

ANALIZA RISCULUI ÎN CADRUL TESTĂRII DE ACCEPTANȚĂ

Drd. Oxana STOROJ, ASEM

În acest articol, se descrie metoda de abordare a testării de acceptanță a utilizatorilor (UAT) pe baza analizei riscului. Sunt prezentate definițiile riscului și abordării testării pe baza riscului. Totodată, prezentăm diferite situații când riscurile pot apărea în timpul testării acceptanței utilizatorilor (UAT) și descriem procesul testării bazat pe riscuri. Propunem folosirea unor metode și tehnici de identificare a riscului, precum Brainstormingul, metoda Delphi, metoda analizei probabilității și altele. De asemenea, este prezentată și matricea trasabilității riscului.

Cuvinte-cheie: risc, testare, calitate, testarea acceptanței utilizatorului, abordarea bazată pe risc.

JEL: C68; C87.

Introducere. Testarea oricărui proiect real este o sarcină care nu poate fi îndeplinită complet, din cauza schimbării permanente a mediului înconjurător extern. Când proiectul este în stadiul final și utilizatorii reali încep testarea, apar alte probleme care previn testarea exhaustivă. Ele sunt:

- cerințele care nu au fost discutate în faza de documentare a proiectului;
- absența experienței în testare;
- lipsa timpului din cauza altor datorii operaționale;
- refuzul de a testa;
- lipsa cunoștințelor privind testarea;
- etc.

Managementul fiecărui sistem trebuie să ia în considerare aceste informații și să prevadă orice eșec, care se poate întâmpla și care ar presupune costuri mari în cazul apariției. În plus, ar trebui planificate unele activități de prevenire, pentru a evita riscurile detectate.

RISK ANALYSES USED IN ACCEPTANCE TESTING

PhD candidate Oxana STOROJ, ASEM

This article is talking about risk based testing approach in user acceptance testing UAT (User Acceptance Testing). There are presented definitions of risk and risk based testing. In addition, we are talking about risks that can appear during UAT and we are describing the process of testing based on risks. We propose some techniques and methods of identifying risks such as using Brainstorming, Delphi method, probability analysis method and others. Also, risk traceability matrix is presented as a method of prioritizing risks.

Key words: risk, testing, quality, user acceptance testing, risk base approach.

JEL: C68; C87.

Introduction. Testing any real-world project is a task than cannot be fully done, due to the permanently changing of external environment. When project is on the final stage and real users begin testing there appear another problems that prevent exhaustive testing. They are:

- requirements that where not discussed on the documentary phase of the project;
- absence of experience in testing;
- lack of time due to other operational duties;
- unwillingness to test;
- unawareness to test;
- etc.

Management of any system needs to take into account this knowledge and estimate any failure that can happen and would cost a lot in case of its occurrence. In addition, some preventing works should be planned, in order to avoid detected risks.

În acest articol, sunt prezentate unele metode de identificare a riscurilor, prioritizarea lor și metodele de analiză.

Definiție a riscului. Testarea bazată pe luarea în calcul a riscurilor este o strategie de stabilire a potențialelor riscuri și de testare a unor părți ale proiectului, care au probabilitate mai mare de eșec și pierderi financiare mai mari [2].

Sunt foarte importante stabilirea nivelului acceptabil al calității proiectului și confirmarea faptului că riscurile rămase după testare sunt acceptabile pentru afacere.

Riscul rezidă în probabilitatea apariției oricărui eveniment sau a oricărei circumstanțe care pot afecta negativ proiectul (figura 1) [1]. Figura 1 reprezintă procesul managementului riscului și în orice moment al procesului apare necesitatea da a calcula riscul.

This article is talking about methods of identifying risks, their prioritizing and methods of their analysis.

Risk definition. Risk based testing is a testing strategy based on determining potential risks and testing parts of the project that has higher probability of failure and higher financial losses [2].

It is very important to determine the acceptable level of project quality and to confirm that risks remained after testing are acceptable to the business.

Risk is a probability of appearance of any event or condition that can negatively affect the project (figure 1) [1]. Figure 1 represents the process of risk management and the moment when becomes necessary to calculate the risk.

