originalni naučni rad

UDK 005.334:004.65]:336.1.07 ; 006.85:336.1(497.11)

MINIMALNI STANDARDI UPRAVLJANJA INFORMACIONIM SISTEMOM FINANSIJSKE INSTITUCIJE

mr Vladan Pantović, PMP

Narodna banka Srbije
vladan.pantovic@nbs.rs

Stanislav Petrović

Narodna banka Srbije
stanislav.petrovic@nbs.rs

Radmila Ristić

Narodna banka Srbije
radmila.j.ristic@nbs.rs

Rezime

Primena modernih informacionih tehnologija u finansijskim institucijama pruža mnoštvo mogućnosti za unapređenje njihovog poslovanja, ali istovremeno dovodi do značajne izloženosti riziku informacionog sistema. Kako bi se izbegle, odnosno ublažile štetne posledice realizacije ovog rizika, nužno je da se osigura adekvatno upravljanje tim sistemima. U tu svrhu, Narodna banka Srbije donela je, početkom 2013. godine, novi podzakonski akt kojim se definišu minimalni standardi i uslovi stabilnog i sigurnog poslovanja finansijskih institucija koji se odnose na upravljanje informacionim sistemom.

U tekstu su izloženi razlozi za donošenje Odluke o minimalnim standardima upravljanja informacionim sistemom finansijske institucije i opisan pristup koji je primenjen, kao i osnovna koncepcija novog propisa. Pored toga, bliže su predstavljeni i obrazloženi pojedini segmenti Odluke.

Ključne reči: informacione tehnologije, informacioni sistem, rizik informacionog sistema, upravljanje informacionim sistemom, standardi, regulativa

JEL: G21, M15

Rad primljen: 30.07.2013.

Odobren za štampu: 05.09.2013.

UDC 005.334:004.65]:336.1.07 ; 006.85:336.1(497.11)

original scientific paper

MINIMUM INFORMATION SYSTEM MANAGEMENT STANDARDS FOR FINANCIAL INSTITUTIONS

Vladan Pantović, MSc PMP

National Bank of Serbia
vladan.pantovic@nbs.rs

Stanislav Petrović

National Bank of Serbia
stanislav.petrovic@nbs.rs

Radmila Ristić

National Bank of Serbia
radmila.j.ristic@nbs.rs

Summary

The implementation of modern information technologies in financial institutions offers a wide range of possibilities for the advancement of their business, at the same time, however, causing considerable exposure to information system risk. In order to avoid or mitigate the adverse effects of this risk, it is necessary to ensure adequate management of these systems. To this end, in early 2013, the National Bank of Serbia adopted a new by-law, defining the minimum standards and conditions for stable and secure operations of financial institutions, relating to information system management.

This paper presents the reasons for adopting the Decision on Minimum Information System Management Standards for Financial Institutions, and describes the implemented approach, along with the main concepts of the new regulation. Moreover, it elaborates on the certain segments of the concerned Decision.

Keywords: information technologies, information system, information system risk, information system management, standards, regulations

JEL: G21, M15

Paper received: 30.07.2013

Approved for publishing: 05.09.2013

U uslovima savremenog načina poslovanja, finansijske institucije i finansijske usluge su u značajnoj meri zavisne od informacionih tehnologija, odnosno od informacionih sistema koji su zasnovani na tim tehnologijama. Brzi razvoj u ovoj sferi donosi nove mogućnosti, ali i nove opasnosti po stabilnost i sigurnost poslovanja. Usled takvih okolnosti, finansijske institucije su izložene različitim izvorima rizika informacionog sistema. Kako bi se stvorio okvir za svođenje ovog rizika na prihvatljiv nivo, odnosno za ublažavanje štetnih posledica njegove realizacije, neophodno je uspostaviti i obezbediti doslednu primenu odgovarajućih standarda u upravljanju informacionim sistemom.

Potrebno je reći da su određene preporuke i najbolje prakse iz ove oblasti već sadržane u opšte priznatim i prihvaćenim standardima i okvirima, kao što su npr. ISO/IEC 38500 i COBIT za korporativno upravljanje i menadžment IT-a, ISO/IEC 20000 i ITIL za upravljanje IT servisima, standardi iz serije ISO/IEC 27000 za informacionu bezbednost, i dr. Standardi imaju ključnu ulogu u transferu savremenih tehnologija jer ih definišu jasnim, konciznim jezikom i u njima su ugrađena najbolja iskustva i zamisli svetskih eksperata.

