ANEXA NR. 2
la Metodologie

MODEL DE RAPORT TEHNIC DE EVALUARE (RTE)

Capitolul I
Introducere

Secțiunea 1 - Elemente generale

1.Această secțiune conține date generale cu privire la procesul de evaluare şi trebuie să prezinte cel puțin următoarele elemente:

a) denumirea, numărul de identificare şi versiunea/modelul produsului INFOSEC supus evaluării;
b) date referitoare la dezvoltatorul produsului INFOSEC şi, dacă este cazul, la subcontractanții care au contribuit la dezvoltarea produsului;
c) date privind solicitantul evaluării;
d) programarea activităților aferente procesului de evaluare;
e) date cu privire la entitatea evaluatoare.

Secțiunea a 2-a - Obiective

2.Această secțiune trebuie să prezinte obiectivele RTE.

3.În principal, obiectivele sunt:

a) prezentarea elementelor necesare susținerii unei anumite concluzii cu privire la produsul INFOSEC supus evaluării;
b) susținerea procesului de reevaluare a produsului INFOSEC, în cazul în care solicitantul doreşte acest lucru.

Secțiunea a 3-a - Domeniu de aplicabilitate

4.Această secțiune trebuie să sublinieze faptul că RTE se referă la întreaga activitate desfăşurată în cursul procesului de evaluare.

5.În caz contrar, trebuie specificate motivele pentru care RTE nu acoperă întreaga activitate de evaluare.

Secțiunea a 4-a - Structură

6.Această secțiune trebuie să prezinte structura RTE.

Capitolul II

Sumar

7.Acest capitol furnizează date cu privire la rezultatele evaluării.

8.Totodată, acest capitol trebuie să conțină informațiile generale necesare introducerii produsului INFOSEC în Catalogul național, după certificare.

9.Prin urmare, sumarul nu trebuie să conțină informații clasificate.

10. Acest capitol trebuie să conțină:

a) date cu privire la entitatea evaluatoare;
b) nivelul de evaluare atins efectiv;
c) numărul de identificare şi versiunea/modelul produsului INFOSEC;
d) sumarul principalelor concluzii ale evaluării;
e) date cu privire la solicitantul evaluării;
f) scurtă descriere a produsului INFOSEC supus evaluării;
g) scurtă descriere a caracteristicilor de securitate ale produsului INFOSEC supus evaluării.

Capitolul III

Descrierea produsului INFOSEC supus evaluării

Secțiunea 1 - Funcționalitatea produsului INFOSEC

11. Această secțiune trebuie să conțină o prezentare succintă a rolului operațional al produsului INFOSEC, precum şi a funcțiunilor pentru care a fost proiectat. Descrierea trebuie să conțină cel puțin următoarele elemente:

a) tipul de date care pot fi procesate utilizând produsul (nivel de clasificare etc.);
b) categoriile de utilizatori care vor utiliza produsul INFOSEC (corelat cu precizările de la punctul anterior).

Secțiunea a 2-a - Etapele procesului de dezvoltare

12. Această secțiune trebuie să prezinte etapele parcurse în realizarea produsului.

13. De asemenea, trebuie prezentate metodologiile, tehnicile, instrumentele şi standardele relevante pentru realizarea produsului.

14. Totodată, această secțiune trebuie să includă descrierea elementelor necesare evaluării puse la dispoziția entității evaluatoare de către solicitant. Descrierea trebuie să includă data la care au fost

puse la dispoziție aceste elemente şi numărul de înregistrare cu care a fost luat în evidență fiecare element.

Secțiunea a 3-a - Arhitectura produsului INFOSEC

15. Această secțiune trebuie să conțină un sumar al proiectului general al produsului INFOSEC. Trebuie să se precizeze gradul de separare între componentele care asigură implementarea securității şi celelalte componente. Secțiunea va prezenta şi modul de implementare şi distribuția între componentele hardware, firmware şi software a elementelor care asigură implementarea securității.

16. Toate numerele modelelor/versiunilor acestor componente trebuie specificate într-o anexă la RTE (Anexa C).

Secțiunea a 4-a - Descrierea componentelor hardware

17. Descrierea componentelor hardware trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare, la nivel de arhitectură.

Secțiunea a 5-a - Descrierea componentelor firmware

18. Descrierea componentelor firmware trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare.

Secțiunea a 6-a - Descrierea software

19. Descrierea componentelor software trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare. Descrierea trebuie să furnizeze o legătura dintre componentele software şi cele hardware şi firmware.

Capitolul IV

Caracteristici de securitate ale produsului INFOSEC

20. Trebuie subliniat că înțelegerea țintei de securitate este un element esențial pentru înțelegerea RTE. De aceea, este recomandabil ca acest capitol să includă descrierea completă a țintei de securitate.

21. Capitolul trebuie să abordeze cel puțin următoarele aspecte:

a) politica de securitate pentru produsul INFOSEC;
b) specificarea funcțiilor de implementare a securității;
c) specificarea mecanismelor de securitate;

d) precizarea nivelului minim estimat de eficienţă a mecanismelor de securitate;

e) nivelul de evaluare solicitat.

