stručni članak

UDK 005.334:004.65 ; 007:004]:336.71

Bankarski rizik 36

UPRAVLJANJE IZLOŽENOŠĆU - ALATI (1)

dr Vesna Matić

Udruženje banaka Srbije
vesna.matic@ubs-asb.com

Rezime

Svest o izloženosti rizicima u poslovanju, kao i o potrebi i mogućnostima da se upravlja njima, inicirala je razvoj discipline upravljanja rizicima, kao i razvoj alata kojima se banka služi u tom procesu. Ceo proces rezultat je novije istorije razvoja, a na njegovu dinamiku i rezultate značajno je uticao razvoj informacionih tehnologija. One su omogućile formiranje baza podataka, kao osnovnog alata za upravljanje izloženošću, ali su otvorile i brojne mogućnosti za razvoj novih, savremenih alata, kojima se izloženost može meriti, kako u odnosu na pojedine vrste rizika, tako i u odnosu na agregatnu izloženost.

Ključne reči: izloženost rizicima, interne/eksterne baze podataka

JEL: C87, G21, L2

Rad primljen: 20.09.2013.
Odobren za štampu: 23.09.2013.

UDC 005.334:004.65 ; 007:004]:336.71

expert article

Banking Risk 36

EXPOSURE MANAGEMENT - TOOLS (1)

Vesna Matić PhD

Association of Serbian Banks
vesna.matic@ubs-asb.com

Summary

The awareness of exposure to business risks, and the need and possibilities for managing them, initiated the development of risk management, along with the development of tools that banks can use throughout this process. The entire process is a result of recent developments, whose dynamics and results have been considerably influenced by the advancement of information technologies. They have enabled the formation of databases, as basic tools for exposure management, at the same time opening numerous other possibilities for the development of new, modern tools for exposure measurement, both in relation to certain types of risk, and in relation to aggregate exposure.

Keywords: risk exposure, internal/external databases

JEL: C87, G21, L2

Paper received: 20.09.2013

Approved for publishing: 23.09.2013

Baze podataka

Baze podataka kao alat za upravljanje izloženošću rizicima, zahvaljujući razvoju informacionih tehnologija, postaju sve pouzdanija osnova za praćenje, merenje i kontrulu izloženosti banke pojedinačnim rizicima, ali i za ocenu agregatne izloženosti.

Banke formiraju ***interne baze podataka***. Modeliraju ih prema specifičnom rizičnom profilu banke, ciljevima upravljanja i kontrole, ali i zahtevima regulatora. Kvalitet internih baza podataka zavisi od:

- kvaliteta sistema identifikacije rizičnih događaja,
- kulture ponašanja zaposlenih u odnosu na izloženost, u smislu poznavanja rizičnih događaja i nivoa svesti o potrebi da se oni prijave i unesu u bazu podataka,
- standardizacije procesa, u smislu definicije klučnih pojmova, opisa rizičnih događaja, procedure klasifikacije i unosa podataka,
- kvaliteta informatičke podrške i
- obuhvatnosti u pogledu broja i kvaliteta podataka.

Formalno, baze podataka rade se u vidu matrica, koje su strukturirane primenom različitih kriterijuma:

- po datumu (nastanka rizičnog događaja, unosa u bazu podataka, knjiženja, završetka rizičnog događaja),
- po vrstama rizika,
- mestu nastanka rizičnog događaja,
- učestalosti i visini gubitaka, korišćenjem opisne skale (visok, srednji, nizak) ili numeričke,
- vrstama gubitka (potencijalni, realizovani, izbegnuti u bruto/neto iznosu) i drugim kriterijumima.

Unos podataka u bazu predpostavlja postojanje ***dokumenta o rizičnom*** događaju i odvija se po unapred utvrđenim i odobrenim procedurama. To znači da svaki unos mora biti proveren i odobren od strane jedinice koje su zadužene za punjenje baze podataka, u nekim slučajevima, i od jedinica zaduženih za kontrolu rizika.

Dokument o rizičnom događaju sadrži kratak opis događaja sa naglaskom na glavne uzroke realizacije rizičnog događaja, vezu sa ostalim rizicima, mere koje je banka preduzela ili će preduzeti kao prevenciju da se ne bi ponovio u budućem periodu.

Rizici korišćenja ovog alata, uglavnom su vezani za dva segmenta - fazu punjenja baze podacima, u smislu kvaliteta i broja unetih podataka, i njihovu pravilnu interpretaciju i korišćenje. Najčešće se javljaju kao problemi organizacione prirode (neefikasna organizacija), problemi koje uzrokuje ljudski faktor (nedovoljna pažnja, koja rezultira unosom duplih podataka, nedostatak volje ili nizak nivo profesionalne kulture zaposlenih da razmenjuju tražene podatke ili prijavljuju rizične događaje), ili kao teškoće u vrednovanju nemonetarnih gubitaka ili potencijalnih gubitaka.

