MINISTERUL EDUCAŢIEI
UNIVERSITATEA „VALAHIA” din TARGOVISTE
IOSUD – ŞCOALA DOCTORALĂ DE ŞTIINŢE ECONOMICE ŞI UMANISTE
DOMENIUL FUNDAMENTAL *ŞTIINŢE ECONOMICE*
DOMENIUL *MANAGEMENT*

MANAGEMENTUL RISCULUI DE SECURITATE A INFORMAȚIILOR ÎN INDUSTRIA SOFTWARE

- Rezumatul tezei de doctorat -

CONDUCĂTOR DE DOCTORAT:

Prof. univ. dr. Marius PETRESCU

Doctorand:

Ion Ionuț I. BRATU

TÂRGOVIȘTE

2022

CUPRINS

1. CUPRINSUL TEZEI DE DOCTORAT

2. CUVINTE CHEIE

Management, risc de securitate, evaluarea riscurilor, atenuarea riscurilor, gestionarea riscurilor, metode și tehnici de management al riscurilor, integrabilitate software, costuri, beneficii, aplicații software de management al riscurilor.

3. REZUMATUL TEZEI

Prezenta lucrare abordează problematica managementului riscului de securitate a informațiilor în producția de elemente software și ia în considerare particularitățile acestui domeniu în țara noastră.

Managementul riscului reprezintă o componentă foarte importantă a managementului care trebuie avută în vedere în industria software, domeniu în care derularea activităților economice sub forma proiectelor determină micșorarea timpului de realizare a produselor software, iar resursele financiare specifice pot fi identificate și urmărite cu mai multă precizie.

Producția de software este orientată în general pe proiecte, având în vedere caracterul de specificitate al acestor produse pentru beneficiar. În practica din acest domeniu se înregistrează însă adesea eșecuri reprezentate de produse software inutilizabile în procente extrem de mari, în special din cauza depășirii semnificative de costuri și termene. De aceea este necesară o optimizare a managementului riscurilor în domeniul producției de software, proces care nu poate avea loc în absența unei cunoașteri aprofundate a elementelor specifice domeniului IT&C.

În afara riscurilor cauzate de factorii de presiune care acționează în aproape orice domeniu – termene strânse, bugete limitate, resurse insuficiente – producția de software se confruntă cu o serie de provocări specifice, generate de schimbările tehnologiilor și rolul central al sprijinului oferit de tehnologia informației și comunicațiilor pentru desfășurarea oricărei activități economice și administrative. În plus, un rol important pentru succesul tuturor entităților producătoare de aplicații software, pe o piață imprevizibilă, îl au aspectele care vizează calitatea produselor realizate.

Utilizarea aplicațiilor software de management al riscurilor reprezintă o abordare proactivă pentru minimizarea incertitudinii și pierderilor potențiale asociate cu un proiect. Un risc reprezintă un eveniment sau o condiție care, în cazul în care se produce, are un efect pozitiv sau negativ asupra obiectivelor unui proiect.

Riscurile reprezintă evenimente viitoare cu o probabilitate de apariție mai mare de 0% și mai mică de 100%. De asemenea, consecințele riscurilor sunt neașteptate și neplanificate. Evenimentele viitoare pot fi clasificate ca oportunități (risc pozitiv), în cazul în care efectele lor sunt favorabile organizațiilor, sau ca amenințări (risc negativ), în cazul în care efectele lor sunt nefavorabile.

Asigurarea informațiilor necesare adoptării deciziilor potrivite trebuie să fie obiectivul principal al managerilor din domeniul software, în scopul unei mai bune gestionări a riscurilor. Managementul riscului vizează două componente majore: procesul de evaluare a riscurilor (identificarea, estimarea și evaluarea riscurilor cu care se confruntă un produs software) și

procesul de gestionare a riscurilor (planificarea, monitorizarea, controlul și alegerea mijloacelor de a elimina sau a reduce probabilitatea de apariție sau consecințele riscurilor descoperite). Aceste activități se realizează în permanență pe durata de realizare a unui produs software, de la faza de inițiere a acestuia și până la finalizare.

Implementarea corespunzătoare a managementului riscului oferă o serie de beneficii, după cum urmează:

- sunt definite, analizate și puse în aplicare strategii corespunzătoare de gestionare a riscurilor;
- sunt identificate riscuri potențiale care ar putea avea impact asupra succesului activității de producție;
- sunt analizate și înțelese probabilitatea de apariție și consecințele acestor riscuri;
- sunt stabilite prioritățile în ceea ce privește ordinea de abordare a riscurilor;
- sunt examinate cu atenție modalitățile de atenuare adecvate pentru fiecare problemă identificată;
- sunt identificate și selectate tehnici de atenuare optimizate pentru toate riscurile;
- sunt dezvoltate în mod proactiv planurile de intervenție în procesul de atenuare a riscurilor;
- sunt colectate și analizate diverse informații în scopul îmbunătățirii politicilor de management al riscului;
- procesele, strategiile și procedurile de gestionare a riscurilor sunt în mod sistematic revizuite și optimizate pentru a reduce cât mai mult riscurile.