Capitolul V

Evaluarea

22. Prevederile prezentului capitol detaliază activităţile efectuate în procesul de evaluare, cu specificarea tuturor problemelor identificate, atât a celor de natură tehnică, cât şi a celor de natură managerială.

23. Capitolul trebuie să conţină date care să sprijine activitatea comisiei de certificare de securitate, în analiza aspectelor de natură tehnică şi managerială. Totodată, datele cuprinse în acest capitol pot să contribuie şi la eficientizarea activităţii entităţii evaluatoare.

Secţiunea 1 - Etapele evaluării

24. Această secţiune este similară celei în care sunt prezentate etapele procesului de dezvoltare şi trebuie să includă date cu privire la:

a) data la care a fost demarat procesului de evaluare;

b) data la care au fost furnizate elementele necesare evaluării, inclusiv ţinta de securitate a produsului INFOSEC;

c) perioada în care au fost realizate testele de penetrare;

d) eventuale vizite efectuate la sediile dezvoltatorului sau ale utilizatorului final al produsului;

e) data la care s-au încheiat activităţile tehnice.

25. Secţiunea trebuie să precizeze toate metodele, tehnicile, instrumentele şi standardele utilizate în procesul de evaluare.

Secţiunea a 2-a - Procedura de evaluare

26. Această secţiune trebuie să conţină un sumar al PAE. Sumarul trebuie să includă:

a) activităţile desfăşurate de evaluator, conform PAE;

b) totalitatea activităţilor desfăşurate în procesul de evaluare, cu evidenţierea activităţilor care nu au fost cuprinse în PAE, dar au fost efectuate în practică; va fi precizată motivaţia existenţei acestor discrepanţe.

Secţiunea a 3-a - Domeniul de aplicare a evaluării

27. Această secţiune trebuie să precizeze componentele care au făcut obiectul evaluării, precum şi ipotezele făcute cu privire la componentele care nu au fost examinate.

Secţiunea a 4-a - Constrângeri şi ipoteze

28. Această secțiune trebuie să precizeze eventualele constrângeri asupra procesului de evaluare şi ipotezele făcute în cursul acestui proces.

Capitolul VI

Sumarul rezultatelor evaluării

29. Prevederile prezentului capitol trebuie să prezinte sumarul rezultatelor evaluării, pentru toate activitățile efectuate în cursul procesului.

30. Se recomandă structurarea pe secțiuni care să corespundă fiecăreia dintre activitățile desfăşurate.

31. Fiecare secțiune trebuie să fie corelată cu setul de activități desfăşurate.

32. Prezentăm în continuare, cu titlu de exemplu, o listă de aspecte care fac obiectul acestui capitol:

a) Eficiența constructivă
   - Aspect 1 – Conformitatea funcționalității
   - Aspect 2 – Inter-relaționarea funcționalităților
   - Aspect 3 – Eficiența mecanismelor
   - Aspect 4 – Evaluarea vulnerabilităților constructive
b) Eficiența operațională
   - Aspect 1 – Flexibilitatea în utilizare
   - Aspect 2 - Evaluarea vulnerabilităților operaționale
c) Realizarea produsului – Procesul de dezvoltare
   - Etapa 1 – Cerințe
   - Etapa 2 – Proiectul arhitecturii
   - Etapa 3 – Proiectul detaliat
   - Etapa 4 – Implementarea
d) Realizarea produsului - Mediul de dezvoltare
   - Aspect 1 – Controlul configurației
   - Aspect 2 – Limbaje de programare şi compilatoare
   - Aspect 3 – Măsurile de securitate implementate de către dezvoltator
e) Operare – Documentația de operare
   - Aspect 1 – Documentația de utilizare
   - Aspect 2 – Documentația de administrare

f) Operare – Mediul operațional

- Aspect 1 – Livrarea şi configurarea produsului
- Aspect 2 – Punerea în funcțiune şi operarea

Secțiunea 1 - Teste de penetrare

33. Rezultatele testelor de penetrare au fost analizate separat deoarece testele de penetrare sunt de cele mai multe ori realizate ca parte a unei anumite activități.

34. Prezenta secțiune trebuie să prezinte toate opțiunile de configurare folosite în timpul testelor de penetrare.

Secțiunea a 2-a - Vulnerabilități exploatabile identificate

35. Prezenta secțiune trebuie să descrie vulnerabilitățile ce pot fi exploatate, care au fost identificate în timpul evaluării, precizând:

a) funcția de implementare a securității la care a fost identificată vulnerabilitatea;
b) descrierea vulnerabilității;
c) acțiunile întreprinse de evaluator în momentul identificării vulnerabilității;
d) activitatea în cursul căreia a fost identificată vulnerabilitatea;
e) persoana care a identificat vulnerabilitatea (dezvoltatorul sau evaluatorul);
f) data la care a fost identificată vulnerabilitatea;
g) dacă vulnerabilitatea a fost remediată (se menționează data) sau nu;
h) sursa generatoare a vulnerabilității (dacă este posibil).

