

Curtea de Conturi RM

AUTOEVALUARE DE INTEGRITATE 14-07-2016



Raport de evaluare

Moderatori: Viorica Verdeș, Irina Gutnic, Iulian Dumitraș (Curtea de Conturi), Noëlle Ruckert (Curtea de Audit, Olanda)

Persoana de contact: Viorica Verdeș

Acest raport este confidențial și este destinat exclusiv CC din Moldova.

CONȚINUT

Introducere.....	3
Rezumat	4
1Descrierea proceselor organizaționale.....	5
2Vulnerabilități	
2.1Vulnerabilități inerente.....	6
2.2Factorii de sporire a vulnerabilităților	7
2.3Profilul vulnerabilităților.....	8
3Nivelul de maturitate al sistemului de control al integrității (pe intern)	9
4Analiza lacunelor și recomandările	11
4.1Analiza lacunelor	11
4.2Recomandări	11
Anexa 1 Lista participanților	12
Anexa 2 Factori de sporire a vulnerabilității	13
Anexa 3 Sistem de control al integrității.....	15

1 Introducere

Acest raport reflectă rezultatele autoevaluării integrității CC.

Autoevaluarea a fost realizată prin aplicarea metodologiei SAINT furnizate de Curtea de Audit din Olanda pentru membrii INTOSAI (IntoSAINT).

Evaluarea a vizat întreaga organizație.

Conceptele de bază ale integrității și a metodologiei SAINT pot fi rezumate după cum urmează:

- Integritatea implică nu numai respectarea regulilor și legilor, ci și o responsabilitate morală.
- Integritatea este un aspect de calitate al unei organizații și, prin urmare, o responsabilitate a managementului.

- Integritatea este o condiție esențială pentru încrederea în sectorul public.
- Prevenirea și cunoașterea vulnerabilităților existente este cea mai eficientă cale pentru a proteja integritatea unei organizații.
- Organizațiile pot preveni încălcările de integritate prin reducerea vulnerabilității acestora și printr-un sistem matur de control al integrității.
- Un sistem de integritate matur este format din controale generale, aspre și blânde.
- Angajații ca persoane din interior sunt de obicei într-o poziție bună pentru a identifica vulnerabilitățile, pentru a detecta punctele slabe ale sistemului de control al integrității și modalități de îmbunătățire a rezistenței la încălcarea integrității.
- Participarea angajaților în evaluarea integrității ridică sensibilizarea cu privire la problema integrității.

Autoevaluarea a fost realizată pe 12 și 13 iulie 2016 de către un grup bine selectat de angajați din cadrul CC. O listă a participanților este inclusă în Anexa 1. În cadrul atelierului, participanții au trecut prin diferitele etape ale metodologiei de autoevaluare.

Acest raport oferă în primul rând un rezumat al rezultatului auto-evaluării și apoi continuă să descrie rezultatele etapelor succesive ale metodei:

- a. descrierea proceselor organizaționale selectate;
- b. identificarea profilului vulnerabilităților;
- c. maturitatea sistemului de control al integrității existente;
- d. analiza diferenței dintre profilul vulnerabilităților și măsurile de control ale integrității din interiorul organizației

Pe baza acestor descrieri au fost formulate recomandări pentru a reduce vulnerabilitatea și de a îmbunătăți sistemul de control al integrității.

Am dori să apreciem bunăvoința și cooperarea Curții de Conturi din Rep. Moldova de a permite desfășurarea atelierului SAINT, în special eforturile participanților la atelier, coordonatorului atelierului, co-moderatorilor și sprijinul angajaților.

2 Rezumat

PM

3 Descrierea proceselor organizaționale

Procesele organizaționale vitale implicate sunt:

Înainte de începerea atelierului în cooperare cu persoana de contact și moderatorii de la Curtea de Conturi a Republicii Moldova a fost făcută preselecția proceselor cheie de la CC. În cadrul atelierului această selecție a fost pusă în discuție, și participanții au confirmat valabilitatea acestor procese selectate pentru autoevaluare.

Procesele vitale organizaționale implicate sunt:

Procese primare:

- Monitorizare și mediul de audit
- Procese de audit
- Procese de dezvoltare. Alocarea resurselor în acest sens.
- Activități internaționale/de protocol
- Publicarea rezultatelor auditurilor (transparența)

Procese secundare:

- Personal / gestionare de resurse umane
- Dezvoltare profesională: instruire
- Management financiar: solicitarea bugetului, monitorizarea utilizării bugetului
- Managementul informațional (inclusiv securitatea informațională)
- Managementul facilităților (inclusiv securitatea fizică)
- Arhivare

Procesele de management și control:

- Planificare strategică
- Monitorizarea implementării politicilor CC

Această listă de procese a servit drept referință pentru celelalte etape ale atelierului IntoSAINT.

4 Vulnerabilitățile

4.1 *Vulnerabilități inerente*

Toate organizațiile sunt într-o anumită măsură vulnerabile la încălcări de integritate. Cu toate acestea anumite activități și funcții în sectorul public sunt în mod special vulnerabile. Acestea sunt numite vulnerabilități inerente și sunt de obicei legate de sarcinile specifice ale unei organizații. În timpul atelierului procesele și funcțiile Curții de Conturi a Republicii Moldova au fost comparate cu o listă de vulnerabilități inerente, așa cum este indicat în tabelul de mai jos.