În practică, există o multitudine de riscuri cu care industria de software se confruntă la nivel global, aspect evidențiat în figura de mai jos. Caracteristicile juridice, mediul social, mediul economic, climatul competitiv etc. impun constrângeri și oferă oportunități care ajută la definirea naturii riscurilor pentru furnizori, cumpărători și alte părți interesate de achiziționarea de soluții software și de procesul de dezvoltare al acestora.

Există numeroase motive din cauza cărora procesele de gestionare a riscurilor nu au implementate pe scară mai largă sau nu s-au bucurat de un succes mai mare. Succesul pieței de afaceri, cumulat cu rigoarea așteptată a unui proces formal de management al riscurilor, a fost considerat a fi, pur și simplu, o pierdere de timp sau bani.

Cu toate acestea, în literatura de specialitate a fost raportat un oarecare succes al procesului de gestionare a riscurilor în domeniul produselor software. În mod evident în ultimii ani s-au realizat progrese importante care trebuie transpuse în practică, în scopul de a utiliza tehnicile de gestionare a riscurilor într-un mod cât mai eficient.

Este recunoscut faptul că riscul implică întotdeauna două caracteristici: probabilitate de apariție și pierdere. În timp ce relația risc – incertitudine este încă de actualitate, există o tendință tot mai mare de a privi riscul atât ca pierdere, cât și ca oportunitate.

Riscul pozitiv se referă la riscul de care putem să profităm pentru că observăm o posibilă oportunitate, ce implică însă și un potențial de eșec (riscul negativ asociat cu pierderea de oportunitate).

Există mai multe tipuri de oportunități ce pot fi observate la nivel de proiect, în cazul în care răspunsurile la acestea sunt oportune și sunt inițiate acțiuni prompte. Acestea includ: oportunități de afaceri (dezvoltarea de produse care, pe timpul ciclului de viață, generează activități cu marjă mare de profit); oportunități operaționale (cu valoare adăugată); oportunități sistemice (economii pe termen lung, asigurări) etc.

Deși cele mai multe dintre abordări se concentrează pe aspectele tradiționale, negative ale riscurilor, ar fi benefic ca fiecare organizație să se gândească la modul în care tehnicile de gestionare a riscurilor ar putea fi adaptate cu succes și în abordarea riscurilor pozitive.

Există foarte multe motive care fac ca managementul riscului să fie dificil de aplicat în mod eficient. Acestea sunt strâns legate de numărul mare de factori de risc care au fost identificați în literatura de specialitate.

Un alt motiv pentru aplicarea relativ scăzută a metodelor formale de gestionare a riscurilor, în practică, este faptul că riscul este un concept abstract iar utilizatorii nu dispun de instrumentele necesare pentru o analiză mai profundă. De asemenea, multe metode de gestionare a riscului se bazează pe cuantificarea riscului iar mulți utilizatori nu au capacitatea de a oferi estimări precise privind probabilitatea și pierderile asociate riscurilor.

Abordările bazate pe tabele pot fi uneori prea părtinitoare sau prea grosiere pentru prioritizarea corectă a riscurilor. Riscurile pot avea, de asemenea, implicații diferite pentru diferite părți interesate. Metodele existente de gestionare a riscurilor nu pot să ofere sprijin pentru rezolvarea acestor diferențe.

De exemplu, cele mai multe abordări care vizează gestionarea riscului se concentrează asupra costurilor, programului sau riscurilor de calitate, dar pot exista combinații de riscuri sau de alte caracteristici, cum ar fi costurile de întreținere, reputația organizației sau răspunderea potențială ori litigiile care ar urma să fie considerate importante în influențarea procesului decizional.

Totodată, multe dintre tehnicile actuale de management al riscurilor pot fi percepute ca fiind prea costisitoare sau prea dificil de utilizat. O soluție la aceste probleme ar putea fi utilizarea tehnicilor simple de gestionare a riscurilor, tehnici care presupun o durată acceptabilă de timp pentru a produce rezultate.

În literatura de specialitate există o serie de surse care expun diferite tipuri de riscuri și probleme aferente industriei software. Deoarece există o mare suprapunere între ele (deși unele au perspective ușor diferite asupra potențialelor riscuri ale produselor software), în prezentul demers științific vor fi abordate doar o parte dintre acestea.

Managerii pot alege să folosească aceste referințe ca un punct de plecare pentru identificarea, evaluarea și analiza riscurilor ce vor fi luate în considerare în dezvoltarea produselor software.

Lucrarea este structurată pe șase capitole, după cum urmează:

În Capitolul I *„Managementul producției în industria de software”* am prezentat o serie de aspecte specifice managementului producției de software în România, care conturează necesitatea creării unui model specific pentru managementul producției în industria IT&C. Acest capitol analizează specificul producției de software în România și pune în evidență principalele caracteristici ale acestui domeniu. Tot în acest capitol sunt prezentate și aspectele generale privind estimarea funcționalității și costurilor în industria de software.

