor publice şi funcţionarilor publici, până la sfârşitul anului 2012, toate autorităţile şi instituţiile publice ce deţin structuri de funcţii publice au primit acces pentru vizualizarea propriilor structuri înregistrate în sistemul informaţional integrat;
- de asemenea, fluxul de transmitere şi recepţionare a datelor privind evidenţa funcţiilor publice se efectuează prin intermediul portalului. Astfel, în această perioadă, numărul de operaţiuni de transfer de date desfăşurate între ... şi instituţiile publice prin intermediul portalului de management al funcţiilor publice şi funcţionarilor publici a fost de 33.604 fişiere transmise de către instituţiile publice către Agenţie prin portal, respectiv 3.053 mesaje preluate de la instituţiile publice prin intermediul acestuia;

- în perioada 3 ianuarie - 28 decembrie 2012 au fost operate un număr de 152.597 de operaţiuni (inclusiv cele prin intermediul portalului, şi fără a fi numărate aici şi validările operaţiunilor);
- astfel, în anul 2012, putem concluziona că, în vederea realizării unui sistem unitar din punct de vedere al tehnologiei informaţiei şi comunicaţiilor, la nivelul Agenţiei au fost elaborate Procedurile Operaţionale de Securitate specifice sistemelor informatice ce vehiculează informaţii clasificate.

În ceea ce priveşte activitatea de implementare a soluţiilor software, care să sprijine activitatea Agenţiei, autoritatea contractantă arată că, accentul a fost pus pe extinderea funcţionalităţi lor ..., cât şi pe extinderea funcţionalităţilor ....

În consecinţă, autoritatea contractantă solicită Consiliului respingerea ca nefondată şi lipsită de obiect a contestaţiei.

Ultimul document, aferent dosarelor cauzei, îl reprezintă adresa nr. 915.04.2013, înregistrată la Consiliu cu nr. 12101/15.04.2013, transmisă de ....

Analizând actele existente la dosarul cauzei, Consiliul constată următoarele:

... a organizat, în calitate de autoritate contractantă, procedura de achiziţie, prin „licitaţie deschisă”, a contractului de achiziţie publică de servicii, având ca obiect: „Servicii de consultanţă privind sistemele informatice în cadrul proiectului – ...– întărirea capacităţii instituţionale a ... în vederea asigurării unui management performant al funcţiei publice şi funcţionarilor publici la nivelul administraţiei publice centrale şi al serviciilor publice din subordinea/coordonarea autorităţilor publice centrale şi locale, prin implementarea de instrumente inovatoare – cod SMIS 36675”, cod CPV 72220000-3, 72611000-6, 72810000-1, sursa de finanţare: „*FSE – Programul Operaţional Dezvoltarea Capacităţii Administrative, Axa prioritară 2 – Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor publice, cu accentul pus pe procesul de descentralizare, Domeniul major de intervenţie: 2.2 Îmbunătăţirea calităţii şi eficienţei furnizării serviciilor Operaţiunea: Implementarea iniţiativelor de reducere a duratei de livrare a serviciilor publice prin folosirea sistemelor informatice de management, respectiv semnătură electronică, arhivare electronică şi flux informatic unitar de raportare şi monitorizare*”, elaborând, în acest sens, documentaţia de atribuire aferentă şi publicând, în SEAP, anunţul de participare nr. .../26.03.2013, conform căruia valoarea estimată a contractului de achiziţie publică este de 974.067,5 lei, fără TVA.

Potrivit documentaţiei de atribuire, criteriul de atribuire a contractului este „preţul cel mai scăzut”.

În baza dispoziţiilor art. 278 alin. (1) din OUG nr. 34/2006, cu modificările şi completările ulterioare, potrivit căruia *„Consiliul se pronunţă mai întâi asupra excepţiilor de procedură şi de fond, iar când se constată că acestea sunt întemeiate, nu se mai procedează la analiza pe fond a cauzei”,* Consiliul va analiza, cu întâietate, excepţia lipsei de obiect a contestaţiilor depuse de ...şi ... invocată de autoritatea contractantă, în punctele de vedere nr. înregistrate la CNSC cu nr. 11664/11.04.2013 şi nr. 11665/11.04.2013.