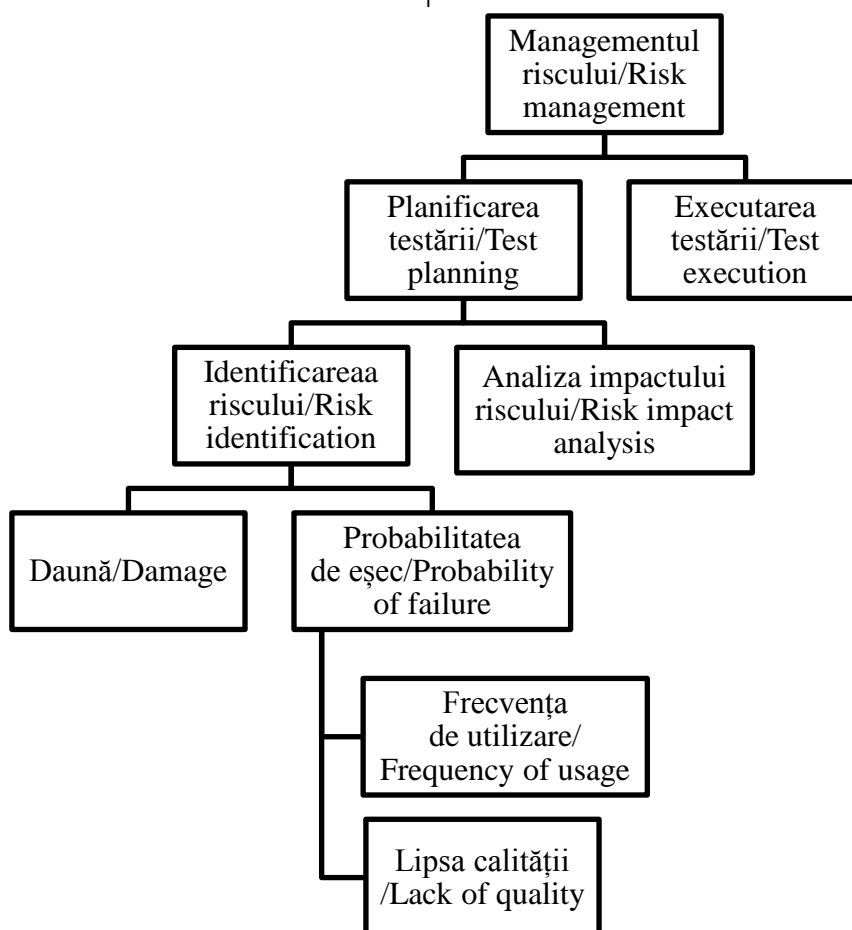


Figura 1. Procesul de testare a riscului/Figure 1. Risk-based testing process

Sursa: articol de STH team member Swati S. March 2016/

Source: article of STH team member Swati S. March 2016

Din figură se vede că riscul reprezintă o legătură între Daună și Probabilitatea de eșec.

Daună[4]

- financiară, pierderea de clienți, dauna identității corporației etc.;
- impactul asupra altor funcții sau sisteme;
- pierderea datelor personalului;
- timpul de detectare și reparare.

Probabilitatea de eșec[4]

- global = dimensiunea (estimată) * * complexitate;
- în detaliu = cunoașterea proiectului de dezvoltare (chiar înainte de testare).

The figure shows that the link between Damage and Probability of failure represents the existing risk.

Damage [4]

- financial, loss of clients, damage to corporate identity, etc.
- impact on other functions or systems
- loss of personnel data
- detection and repair time

Probability of failure [4]

- globally = (estimated) size * complexity
- in detail = knowledge of development project (just before testing)

$$Risc = D * P$$

unde: *D* – Daună și *P* – Probabilitate.

Testarea acceptanței utilizatorului (UAT) [8] – este o testare finală făcută de utilizatori reali pentru a se lua decizia dacă aplicația este acceptabilă pentru utilizare sau nu. UAT poate fi efectuată de către dezvoltator sau de către client. Când este făcută de către dezvoltator, este parte a testării funcționabilității și nu include toate modalitățile posibile de utilizare a afacerii. Când testarea se face din partea clientului și de către client, aceasta nu include toate scenariile posibile de afacere. Aplicația poate fi considerată pregătită pentru UAT, când nu are blocaje și buguri critice și când cel puțin 90-95% dintre bugurile minore și majore au fost reparate.