În Capitolul II *„Investițiile în producția de software”* s-au prezentat conceptul, structura și rolul important pe care-l au investițiile în creșterea economică a unei activități economice și, în special, în domeniul IT&C. Totodată s-au prezentat și principalele tipuri de investiții realizate în domeniul producției de software în România.

În acest capitol sunt prezentate aspectele specifice domeniului software, precum și indicatorii specifici, dar și importanța urmăririi riscului specific activităților de investiții. În activitatea de investiții, datorită impactului major în viitor al acestora, se impune estimarea cu o precizie maximă a parametrilor ce caracterizează investiția. Aceste estimări, deoarece sunt făcute în prezent, pot prezenta diferențe substanțiale față de valorile ce vor fi efectiv înregistrate datorită factorilor de influență ce urmează să apară până la manifestarea lor.

În Capitolul III *„Riscul și managementul riscului în producția de software”* s-au prezentat atât caracteristicile generale ale procesului de management al riscurilor, cât și importanța acestui proces în domeniul producției de software. Managementul riscurilor este un element important pentru orice organizație și trebuie să cuprindă toate activitățile care afectează profilul de risc.

Principalele etape ale managementului riscurilor sunt: identificarea riscurilor, măsurarea riscurilor, elaborarea metodelor și tehnicilor de management al riscurilor, monitorizarea și controlul riscurilor. În acest capitol au fost prezentate metode de identificare, măsurare, gestionare, monitorizare și control ale tuturor riscurilor care afectează activitatea unei organizații producătoare de soluții software.

Capitolul IV *„Integrabilitatea software și reutilizarea produselor software”* este capitolul în care se evidenţiază idei şi concepte existente în literatura de specialitate care au dus la realizarea de cercetări ştiinţifice în domeniul reutilizării software.

Dezvoltarea majorităţii produselor software se bazau pe blocuri monolitice, formate dintr-un număr considerabil de părţi cu strânsă legătură între ele, unde aceste relaţii erau în mare parte implicite.

Dezvoltarea bazată pe componente a apărut ca o nouă perspectivă pentru domeniul dezvoltării software, având drept ţintă spargerea blocurilor monolitice în componente interoperaţionale, scăzând astfel complexitatea dezvoltării precum şi a costurilor.

Se analizează indicatorii de apreciere a reutilizabilităţii software cu scopul oferirii unor instrumente care vin în sprijinul managerului de proiect în ceea ce priveşte decizia de integrare a unei componente în sistemul nou dezvoltat.

Prezentarea noţiunilor generale de integrabilitate şi locul unui sistem ERP (Enterprise Risk Management) în managementul deciziei oferă o imagine mai bună a evoluţiei înregistrată de organizații prin trecerea de la componentele dezvoltate disparat la un sistem integrat.

Abordarea problemei integrabilităţii se realizează din perspectiva evaluării mai multor tipuri de integrare şi în funcţie de componentele integrabile disponibile.

Capitolul V se referă la *„Caracteristicile de calitate ale produselor program”* şi punctează aceste aspecte ţinând cont de particularităţile lor comparativ cu alte produse industriale. Încrederea utilizatorilor în produse software testate anterior pe durate lungi de timp acţionează în sensul sprijinirii deciziei clienţilor pentru produsul respectiv, motiv pentru care activitatea de integrare nu trebuie să afecteze în niciun fel calitatea produsului final.

Trebuie avute în vedere şi aspectele financiare ale procesului de asigurare a calităţii, managerul de proiect realizând un echilibru între bugetul alocat şi dimensiunea calitativă a produsului rezultat.

În Capitolul VI *“Modelul conceptual pentru managementul riscului în producția de software - TESRISK”* s-a prezentat un model nou de abordare a riscurilor și a consecințelor acestora specific producției de software în România. În acest capitol este descris un model de management al riscului specific domeniului IT&C, mai precis pentru elaborarea produselor software.

Modelul propus integrează recomandări actuale ale specialiștilor din domeniile managementului riscului și producției de software. Structura modelului este una clară, care pornește de la strategia și politicile de abordare a riscurilor în industria software și detaliază zona riscurilor importante (care au o probabilitate mare de manifestare și un impact deosebit asupra producției software).

Acest model este structurat pe etapele ce urmează a fi parcurse în identificarea, caracterizarea, analiza, controlul și urmărirea riscurilor. Pe această structură este dezvoltat modelul conceptual care se dorește a fi un instrument util pentru managementul organizației.

Existența riscurilor în domeniul IT este o certitudine, iar consecințele acestor riscuri influențează decisiv realizarea produselor software. Managementul riscului presupune eliminarea sau minimizarea rezultatelor negative pe care riscurile le-ar putea provoca în industria de software, dar și de a limita apariția riscurilor.