În acest sens, Consiliul va avea în vedere următoarele dispoziţii legale:

- art. 255 alin. (1), (2) şi (3) din OUG nr. 34/2006: *„(1) Orice persoană care se consideră vătămată într-un drept ori într-un interes legitim printr-un act al autorităţii contractante, prin încălcarea dispoziţiilor legale în materia achiziţiilor publice, poate solicita, prin contestaţie, anularea actului, obligarea autorităţii contractante de a emite un act, recunoaşterea dreptului pretins sau a interesului legitim pe cale administrativ-jurisdicţională, în condiţiile prezentei ordonanţe de urgenţă.*

*b) a suferit, suferă sau riscă să sufere un prejudiciu ca o consecinţă a unui act al autorităţii contractante, de natură să producă efecte juridice, ori ca urmare a nesoluţionării în termenul legal a unei cereri privind respectiva procedura de atribuire.*

*(3) În sensul prevederilor alin. (1), prin act al autorităţii contractante se înţelege orice act administrativ, orice altă operaţiune administrativă care produce sau poate produce efecte juridice, neîndeplinirea în termenul legal a unei obligaţii prevăzute de prezenta ordonanţă de urgenţă, omisiunea ori refuzul de a emite un act sau de a efectua o anumită operaţiune, în legătură cu sau în cadrul procedurii de atribuire”;*

- art. 270 alin. (1) din OUG nr. 34/2006: *„Contestaţia se formulează în scris şi trebuie să conţină următoarele elemente: (…) d) obiectul contestaţiei”.*

Analizând conţinutul celor două contestaţii, Consiliul reţine că acestea sunt formulate în concordanţă cu dispoziţiile legale citate anterior, fiind formulate împotriva documentaţiei de atribuire elaborată de autoritatea contractantă în vederea derulării contractului de achiziţie publică de servicii, în calitate de operatori economici interesaţi în participarea la procedură, formulând în acest sens, solicitări privind obligarea autorităţii contractante la adoptarea de măsuri de remediere

cu privire la cerinţele de calificare din fişa de date a achiziţiei şi, în subsidiar, anularea procedurii de atribuire în cauză.

Pe cale de consecinţă, faţă de cele expuse anterior, în baza art. 278 alin. (1) şi (5) din OUG nr. 34/2006, Consiliul va respinge excepţia lipsei de obiect, invocată de autoritatea contractantă, faţă de cele două contestaţii, supuse soluţionării.

Pe fondul cauzei, Consiliul reţine că, ulterior luării la cunoştinţă a conţinutului documentaţiei de atribuire, ... şi ... au formulat contestaţiile deduse soluţionării, solicitând „obligarea autorităţii contractante la adoptarea de măsuri corective cu privire la documentaţia de atribuire; în subsidiar, anularea procedurii" şi „suspendarea procedurii de atribuire în cauză; în principal, modificarea cerinţelor de calificare şi selecţie de la pct. III.2.3.a din fişa de date a achiziţiei; în subsidiar, anularea procedurii."

Deoarece ... a solicitat, în cadrul contestaţiei, printre altele şi suspendarea procedurii de atribuire în cauză, Consiliul a emis Decizia nr. ... prin care a admis suspendarea acesteia, în baza art. 275¹ alin. (1) din OUG nr. 34/2006, pentru a preveni producerea unor pagube iminente şi evitarea apariţiei unor situaţii care să conducă la încălcarea principiilor consacrate de art. 2 alin. (2) din OUG nr. 34/2006; potrivit informaţiilor existente în SEAP, la rubrica „stare procedură", procedura de atribuire în cauză a fost suspendată din ...

Apreciind că cele două contestaţii tratează anumite aspecte comune, privind cerinţele de calificare formulate de autoritatea contractantă în documentaţia de atribuire, Consiliul va proceda la analiza acestora în mod unitar, raportat la conţinutul documentaţiei de atribuire, inclusiv nota justificativă privind criteriile de calificare ce trebuie îndeplinite de către ofertanţi, precum şi cu luarea în considerare a dispoziţiilor legale aplicabile.

În acest sens, procedând la analiza dosarului cauzei, Consiliul reţine că la pct. III.2.3.a) Capacitatea tehnică şi/sau profesională - Informaţii privind calificările şi experienţa profesională a experţilor din cadrul echipei de proiect, se menţionează că: *„Echipa propusă trebuie să includă cel puţin următorii specialişti (cele 5 poziţii de mai jos nu se pot cumula). Pentru personalul de specialitate propus pentru proiect, se vor prezenta următoarele documente:*

*- CV actual aferent fiecărei persoane propusă în cadrul echipei, semnat de către fiecare titular în parte;*

*- Documente suport (diplome, atestate, certificări), din care să rezulte pregătirea şi competenţele/calificările profesionale ale personalului de specialitate propus în cadrul echipei de proiect.*