Acest lucru înseamnă că alte riscuri, în afară de riscurile pentru testarea funcționalității, au fost detectate. Ele sunt mai mult operaționale decât tehnice.

Testarea bazată pe risc a acceptanței utilizatorului poate fi performată în două moduri principale:

- riscul calității produsului – poate avea un randament negativ asupra produsului însuși;
- planificarea riscurilor – poate avea influență negativă asupra proiectului în sine.

Pentru a porni o testare eficientă bazată pe risc, prezintă importanță estimarea fiecărui risc și începerea testării acelor porțiuni care au

where *D* – Damage and *P* – Probability.

User Acceptance testing (UAT) [8] – is a final testing by real users in order to take a decision if application is acceptable for usage or not. UAT can be done on developer side or on client side. When it is done on developer side, it is a part of Functional testing and it does not include all possible ways of business using. When it is done on client side and by client, testing include all possible business scenarios. Application can be considered ready for UAT, when it has not blocker and critical bugs and at least 90-95% of major and minor bugs are fixed.

That means that other risks, different from risks for functional testing, are detected. They are more operational than technical.

Risk based user acceptance testing can be performed in two main ways:

- product quality risks – can make negative output on product itself.
- planning risks – can have negative influence on overall project.

In order to start an effective risk based testing it is important to estimate every risk and to start testing that parts that have higher risk severity and priority. Moreover, it is important to

o gravitate și o prioritate a riscului mai mare. În plus, este important să fie convinsă echipa de testare, formată din utilizatori reali, să detecteze și să testeze cât mai bine zonele critice.

Procesul de testare bazată pe risc

Orice proces de testare începe cu identificarea scopurilor principale și ajutoarele de testare. În cazul testării bazate pe risc, putem afirma că scopul principal constă în îmbunătățirea calității produsului prin determinarea tuturor riscurilor și reducerea probabilității apariției lor. Procesul de testare poate consta în următorii pași [2]:

- întocmirea unei liste cu riscuri și identificarea priorității lor;
- efectuarea de teste orientate spre cazurile de testare pentru cercetarea/investigarea fiecărui risc;
- în cazul apariției unor noi riscuri, domeniul de testare este actualizat și sunt efectuate noi teste.

Acest proces va lua sfârșit în cazul în care nivelul de calitate cerut este atins (figura 2).

convince testing team of real users to detect and test as good as possible critical areas.

Risk-Based testing process

Any testing process is starting with identifying main goals and testing aids. In case of risk based testing, we can say that main goal is improving product quality by determining all risks and reducing probability of their appearance. Testing process can consist of the next steps [2].

- making list of risks and identifying their priority.
- producing tests oriented test cases to research of each risk.
- in case of new risk appearance, testing scope is updating and new tests are producing.

This process will stop in case if required quality level is achieved (figure 2).