Modelul propus a identificat ceea ce părea ca o listă de riscuri care sunt luate în considerare într-o achiziție de software și de dezvoltare a proiectului. Știind care ar putea fi aceste riscuri, nu este același lucru cu a ști care sunt riscurile produsului software special în condiții specifice. Există un număr nelimitat și unic de scenarii inerente interne / externe, scenarii care pot influența riscurile posibile la care proiectul nostru sau organizația este susceptibilă. Cheia pentru gestionarea cu succes a riscurilor constă în capacitatea de a adapta procesul formal de gestionare a riscului, astfel încât să abordeze nevoile complementare de afaceri și clienții organizației.

Un proces formal de managementul riscului este un proces continuu pentru abordarea în mod sistematic a riscului pe întreg ciclul de viață al produsului / proiectului. Riscurile pot fi identificate (în stare latentă sau nu), în etapele inițiale ale unui software de-a lungul ciclului său de viață. Capacitatea de a identifica riscurile mai devreme înseamnă eliminarea mai rapidă a riscului, la costuri mai mici și o probabilitate mai mare de succes a proiectului.

Riscul software-ului include atât managementul cât și procedurile tehnice de lucru. În cadrul procedurilor de gestionare a riscului pot fi regăsite activități cum ar fi planificarea, angajarea de personal, urmărirea, asigurarea calității și managementul configurațiilor. În procesele tehnice, acestea pot fi regăsite în activități cum ar fi stabilirea cerințelor de analiza, design, cod și de testare. Planificarea este procesul de management al riscurilor, care este cel mai frecvent raportat. Riscul tehnic de proces cel mai raportat este procesul de dezvoltare software în sine.

Riscul produselor software-ul conține caracteristici de lucru intermediare și finale de produs. În primul rând ca responsabilitate tehnică, riscul de produs poate fi regăsit în cerințele de stabilitate, performanță de proiectare, complexitatea codului și a specificațiilor de testare. Riscul de produs este dificil de gestionat deoarece cerințele de software-ului sunt adesea percepute ca fiind flexibile. Cerințele sunt cele mai importante riscuri de produs raportate în evaluările de risc.

Dincolo de tehnica și gestionarea surselor de risc, ar putea exista, de asemenea, riscuri provenite din surse externe proiectului sau a organizației (de exemplu, natura pieței, cultura de afaceri, etc.).

Complexitatea riscurilor specifice software-ului, apoi, necesită o metodologie formală pentru planificarea, identificarea, evaluarea, monitorizarea și controlul lor - un proces formal de managementul riscului.

Poate fi trasată o hartă de management al riscului pentru creșterea capacității de a gestiona riscul specific activității de realizare a unui software. Această hartă de management al riscului conține următoarele etape de gestionare a riscului, și anume:

- descrierea detaliată a produsului software;
- identificarea riscurilor;
- caracterizarea riscurilor;
- analiza riscurilor;
- raportarea situației inițiale a riscurilor;
- stabilirea acțiunilor pentru diminuarea sau chiar eliminarea influenței riscurilor;
- controlul și monitorizarea permanentă a riscurilor și
- concluzii și recomandări utile managementului riscului pentru producerea de software în viitor.

Între fiecare dintre etape sunt viziuni, obiective și strategii care guvernează modul în care organizația intenționează să realizeze tranziția între etape. Viziunea reprezintă o stare ideală a practicii care ghidează procesul de management al riscului, acționând ca o forță de conducere, care oferă motivația necesară pentru a continua îmbunătățire a efortului de gestionare a riscurilor. Scopurile sunt stabilite și realizate pentru a atinge viziunea. Odată ce o poziție actuală este înțeleasă, obiectivele vor determina domeniul de aplicare al sarcinilor următoare.

În cele din urmă, strategia de abordare specifică pentru a realiza obiectivele, care conține informații importante despre cum să se atingă obiectivele și activitățile de definire care vor ajuta la a verificarea rezultatelor. În cazul în care rezultatele nu implică atingerea obiectivelor, ajustări tactice se pot realiza cu privire la strategia elaborată. Harta de gestionare a riscului împarte responsabilitatea între cei patru factori majori de capacitate de gestionare a riscurilor și oferă cinci obiective pentru fiecare factor important.

Acest document, până în prezent, a identificat o multitudine de riscuri la care un proiect de software poate fi vulnerabil, și a furnizat o imagine de ansamblu a proceselor de gestionare a riscurilor formale care pot fi utilizate și adaptate pentru a identifica, analiza, prioritiza, planifica, monitoriza și rezolva/ atenua aceste riscuri. Această secțiune, apoi, identifică unele dintre instrumentele și template-uri care sunt disponibile (sau pot fi adaptate) pentru a ajuta organizațiile și în mod oficial proiectele pentru gestionarea riscurilor lor.

Listele de control sunt unul din instrumentele mai importante în a ajuta la gestionarea riscurilor în proiecte de software, și ele nu sunt neapărat limitate la probleme de identificare a riscului. În lucrare se prezintă o listă de verificare relativ detaliată pentru tipurile de probleme pe care le va aborda managementul riscurilor în producția și comercializarea de software.