Informacione tehnologije i rizici

Odvijanje poslovnih procesa, pružanje usluga klijentima i obezbeđenje pravovremenih i tačnih informacija koje su kritične za donošenje poslovnih odluka danas su gotovo nezamislivi bez primene informacionih tehnologija. Kompanija koja želi da bude uspešna i konkurentna mora pratiti trendove i koristiti na pravi način mogućnosti koje pružaju tehnološke inovacije. U sektoru finansijskih institucija, primena modernih tehnologija omogućila je, pored ostalog, da se klijentima ponude novi proizvodi i usluge, odnosno da se oni tradicionalni učine dostupnim putem novih distributivnih kanala (npr. plaćanje karticama preko POS terminala, podizanje ili uplaćivanje gotovine na bankomatima, internet bankarstvo, mobilno bankarstvo itd.). Elektronske transakcije odavno su u drugi plan potisnule tradicionalne načine plaćanja, pri čemu je sve veći broj ovih transakcija iniciran putem interneta.

Međutim, uz mogućnosti da se unapredi poslovanje, nove tehnologije istovremeno nose i nove izvore pretnji. Primer su različiti oblici visokotehnološkog kriminala kao što su hakerski upadi, instalacija malicioznog softvera, krađa i zloupotreba podataka o platnim karticama, napadi na onlajn servise i sl. Osim toga, i određeni neželjeni događaji koji nisu direktno uslovljeni primenom informacionih tehnologija u ovim okolnostima poprimaju nove forme. Tako npr., interne prevare radi ostvarivanja lične koristi mogu uključiti i neovlašćeno otkrivanje ili izmenu podataka uz zaobilaženje kontrola pristupa sistemu, manipulacije u vezi s podešavanjima sistema, njegovim funkcijama i sl. Isto tako, u uslovima kada je za redovno odvijanje poslovnih procesa neophodna raspoloživost resursa informacionog sistema, moguće katastrofe (prirodne ili izazvane delovanjem ljudskog faktora) nameću potrebu za odgovarajućim pristupom u pogledu fizičke zaštite tih resursa i planiranja kontinuiteta poslovanja. Ljudske greške i propusti u radu takođe se dešavaju nevezano od korišćenja informacionih tehnologija, ali u ovom kontekstu to mogu biti greške u projektovanju, implementaciji, testiranju, unosu i obradi podataka itd.

Dodatno, usled širenja palete finansijskih usluga, rasta obima transakcija i usložavanja poslovnih procesa, ali i različitih statusnih promena, informacioni sistemi finansijskih institucija postaju još složeniji i potencijalno ranjiviji.

U opisanim uslovima, neadekvatno upravljanje informacionim sistemom ili postojanje drugih slabosti u tom sistemu dovelo bi do značajne izloženosti poslovanja finansijske institucije riziku informacionog sistema. Realizacija ovog rizika može neposredno ugroziti bezbednost i funkcionalnost informacionog sistema, kao i kontinuitet poslovanja, odnosno pružanja usluga klijentima. Posledice mogu biti negativni efekti kako po finansijski rezultat i finansijsko stanje institucije (profitabilnost, likvidnost, kapital), tako i po njenu reputaciju. Takođe, posledice se mogu ogledati i u smanjenju poverenja u pojedine finansijske proizvode i u krajnjoj instanci - u finansijski sistem.

In the contemporary business environment, financial institutions and financial services are to a large extent dependent upon information technologies, i.e. upon information systems based on these technologies. The swift developments in this area have brought about new possibilities, but also new threats to the stability and security of operations. Under such circumstances, financial institutions are exposed to various sources of information system risk. In order to create a framework for reducing this risk to an acceptable level, and for mitigating the harmful consequences of its realization, it is necessary to establish and ensure consistent implementation of the appropriate standards in information system management.

It has to be said that certain recommendations and best practices in this field are already to be found in the generally recognized and accepted standards and frameworks, such as, for instance, ISO/IEC 38500 and COBIT for IT governance and IT management; ISO/IEC 20000 and ITIL for IT services management; standards from the series ISO/IEC 27000 for information security, etc. The standards have a key role in the transfer of modern technologies, because they define them in a clear, concise manner, and because they are based on the best experiences and ideas of global experts.