	Domenii/activități/acțiuni vulnerabile		Scor mediu¹	Nivel
<i>Relația entității cu mediul acesteia</i>	Contractare	achiziții publice, tendere, comenzi, desemnare, atribuire	1.82	Înalt
	Plăți	subvenții, beneficii, indemnizații, granturi, sponsorizare	0.71	Scăzut
	Eliberare/emitere	permise, licențe, cărți de identitate, autorizații, certificate	0.18	Scăzut
	Reglementare	condiții pentru permise, stabilirea standardelor/criteriilor	0.18	Scăzut
	Inspecție/audit	supraveghere, control, inspecție, audit	2.59	Ridicat
	Executare	urmărire penală, justiție, sancționare, pedepsire	1.71	Ridicat
<i>Administrarea proprietății publice</i>	Informații	securitate națională, informații confidentiale, documente, dosare, drepturi de autor	2.35	Ridicat
	Bani	trezorerie, instrumente financiare, administrarea portofoliului, numerar, prime, cheltuieli, sporuri, indemnizații, etc.	1.82	Ridicat
	Bunuri	gestionare, management și consum (stocuri, computere)	1.47	Mediu
	Imobil	Vînzare/cumpărare	0.44	scăzut

În cele două coloane de pe dreapta, tabelul indică scorurile medii ale participanților la atelier și nivelul inerent de vulnerabilitate.

Acest nivel poate fi scăzut, mediu sau ridicat, pe baza următoarelor criterii:

Scor mediu	Nivel
mediu < 0,8	Scăzut
0,8 ≤ mediu ≤ 1,6	Mediu
mediu > 1,6	Ridicat

¹ Legenda: 0 = nesemnificativ, 1 = relevant, 2 = important, 3 = foarte important

Vulnerabilitatea medie inerentă identificată în timpul atelierului este la un nivel mediu. Din tabel se poate concluziona că domeniile vulnerabile cele mai relevante sunt (în ordinea relevanței):

- Inspecție / audit
- informații
- contractare
- bani
- executare

Discuțiile ulterioare au arătat că scorul pentru "bani" ar putea fi un pic mare, deoarece angajații Curții de Conturi a Republicii Moldova nu au foarte multe procese care implică bani. Bani, în mare parte, se referă doar la salarizare.

De asemenea, în ceea ce privește aspectul de executare, trebuie remarcat faptul că Curtea de Conturi a Republicii Moldova nu are o autoritate directă. Constatările sale pot fi elemente de probă într-o instanță și utilizate în hotărâri pentru aplicarea amenzilor.

4.2 Factorii de sporire a vulnerabilității

Suplimentar la activitățile în mod inerent vulnerabile, anumite circumstanțe sau factori pot spori vulnerabilitatea la încălcări de integritate. Acești factori pot crește vulnerabilitatea, deoarece:

- cresc probabilitatea producerii incidentului
- cresc consecințele (impactul) incidentului (nu doar financiar dar de asemenea cu referire la credibilitate, atmosfera de lucru, relații, imagine etc.)

Multe dintre circumstanțele de sporire a vulnerabilității sau a factorilor care oferă această oportunitate și / sau motivare și / sau raționalizare pentru încălcarea integrității. Alți factori sunt cunoscuți ca indicatori potențiali ai unei culturi de integritate slabe în cadrul unei organizații.

Trebuie subliniat faptul că prezența unuia sau a mai multora dintre acești factori nu implică faptul că încălcarea integrității are loc. Implică numai faptul că organizația este mai vulnerabilă și că există un risc mai mare de încălcări de integritate.

Pe parcursul atelierului participanții au evaluat și au discutat lista completă a factorilor de sporire a vulnerabilității. Această listă și punctajul mediu pentru fiecare factor de sporire a vulnerabilității poate fi găsit în Anexa 2.

Scorurile medii ale participanților la atelier per grup și nivelul rezultat de vulnerabilitate sunt indicate în tabelul de mai jos.

Grupuri a factorilor de sporire a vulnerabilității	Scor mediu (0-3) ²	Nivel
1. Complexitate	0.94	Mediu
2. Schimbare/Dinamică	0.9	Mediu
3. Management	1.05	Mediu
4. Personal	0.9	Mediu
5. Istoricul incidentelor	0.41	Scăzut
Scor mediu total	0.89	Mediu

Similar vulnerabilităților inerente, nivelul de vulnerabilitate sporit poate fi scăzut, mediu sau ridicat, pe baza următoarelor criterii:

Scor mediu	Nivel
mediu < 0,8	Scăzut
0,8 ≤ mediu ≤ 1,6	Mediu
mediu > 1,6	Ridicat

Putem specifica evaluarea vulnerabilității factorilor de creștere pentru fiecare grup, ceea ce face posibil de a identifica motivele care stau la baza pentru nivelul scorurilor de grup (a se vedea anexa 2).

Din tabel se poate concluziona că factorii cei mai relevanți de sporire a vulnerabilității sunt :

- administrare
- complexitate
- Modificare / dinamică
- Personal

Cu toate acestea, trebuie remarcat faptul că toate aceste scoruri sunt în raza frecvențelor joase din categoria medie.

Una dintre principalele preocupări ale participanților a avut de a face cu modul în care Parlamentul percepe rolul Curții de Conturi. Una dintre criticile (implicite) pare a fi că Curtea de Conturi nu asigură că recomandările sale sunt implementate. Făcînd ca Curtea de Conturi să fie o organizație cu o eficacitate limitată (gen – cîinele care latră, dar nu mușcă"). Deoarece rădăcina problemei acestei percepții greșite se află în poziția de informare a Parlamentului, acest lucru poate fi remediat numai prin comunicare. Unul dintre participanți a remarcat că totuși există o evoluție pozitivă. Valoarea adăugată a unei organizații care

² Legenda: Legenda: 0 = nesemnificativ, 1 = relevant, 2 = important, 3 = foarte important

semnalează probleme în cadrul guvernului este din ce în ce mai văzută.