Numirea unui ofițer de risc și stabilirea unei baze de date de risc sunt precursori importanți ai asigurării că toate sarcinile de achiziție în proiect sunt stabilite. Există, de asemenea o serie de

întrebări care să fie puse în raport cu desfășurarea programului de gestionare a riscurilor în scopul de a se asigura că toate riscurile vor fi rezolvate în mod corespunzător.

Este important ca echipa de proiect să fie în situația nu doar de a monitoriza și de a analiza riscurile identificate anterior pe parcursul întregului ciclu de viață, dar, de asemenea, să fie sensibilă la apariția unor noi riscuri pe măsură ce ciclul de viață avansează de la dezvoltare, prin testare și de producție, la funcționare efectivă.

Fiecare eveniment (risc posibil) urmează să aibă propriul profil de risc care să documenteze probabilitatea de apariție, impactul acestui eveniment, severitatea impactului, precum și întârzierile care rezultă ca impact asupra proiectului. Aceste profiluri urmează să fie actualizate în mod regulat, în funcție de circumstanțe. Planul oficial de management al riscului urmează să cuprindă dispoziții explicite pentru a alerta părțile interesate și factorii de decizie-cheie în cazul în care un risc este considerat iminent.

În plus, liste de verificare și de auto-evaluare cuprind: viziune și obiective, responsabilitate, proceduri, metode, clasificarea riscurilor, situațiile de risc și recenzii, părțile interesate, evaluarea riscurilor, planificarea riscurilor, instrumente de gestionare a riscurilor, reducerea riscurilor și implementarea și supravegherea și urmărirea riscului.

Un alt element comun pentru toate activitățile formale de gestionare a riscurilor este crearea unei baze de date de management al riscului. Elemente minime recomandate ale unei astfel de baze de date sunt definite în tabelul .

Un element important în identificarea riscurilor este stabilirea limitelor expunerilor pentru fiecare tip de risc. Aproape toți factorii de risc pot fi identificați și cuantificați prin utilizarea informațiilor care pot fi observate direct din istoricul activității organizației și al domeniului.

Procesele de monitorizare a riscurilor sunt stabilite cu scopul de a evalua performanța strategiilor și politicilor organizațiilor de a atinge obiectivele stabilite. Managementul asigură eficacitatea procesului de management al riscului.

Managementul riscului în industria de software presupune evaluarea adecvată a măsurilor de control, atât din punctul de vedere al eficacității în reducerea probabilității apariției unui risc dat, cât și în eficacitatea în reducerea impactului care ar putea apărea. Dacă este necesar, se pot lua măsuri pentru a realiza și implementa soluții eficiente pentru a reduce riscul la un nivel acceptabil. Un proces permanent de monitorizare este esențial pentru managementul eficient al riscurilor. O monitorizare permanentă a activităților poate oferi avantajul unei detectări corecte și în timp util a unor deficiențe în politicile, procesele și procedurile de control a riscurilor.

Prin analiza riscurilor la care este supusă producția de software, a fost atins obiectivul managementului riscului. Astfel, au fost stabilite cauzele riscurilor și s-au făcut propuneri în vederea adoptării unor decizii fundamentate cu ajutorul aplicației dezvoltate pe modelul TESRISK.

4. CURRICULUM VITAE

Informații personale

Nume/prenume: BRATU ION IONUT

Adresă: str. Sibiu nr. 12, sector 6, București

Email: iondinrom@gmail.com

Educație și formare

Perioada: 2004-2009

Universitatea Bioterra, București

Licență în științe juridice

Perioada: 1994-1998

Academia F.A. „Henri Coandă”, Brașov

Licență în managementul organizației

Perioada: 1994-1998

L.M. „Dimitrie Cantemir”, Breaza

Diplomă de bacalaureat

Experiența profesională

2004-prezent

Funcționar

Administrația publică centrală

1998-2004

Instructor

Ministerul Apărării Naționale

Aptitudini și competențe:

Competențe lingvistice:

Limba maternă: limba română

Limbi străine: engleză, franceză

Aptitudini si competente sociale:

Experiență în lucru cu oamenii, bună relaționare interpersonală, abilitați de comunicare, evitare și aplanare a situațiilor conflictuale, adaptabilitate la situații noi, dobândite ca urmare a desfășurării de activități în echipă și într-o poziție în care comunicarea este importantă.

Aptitudini si competente organizatorice:

Spirit organizatoric, cooperant, capacitate de a lucra în echipă și în condiții de stres, atenție distributivă, adaptabilitate, inițiativă, dobândite ca urmare a conducerii activității unor persoane la locul de muncă și în cadrul evenimentelor organizate.

Competente și aptitudini de utilizare a calculatorului:

Microsoft Office, Internet Explorer, Outlook, Microsoft Exchange, SQL Server.

Certificat absolvire:

Certificat de absolvire abilitare funcționare în calitate de cadru didactic, 1998
Certificat de competență lingvistică limba engleză, 2000.