Baze podataka su ključ za izradu i korišćenje drugih alata za upravljanje izloženošću rizicima (scenario analiza), ili primenu visoko sofisticiranijih statističkih modela za kvantitativno merenje izloženosti i kalkulaciju kapitalnog troška.

Interne baze podataka, međutim, nisu dovoljan alat za kvalitetno upravljanje rizicima, pa banke koriste i podatke ***iz eksternih baza***, koje su vredan dodatni alat menadžerima rizika u edukativnom i iskustvenom smislu. Na taj način proširuju svoju informacionu bazu podacima o rizičnim događajima i gubicima, koji nisu rezultat njihovog iskustva. Ovo je veoma važno kada je reč o rizicima koji se retko realizuju i rezultiraju visokim neočekivanim gubicima, koji mogu dovesti u pitanje i sam opstanak banke.

Eksterne baze podataka najčešće formiraju konzorcijumi banaka, a način njihovog rada (punjenje baze, korišćenje podataka, sigurnost podataka i drugo), precizno su definisani i uređeni.

Korišćenje podataka iz eksternih baza nosi i određene rizike, ukoliko se pravilno ne izvrši odabir podataka koji odgovaraju rizičnom profilu banke i ne spozna prava korelaciona veza uzetih podataka sa konkretnom bankom, odnosno, primenljivost na konkretnu banku, obzirom da su ove veze najčešće nepoznate kada se podaci koriste.

Literatura / References

1. Lore Marc and Borodovski Lev, *The Professional's Handbook of Financial Risk Management,* Butteworth-Heinemann, Oxford 2000
2. Dr Vesna Matić, *Operativni rizici,* Institut za poslovna istraživanja, Beograd, 2008.

Databases

As a tool for risk exposure management, databases have, thanks to the information technologies development, become an increasingly reliable foundation for monitoring, measurement and control of a bank's exposure to specific risks, but also for the assessment of aggregate exposure.

Banks form ***internal databases***. They model them according to the bank's specific risk profile, its management and control objectives, but also according to the regulator's requirements. The quality of internal databases depends on the following:

- Quality of the system for risk events identification;
- Behavior of the employees concerning exposure, in terms of their knowledge of risk events and their awareness of the necessity to report them and enter them into the database accordingly;
- Standardization of processes, in terms of key concepts' definitions, risk events descriptions, classification and data entry procedures;
- Quality of IT support; and
- Comprehensiveness in terms of data quantity and quality.

Databases are designed in the form of tables, structured by means of the various criteria:

- Date (date of risk event occurrence, date of database entry, date of book-keeping, end date of the risk event);
- Type of risk;
- Venue of a risk event;
- Frequency and amount of loss, measured on a descriptive scale (high, medium, low) or a numerical scale;
- Type of loss (potential, realized, avoided, in gross/net amount); and other relevant criteria.

The entry of data into a database is conducted on the basis of a ***risk event document***, according to the previously defined and approved procedures. This means that each entry has to be double-checked and ratified by the units in charge of filling in the database, and, in some cases, by the units in charge of risk control.

A risk event document contains a brief description of the event, focusing on the major causes of its occurrence, its relatedness to other risks, along with the measures that the bank has undertaken or will undertake as a form of precaution, in order to prevent the concerned event from reoccurring in the future.

The risks of using this tool are mostly related to two segments - the stage of filling in the database, in terms of the quantity and quality of entered data; and their proper interpretation and usage. The most frequent problems are organizational in nature (inefficient organization), followed by the human-induced problems (lack of attention, resulting in double entries of data, lack of will or low levels of professionalism of employees when it comes to exchanging the requested data or reporting risk events), and difficulties in valorizing non-monetary losses or potential losses.

Databases are a key for preparation and usage of other tools for risk exposure measurement (scenario analysis), or for designing highly sophisticated, statistical models for quantitative exposure measurement and capital costs calculation.

Internal databases, however, are not a sufficient tool for high-quality risk management, which is why banks resort to using data from ***external databases***, as a valuable additional tool for risk managers, both in terms of education and experience. Thereby, banks expand their information databases by adding data on risk events and losses that were not a result of their own experience. This is rather important when it comes to risks that rarely get realized, but result in high unexpected losses, which might even bring into question the very survival of the concerned bank.

External databases are most often formed by bank consortiums, their manner of functioning (filling in the database, data utilization, data security, etc.) being precisely defined and arranged.

Using data from external databases also entails certain risks, in case of an improper selection of data unsuitable for the bank's risk profile, when the true correlation of used data and the concrete bank is not recognized, i.e. when the data are not applicable to the concerned bank, given that such correlations are usually unknown at the moment of accessing the data.