*Diplomle, atestatele, certificările trebuie prezentate în copie legalizată sau copie lizibilă certificată de reprezentantul ofertantului cu menţiunea conform cu originalul, în limba română sau însoţite de traducere autorizată în limba română, dacă este cazul. Experienţa generală sau specifică în domeniu poate fi demonstrată prin copie cu cartea de muncă/contracte de muncă, contract de colaborare/prestări servicii, adeverinţe sau orice alte documente similare;*

*- Declaraţie de disponibilitate, semnată de fiecare persoană nominalizată, în original, în conformitate cu formularul din Formularul nr. 11 din Secţiunea III".*

*1. Expert în securitatea informaţiei – 1 expert:*

*- Diplomă de absolvire a studiilor universitare;*

*- Minim 3 ani experienţă în domeniul Securităţii Informatice;*

*Capabilităţi şi certificări recunoscute internaţional în domeniul securităţii informatice:*

*- Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent);*

*-Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional - CSSLP) sau echivalent;*

*- Certificare independentă privind auditarea sistemelor informatice (Certified Information Systems Auditor (CISA) sau echivalent;*

*- Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager - CISM) sau echivalent.*

*2. Expert în Servicii IT – 1 expert*

*- Diplomă de absolvire a studiilor universitare;*

*- Minim 3 ani experienţă în domeniul IT&C;*

*- Certificat ITIL Expert v3 sau echivalent;*

*- Cunoaşterea metodologiei Six Sigma demonstrată prin participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metologii echivalente.*

*3. Expert Infrastructura Hardware – 1 expert*

*- Diploma de absolvire a studiilor universitare;*

*- Minim 3 ani experienţă în domeniul IT&C;*

*Capabilităţi şi certificări recunoscute internaţional:*

*- Certificat ITIL Foundation v3 sau echivalent;*

*- Cunoaşterea a cel puţin 1 tehnologie de stocare a datelor de tip SAN (Storage Area Network) sau echivalent dovedită prin deţinerea de certificări tehnice;*

*- Cunoaşterea a cel puţin 1 tehnologie de back-up a datelor, dovedite prin deţinerea de certificări tehnice;*
*- Cunoaşterea a cel puţin unei soluţii de virtualizare, dovedite prin deţinerea a cel puţin unei certificări tehnice;*
*- Certificare de specializare într-un sistem de operare(....).”*

Faţă de cele de mai sus, Consiliul va lua în considerare faptul că la pct. II.1.2) Tipul contractului şi cap. II.6 Clasificare CPV, din anunţul de participare nr. .../26.03.2013, este menţionat că tipul contractului de achiziţie publică ce urmează a fi atribuit este de „servicii informatice şi servicii conexe’’, respectiv de „servicii de consultanţă privind sistemele informatice şi servicii de consultanţă tehnică”, „servicii de asistenţă tehnică informatică” şi „servicii de audit informatic”, conform codurilor CPV corespondente.

În soluţionarea contestaţiilor, Consiliul va avea în vedere natura contractului de achiziţie publică ce urmează a fi atribuit, care, potrivit informaţiilor cuprinse în caietul de sarcini aferent procedurii de atribuire, la cap. 3, privind obiectul achiziţiei şi rezultatele aşteptate, obiectivele acestuia sunt următoarele:

1. Auditarea sistemului informatic al ... în vederea implementării sistemului de semnătură digitală şi arhivare electronică;

2. Derularea fazei de precontractare, cu următoarele faze solicitate: întocmirea Studiului de Fezabilitate, a Proiectului Tehnic, a Documentaţiei de Atribuire, conform OUG nr. 34/2006; asigurarea documentării şi pregătirii personalului din partea achizitorului;

3. Derularea procedurii de achiziţie, cu următoarele rezultate solicitate:
- identificarea şi justificarea tipului de achiziţie publică;
- asistenţă de specialitate pe toată perioada desfăşurării procedurii de achiziţie, inclusiv în cadrul evaluării ofertelor;

4. Implementarea proiectului, cu următoarele rezultate solicitate: monitorizarea realizării şi implementării sistemului de semnătură digitală şi arhivare electronică, în vederea asigurării deplinei funcţionalităţi a acestuia, a integrării depline a echipamentelor/ sistemelor cu care se va conecta.

De asemenea, Consiliul va lua în considerare şi faptul că obiectivul general al contractului de servicii, potrivit art. 2.1 din caietul de sarcini, este îmbunătăţirea calităţii şi eficienţei serviciilor furnizate de ... contribuind la realizarea bazei de date cu documentaţia transmisă de autorităţile şi instituţiile publice din România în format electronic, precum şi alinierea administraţiei publice la tendinţele tehnologice prin

implementarea semnăturii electronice în 1930 de autorităţi şi instituţii publice, de pe teritoriul ţării.