O altă preocupare care a fost exprimată a fost că în perioada următoare, volumul de lucru este de așteptat să crească, din cauza unor modificări legislative care măresc numărul de organizații care trebuie să fie auditate de către CC. Însă nu există dispoziții pentru a crește capacitatea de audit. În cele din urmă, acest fapt poate prezenta un risc pentru calitatea activității de audit.

În rezumat, următoarele remarci suplimentare au fost făcute atunci când am discutat factorii cei mai relevanți de sporire a vulnerabilității, așa cum sunt enumerate mai jos:

- Conducerea nu acordă suficientă atenție opiniei / sfaturilor auditorilor atunci când planifică programul anual de audit
- O interpretare diferită a prevederilor legale este posibilă. De asemenea, aceeași normă este inclusă în diferite acte normative (acte fiscale și vamale) lăsând loc de interpretare. În cele din urmă, acest lucru înseamnă că anumite constatări de audit trebuie să fie stabilite într-o instanță de drept, în loc de Curtea de Conturi în sine.
- Membrii Curții de Conturi sunt numiți de Parlament pentru o perioadă de cinci ani. Acest lucru conferă o influență politică a Parlamentului, chiar dacă membrii odată numiți sunt obligați să fie neutri politic.
- Parlamentul este selectiv vizavi de constatările Curții de Conturi: se acordă mai multă atenție acelor constatări, care sunt favorabile fracțiunii politice. De asemenea, unele rezultate de audit nu primesc nici o atenție din partea Parlamentului.
- Există un nivel ridicat de fluctuație a personalului. Acest lucru duce la o pierdere de cunoștințe și pierderea capacității ca urmare a necesității de a ajuta noii colegi să se acomodeze. Acest lucru poate fi un risc pentru calitatea auditului. O cauză importantă a acestei cifre ridicate este considerat a fi nivelul de salarizare (scăzut), deoarece acest lucru este adesea citat ca un motiv de plecare din cadrul organizației. Pe de altă parte, acest lucru ar putea fi, de asemenea, un lucru "firesc": oamenii sunt mereu în căutarea unor modalități de a-și îmbunătăți poziția.
- Un angajat poate obține un salariu variabil de până la 15% ca spor la salariul său de bază timp de 6 luni, în dependență de performanță. Calitatea performanței este determinată de superiorul direct.

Curtea de Conturi a prezentat Parlamentului un proiect al unei noi legi prin care se intenționează să se reorganizeze structura instituției. Odată cu aprobarea noii legi unele vulnerabilități vor fi diminuate. Noua lege conține prevederi referitoare la politica de remunerare, de asemenea va rezolva problemele legate de influența politică. În acest sens,

auditorul general, va fi numit pe o perioada de 7 ani, în loc de 5 ani, precum și Consiliul va fi înlocuit de către auditorul general și 2 auditori-generalii adjuncți.

4.3 Profilul de vulnerabilitate

Nivelul global de vulnerabilitate, profilul de vulnerabilitate se bazează pe "imaginea" de ansamblu a vulnerabilităților inerente și a factorilor de sporire a vulnerabilităților. Nivelurile combinate ale vulnerabilităților inerente și a factorilor de sporire a vulnerabilității conduc la modificarea nivelului global de vulnerabilitate.

Nivelul inerent de vulnerabilitate evaluat de către participanți este mediu. Nivelul de vulnerabilitate sporită este mediu. Împreună, acesta rezultă într-un profil de vulnerabilitate medie. Acest profil al vulnerabilității este luat în considerare atunci când se compară acest nivel cu nivelul de maturitate al sistemului de control al integrității și joacă un rol, ca parte a analizei lacunelor.

5 Nivelul de maturitate al sistemului de control al integrității

Un element-cheie al metodologiei este evaluarea "nivelului de maturitate" a sistemului de control de integritate. Sistemul de control al integrității este organul de măsuri menite să promoveze, să monitorizeze și să mențină integritatea.

Sistemul de control al integrității organizației este descris utilizând un set extins de măsuri de integritate, împărțite în trei grupe principale (controale generale, dure și blînde).

Controalele dure, după cum sugerează termenul, sunt preocupate în principal cu reglementările, procedurile și sistemele tehnice. Controalele blînde sunt concepute pentru a influența comportamentul, atmosfera și cultura de lucru în cadrul organizației. Grupele din categoria controalelor generale sunt mai largi sau au un amestec de elemente dure și blînde.

Rezultatul evaluării sistemului de control al integrității este prezentat mai jos pentru fiecare grup de măsuri.

Nr.	Grupuri de controale	Mediu	Nivel
	Controale generale		
1	Cadrul de politici	2.26	Ridicat
2	Analiza vulnerabilității/ analiza riscurilor	1.82	Mediu
13	Angajare și selectare	2.63	Ridicat
14	Răspuns la încălcările de integritate	2.64	Ridicat
15	Răspundere	2.53	Ridicat

16	Audit și monitorizare	1.98	Mediu
Controale dure			
3	Responsabilități	2.24	Ridicat
4	Cadrul juridic ISA	2.76	Ridicat
5	Legislația și reglementările privind integritate	2.24	Ridicat
6	Organizarea administrativă și control intern	2.39	Ridicat
7	Securitate	2.97	Ridicat
Controale blinde			
8	Valori și standarde	2.95	Ridicat
9	Standarde profesionale ISA	2.68	Ridicat
10	Recunoaștere a integrității	2.29	Ridicat
11	Atitudinea conducerii	2.57	Ridicat
12	Cultura organizațională	2.37	Ridicat
Scor global mediu pe toate grupurile		2.46	Ridicat

Evaluarea nivelului de maturitate al sistemului de control al integrității ia în considerare existența, punerea în aplicare, funcționarea și efectuarea controalelor. Scorurile privind măsurile individuale variază de la 0, când o măsură este inexistentă, la 3, atunci când există o măsură, este respectată și eficientă, așa cum este indicat în tabelul de mai jos.