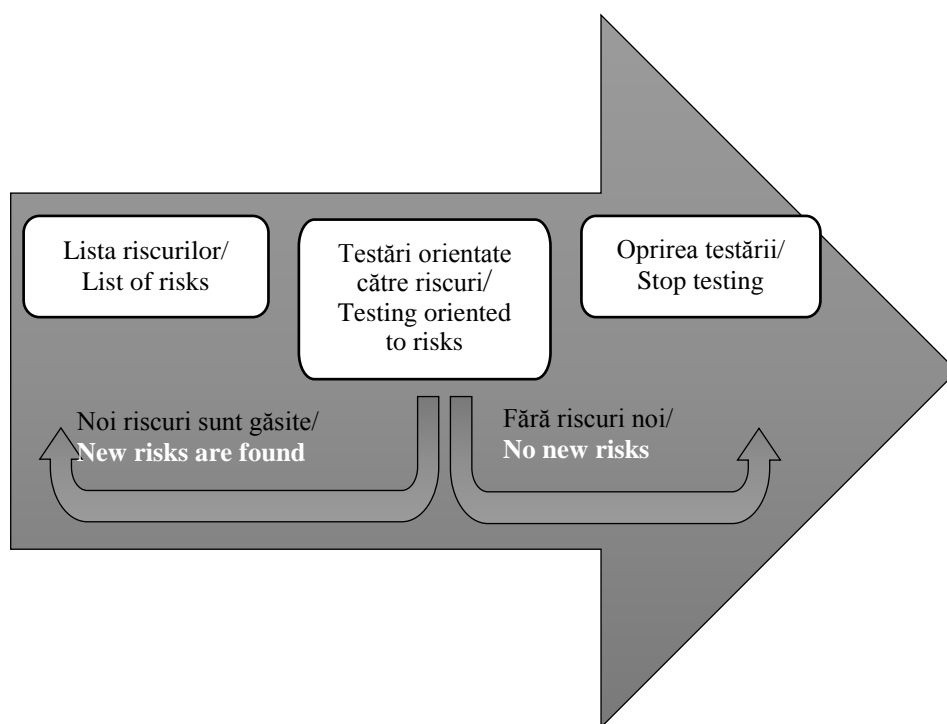


Figura 2. Procesul testării bazate pe risc/ Figure 2. Risk-based testing process

Sursa: James Bach, „Destul de bună calitate: dincolo de Buzzword”, IEEE Computer, Aug. 1997, pp. 96-98/ Source: James Bach, „Good Enough Quality: Beyond the Buzzword”, IEEE Computer, Aug. 1997, pp. 96-98

Obiectivul principal al abordării UAT bazate pe risc constă în găsirea celor mai importante defecte, cât mai devreme posibil și la prețul cel mai mic. Acest lucru presupune că cele mai probabile riscuri trebuie detectate în cele mai critice zone ale aplicației. Aici, două echipe ar trebui să lucreze pentru identificarea acestor riscuri și zone [3]:

- echipa tehnică, cu ingineri în asigurarea calității (QA) experimentați;
- echipa de business, cu utilizatori reali experimentați.

Rolul inginerilor QA rezidă în identificarea zonelor din aplicație predispuse la mai multe buguri. Acest lucru a fost făcut pe baza următoarelor lucruri:

- cunoștințe de arhitectură a aplicației;
- cunoștințe despre mediul în care aplicația este integrată;
- experiență în proiecte asemănătoare.

QA încearcă să identifice acele puncte slabe ale aplicației, care au mai multă influență asupra sistemului de lucru. Bazându-se pe aceste cunoștințe obținute, QA creează scenarii de teste. Acestea sunt executate de echipa de business, dintre care unii au nevoie, implicit, de experiență tehnică de testare.

Rolul echipei de business îl constituie identificarea zonelor din procesul de afacere, care pot avea cele mai mari riscuri operaționale și financiare [3]. Acest lucru este făcut în baza următoarelor condiții:

- cunoașterea procesului de afacere;
- cunoașterea personalului, în special impactul factorului uman;
- cunoașterea zonelor care manipulează informația personală, financiară, securitatea datelor etc.

Echipa de business încearcă să identifice acele puncte slabe ale aplicației, care au o influență mai mare asupra procesului de afaceri. Pornind de la aceste cunoștințe obținute, ei creează cazuri de utilizare sau impresii ale utilizatorilor. Ținând cont de aceste cazuri de utilizare, QA creează scenarii de teste. Așadar, cea mai critică parte a aplicației este acoperită de scenariile testelor.

The main objective of UAT risk based approach is to find the most important defects as early as possible and at the lowest price. That means that there should be detected the most probable risks in the most critical areas of the application. Here two teams should work to identify those risks and areas [3]:

- technical team with experienced quality assurance (QA) engineers;
- business team with experienced real users.

Role of QA engineers is identification of areas in application that can have more bugs. That is done based on the next things:

- knowledge of application architecture;
- knowledge of environment where application is integrated;
- experience in the same projects.

QA tries to identify those weak points in application, which have bigger influence on systems working. Based on these obtained knowledge QA create test scenarios. They are executed by business team and some of them need implication of technical experiences testers.

Role of Business team is identification of areas in the business process that can have the bigger operational and financial risks [3]. That is done based on the next things:

- knowledge of business process;
- knowledge of personnel, notably human factor impact;
- knowledge of areas that have handle financial, personal information, data security etc.

Business team tries to identify those weak points in application, which have bigger influence on business process. Based on these obtained knowledge they create use cases or user stories. Based on these cases of usage, QA creates test scenarios. So, the most critical parts of the application are covered by test scenarios.