Consiliul apreciază că, în prezenta cauză, sunt incidente următoarele dispoziţii legale aplicabile:

- Art. 177 din OUG nr. 34/2006: *„(1) Operatorii economici au dreptul de a prezenta certificate emise de către o autoritate publică competentă sau de către un organism de drept public sau privat care respectă standarde europene de certificare, pentru demonstrarea îndeplinirii unor criterii de calificare şi selecţie formulate în conformitate cu prevederile art. 176.*

*(2) Autoritatea contractantă nu are dreptul de a impune candidaţilor/ofertanţilor obligativitatea prezentării unei certificări specifice, aceştia din urmă având dreptul de a prezenta, în scopul demonstrării îndeplinirii anumitor cerinţe, orice alte documente echivalente cu o astfel de certificare sau care probează, în mod concludent, îndeplinirea respectivelor cerinţe. Autoritatea contractantă are dreptul de a solicita, dacă se consideră necesar, clarificări sau completări ale documentelor prezentate”.*

- Art. 179 alin. (1) din OUG nr. 34/2006: *„Criteriile de calificare şi selecţie stabilite de către autoritatea contractantă trebuie să aibă o legătură evidentă cu obiectul contractului ce urmează să fie atribuit”.*

- Art. 7 din HG nr. 925/2006: *„Criteriile de calificare şi selecţie, astfel cum sunt prevăzute la art. 176 din ordonanţa de urgenţă, au ca scop demonstrarea potenţialului tehnic, financiar şi organizatoric al fiecărui operator economic participant la procedură, potenţial care trebuie să reflecte posibilitatea concretă a acestuia de a îndeplini contractul şi de a rezolva eventualele dificultăţi legate de îndeplinirea acestuia, în cazul în care oferta sa va fi declarată câştigătoare”.*

- Art. 8 alin. (2) din HG nr. 925/2006: *„Atunci când impune cerinţe minime de calificare referitoare la situaţia economică şi financiară ori la capacitatea tehnică şi/sau profesională, astfel cum este prevăzut la art. 178 alin. (1) din ordonanţa de urgenţă, autoritatea contractantă trebuie să fie în măsură să motiveze aceste cerinţe, elaborând în acest sens o notă justificativă care se ataşează la dosarul achiziţiei”.*

... critică, în cuprinsul contestaţiei, următoarele cerinţe de la cap. III.2.3.a) din fişa de date a achiziţiei, solicitând eliminarea acestora:

1. *Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional - CSSLP) sau echivalent”,* solicitată de autoritatea contractantă pentru expertul în securitatea informaţiei.

Cu privire la această cerinţă, Consiliul va lua în considerare că, în nota justificativă nr. 8654/06.03.2013, întocmită de autoritatea contractantă, privind criteriile de calificare ce trebuie îndeplinite de către ofertanţi, se precizează că această cerinţă este necesară, deoarece atestă capacitatea de evaluare a aplicaţiilor software, a ciclului de dezvoltare şi implementare în sistem.

2. *Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent)",* solicitată de autoritatea contractantă, tot pentru expertul în securitatea informaţiei.

Referitor la această cerinţă, în nota justificativă aferentă procedurii de atribuire, autoritatea contractantă a precizat faptul că expertul în cauză, trebuie să demonstreze „capabilităţi de a avea o viziune globală asupra tuturor aspectelor şi elementelor necesare realizării sistemului, pentru a se obţine o imagine obiectivă, a aplicaţiilor şi proiectelor viitoare şi pentru evaluarea infrastructurii hardware şi elaborarea documentaţiei de atribuire".

Ţinând cont de natura şi complexitatea contractului de servicii ce urmează a fi atribuit, precum şi de obiectivele acestuia, prevăzute în cadrul documentaţiei de atribuire şi expuse anterior, Consiliul consideră că autoritatea contractantă a stabilit aceste cerinţe în conformitate cu dispoziţiile art. 179 alin. (1) din OUG nr. 34/2006, precum şi ale art. 7 din HG nr. 925/2006, prin modul de formulare a cerinţelor respective, respectiv prin adăugarea sintagmei „sau echivalent", lăsând deschise posibilităţi de echivalare pentru operatorii econimici interesaţi. Prin urmare, Consiliul va respinge ca nefondate criticile vizând aceste cerinţe de calificare.

3. *„Certificat ITIL Expert v3 sau echivalent",* solicitat pentru expertul în servicii IT şi expert infrastructura hardware; Consiliul va lua în considerare că în nota justificativă privind alegerea criteriilor de calificare, autoritatea contractantă a precizat că sunt necesari experţi având aceste certificări, deoarece aceasta presupune deţinerea unei expertize recunoscute la nivel internaţional, acordată persoanelor care au demonstrat expertiză în utilizarea standardelor şi a bunelor practici recunoscute în ceea ce priveşte managementul serviciilor IT.