Nivel	Criterii
0 – scăzut	<ul style="list-style-type: none"> ▪ Măsura nu există
1 – scăzut	<ul style="list-style-type: none"> ▪ Măsura există ▪ Măsura nu este implementată/respectată.
2 – Mediu	<ul style="list-style-type: none"> ▪ Măsura există ▪ Măsura este implementată/respectată ▪ Măsura nu este efectivă
3 - Ridicat	<ul style="list-style-type: none"> ▪ Măsura există ▪ Măsura este implementată/respectată ▪ Măsura este efectivă

În principiu, cel mai înalt nivel, nivelul de maturitate 3 - este necesar. Scorurile pentru măsurile individuale conduc la scoruri de grupuri și în cele din urmă la un nivel total de maturitate pentru sistemul de control al integrității, în ansamblu. Sistemul de control de integritate globală și scorurile de maturitate pentru fiecare măsură de control pot fi găsite în anexa 3.

Scorul mediu global determină nivelul de maturitate al sistemului de control al integrității, în ansamblu. A se vedea tabelul de mai jos.

Scor pe maturitatea sistemului de control al integrității	Nivel
$0 \leq x \leq 1$	1 Scăzut
$1 < x \leq 2$	2 Mediu
$2 < x \leq 3$	3 Ridicat

Tabelul arată că nivelul general de maturitate al corpului de măsuri este ridicat. Principalele puncte forte ale sistemului pot fi găsite în securitate și valori și standarde. Principalele puncte slabe sunt la analiza de vulnerabilitate / riscuri și audit / monitorizare. Cu toate acestea, nivelul de maturitate al acestor controale totuși este evaluat ca mediu.

În general, se poate spune că controalele blinde au un nivel foarte ridicat de maturitate. Ei au marcat un scor mai înalt decât cele dure, și în special controalele generale. În categoria controalelor blinde, cel mai înalt scor a fost la "valori și standarde". Politica de integritate este o parte a mediului organizațional. În această privință, Curtea de Conturi a elaborat și a aprobat un cod de conduită care conține un set de reguli și standarde de comportament pentru auditori. Acestea sunt derivate din standardele internaționale și cadrul legislativ național. O atenție deosebită este acordată punerii în aplicare a acestui cod de conduită. Nou-veniții sunt familiarizați cu prevederile acestei politici. În plus, pentru noii funcționari publici, jurământul sau pledoaria este obligatorie. Există o ceremonie specială pentru acest lucru.

Următoarele comentarii s-au făcut cu referire la controale

Controale generale

- Elemente ale politicii de integritate sunt încorporate în: acte normative naționale, legea Curții de Conturi, strategia de dezvoltare instituțională, cod de conduită, orientări privind calitate, regulamentele și reglementările cu privire la cadouri și declarații.
- Comunicare cu privire la măsurile de integritate se fac în mai multe moduri: instruire internă, transmiterea informațiilor prin e-mail și pe pagina de internet a Curții de Conturi.
- Curtea de Conturi asigură că informațiile au fost primite/persoanele sunt informate de ceea ce a fost discutat de: lista prezenței (pentru instruire), confirmarea faptului că e-mail-ul a fost primit.
- Angajare și selectare: procedura este respectată cu strictețe. Personalul este angajat în urma unei proceduri legale și a fost făcut cât mai obiectiv posibil. Există 2 runde: proba scrisă, ceea ce duce la o primă selecție și după aceea un interviu (proba orală). Întrebările pentru interviu sunt standardizate. Decizia este luată de către o comisie care constă din 5 persoane la diferite niveluri de responsabilitate din cadrul Curții de Conturi.
- Reacție la încălcarea integrității: încălcări ale integrității în trecut au fost acționate. Există o comisie de disciplină care are dreptul să examineze cazurile de încălcare a integrității suspectate și pot prezenta concluziile lor președintelui. Președintele, în cele din urmă, propune o decizie cu privire la măsurile disciplinare. Procedura exactă nu a fost cunoscută de toată lumea, dar rezultatul (măsurile disciplinare impuse) au fost vizibile.
- Responsabilitatea de integritate: există un cadru normativ privind integritate și există o raportare sistematică. Cu toate acestea, nu toți sunt cunoscuți cu această procedură.
- Audit și follow up: auditul extern privind raportul financiar nu se face. Dar, o evaluare externă privind integritatea se face de către ONG-uri (Transparency International). În acest raport, Curtea de Conturi a fost clasată ca fiind una dintre cele mai puțin corupte organizații.

Controale dure

- Securitate: Curtea de Conturi are un înalt nivel de securitate IT și de securitate fizică. Fiecare auditor are propriul său laptop, cu parola proprie și o rețea de internet închisă. Există o schimbare lunară obligatorie a parolelor. Securitatea fizică a proprietății Curții de Conturi și a bunurilor este asigurată printr-un control de acces la intrare în incintă.
- Curtea de Conturi raportează în mod periodic către agențiile naționale în ceea ce privește nivelul de implementare a politicilor privind integritate și prevenirea corupției. Monitorizarea și rapoartele sunt elaborate / prezentate de către o echipă mică din partea instituției. Participanții nu erau informați de acest lucru. Acesta este motivul pentru care a existat un scor scăzut la măsura privind "coordonatorul de integritate".

Controale blinde:

- O mulțime de training-uri sunt organizate pentru personal la tematica de integritate (incluse în planurile de formare, dar nu ca subiect unic)
- Există cineva care este responsabil pentru lupta împotriva fraudei și corupției, dar el / ea nu este responsabil/ă pentru alte aspecte ale integrității (de prevenire). Este necesar să

se intensifice această activitate pentru a lărgi gama de activități a consilierului/coordonatorului pe integritate.