5. LISTĂ DE LUCRĂRI

1. **Risk and Uncertainty in Information Society**
   Florentina Raluca Bîlcan , Ionuț Adrian Ghibanu, **Ion Ionuț Bratu**, George Adrian Bîlcan

   Academic Journal of Economic Studies
   Vol. 5, No. 4, December 2019, pp. 126–131
   ISSN 2393-4913, ISSN On-line 2457-5836

2. **The Relationship between Internal Control and Security Risk Management**
   Florentina Raluca Bîlcan , Ionuț Adrian Ghibanu, **Ion Ionuț Bratu**, George Adrian Bîlcan

   Academic Journal of Economic Studies
   Vol. 5, No. 4, December 2019, pp. 139–144
   ISSN 2393-4913, ISSN On-line 2457-5836

3. **Information Security Risk Audit in Organizations**
   Ion Ionuț Bratu

   Global Conference on Business and Finance Proceedings
   Volume 16, Number 2, May 2021, pp. 126-128
   ISSN 1941-9589 ONLINE, ISSN 2168-0612 USB Flash Drive

4. **Corporate Governance Based on Ethical Governance**
   Marian Catalin Burcescu, Oana Cristina Balacciu (Ene), Aurelian Vrânceanu, Sebastian Gabor, **Ion-Ionuț Bratu**, Ionica Oncioiu

   Global Conference on Business and Finance Proceedings
   Volume 17, Number 1, January 2022, pp. 88-90
   ISSN 1941-9589 ONLINE, ISSN 2168-0612 USB Flash Drive

6. TABLE OF CONTENTS

7. KEY WORDS

Management, security risks, risk assessment, risk mitigation, risk management, methods and technics used for risk management, software integrability, costs, benefits, software products for management risk.

8. SUMMARY

This paper addresses the issue of information security risk management in the production of software and takes into account the particularities of this field in our country.

Risk management is a very important component of management that must be considered in the software industry, an area in which the development of economic activities in the form of projects reduces the time to make software products, and specific financial resources can be identified and tracked more accurately.

Software production is generally project-oriented, given the specific nature of these products for the beneficiary. In practice in this field, however, there are often failures represented by unusable software products in extremely high percentages, mainly due to the significant exceeding of costs and deadlines. That is why it is necessary to optimize the risk management in the field of software production, a process that cannot take place in the absence of an in-depth knowledge of the specific elements of the IT&C field.

In addition to the risks posed by pressure factors operating in almost any field - tight deadlines, limited budgets, insufficient resources - software production faces a number of specific challenges posed by changes in technology and the central role of information technology support, and communications for carrying out any economic and administrative activity. In addition, an important role for the success of all entities producing software applications, in an unpredictable market, is played by the aspects aimed at the quality of the products made.

The use of risk management software applications is a proactive approach to minimizing the uncertainty and potential losses associated with a project. A risk is an event or condition that, if it occurs, has a positive or negative effect on the objectives of a project.

Risks are future events with a probability of occurrence greater than 0% and less than 100%. The consequences of the risks are also unexpected and unplanned. Future events can be classified as opportunities (positive risk) if their effects are favorable to organizations, or as threats (negative risk) if their effects are unfavorable.

Providing the information needed to make the right decisions must be the main goal of software managers in order to better manage risk. Risk management covers two major components: the risk assessment process (identifying, estimating and assessing the risks faced by a software product) and the risk management process (planning, monitoring, controlling and choosing the means to eliminate or reduce the likelihood of occurrence or consequences of discovered risks). These activities are performed continuously during the development of a software product, from its initiation phase to completion.

Proper implementation of risk management offers a number of benefits, as follows:

- appropriate risk management strategies are defined, analyzed and implemented;
- potential risks are identified that could have an impact on the success of the production activity;
- the probability of occurrence and the consequences of these risks are analyzed and understood;
- priorities are set in terms of the order in which risks are addressed;
- the appropriate mitigation modalities for each identified problem are carefully examined;
- mitigation techniques optimized for all risks are identified and selected;
- intervention plans in the risk mitigation process are proactively developed;
- various information is collected and analyzed in order to improve risk management policies;
- risk management processes, strategies and procedures are systematically reviewed and optimized to minimize risks.

In practice, there are a multitude of risks that the software industry faces globally, as highlighted in the figure below. Legal characteristics, social environment, economic environment, competitive climate, etc. impose constraints and provide opportunities that help define the nature of risks for vendors, buyers, and other stakeholders in purchasing software solutions and developing them.

There are many reasons why risk management processes have not been implemented on a larger scale or have not been more successful. The success of the business market, combined with the expected rigor of a formal risk management process, was considered to be simply a waste of time or money.

However, some success of the software risk management process has been reported in the literature. Clearly, significant progress has been made in recent years that needs to be put into practice in order to use risk management techniques as effectively as possible.

It is recognized that risk always involves two characteristics: probability of occurrence and loss. While the risk-uncertainty relationship is still relevant, there is a growing tendency to view risk as both a loss and an opportunity.

Positive risk refers to the risk that we can take advantage of because we observe a possible opportunity, but which also implies a potential for failure (negative risk associated with the loss of opportunity).