Deoarece ITIL aduce o abordare sistematică şi profesională pentru gestiunea serviciilor IT, iar adoptarea unei practici de acest gen oferă o serie de beneficii societăţii, cum ar fi reducerea costurilor, îmbunătăţirea serviciilor IT, o mai bună utilizare a abilităţilor şi a experienţei, în concluzie, o mai bună furnizare a serviciilor IT, ţinând cont de obiectul contractului ce urmează a fi atribuit, precum şi de

activităţile cuprinse în caietul de sarcini, Consiliul apreciază că autoritatea contractantă a formulat o cerinţă în concordanţă cu conţinutul acestora, mai ales că a permis operatorilor economici să prezinte un echivalent al acesteia.

4. *„Certificare independentă privind auditarea sistemelor informatice (Certified Information Systems Auditor (CISA) sau echivalent";*

Potrivit notei justificative nr. 8654/06.03.2013, autoritatea contractantă ar avea nevoie de un expert în securitatea informaţiei, cu o astfel de certificare, deoarece în acest mod, se atestă „capacitatea de realizare a auditurilor asupra sistemelor informatice". În mod similar, ţinând cont de faptul că obiectul contractului de servicii priveşte, în principal, auditarea sistemului informatic al ..., precum şi faptul că se permite inclusiv prezentarea unei certificări echivalente, Consiliul va respinge ca nefondată solicitarea contestatorului vizând eliminarea acestei cerinţe, pe motiv că are un caracter restrictiv, raportat la obiectul contractului.

5. *„Cunoaşterea a cel puţin 1 tehnologie de stocare a datelor de tip SAN (Storage Area Network) sau echivalent dovedită prin deţinerea de certificări tehnice*".

În analiza acestei cerinţe, Consiliul va lua în considerare că, în nota justificativă privind alegerea criteriilor de calificare, autoritatea contractantă a motivat alegerea acesteia, după cum urmează: „pentru a putea evalua corespunzător sistemele existente pe piaţă şi a propune cele mai bune soluţii privind noua infrastructură hardware privind stocarea datelor". În opinia Consiliului, autoritatea contractantă a solicitat ca operatorii economici să prezinte experienţă într-un anumit sistem de operare, la un anumit nivel, fiindu-i necesară pentru a demonstra experienţă în acest sens, posibilităţile de migrare în centre de date noi precum şi realizarea de back – up şi restaurare a sistemului.

6. *„Cerinţa privind cunoaşterea metodologiei SixSigma demonstrată prin „participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metodologii echivalente",* solicitată pentru expertul în Servicii IT.

Cu privire la această cerinţă de calificare, Consiliul reţine că autoritatea contractantă a precizat că, în vederea remodelării fluxurilor de lucru, are nevoie de o persoană calificată corespunzător, care să cunoască o metodologie de lucru recunoscută pe plan internaţional, aşa cum este Six Sigma, sau o metodologie echivalentă acesteia, cunoaşterea metodologiei fiind demonstrată prin participarea la cel puţin un curs de instruire nivel Green Belt.

În aprecierea Consiliului, autoritatea contractantă nu a formulat o cerinţă restrictivă, din acest punct de vedere, deoarece a oferit posibilitatea operatorilor economici să prezinte o certificare echivalentă celei solicitate.

În sensul celor menţionate, Consiliul va respinge alegaţiile contestatorului cu privire la faptul că cerinţa în cauză nu are legătură cu caietul de sarcini şi cu scopul contractului, deoarece, potrivit caietului de sarcini aferent procedurii de atribuire, activităţile ce se vor derula în cadrul contractului, privesc şi analiza fluxurilor informatice existente în cadrul ..., remodelarea şi actualizarea fluxurilor informatice prin raportare la cadrul legal existent, cadrul de funcţionare, atribuţii şi competenţe instituţionale.

Astfel, Consiliul va respinge ca nefondată critica contestatorului vizând eliminarea din fişa de date a achiziţiei, a cerinţei privind cunoaşterea metodologiei SixSigma demonstrată prin „participarea la cel puţin un curs de instruire pentru nivelul Green Belt sau a unei metodologii echivalente”.

De asemenea, ... contestă şi faptul că autoritatea contractantă, a solicitat în ceea ce priveşte experţii în securitatea informaţiei şi în infrastructura hardware, ca aceştia să deţină „capabilităţi şi certificări recunoscute internaţional”.