- Restricții de personal pentru a desemna un coordonator pe integritate (nu există prevedere în acte normative/legale)

Scorurile detaliate privind nivelurile de maturitate au fost utilizate de către participanții la atelier pentru a discuta posibile îmbunătățiri ale sistemului de control al integrității. Participanții au considerat, de asemenea, că controalele au fost deja realizate la un nivel satisfăcător sau nu au nevoie de îmbunătățiri, deoarece acestea nu se aplică la situația din cadrul Curții de Conturi a Republicii Moldova sau ar cauza prea multă birocrație, în raport cu contribuția lor la sistemul de control al integrității. Rezultatele finale a acestui exercițiu sunt reflectate în capitolul privind recomandările.

6 Analiza lacunelor și recomandările

6.1 Analiza lacunelor

După finalizarea evaluării vulnerabilităților și a nivelului de maturitate al sistemului de control al integrității, devine posibil să se analizeze dacă sistemul existent de control este mai mult sau mai puțin în echilibru cu nivelul de vulnerabilitate a organizației și a proceselor sale. În cazul în care ambele niveluri nu sunt în echilibru, există un decalaj, de obicei, indicând faptul că sistemul de control al integrității are nevoie de consolidare. Chiar și în cazul unui echilibru între nivelul de vulnerabilitate și nivelul de maturitate a controalelor de integritate, poate fi încă de dorit să se reducă unele dintre vulnerabilitățile identificate, sau să se abordeze controale specifice care au nevoie de consolidare.

Pe parcursul atelierului, participanții au efectuat o evaluare a nivelului general al vulnerabilităților și a rezistenței. Pentru Curtea de Conturi a Republicii Moldova atelierul a stabilit un echilibru între profilul de vulnerabilitate (nivel: mediu și nivelul de maturitate al sistemului de control al integrității (nivel de maturitate: ridicat). Nivelul de maturitate al sistemului de control al integrității depășește, astfel, nivelul de vulnerabilitate. Cu toate acestea, participanții nu au simțit că acest rezultat justifică "micșorarea" sistemului de control al integrității. Din moment ce, în opinia lor, era încă posibilă reducerea unor vulnerabilități și anumite zone ale sistemului de integritate de control ar putea fi în continuare consolidate, au fost discutate recomandări în această privință.

6.2 Recomandări

Pe baza evaluării vulnerabilităților și (nivelului de maturitate al) sistemul de control al integrității participanții la atelier au formulat o serie de recomandări către conducere. Aceste recomandări pot fi grupate în funcție de temă, după cum urmează.

Recomandările ce vizează reducerea vulnerabilităților

- Creșterea salariilor
- Implicarea auditorilor în procesul anual de planificare
- Asigurarea faptului că aceeași auditori execută misiuni de follow up
- Evitarea faptului desemnării consecutive ale acelorași auditori la misiunile de audit care au ca subiect aceleași entități auditate
- Monitorizarea modificărilor în cadrul regulatoriu
- Îmbunătățirea comunicării cu Parlamentul, ca urmare a aprobării Regulamentului privind cooperarea cu Parlamentul, cu scopul de a spori nivelul de implementare a recomandărilor de audit.

Recomandările formulate pentru a consolida sistemul de control al integrității

- De a organiza instruirii cu tematica de integritate

- De a realiza testul de personalitate (MBTI) pentru angajații CC
- De a actualiza registrul de riscuri (ce ține de riscuri de integritate) și acțiuni formulate pentru a diminua aceste riscuri
- De a îmbunătăți comunicarea internă

Noi credem că implementarea recomandărilor prezentate în acest capitol va contribui la îmbunătățirea gradului de sensibilizare a integrității și a sistemului de control al integrității în cadrul Curții de Conturi a Republicii Moldova.

7 Anexa 1 Lista participanților la atelier

Chiosa Aurel	controlor de stat principal
Certan Alina	controlor de stat principal
Andrieș Violeta	controlor de stat principal
Bulmaga Liuba	controlor de stat superior
Secrieru Vasile	controlor de stat
Baxanean Natalia	controlor de stat superior
Caraman Tatiana	controlor de stat
Babanuța Irina	controlor de stat
Zamăneagră Lilia	controlor de stat superior
Ceban Larisa	controlor de stat
Pavalachii Iulian	controlor de stat
Bogațireț Reghina	controlor de stat principal
Stegărescu Ludmila	consultant superior
Balan Violeta	șef Serviciu
Triboi Tatiana	specialist principal
Oprea Tatiana	specialist principal
Ciolan Alina	redactor principal

Persoana de contact în cadrul CC:

Viorica Verdeș

8

9 Anexa 2 Factori de sporire a vulnerabilității

	Scor (0-3)
1. Complexitate	
1.1 Sisteme inovative /tehnologii informatice avansate	0,94
1.2 Legislație complexă	1,47
1.3 Sisteme speciale (legal / fiscal)	0,47
1.4 Birocrație	1,35
1.5 Lobby	0,65
1.6 Relaționare	1,12
1.7 Imixtiune de interese publice-private(comerț / concurență)	0,47
1.8 Necesitate de expertizare externă	0,59
1.9 Influență/intervenție politică	1,41
2. Schimbări/Dinamica	
2.1 Organizație tânără	0,35
2.2 Legislația frecvent în modificare	1,24
2.3 Creșteri sau reduceri semnificative	1,24
2.4 Privatizare / Cumpărare de cote părți	0,29
2.5 Outsourcing	0,71
2.6 Criza (reorganizare, amenințări cu impact major, supraviețuirea organizației sau postului în cauză)	1,18
2.7 Presiune externă (presiune privind performanța, cheltuieli, timp, presiune politică, deficiențe /resurse slabe în comparație cu volumul de lucru)	1,29
3. Tip de conducere	
3.1 Dominant	1,12
3.2 Manipulativ	0,82
3.3 Formal / birocratic	1,00
3.4 Solistic	0,88
3.5 Remunerare dependentă pe performanță	1,12
3.6 Lipsa de răspundere	0,94
3.7 Ignorarea semnalelor/sfaturilor	1,29
3.8 Reacție defensivă la critică sau plângeri	1,24
4. Personal	
Mediu de lucru / Loialitate	
4.1 Presiune asupra performanței / venit dependent de performanță	1,24
4.2 Statut scăzut/lipsa de încredere/prime mici/perspectivă slabe de creștere	1,35
4.3 Condiții proaste de lucru/Volum de lucru ridicat	1,00
4.4 Loialitate de grup	1,00
4.5 Puterea de a obstrucționa	1,00

