Notă de fundamentare a
proiectului Instrucțiunii privind Adecvarea Sistemelor Informatice
utilizate de entitățile reglementate, autorizate/avizate și supravegheate de A.S.F.

Contextul proiectului

În domeniile reglementate și supravegheate de către A.S.F. există un număr semnificativ de reglementări emise de a lungul timpului care fac trimitere la organizarea, adecvarea și auditarea sistemelor informatice pentru entitățile celor trei piețe financiare reglementate și supravegheate.

Instrucţiunea C.N.V.M. nr.2/2011 privind auditarea sistemelor informatice utilizate de entitățile autorizate, reglementate și supravegheate de Comisia Națională a Valorilor Mobiliare, aprobată prin Ordinul preşedintelui Comisia Națională a Valorilor Mobiliare nr. 10/2011, cu modificările şi completările ulterioare, este suspendată în prezent până pe 31 martie 2014 și urmează a fi înlocuită de forma finală a instrucțiunii rezultate din procesul de consultare publică.

Având în vedere observațiile referitoare la instrucțiunea suspendată, discuțiile cu entitățile supravegheate de către sectoarele A.S.F. și cu asociațiile profesionale, **s-a urmărit**:

- **clarificarea** anumitor aspecte ale reglementărilor actuale;
- **eliminarea abordării tehniciste** a auditării IT, orientarea către o abordare de business din perspectiva managementului riscurilor, a stabilității pieței și a protecției consumatorilor;
- **eliminarea obligativității auditării anuale** la toate tipurile de entități indiferent de gradul de risc operațional și sistemic care îl pot genera;
- prevederea de **forme alternative** de auditare:
  - cu resurse interne certificate;
  - prin testări;
  - echivalarea auditărilor la nivel de grup financiar efectuate de companiile mamă, cu acoperirea cerințelor parametrilor instrucțiunii;
- **reducerea costurilor cu privire la auditul** IT prin:
  - introducerea unor forme alternative de auditare;
  - eliminarea obligativității auditării complete pe unul sau mai multe standarde;
  - selectarea elementelor importante de urmărit în cadrul auditării, elemente adaptate la apetitul de risc și categoria fiecărei entități;
- stabilirea de **parametrii diferențiați pe tipuri de entități**;
- **evaluarea proprie de către entități a riscurilor** operaționale generate de utilizarea sistemelor informatice;

- **permiterea de economii de scară** prin utilizarea tehnologiilor digitale de tip cloud-computing, arhivare electronică, data-center externalizat etc. pentru reducerea cheltuielilor conexe activității de bază, în condiții de securitate și calitate stipulate de instrucțiune, standarde, certificări și bune practici internaționale;
- replicarea cerințelor adresate entităților către furnizorii IT, pentru **diminuarea riscurilor generate de serviciile externalizate;**
- **înscrierea centralizată și unitară a auditorilor și a furnizorilor** de servicii externalizate;
- **asigurarea unui cadru profesionist al serviciilor preluate prin externalizare**, la un nivel unitar de standarde si cerințe, care să asigure diminuarea riscurilor precum și un nivel de calitate echivalent cu cel solicitat fiecărui tip de entitate;
- pregătirea unui **suport pentru entitățile reglementate și supravegheate în lupta cu criminalitatea informatică**, prevenirea riscurilor sistemice exogene (generate de terți, interese ostile naționale sau sectoriale, concurențiale, terorism și spionaj cibernetic, furnizori, personal extern, etc.) și a factorilor care pot afecta capacitatea operațională sau sistemică.

Expunere de motive

Obiectul instrucţiunii vizează evaluarea continuă a **riscurilor** operaționale și sistemice **generate de sistemele informatice și de comunicații** în cadrul principalelor activităţi desfăşurate de către entităţile reglementate, direct prin intermediul propriilor oameni, procese și sisteme, sau prin intermediul furnizorilor de servicii, în funcţie de expunerea sistemică și maturitatea entităţilor, pe baza celor mai bune practici in domeniu.

Situația actuală:

- prezenţa în cadrul entităţilor analizate a unor niveluri de maturitate diferite, în funcție de dimensiunea și specificul activității, cu diverse grade de expunere și de apetit la risc;
- neidentificarea tratării la nivelul tuturor entităților a riscurilor operaționale generate de sisteme, oameni, procese și mediul extern, lipsa registrelor de riscuri și a punctelor de control aferente acestor riscuri;
- unele dificultăți întâmpinate cu privire la organizarea pe procese, a controlului modificărilor aduse în sisteme, a lipsei managementului schimbării;
- unele dificultăți întâmpinate cu privire la segregarea de atribuții și a accesesului la nivel de informații și baze de date;
- unele dificultăți întâmpinate de documentare, trasabilitate;
- existența în unele cazuri a dependenței excesive de persoane cheie și furnizori;
- existenţa unor riscuri generate de furnizorii de servicii informatice prin lipsa unui mod de lucru structurat între părți și a nerespectării celor mai bune practici detaliate în standardele relevante.