În opinia Consiliului, având în vedere specificul aparte al contractului de servicii, conform celor expuse anterior, autoritatea contractantă trebuie să se asigure că acesta se va realiza la standarde profesionale ridicate, fapt ce nu poate avea loc decât utilizând personal calificat şi cu experienţă relevantă în domeniu, astfel cum, de altfel, a precizat în nota justificativă privind criteriile de calificare.

Consiliul va respinge ca nefondată această critică formulată de contestator privind acest aspect, ţinând cont de unicitatea şi complexitatea proiectului, precum şi de dispoziţiile art. 177 alin. (1) din OUG nr. 34/2006, care permite operatoriilor economici să prezinte „certificate emise de către o autoritate publică competentă sau de către un organism de drept public sau privat care respectă standarde europene de certificare, pentru demonstrarea îndeplinirii unor criterii de calificare şi selecţie formulate în conformitate cu prevederile art. 176”.

Consiliul reţine că, în nota justificativă nr. 8654/06.03.2013, întocmită de autoritatea contractantă în baza art. 8 alin. (2) din HG nr. 925/2006, se precizează că, în ceea ce priveşte personalul angajat, „experţii solicitaţi precum şi cerinţele referitoare la experienţa lor, au fost concepute după cerinţele şi activităţile din caietul de sarcini”.

De asemenea, Consiliul nu va reţine alegaţiile contestatorului cu privire la existenţa unui număr restrâns de persoane care deţin aceste certificări, deoarece nu probează în niciun susţinerile sale în acest sens.

În contextul menţionat anterior, Consiliul consideră că achiziţia în cauză are un grad ridicat de **complexitate** şi, de asemenea, deţine o serie de elemente de **unicitate** la nivel naţional, astfel încât consultanţa aferentă să fie asigurată de experţi calificaţi în domeniu, existenţi la momentul actual, care să fie în măsură să asigure derularea contractului în condiţii optime.

De asemenea, Consiliul constată şi faptul că autoritatea contractantă, în elaborarea documentaţiei de atribuire, a avut în vedere şi respectarea dispoziţiilor art. 33 alin. (1) din OUG nr. 34/2006, care prevede că: *„Autoritatea contractantă are obligaţia de a preciza în cadrul documentaţiei de atribuire orice cerinţă, criteriu, regulă şi alte informaţii necesare pentru a asigura ofertantului/candidatului o informare completă, corectă şi explicită cu privire la modul de aplicare a procedurii de atribuire”.*

Având în vedere cele expuse anterior în cadrul motivării anterioare, Consiliul, în baza art. 278 alin. (5) din OUG nr. 34/2006, cu modificările şi completările ulterioare, va respinge, ca nefondată, contestaţia formulată de ... în contradictoriu cu autoritatea contractantă ...

În opinia contestatorului ..., certificările solicitate pentru experţi, sunt disproporţionate faţă de cerinţele caietului de sarcini, acestea suprapunându – se, sau fiind nejustificate, raportat la cerinţele caietului de sarcini.

Astfel, în ceea ce priveşte cerinţele pentru expertul în securitatea informaţiei, vizând *„Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional - CSSLP) sau echivalent”,* contestatorul solicită eliminarea acesteia, pe motiv că se suprapune cu *„Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent)”,* pentru acelaşi expert.

Referitor la afirmaţia contestatorului, cu privire la faptul că unele dintre domeniile celor două certificări se suprapun, nefiind necesare ambele, Consiliul reţine că certificarea „Certified Secure Software LifeCycle Professional – CSSLP”, conform documentaţiei oficiale - Anexa nr.l_CSSLP-Brochure.pdf, acoperă următoarele domenii: Secure Software Concepts, Secure Software Requirements, Secure Software

Design, Secure Software Implementation/Coding, Secure Software Testing, Software Acceptance, Software Deployment, Operations, Maintenance and Disposal. Pe de altă parte, „Certified Information Systems Security Professional – CISSP”, conform documentaţiei oficiale Anexa nr.2_CISSP-WEB.pdf, acoperă domeniile: Access Control, Telecommunications and Network Security, Information Security Governance and Risk Management, Software Development Security, Cryptography, Security Architecture and Design, Operations Security, Business Continuity and Disaster Recovery Planning, Legal, Regulations, Investigations and Compliance, Physical (Environmental) Security.