There are several types of opportunities that can be observed at project level, if the answers to them are timely and prompt actions are initiated. These include: business opportunities (development of products that, during the life cycle, generate activities with a high profit margin); operational opportunities (with added value); systemic opportunities (long-term savings, insurance), etc.

Although most of the approaches focus on traditional, negative aspects of risk, it would be beneficial for each organization to think about how risk management techniques could be successfully adapted and how to address positive risks.

There are many reasons why risk management is difficult to apply effectively. These are closely related to the large number of risk factors that have been identified in the literature.

Another reason for the relatively low application of formal risk management methods, in practice, is that risk is an abstract concept and users do not have the necessary tools for a deeper analysis. Also, many methods of risk management are based on risk quantification and many users do not have the capacity to provide accurate estimates of the probability and losses associated with the risks.

Table-based approaches can sometimes be too biased or too crude to properly prioritize risk. Risks may also have different implications for different stakeholders. Existing risk management methods cannot provide support for resolving these differences.

For example, most risk management approaches focus on quality costs, program, or risks, but there may be combinations of risks or other characteristics, such as maintenance costs, the reputation of the organization, or potential liability, or subsequent litigation. be considered important in influencing the decision-making process.

At the same time, many of the current risk management techniques may be perceived as too expensive or too difficult to use. One solution to these problems could be to use simple risk management techniques, which take an acceptable amount of time to produce results.

In the literature there are a number of sources that expose different types of risks and problems related to the software industry. As there is a large overlap between them (although some have slightly different perspectives on the potential risks of software products), only some of them will be addressed in this scientific approach.

Managers may choose to use these references as a starting point for identifying, assessing and analyzing the risks that will be considered in software development.

This paper is structured in six chapters, as follows:

In Chapter I "Production management in the software industry" we presented a series of specific aspects of software production management in Romania, which outlines the need to create a specific model for production management in the IT & C industry. This chapter analyzes the specifics of software production in Romania and highlights the main features of this field. Also in this chapter are presented the general aspects regarding the estimation of functionality and costs in the software industry.

Chapter II "Investments in software production" I presented the concept, structure and important role that investments have in the economic growth of an economic activity and, in

particular, in the IT&C field. At the same time, the main types of investments made in the field of software production in Romania were presented.

This chapter presents the specific aspects of the software field, as well as the specific indicators, but also the importance of tracking the specific risk of investment activities. In the investment activity, due to their major impact in the future, it is necessary to estimate with maximum precision the parameters that characterize the investment. These estimates, as they are currently Chapter IV "Software integrability and reuse of software products" made, may present substantial differences from the values that will actually be recorded due to the influencing factors that will occur until their manifestation.

Chapter III "Risk and risk management in software production" presented both the general characteristics of the risk management process and the importance of this process in the field of software production. Risk management is an important element for any organization and must include all activities that affect the risk profile.

The main stages of risk management are: risk identification, risk measurement, development of risk management methods and techniques, risk monitoring and control. This chapter presents methods for identifying, measuring, managing, monitoring and controlling all risks that affect the activity of an organization producing software solutions.

is the chapter that highlights ideas and concepts existing in the literature that have led to scientific research in the field of software reuse.

The development of most software products was based on monolithic blocks, consisting of a considerable number of closely related parts, where these relationships were largely implicit.

Component-based development has emerged as a new perspective for the field of software development, aiming at breaking monolithic blocks into interoperable components, thus reducing the complexity of development as well as costs.

The indicators of appreciation of software reusability are analyzed in order to provide tools that support the project manager in terms of the decision to integrate a component in the newly developed system.

The presentation of the general notions of integrability and the place of an ERP (Enterprise Risk Management) system in decision management provides a better picture of the evolution of organizations by moving from disparately developed components to an integrated system.

The approach to the problem of integrability is made from the perspective of evaluating several types of integration and depending on the available integrable components.

Chapter V refers to the "Quality characteristics of program products" and points out these aspects taking into account their particularities compared to other industrial products. Users 'trust in previously tested software for long periods of time acts in support of the customers' decision

for the product, which is why the integration activity must not affect the quality of the final product in any way.

The financial aspects of the quality assurance process must also be taken into account, the project manager achieving a balance between the allocated budget and the qualitative dimension of the resulting product.

Chapter VI “Conceptual model for risk management in software production - TESRISK” presented a new model for addressing risks and their consequences specific to software production in Romania. This chapter describes a risk management model specific to the IT&C field, more precisely for software development.

The proposed model integrates current recommendations of specialists in the fields of risk management and software production. The structure of the model is a clear one, which starts from the strategy and policies of addressing the risks in the software industry and details the area of important risks (which have a high probability of manifestation and a particular impact on software production).

This model is structured on the steps to be taken in identifying, characterizing, analyzing, controlling and tracking risks. On this structure is developed the conceptual model that is intended to be a useful tool for the management of the organization.

The existence of risks in the IT field is a certainty, and the consequences of these risks decisively influence the development of software products. Risk management involves eliminating or minimizing the negative results that risks could cause in the software industry, but also to limit the occurrence of risks.