Individuală		
4.6	Existența altor interese (munci în afară etc.)	0,47
4.7	Datorii personale	0,82
4.8	Mod de viață (cheltuieli excesive)	1,06
4.9	Secrete personale (vulnerabilitate la șantaj)	0,94
4.10	Amenințări personale	0,65
4.11	Dependențe fizice (alcool, droguri)	0,35
5. Istoricul problemelor		
5.1	Plîngerii	0,53
5.2	Bîrfe și zvonuri	0,88
5.3	Semnale / avertizori de integritate	0,94
5.4	Incidente trecute (recidivism)	0,53
5.5	Probleme administrative (restanțe, inconsistențe, tendințe neordinare etc.)	0,41

10 Anexa 3 Sistem de control al integrității

Cluster	Measure		Nivel de maturitate
1		Cadrul de politici	
	1.1	Măsuri de integritate încorporate în cadrul sistematic de politici	2,59
	1.2	Obiective concrete formulate ca parte a sistemului de integritate	2,35
	1.3	Timp și fonduri bugetate pentru implementarea măsurilor de integritate	1,82
	1.4	Comunicare despre măsurile de integritate	2,35
	1.5	Politica de integritate oficial consfințită în planul global de politici	2,18
		Scor mediu pe grup	2,26
2		Analiza vulnerabilității/analiza riscurilor	
	2.1	Analiza la vulnerabilitate generală/analiza riscurilor efectuată periodic	1,88
	2.2	Analiza aprofundată la domenii și poziții vulnerabile	1,76
		Scor mediu pe grup	1,82
3		Responsabilități	
	3.1	Reponsabilități funcționale pentru integritate	2,53
	3.2	Consultarea sistematică între colaboratori responsabili pentru integritate	2,06
	3.3	Consilier pe integritate	2,41
	3.4	Coordonarea periodică cu organizații și actori din exterior	2,18
	3.5	Coordonator desemnat pentru politici de integritate (extern)	2,00
		Scor mediu pe grup	2,24
4		Cadrul juridic ISA	
	4.1	Existența și independența ISA încorporată în Constituție (ISSAI 10; principiul 1)	2,94
		Cadrul juridic existent pentru a garanta	

Cluster	Measure		Nivel de maturitate
	4.2	- Independența conducătorilor ISA și a membrilor (ai instituțiilor colegiale), inclusiv securitatea posesiei și imunitatea juridică în exercitarea normală a funcțiilor lor (ISSAI 10, principiul 2)	2,76
	4.3	- Un mandat suficient de larg și discreție deplină, în exercitarea funcțiilor ISA (ISSAI 10, principiul 3)	2,65
	4.4	- acces nerestricționat la informații (ISSAI 10, principiul 4)	2,71
	4.5	- dreptul și obligația de a raporta cu privire la activitatea și libertatea ISA de a decide conținutul și calendarul rapoartelor de audit și publicarea și difuzarea acestora (ISSAI 10, Principiul 5/6)	3,00
	4.6	- autonomie administrativă / financiară și managerială și disponibilitatea resurselor, materiale și monetare adecvate (ISSAI 10, principiul 8)	2,53
		Scor mediu pe grup	2,76
5		Legislația și reglementări privind integritate; Există reguli privind:	
		<i>Conflicte de interes</i>	
	5.1	- poziții externe/interese financiare	2,47
	5.2	- acceptare de cadouri/invitații	2,76
	5.3	- confidențialitate	2,82
	5.4	- prevenirea fenomenului "ușilor turnante"	2,12
	5.5	- screening extern al contractorilor și/sau solicitanților de licențe	1,29
	5.6	- lobby	1,59
	5.7	- influența politicianilor asupra funcționarilor publici	2,00
		Integritate cu organizații	
	5.8	- combaterea/adresarea comportamentului necuviincios	2,24
	5.9	- solicitări privind rambursarea cheltuielilor	2,65
	5.10	- utilizare de email, internet I telefon	2,06
	5.11	- utilizarea proprietății angajatorului	2,65
		Scor mediu pe grup	2,24
6		Organizarea administrativă și control intern	
	6.1	Specificarea activităților și pozițiilor vulnerabile	2,18
	6.2	Există proceduri specifice pentru conducerea activităților vulnerabile	1,82
	6.3	Fișe de post pentru tot personalul	3,00
	6.4	Segregarea sarcinilor	3,00
	6.5	Principiul celor 4 ochi - aplicat	2,88
	6.6	Reglementări de mandat	2,88
	6.7	Schema rotației posturilor (ISSAI 40, 6b, element 2)	1,00
		Scor mediu pe grup	2,39