De asemenea, Consiliul are în vedere motivaţia cuprinsă în nota justificativă privind criteriile de calificare şi selecţie, aflată la dosarul cauzei, unde autoritatea contractantă a precizat următoarele, cu privire la cele două certificări:

- *Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional - CSSLP) sau echivalent”* – atestă capacitatea de evaluare a aplicaţiilor software, a ciclului de dezvoltare şi implementare în sistem;

- *Certificare independentă privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent)”* – capabilităţi de a avea o viziune globală asupra tuturor aspectelor şi elementelor necesare realizării sistemului, pentru a se obţine o imagine obiectivă, a aplicaţiilor şi proiectelor viitoare şi pentru evaluarea infrastructurii hardware şi elaborarea documentaţiei de atribuire.

Astfel, Consiliul nu poate reţine alegaţia contestatorului vizând „evidenta suprapunere aproape de identificare a sistemelor între domeniile” acoperite de cele două certificări, menţionate anterior, autoritatea contractantă justificând, prin documentul menţionat, îndeplinirea în mod cumulativ a cerinţelor, expertul în securitatea informaţiei având rolul de a coordona activitatea de audit a sistemului informatic, atât din punct de vedere al infrastructurii hardware şi de comunicaţii, al aplicaţiilor informatice precum şi al politicilor şi procedurilor de lucru, realizarea unui studiu privind serverele disponibile, întocmirea documentaţiei în vederea achiziţiei echipamentelor hardware şi software , a licenţelor aferente pentru buna implementare a proiectului, precum şi o sere de alte activităţi, precizate în caietul de sarcini, aferent procedurii de atribuire în cauză. Prin urmare, faţă de cele expuse anterior, Consiliul va respinge solicitarea

contestatorului vizând eliminarea din fişa de date a achiziţiei a cerinţei vizând *„Certificare independentă privind securitatea aplicată la nivelul ciclului de dezvoltare software de nivel profesional (Certified Secure Software LifeCycle Professional - CSSLP) sau echivalent”.*

Tot în ceea ce priveşte expertul în securitatea informaţiei, contestatorul solicită eliminarea cerinţei vizând *„Certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager - CISM) sau echivalent”,* deoarece, în opinia sa, se suprapune cu certificarea *„privind securitatea sistemelor informatice de nivel profesional (Certified Information Systems Security Professional (CISSP) sau echivalent)”.*

Având în vedere că, astfel cum s-a menţionat anterior, CISSP acoperă domeniile: Access Control, Telecommunications and Network Security, Information Security Governance and Risk Management, Software Development Security, Cryptography, Security Architecture and Design, Operations Security, Business Continuity and Disaster Recovery Planning, Legal, Regulations, Investigations and Compliance, Physical (Environmental) Security.

Pe de altă parte, Certificarea CISM (conform site-ului oficial al furnizorului http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Prepare-for-the-Exam/ Job- Practice-Areas/Pages/default.aspx), domeniile acoperite sunt: Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, Information Security Incident Management.

Din analiza comparativă a domeniilor pe care cele două certificări le acoperă, Consiliul reţine că „Security Governance”, „Risk Management” şi „Compliance” se suprapun, fiind cuprinse în ambele certificări. Astfel, având în vedere cele precizate anterior, ţinând cont că domeniile aferente certificării Certified Information Security Manager – (CISM) se regăsesc printre cele solicitate pentru (Certified Information Systems Security Professional (CISSP), pentru care autoritatea contractantă a făcut menţiunea „sau echivalent”, Consiliul consideră întemeiată critica contestatorului şi, pe cale de consecinţă, va admite cererea acestuia vizând eliminarea, de la cap. III. 2.3.a) din fişa de date a achiziţiei, a cerinţei vizând certificării „Certified Information Security Manager – (CISM)”.

Contestatorul aduce critici şi cu privire la cerinţa de la Cap. III.2.3.b), Standarde de asigurare a calităţii şi de protecţie a mediului - Informaţii referitoare la standardele de management al securităţii

informaţiei: *„Certificat ISO 27001 sau echivalent. Documente emise de organisme naţionale sau internaţionale acreditate care confirmă certificarea sistemului de management al securităţii informaţiei, respectiv Certificatul ISO 27001 sau echivalent, în copie certificată pentru conformitate cu originalul”,* a căror eliminare o solicită, pe motiv că în fapt, caietul de sarcini aferent procedurii de atribuire se referă, preponderent, la activităţi de management de proiect şi nu la monitorizare tehnică din punct de vedere al informaţiei, Consiliul va lua în considerare faptul că, în nota justificativă nr. 8654/06.03.2013, aferentă procedurii de atribuire în cauză, autoritatea contractantă a expus argumentele ce au stat la baza alegerii aceastei cerinţe, precizând că, a avut în vedere *„caracterul tehnic specific al informaţiilor cu care intră în contact ofertanţii, faptul că se cere realizarea unui audit al sistemului informatic şi realizarea şi implementarea unei soluţii informatice pentru semnătura digitală şi arhivarea electronică în condiţii de siguranţă şi securitate specifice”.*