The proposed model identified what appeared to be a list of risks that are considered in a software acquisition and project development. Knowing what these risks might be is not the same as knowing what the risks of the particular software product are in specific conditions. There are an unlimited and unique number of inherent internal / external scenarios, scenarios that can influence the possible risks to which our project or organization is susceptible. The key to successful risk management is the ability to adapt the formal risk management process to address the complementary needs of the organization's business and customers.

A formal risk management process is an ongoing process for systematically addressing risk throughout the product / project life cycle. Risks can be identified (latent or not) in the initial stages of a software throughout its life cycle. The ability to identify risks earlier means eliminating risk faster, at lower costs and a higher probability of project success.

Software risk includes both management and technical work procedures. Activities such as planning, staffing, tracking, quality assurance and configuration management can be found in risk management procedures. In technical processes, they can be found in activities such as setting analysis, design, code, and testing requirements. Planning is the most commonly reported risk

management process. The most reported technical process risk is the software development process itself.

Product Risk Software contains intermediate and final product working features. First of all as a technical responsibility, the product risk can be found in the requirements of stability, design performance, complexity of the code and test specifications. Product risk is difficult to manage because software requirements are often perceived as flexible. Requirements are the most important product risks reported in the risk assessments.

Beyond the technique and management of risk sources, there may also be risks from sources outside the project or organization (eg market nature, business culture, etc.).

The complexity of software-specific risks, then, requires a formal methodology for planning, identifying, evaluating, monitoring and controlling them - a formal risk management process.

A risk management map can be drawn to increase the capacity to manage the risk specific to the software development activity. This risk management map contains the following risk management steps, namely:

- detailed description of the software product;
- identifying risks;
- risk characterization;
- risk analysis;
- reporting the initial risk situation;
- establishing actions to reduce or even eliminate the influence of risks;
- permanent control and monitoring of risks and
- conclusions and recommendations useful for risk management for future software production.

Between each of the stages are visions, objectives and strategies that govern how the organization intends to make the transition between stages. The vision is an ideal state of practice that guides the risk management process, acting as a driving force, providing the motivation needed to continue to improve the risk management effort. Goals are set and achieved to achieve vision. Once a current position is understood, the objectives will determine the scope of the following tasks.

Finally, the specific approach strategy to achieve the objectives, which contains important information on how to achieve the objectives and defining activities that will help to verify the results. If the results do not involve achieving the objectives, tactical adjustments can be made to the strategy developed. The risk management map divides the responsibility between the four major factors of risk management capacity and provides five objectives for each important factor.

This document has so far identified a multitude of risks to which a software project may be vulnerable, and has provided an overview of formal risk management processes that can be used and adapted to identify, analyze, prioritize , plan, monitor and resolve / mitigate these risks. This section then identifies some of the tools and templates that are available (or can be adapted) to help organizations and officially their risk management projects.

Checklists are one of the most important tools in helping manage risk in software projects, and they are not necessarily limited to risk identification issues. The paper presents a relatively detailed checklist for the types of problems that risk management will address in software production and marketing.

The appointment of a risk officer and the establishment of a risk database are important precursors to ensuring that all procurement tasks in the project are set. There are also a number of questions to be asked in relation to the development of the risk management program in order to ensure that all risks will be properly addressed.

It is important for the project team not only to be able to monitor and analyze previously identified risks throughout the life cycle, but also to be sensitive to new risks as the life cycle progresses. to development, testing and production, to effective operation.

Each event (possible risk) must have its own risk profile that documents the probability of occurrence, the impact of this event, the severity of the impact, as well as the resulting delays as an impact on the project. These profiles are to be updated regularly, depending on the circumstances. The formal risk management plan should include explicit provisions to alert stakeholders and key decision-makers if a risk is considered imminent.

In addition, checklists and self-assessments include: vision and objectives, responsibility, procedures, methods, risk classification, risk situations and reviews, stakeholders, risk assessment, risk planning, risk management tools, risk reduction and implementation and supervision and risk tracking.

Another common element for all formal risk management activities is the creation of a risk management database. The minimum recommended elements of such a database are defined in the table.

An important element in identifying risks is setting exposure limits for each type of risk. Almost all risk factors can be identified and quantified by using information that can be observed directly from the history of the organization and the field.

Risk monitoring processes are established in order to assess the performance of organizations' strategies and policies to achieve the set objectives. Management ensures the effectiveness of the risk management process.

Risk management in the software industry requires an adequate assessment of control measures, both in terms of effectiveness in reducing the likelihood of a given risk occurring and

in effectiveness in reducing the impact that may occur. If necessary, steps can be taken to achieve and implement effective solutions to reduce the risk to an acceptable level. An ongoing monitoring process is essential for effective risk management. Ongoing monitoring of activities can provide the advantage of correct and timely detection of deficiencies in risk control policies, processes and procedures.

By analyzing the risks to which software production is subjected, the objective of risk management has been achieved. Thus, the causes of the risks were established and proposals were made for informed decisions using the application developed on the TESRISK model.