Cluster	Measure		Nivel de maturitate
7		Securitate; Au fost luate măsuri privind:	
	7.1	Securitate fizică (lacături, ferestre, uși, safeuri, etc.)	3,00
	7.2	Securitate informațională (Securitate IT, politica meselor curate, clasificarea informației drept confidențială, autorizare de acces, sisteme de perfectare)	2,94
		Scor mediu pe grup	2,97
8		Valori și standarde	
	8.1	Integritatea este parte a misiunii organizației	3,00
	8.2	Valori fundamentale au fost formulate (de ex. Imparțialitate, profesionalism etc.)	2,94
	8.3	(Cod de conduită (integritate)	3,00
	8.4	Jurământ	3,00
	8.5	Ceremonie specială pentru dare de jurământ	2,82
		Scor mediu pe grup	2,95
9		Standarde profesionale ISA	
	9.1	ISA nu este implicată (sau observată să fie implicată), în orice mod, în managementul organizațiilor pe care le auditează (ISSAI 11, principiul 3, liniile directoare)	2,76
	9.2	În lucrul cu executivul, auditorii acționează numai în calitate de observatori și nu participă la procesul de luare a deciziilor (ISSAI 11, principiul 3, liniile directoare)	2,65
	9.3	Liniile directoare emise de ISA pentru a se asigura că personalul său nu dezvoltă o relație prea apropiată cu entitățile pe care le auditează, astfel încât acestea să rămână obiective și să pară obiective (ISSAI 11, principiul 3, linii directoare)	2,76
	9.4	Cursuri de instruire oferite personalului introducând importanța independenței în cultura IISA și accentuând standardele de calitate și de performanță cerute, asigurându-se că locul de muncă este autonom, obiectiv și fără părtinire (ISSAI 11, principiul 3, bunele practici)	2,65
	9.5	ISA are un cod de etică și standarde cu importanță etică, ce acoperă: - încredere, siguranță și credibilitate (ISSAI 30, capitolul 1); - integritate (ISSAI 30, capitolul 2); - independență, obiectivitate, imparțialitate, neutralitate (politică), evitarea conflictelor de interese (ISSAI 30, capitolul 3; ISSAI 200/2.1-2.32); - secret profesional (ISSAI 30, capitolul 4); - atenție cuvenită și competență (ISSAI 30, capitolul 5; ISSAI 200/2.1, 2.33-2.46).	3,00

Cluster	Measure		Nivel de maturitate
	9.6	Angajații au fost implicați în formularea codului de etică și/sau standardelor cu importanță etică	2,24
		Scor mediu pe grup	2,68
10		Sensibilizare cu privire la integritate	
	10.1	Integritatea este o cerință expresă pentru toate posturile	2,88
	10.2	Cursuri de instruire periodice privind integritate	1,65
	10.3	Angajații la posturi vulnerabile informați cu privire la riscurile particulare și măsuri de contracarare	2,29
	10.4	Asistență specială și/sau consiliere pentru angajați pentru a face față riscurilor de integritate	2,35
		Scor mediu pe grup	2,29
11		Atitudinea conducerii	
	11.1	Conducerea promovează activ importanța integrității	2,71
	11.2	Conducerea caută activ implementarea unei politici de integritate și măsurilor de integritate	2,41
	11.3	Conducerea întotdeauna răspunde adecvat la probleme de integritate	2,59
	11.4	Conducerea ca atare se conformează reglementărilor de integritate și/sau codului de conduită servind ca un exemplu al unui comportament etic adecvat (ISSAI 40, 6b, element 2)	2,59
		Scor mediu pe grup	2,57
12		Cultura organizațională	
	12.1	Se acordă atenție constantă importanței integrității	2,65
	12.2	Aspecte de integritate pot fi discutate confidențial	2,65
	12.3	Există suficiente oportunități pentru a exprima critici	2,00
	12.4	Importanța integrității este clar explicată la relații externe	2,59
	12.5	Comunicare deschisă pe încălcări ale integrității și cum sînt abordate	2,18
	12.6	Cultura de responsabilizare a persoanelor pentru conduita sa	2,65
	12.7	Considerarea suficientă a aspectului de satisfacție cu munca	1,88
		Scor mediu pe grup	2,37
13		Angajare și selectare	
	13.1	Proceduri fixe pentru gestionarea cererilor de angajare	2,94
	12.2	Comisia de Selectare	2,82
	13.3	Verificarea CV-urilor, diplomelor, referințelor etc.	2,76
	13.4	Membrii și personalul de audit al ISA sunt evaluați (screening-ul de pre-angajare) privind calificarea și integritatea morală necesară pentru a îndeplini în totalitate sarcinile lor (ISSAI 1: Declarația de la Lima, secțiunea 14.1)	2,65
	13.5	Integritatea este parte a programului de introducere pentru noii angajați	2,76
	13.6	Declarația de confidențialitate semnată de angajați	2,65