Toate riscurile ar trebui raportate la specificațiile particulare ale produsului și la scenariile de teste. Dacă specificația respectivă nu prezintă niciun risc, este necesar să se afle de ce: a) probabil, pentru că funcționalitatea nu are decât o importanță minoră; b) pentru că aceasta este puțin cunoscută și, deci, riscurile sunt imposibil de identificat. În cel de-al doilea caz, inginerul QA trebuie să verifice respectiva funcționalitate pentru a găsi riscurile, bazându-se pe propria sa experiență.

Acest proces este repetat de la o lansare la alta, astfel, încât domeniul de testare și orele de muncă să se schimbe cu fiecare dezvoltare. Este necesar de menționat faptul că, în realitate, nu doar absența unor noi riscuri importante poate opri procesul de testare, dar pot surveni și multe alte situații, precum [4]:

- cele mai importante buguri și riscurile cu prioritate ridicată au fost reparate;
- termenul-limită este prea apropiat;
- bugetul a fost folosit complet;
- proiectul nu mai prezintă interes etc.

Identificarea riscurilor

Nu toate riscurile sunt egale și există mai multe modalități de a evalua nivelul riscului. Așadar, este foarte important să se știe cum se face identificarea riscurilor, evaluarea nivelurilor lor, implementarea unor teste adecvate și a altor controale și raportarea rezultatelor testelor bazate pe factorul riscului. Identificarea riscului necesită colectarea de informații despre proiect și clasificarea lor pentru a determina cantitatea de riscuri potențiale în faza de testare și în producție.

Problemele fundamentale [5] constau în:

- dificultatea de a măsura impactul riscului;
- incapacitatea de a ține cont de compensarea riscurilor (oamenii compensează, pentru siguranță mai mare, prin asumarea mai multor riscuri).

Primul pas, în abordarea UAT a condițiilor de risc, îl constituie „alcătuirea listei de riscuri” și este mai important decât ceilalți pași. Procesul identificării și analizării riscurilor constă în mai mulți pași:

All risks should be linked to specific product specifications and test scenarios. If any specification does not have any risk, it is necessary to find out why. It can be that functionality is of low importance, or functionality can be little-known and it is impossible to identify any risks. In second case QA engineer has to examine mentioned functionality to find risks based on its own experience.

This process is repeated from one release to another. Thereby testing scope and man-hours will change every new build. It is important to mention that in reality not only absence of new important risks can stop testing process. There can be many other reasons, for example [4]:

- the most important bugs and first-priority risks were fixed;
- delivery date is too close;
- budget was used up;
- project is no more in use, etc.

Risks identification

Not all risks are equal and there are a number of ways to assess the level of risk. So, it's very important to know how to identify risks, to assess their level, to implement appropriate tests and other controls, and to report test results based on risk. Risk identification involves collecting information about the project and classifying it to determine the amount of potential risk in the test phase and in production.

Fundamental problems [5]:

- difficult to measure risk impact;
- failure to account for risk compensation (people compensate for greater safety by taking more risk).

First step in UAT risk base approach is “Making list of risks” is more important than the other steps. The process of risk identifying and analysing consist of some more steps.

1. Identifying the quality risk analysis team;
2. Selecting an analysing method (informal analysing, according to ISO 9126, cost of failure, detailed risk effect etc.);

1. Identificarea echipei de analiză a calității riscului;
2. Selectarea unei metode de analiză (analiză informală, în conformitate cu ISO 9126, costul eșecului, efectul detaliat al riscului etc.);
3. Identificarea calității riscului: prioritizarea, selectarea măsurilor adecvate de reducere a riscurilor. Poate include și revizuirea cerințelor, designului, codului, tehnicilor de programare și a altor documente. Dacă asemenea probleme sunt identificate, trebuie rezolvate imediat;
4. Revizuirea, corectarea și finalizarea documentației privind analiza calității riscului.

Prioritatea (urgența riscului) – este o altă noțiune importantă în procesul managementului riscului. Nivelul de prioritate indică dacă riscul trebuie testat sau dacă testul poate fi amânat până la următoarea dată de lansare. Statutul priorității este setat în funcție de cerințele clientului. Prioritatea se poate schimba în funcție de orar, cerințe sau planul de testare.