Consiliul va lua în considerare faptul că implementarea şi certificarea unui sistem de management al securităţii informaţiei, garantează securitatea informaţiilor la nivelul unei societăţi, dar şi a informaţiilor clienţilor şi partenerilor acestuia, având în vedere ca majoritatea datelor sunt pe suport informatic, iar un Sistem de Management al Securităţii Informaţiei (ISMS), ISO/IEC 27001:2005, reprezintă o abordare sistematică a managementului informaţiei, astfel încât aceasta sa fie în siguranţă. Acest lucru implica angajaţii, procesele şi sistemele IT, fiind necesară o Politică de Securitate a Informaţiei pentru organizaţie, de confidenţialitate, integritate şi disponibilitate atât pentru societatea respectivă, cât şi pentru informarea clienţilor.

Consiliul va reţine că, potrivit informaţiilor existente în caietul de sarcini aferent procedurii de atribuire în cauză, contractul de servicii ce urmează a se atribui presupune activităţi precum: realizarea unui audit informatic iniţial la sediul autorităţii contractante, întocmirea documentaţiei de atribuire în vederea achiziţionării echipamentelor software şi hardware şi a licenţelor aferente pentru buna implementare a contractelor, care îşi propun să reflecte în mod cât mai detaliat climatul general de securitate, inclusiv analiza planului şi politicilor de securitate la nivelul instituţiei, activităţile au ca scop implementarea sistemului de semnătură digitală şi arhivare electronică, şi nu „consultanţă pentru management de proiect”, astfel cum susţine contestatorul. Auditul de securitate presupune o serie de teste realizate de către auditor asupra unui sistem IT şi care vizează identificarea

conformităţii măsurilor implementate cu standardele internaţionale în vigoare.

În contextul menţionat anterior, Consiliul apreciază că faptul că cerinţa privind „certificatul ISO 27001 sau echivalent” este justificată, prin raportare la complexitatea şi importanţa strategică a proiectului, ţinând cont totodată de implicarea unui număr mare de autorităţi şi instituţii publice, cu care ... face schimb de informaţii, precum şi de operarea de date cu caracter personal, considerând că, în acest sens, autoritatea contractantă a aplicat dispoziţiile art. 179 alin. (1) din OUG nr. 34/2006, potrivit cărora *„Criteriile de calificare şi selecţie stabilite de către autoritatea contractantă trebuie să aibă o legătură evidentă cu obiectul contractului ce urmează să fie atribuit”,* precum şi ale art. 8 alin. (2) din HG nr. 925/2006, care prevede că *„atunci când impune cerinţe minime de calificare referitoare la situaţia economică şi financiară ori la capacitatea tehnică şi/sau profesională, astfel cum este prevăzut la art. 178 alin. (1) din ordonanţa de urgenţă, autoritatea contractantă trebuie să fie în măsură să motiveze aceste cerinţe, elaborând în acest sens o notă justificativă care se ataşează la dosarul achiziţiei”.*

Faţă de cele expuse anterior, Consiliul va respinge ca nefondată solicitarea formulată de ...privind eliminarea „certificatul ISO 27001 sau echivalent”, de la cap. III.2.3.b) din fişa de date a achiziţiei.

Faţă de cele expuse anterior, Consiliul, în baza dispoziţiilor art. 278 alin. (2) şi (4) din OUG nr. 34/2006, cu modificările şi completările ulterioare, va admite, în parte, contestaţia formulată de SC BUSSINES ADVISORY TEAM SRL, astfel:

- va admite solicitarea contestatorului privind eliminarea din fişa de date a achiziţiei a cerinţei privind „certificare independentă privind managementul securităţii informaţiei (Certified Information Security Manager - CISM), sau echivalent” şi va obliga autoritatea contractantă la eliminarea acesteia;
- va respinge, pentru motivele expuse în motivarea anterioară, solicitarea privind eliminarea, din fişa de date a achiziţiei, a celorlalte cerinţe de calificare.

Consiliul va respinge solicitările contestatorilor privind anularea procedurii de atribuire în cauză, deoarece remedierea documentaţiei de atribuire este posibilă fără încălcarea principiilor prevăzute la art. 2 alin. (2) lit. a) – f) din OUG nr. 34/2006, cu modificările şi completările ulterioare.

**PREŞEDINTE COMPLET**
**...**

**MEMBRU COMPLET** **MEMBRU COMPLET**
**...** **...**

...