Principiile urmărite de către proiectul Instrucțiunii

În vederea asigurării stabilității financiare și pentru diminuarea efectelor incidentelor de funcționare a entităților supravegheate de ASF, trebuie aplicate **reguli pentru analizarea, identificarea, prevenirea și reducerea** impactului potențial negativ al materializării vulnerabilităților **generate de utilizarea tehnologiei informației și a comunicațiilor** la nivel de oameni, procese, sisteme și mediu extern.

Prevederile instrucțiunii urmăresc:

1. stabilirea unui **cadru de supraveghere prudențială a ASF**, în mod continuu, pe baza principiilor de supraveghere plecând de la riscuri și a creșterii capacității de analiză, prin intermediul unui sistem de raportare relevant;
2. stabilirea unor **activități solicitate entităților** pentru creșterea gradului de maturitate, pentru îmbunătățirea mediului de evaluare, precum și pentru creșterea eficienței funcției de control intern din cadrul acestora;
3. **alocarea diferențiată a activităților** solicitate entităților în funcție de obiectivul de activitate, dimensiunea și riscul operațional și sistemic prezentat de respectivele entități;
4. **prevenirea riscurilor sistemice exogene** (generate de terți, interese ostile naționale sau sectoriale, concurențiale, terorism și spionaj cibernetic, furnizori, personal extern, etc.) generate de **criminalitatea informatică** externă și a factorilor care pot afecta capacitatea operațională sau sistemică.

Supraveghea prudențială pe bază de riscuri a ASF se va realiza prin analiza încrucișată a informațiilor cuprinse în:

- rapoartele de evaluare internă a riscurilor și registrul de riscuri elaborate de către entități, prin definirea riscurilor, vulnerabilităților identificate și a măsurilor luate pentru diminuare si încadrare in profilul de risc, cu periodicitate anuală;
- rapoartele electronice trimestriale cuprinzând indicatorii cantitativi aferenți activităților și proceselor interne ale entității, pe baza cărora ASF va realiza un punctaj specific fiecărei entități, urmărind încadrarea entităților în cel puțin 90% din punctajul minim solicitat;
- raportul de audit IT:
    - pentru **entitățile încadrate în categoria de risc major,** audit extern, cu periodicitate anuală;
    - pentru **entitățile încadrate în categoria de risc important,** audit extern sau cu resurse interne, cu periodicitate anuală;
    - pentru **entitățile încadrate în categoria de risc mediu și mic,** audit extern sau cu resurse interne ori prin testare a sistemului informatic cu periodicitate de trei ani;
- **raportări speciale la solicitarea expresă a ASF,** ca urmare a concluziilor controlului periodic, inopinat sau permanent, sau a neîncadrării în cel puțin 90% din punctajul minim necesar pentru două perioade de raportare către ASF.

Îmbunătățirea mediului de control intern, a creșterii gradului de maturitate a organizării entităților se va realiza prin luarea de către entități a unor măsuri diferențiate **în funcție de categoria de risc a entității**:

a) evaluarea internă a riscurilor operaționale – definire proprie a riscurilor referitoare la oameni, procese, sisteme si mediul extern, incluzând cel de fraudă, prin:
   - definirea apetitului și a toleranței la risc;
   - determinarea riscurilor inerente și reziduale;
   - înființarea registrului de riscuri cu evaluarea frecvenței, severității și mijloacele de măsurare afer ente pentru fiecare risc;
   - măsuri pentru limitarea riscurilor care depășesc nivelul asumat prin apetitul și toleranța la risc.

b) implementarea de puncte de măsură și control al riscurilor la nivel general, la nivel de programe informatice și la nivel de flux financiar pentru eliminarea vulnerabilităților – controale pot să fie preventive, corective și detective, pe baza principiului segregării responsabilităților, implementarea de fluxuri de aprobare, înregistrare și păstrare a jurnalelor de activități;

c) organizarea pe procese (managementul continuității, a schimbării, al nivelului de servicii, disponibilității, incidentelor, problemelor, configurațiilor);

d) implementarea managementului securității prin aplicarea cerințelor generale, specifice și a celor de securitate a accesului la piețe;

e) implementarea de indicatori cheie de risc;

f) implementarea managementului securității prin măsuri organizatorice, prin elaborarea unui manual al securității informatice și prin implementarea unor proceduri de securitate informatică;

g) participarea în cadrul planului de cooperare cu ASF, cu privire la colectarea, analizarea, avertizarea și a răspunsului la incidente și crize de natură cibernetică.