Prioritatea trebuie stabilită și trebuie să reflecte importanța testării. Conform experienței mai multor echipe de testare, este suficientă definirea a trei sau patru niveluri de prioritate, în funcție de mărimea proiectului. În acest sens, propunem patru niveluri:

1. Risc critic – apariția sa blochează anumite părți ale testării fără metode de a depăși problema. Este foarte vizibil clientului.
2. Risc mare – provoacă apariția unor defecte foarte mari, dar cu metode de depășire a problemei. Mulți clienți s-ar plânge de problemă. Problema nu este conformă cu cerințele stabilite pentru lansare.
3. Risc mediu – această categorie include toate celelalte riscuri, în momentul în care există metoda de depășire a problemei sau impactul asupra testării este foarte mic. Unii clienți sunt afectați de riscul mediu, dar există o metodă de rezolvare. Problemele care pot apărea nu afectează zonele critice ale sistemului.
4. Risc scăzut – în cazuri în care defectele care apar sunt banale sau de ordin cosmetic. Doar

3. Identifying the quality risks: prioritizing, selecting appropriate risk mitigation actions. It may include also reviews of requirements, design, code, programming techniques and other documents. If such problems were identified they should be immediately resolved;
4. Review, revise, and finalize the quality risk analysis document.

Priority (urgency of the risk) – is another important notion of risk based testing. The level of priority indicates whether the risk must be tested or can be postponed to next releases. The priority status is set based on the customer requirements. Priority might change according to schedule, requirements and test plan.

Priority should be set and should reflect importance for testing. According to experience of many testing teams, it is enough to define 3 or 4 priority levels. It depends on project size. I propose four levels.

1. Critical risk – in case of its appearance it blocks some parts of testing without workaround. It is very visible to customer.
2. High risk – provoke appearance of very bad defect but with workaround. Many customers would complain about the issue. The issue does not conform to what was stated as a requirement for the release.
3. Medium risk – all other risks when workaround exist or when impact on testing is very small. Some customers are impacted by it but there is a workaround. Issue than can appear affects not critical areas of the system.
4. Low risk – in case when defects that can appear are cosmetic or trivial. Only few customers even notice it much less are impacted by it (i.e., not very visible or detrimental).

unii clienți observă aceste defecte și sunt cu atât mai puțin afectați de ele (deoarece nu sunt foarte vizibile sau dăunătoare).

Pentru estimarea riscurilor, se poate recurge la matricea de trasabilitate a riscului. Intersectarea probabilității apariției cu impactul apariției ne oferă gravitatea și prioritatea.

$$Risc = Costul Eșecului = Probabilitatea \text{ Apariției} \times Impactul \text{ Apariției}$$

În acest caz, avem de-a face cu o matrice a priorității riscului [6]. În continuare, este prezentată matricea trasabilității.

Risk traceability matrix can be used for risk estimating. Intersection of probability of occurrence and impact of occurrence gives us the risk severity and priority.

$$Risc = Cost \text{ of Failure} = Probability \text{ of Occurrence} \times Impact \text{ of Occurrence}$$

Here is a matrix of risk priority [6]. Below traceability matrix is presented.

Probabilitate ↑	Critic	Mare	Mare	Critic	Critic
	Mare	Mediu	Mare	Mare	Critic
	Mediu	Scăzut	Mediu	Mare	Critic
	Scăzut	Scăzut	Scăzut	Mediu	Mare
		Scăzut	Mediu	Mare	Critic
		Impact →			

Figura 3. Matricea priorității riscului / Figure 3. Matrix of risk priority

Sursa: elaborată de autor / Source: developed by the author

Metode de analiză a riscului

Există o multitudine de metode de prioritarizare a riscurilor. Selectarea uneia dintre ele depinde de tipul proiectului, timpul alocat testării, experiența echipei, bugetul proiectului și alți factori [7]. În mod normal, riscurile sunt grupate sau organizate în categorii majore de risc, cum ar fi funcționabilitatea, performanța, securitatea etc. Odată ce sunt identificate, fiecărui risc îi este alocat un anumit nivel – o măsurătoare a gradului de importanță și prioritate, așa cum este menționat mai sus. În continuare, vom examina câteva metode de analiză a riscului:

1. **Brainstorming** (sau informal). Constă în o încercare simplă, dar eficientă de a

Risk analyses methods

There are a plenty of different methods of prioritizing risks. Selecting one of them depends on project type, time for testing, team experience, project budget and other factors [7]. Typically, the risks are grouped or organized by major risk categories, such as functionality, performance, security, and so forth. Once the risks are identified, each risk is assigned a level – a measure of its degree of importance and priority, as was mentioned above. Following are some methods for risk analysis [9].