Secțiunea a 3-a - Observații legate de vulnerabilități ce nu pot fi exploatate

36. Prezenta secțiune trebuie să descrie vulnerabilitățile ce nu pot fi exploatate şi au fost identificate în cadrul evaluării (subliniindu-le pe cele rămase în produsul operațional).

Secțiunea a 4-a - Erori identificate

37. Prezenta secțiune trebuie să precizeze impactul pe care îl pot avea erorile identificate în cadrul procesului de evaluare.

Capitolul VII

Ghid pentru reevaluare şi analiză a impactului

Prezentul capitol este opțional. Poate fi omis dacă solicitantul evaluării a declarat că nu necesită informații privind o reevaluare sau analiză a impactului.

38. Dacă va fi inclus, acest capitol trebuie să precizeze:

a) includerea fiecărei componente a produsului INFOSEC într-una din următoarele categorii: componente care asigură implementarea securității, componente relevante pentru securitate sau componente care nu sunt relevante pentru securitate;
b) identificarea instrumentelor de dezvoltare care sunt relevante pentru securitate;
c) modalitatea în care constrângerile sau ipotezele făcute în procesul de evaluare pot avea impact în cazul reevaluării sau refolosirii produsului INFOSEC;
d) orice concluzii privind tehnici de evaluare sau instrumente care pot fi utile în cazul unei reevaluări;
e) detalii de arhivare necesare reînceperii evaluării;
f) pregătire specifică necesară reevaluatorilor pentru demararea unui proces de reevaluare.

Capitolul VIII

Concluzii şi recomandări

39. Prezentul capitol trebuie să prezinte concluziile şi recomandările evaluării. Concluzia principală va preciza dacă produsul INFOSEC îndeplineşte obiectivul de securitate stabilit şi dacă are vulnerabilități ce pot fi exploatate.

40. Trebuie să se specifice faptul că recomandările se referă la componentele produsului care au făcut obiectul evaluării şi că pot exista şi alți factori de care evaluatorii nu sunt conştienți, iar aceşti factori pot influența procesul de certificare a produsului INFOSEC.

41. Recomandările pot include sugestii către alte entități, precum solicitantul evaluării sau dezvoltatorul produsului INFOSEC, pentru a fi înaintate comisiei de certificare de securitate.

42. Trebuie să se specifice faptul că rezultatele evaluării sunt valabile numai pentru o anumită versiune a produsului INFOSEC, configurată într-un anumit mod, iar comisia de certificare de securitate trebuie informată despre orice schimbări aduse produsului INFOSEC.

Capitolul IX

Anexele (RTE)

Anexa A- Lista Elementelor necesare evaluării

43. Această anexă trebuie să identifice, cu numerele versiunii şi datele la care au fost recepționate, toate elementele necesare evaluării sau se face o referire la lista elementelor.

Anexa B – Lista de acronime/Glosar de termeni

44. Această anexă trebuie să explice toate acronimele şi abrevierile folosite în RTE. De asemenea, trebuie să definească termenii specifici utilizați.

Anexa C – Configurația Evaluată

45. Configurațiile produsului INFOSEC examinate în cadrul evaluării (în special configurații folosite la testele de penetrare, verificare a fiabilității) trebuie identificate clar.

46. Trebuie precizate orice presupuneri făcute sau configurații care nu au fost luate în considerare.

Descrierea componentelor hardware

47. Descrierea componentelor hardware trebuie să furnizeze informații despre configurație, privind toate componentele la nivel arhitectural ce sunt relevante pentru evaluare şi, în consecință, pentru implementarea securității.

Descrierea componentelor firmware

48. Descrierea firmware trebuie să furnizeze informații despre configurație, despre toate componentelor care sunt relevante pentru procesul de evaluare şi, în consecință, pentru implementarea securității.

Descrierea componentelor software

49. Descrierea componentelor software trebuie să furnizeze informații despre configurație privind părți ale aplicațiilor software utilizate de produsul INFOSEC care sunt relevante pentru procesul de evaluare şi, în consecință, pentru implementarea securității.

Anexa D – Rapoartele activităților de evaluare

50. Această anexă nu este necesară dacă toate rapoartele de activitate sunt incluse în Capitolul VI al RTE.

51. Dacă este prezentă, această anexă trebuie să cuprindă înregistrări ale tuturor activităților de evaluare (incluzând rezultatele testelor efectuate, tehnici şi instrumente utilizate).

Anexa E – Probleme identificate

52. Această anexă trebuie să cuprindă rapoarte cu privire la toate problemele identificate în cursul procesului de evaluare.

53. Rapoartele pot fi emise şi înainte de finalizarea evaluării şi trebuie să conțină cel puțin următoarele elemente:

a) numărul şi versiunea produsului INFOSEC supus evaluării;
b) activitatea în cursul căreia a fost identificată problema;
c) descrierea problemei identificate.