Cluster	Measure		Nivel de maturitate
	13.7	Integritatea este periodic examinată în ședințe de lucru și interviuri privind performanța	2,47
	13.8	Integritatea este un considerent specific la angajarea personalului temporar și din exterior (ISSAI 40, 6b, element 2)	2,47
	13.9	Integritatea se ia în considerare când personalul pleacă din organizație sau în cadrul interviurilor de plecare	2,12
		Scor mediu pe grup	2,63
14		Răspuns la încălcările de integritate	
	14.1	Există procedura de notificare pentru ca angajații să poată raporta suspiciuni privind încălcări (procedura avertizorilor) (ISSAI 40, 6b, element 2)	2,41
	14.2	Conducătorii sînt la dispoziția angajaților pentru raportarea suspiciunilor privind încălcări	2,76
	14.3	Consilierul de integritate este implicat în notificarea încălcărilor	2,65
	14.4	Procedura pentru gestionarea semnalelor și plîngerilor din surse externe	2,76
	14.5	Protocolul pentru anchetarea pretinselor încălcări de integritate	2,65
	14.6	Înregistrarea centralizată a încălcărilor de integritate	2,71
	14.7	Organizația permanent răspunde la încălcările de integritate	2,82
	14.8	Suspiciuni de infracțiuni sînt permanent raportate procuraturii sau poliției	2,12
	14.9	Incidentele sînt evaluate și discutate cu angajații	2,88
		Scor mediu pe grup	2,64
15		Răspundere	
		<i>General</i>	
	15.1	Conducerea de vîrf ia în calcul rapoartele pentru politica de integritate	2,59
	15.2	Personalul reprezentativ primește rapoarte de care ține cont la implementarea politicii de integritate	2,29
	15.3	Autoritățile alese în mod democratic (Parlamentul, Consiliul municipal, etc.) primesc rapoarte de care ține cont la implementarea politicii de integritate.	1,88
	15.4	Rapoartele sunt structurate în mod sistematic și conțin indicatori clari.	2,00
		<i>Specific ISA</i>	
	15.5	Mandatul ISA, rolul, responsabilitățile, organizarea, misiunea, strategiile, manualele, procedurile și criteriile acesteia sunt publice (ISSAI 20, capitolul 2/3)	3,00
	15.6	Constatările și concluziile de audit ale ISA sunt supuse unor proceduri de coroborare (consultare cu entitatea auditată) (ISSAI 20, capitolul 3))	3,00
	15.7	Conturile ISA sunt publice și supuse unui audit extern sau revizuirii parlamentare (ISSAI 20, capitolul 4)	1,59
	15.8	ISA este deschisă cu privire la măsurile de prevenire a corupției și de asigurare a clarității și legalității în propriile sale operațiuni (de exemplu, sancțiuni disciplinare) (ISSAI 20, capitolul 5)	2,76
	15.9	Statutul de auditori (magistrați în modelul Curții, funcționari publici sau altele), competențele și obligațiile acestora sunt publice (ISSAI 20, capitolul 5)	2,76

Cluster	Measure		Nivel de maturitate
	15.10	Externalizarea, expertiza și împărtășirea activității de audit cu alte entități externe, publice sau private, sunt efectuate sub responsabilitatea ISA și sunt subiect a unor reguli precise (ISSAI 20, capitolul 5)	2,47
	15.11	Codurile de etică sunt elaborate și publice	3,00
	15.12	ISA elaborează rapoarte publice cu privire la constatările de audit, management, performanță și comunică în mod deschis cu mass-media sau alte părți interesate (ISSAI 20, capitolul 6)	3,00
		Scor mediu pe grup	2,53
16		Audit și monitorizare	
	16.1	Sistemul de integritate este auditat periodic de către un auditor intern	1,41
	16.2	Sistemul de integritate este revizuit periodic de către un auditor extern și / sau supraveghetor	1,76
	16.3	Sistemul de integritate este monitorizat sau evaluat periodic de către conducere.	2,76
		Scor mediu pe grup	1,98
		Scor total = scor mediu pentru toate grupurile	2,46

11

12 Anexa 4: Lista completă a recomandărilor

Recomandare	Termen scurt	Termen mediu	Termen lung
Creșterea salariilor	13		
Implicarea auditorilor la procesul anual de planificare	4	7	1
Efectuarea testului de personalitate pentru angajații CC (teste MBTI)	2	3	6
A asigura că aceiași auditori execută misiuni de follow up	4	2	3
Actualizarea registrului de riscuri (cu riscuri de integritate) și acțiuni formulate pentru a atenua aceste riscuri			9
Evitarea desemnării consecutive ale acelorași auditori pentru misiunile de audit care au ca subiecți aceleași entități auditate	7	2	

Monitorizarea modificărilor în cadrul regulatoriu		2	7
Îmbunătățirea comunicării interne	5	4	
Îmbunătățirea comunicării cu Parlamentul, ca rezultat aprobarea regulamentului privind cooperare cu Parlamentul, pentru a îmbunătăți nivelul de implementare a recomandărilor de audit		3	4
Organizarea instruirilor cu tematica de integritate		6	
Ajustarea cadrului metodologic cu privire la selectarea tematicii de audit cu justificarea corespunzătoare		4	2
Implementarea prevederilor Strategiei de comunicare și Codului de Etică și procedurilor de mentorat managerial	1	4	1
Revizuirea și ajustarea membrilor reprezentativi pentru noul mandat		3	2
Asigurarea continuității instruirilor ce țin de formularea recomandărilor de audit	1	2	2
Continuarea procesului de identificare a curențelor în legislație			3
Diseminarea informațiilor aferente posibilității angajaților de a fi consultați pe aspecte de integritate		2	

Orizontul de implementa

Recommendation	short term	medium term	long term
Increase the wages	13		
Involvement of the auditors in the audit planning process	4	7	1
Carry out the personality test of CoA employees (MBTI)	2	3	6
Ensure that the same auditors are carrying out the follow -up assignments	4	2	3
Update the risk register (in terms of integrity risks) and actions developed to mitigate those risks			9

Avoiding consecutively appointment of the same auditors for audit missions that has as subjects same auditees	7	2	
Monitoring of changes in the regulatory framework		2	7
Improve the internal communication	5	4	
Improve the communication with the Parliament, as a result of approving the regulation regarding the cooperation with Parliament, in order to enhance the level of implementation of audit recommendations.		3	4
Organise trainings on integrity topics		6	
Adjust the methodological framework regarding the selection of audit topics with the proper justification of choosing it		4	2
Implementation of the provisions of Communication Strategy and of Code Ethics and of coaching managerial procedures	1	4	1
Revise and adjust the members of staff according to the new mandate		3	2
Ensure the continuity of training related to the writing of recommendations	1	2	2
Continue the process of identification of law deficiencies			3
Disseminate the information related to the possibility of employees to be consulted on integrity aspects		2	