1. **Brainstorming** (or informal). It is a simple but effective attempt to help people

ajuta oamenii să gândească în mod creativ în cadrul unui grup, fără a se simți inhibați sau criticați de către ceilalți. O astfel de metodă reprezintă o modalitate ușoară de a proceda la analiza calității riscului, fiind folosită, în special, la planificarea proiectului formativ precum și la identificarea scenariilor de risc într-un anumit proiect. Intenția constă în încurajarea a cât mai multor idei, ceea ce declanșează, în schimb, ideile altora.

2. **Conform ISO 9126**, metodele de analiză a calității riscurilor trebuie să descrie caracteristici și sub-caracteristici standard ale calității sistemului. Cele șase caracteristici principale ale calității sunt: funcționabilitatea, fiabilitatea, gradul de utilizare, eficiența, mentenabilitatea și portabilitatea. În fiecare categorie, există două sau mai multe sub-caracteristici.
3. **Metoda de analiză a calității riscului costului de eșec** se concentrează pe următoarea întrebare: „Care sunt pierderile așteptate asociate cu diverse riscuri și cât de mult ar trebui să se cheltuiască pentru a se reduce aceste riscuri?” O pierdere așteptată o constituie produsul probabilității pierderii înmulțită cu costul pierderii. Astfel de tehnici permit echipei de management de proiect să ia decizii realiste și economice cu privire la testare.
4. **Metoda analizei probabilității**. Echipa AC trebuie să specifice o distribuție a probabilității pentru fiecare variabilă, iar apoi să ia în considerare situații care prevăd că oricare sau toate variabilele pot fi schimbate în același timp. Definirea probabilității apariției oricărei variabile specifice poate fi destul de dificilă, în special, din cauză că mediile politice și comerciale se pot schimba destul de rapid.
5. **Metoda Delphi**. Conceptul de bază îl reprezintă obținerea unui consens cu ajutorul unui grup de experți pentru a ajunge la o soluție convergentă a unei probleme specifice. Această metodă este folositoare,

think creatively in a group setting without feeling inhibited or being criticized by others. This method provides an easy way to get started in quality risk analysis. Is used mostly in formative project planning and can also be used to identify risk scenarios for a particular project. The intent is to encourage as many ideas as possible, which may in turn, trigger the ideas of others.

2. **According ISO 9126** quality risks analysis methods should describe characteristics and sub characteristics of system quality standard. The six main characteristics of quality are: Functionality, Reliability, Usability, Efficiency, Maintainability, and Portability. In each category there are two or more sub characteristics.
3. **Cost of failure quality risk analysis method focus** on the following question: What are the expected losses associated with various risks, and how much should one spend to reduce those risks? An expected loss is the product of the probability of the loss multiplied by the cost of the loss. Such techniques allow the project management team to make a hard-nosed, economic decision about testing.
4. **Probability analysis method**. QA team should specify a probability distribution for each variable, and then consider situations where any or all of these variables can be changed at the same time. Defining the probability of occurrence of any specific variable may be quite difficult, particularly as political or commercial environments can change quite rapidly.
5. **Delphi method**. The basic concept is to derive a consensus using a panel of experts to arrive at a convergent solution to a specific problem. This is particularly

în special, la impunerea probabilităților de evaluare referitoare la evenimentele viitoare, în care impactul riscurilor este mare sau critic. Primul și cel mai important pas îl constituie alegerea unui grup de indivizi care au experiență în zona în cauză. Pentru cele mai bune rezultate, membrii grupului nu ar trebui să se cunoască între ei, iar procesul să fie efectuat cu fiecare, în locații diferite. Răspunsurile, împreună cu opiniile și justificările, sunt evaluate, iar feedback-ul statistic este îmbunătățit alături de fiecare membru al grupului în următoarea reiterație. Procesul este continuat până când răspunsurile grupului ajung la o anumită soluție.

Fapte despre abordarea testelor de acceptanță a condițiilor de risc:

1. Testarea nu identifică toate greșelile;
2. Cu cât mai multe greșeli găsești, cu atât mai multe există încă;
3. Densitatea erorilor după lansare se corelează cu densitatea erorilor de testare;
4. 90% din problemele majore sunt găsite în 2-3% din unități;
5. 80% din problemele normale sunt găsite în 20% din unități.

Acest lucru denotă că prezintă o foarte mare însemnătate detectarea unităților cu probabilitate mare de descoperire a riscurilor. De aceea, abordarea condițiilor de risc este importantă în Testele de Acceptanță a Utilizatorului [7].

Concluzii

Abordarea condițiilor de risc, în timpul UAT, ajută la îmbunătățirea sistemului prin descoperirea celor mai critice zone și a celor mai critice erori și prin repararea acestora. Este o tehnică puternică de testare, care permite echipelor QA și de business să raționalizeze eforturile de testare. Organizațiile care implementează această tehnică sunt într-o mai mare cunoștință de cauză în ceea ce privește riscurile inerente ale aplicațiilor lor și riscurile care sunt, într-adevăr, semnificative. Tehnica permite echipelor QA să ia decizii documentate, stabilind în același timp criterii clare de ieșire din situație.

useful in arriving at probability assessments relating to future events where the risk impacts are large and critical. The first and vital step is to select a panel of individuals who have experience in the area at issue. For best results, the panel members should not know each other identity and the process should be conducted with each at separate locations. The responses, together with opinions and justifications, are evaluated and statistical feedback is furnished to each panel member in the next iteration. The process is continued until group responses converge to a specific solution.

Facts about risk based testing approach:

1. Testing does not find all faults.
2. The more you find, the more are left.
3. Post-release fault density correlates with test fault density!
4. 90% of high severity issues are found in 2-3% of the units.
5. 80% of normal severity issues are found in 20% of units.

That means that is very important to detect these units with high probability of risk finding. That is why risk based approach is important in User Acceptance Testing [7].

Conclusions

Risk based testing approach during UAT helps to make system better by finding the most critical areas and the most critical failures and fixing them. It is a powerful testing technique that enables the QA team and business team to streamline their testing efforts. Organizations that implement this technique are in a better know-how of the risks that are inherent in their applications and of the risks that are actually significant. It allows QA teams to make informed decisions while setting a clear test exit criteria.

Risk Based Testing is an approach that requires skill and experience to isolate the most

Testarea condițiilor de risc este o abordare care necesită îndemânare și experiență pentru izolarea celor mai importante teste bazate pe constrângeri tehnice și de afaceri.

Acest articol analizează doar o parte din teoria abordării testării bazate pe riscuri. Există o mulțime de metode și tehnici de acest tip de testare. Metoda descrisă a fost folosită în Raiffeisen Bank România în UAT.

important tests based on technical and business constraints.

This article is describing a part of risk based testing approach. There are much more methods and techniques of this kind of testing. Described approach was applied in Raiffeisen Bank Romania during UAT.

Bibliografie/Bibliography:

1. <http://www.softwaretestinghelp.com/risk-management-during-test-planning-risk-based-testing/> - *STH team member Swati S.March 2016.*
2. <http://www.methodsandtools.com/archive/archive.php?id=31> – „Risk Based Testing, Strategies for Prioritizing Tests against Deadlines” by Hans Schaefer, Software Test Consulting.
3. Article by Rex Black „Quality Risk Analysis”, 2003.
4. Presentation by CIBC – TASSQ – „Risk Based Testing. Why We Need It & How To Do It”, November 2010.
5. SCHAEFER Hans, *Risk based testing: How to choose what to test more and less*, 2004.
6. BEIZER Boris, *Software Testing Techniques Second Edition*, 1990.
7. BACH James, *Good Enough Quality: Beyond the Buzzword*, *IEEE Computer*, Aug. 1997, pp. 96-98.
8. „Сертифицированный тестировщик ISTQB. Программа обучения Базового уровня” – version 2011 г.
9. „International Software Testing Qualifications Board”, Erik van Veenendaal (Netherlands) Version 2.1 (April 2010).