Information Technologies and Risks

Business processes, provision of services to the clients, and procurement of timely and accurate information critical for business decision-making are today almost impossible without the usage of information technologies. A company wishing to be successful and competitive must follow the trends and utilize in the right way all the possibilities provided by technological innovations. In the financial institutions sector, the implementation of modern technologies has, among other things, enabled the clients to be offered new products and services, or the traditional products and services to be made available through new channels of distribution (e.g. payment by cards via POS terminals, withdrawal or payment of cash on ATMs, Internet banking, mobile banking, etc.). Electronic transactions have long ago superseded traditional payment methods, with the increasingly large number of these transactions being initiated over the Internet.

However, in addition to generating possibilities for business enhancement, new technologies may at the same time bring about new sources of threat. Examples can be seen in various forms of high-tech crimes, such as hacking, malicious software installation, theft and abuse of payment cards data, online services attacks, etc. Moreover, certain unwanted events that are not directly conditioned by the information technologies implementation under such circumstances take new forms. Thus, for instance, internal frauds with the intention of yielding personal gain may include unauthorized disclosure or amendment of data, along with by-passing of system access controls, manipulating system configuration, its functions, etc. Similarly, when regular business processes require the availability of information system resources, potential disasters (either natural or human-induced) impose the need for an appropriate approach in terms of physical protection of those resources and business continuity planning. Human errors and operational oversights also occur regardless of information technologies, but in this context those can be errors in respect of design, implementation, testing, entering or processing of data, etc.

Furthermore, due to the wider array of financial services, expanded volume of transactions and increasingly complex business processes, but also various status-related changes, information systems of financial institutions are becoming even more complex and potentially vulnerable.

In the described environment, inadequate information system management or the existence of other weaknesses in the concerned system would cause considerable exposure of the financial institution's business to information system risk. Realization of this risk may directly jeopardize the information system security and functionality, along with the business continuity, i.e. the provision of services to the clients. This may have some adverse effects on the financial result and financial position of the concerned institution (profitability, liquidity, capital), as well as on its reputation. The consequences may also be

Upravljanje informacionim sistemom finansijske institucije

U cilju ublažavanja rizika informacionog sistema kome su u svom poslovanju izložene, finansijske institucije treba da upravljaju svojim informacionim sistemima na adekvatan način, primenjujući dobre poslovne običaje i pridržavajući se u tom smislu određenih standarda. U institucijama koje su članice većih grupacija često se mnogi segmenti poslovanja, uključujući i ovaj, uređuju na nivou grupe, odnosno određene politike, standardi i prakse prenose se iz matične kuće. Međutim, usled potrebe da se uspostavi sveobuhvatan i jedinstven pristup na nivou čitavog finansijskog sektora, Narodna banka Srbije donela je, početkom 2013. godine, Odluku o minimalnim standardima upravljanja informacionim sistemom finansijske institucije („Službeni glasnik RS“, br. 23/2013) kojom se uvodi određeni set minimalnih standarda i uslova koje svaka finansijska institucija treba da zadovolji, naravno primereno prirodi, obimu i složenosti svog poslovanja, odnosno složenosti svog informacionog sistema. U daljem tekstu predstavljene su osnovne oblasti koje se Odlukom uređuju.

Okvir za upravljanje informacionim sistemom

Cilj upravljanja informacionim sistemom je podrška poslovnim ciljevima i strategiji finansijske institucije uz efikasno korišćenje resursa informacionog sistema i adekvatno upravljanje rizikom. Finansijska institucija treba da uspostavi, nadzire, preispituje i stalno unapređuje proces upravljanja informacionim sistemom, pri čemu dobre prakse nalažu da ovlašćenja i odgovornosti u tom smislu budu na najvišim organima upravljanja i nadzora u finansijskoj instituciji. Pojedina ovlašćenja i odgovornosti mogu se dalje delegirati na niže nivoe menadžmenta i uspostavljanjem odgovarajućih funkcija i odbora, a u zavisnosti od veličine institucije.

Odgovarajući okvir za upravljanje informacionim sistemom podrazumeva i postojanje strategije razvoja informacionog sistema, ili IT strategije, koja je u svakom trenutku u skladu s poslovnom strategijom i utvrđenim poslovnim ciljevima. Takođe, potrebno je obezbediti adekvatnu organizacionu strukturu, sa odgovarajućom podelom (razdvajanjem) poslova i dužnosti, odnosno sa kontrolama kojima se sprečava sukob interesa, kao i sa uređenim internim linijama izveštavanja nadležnog organa o relevantnim činjenicama u vezi sa informacionim sistemom. Upravljanje projektima u vezi sa informacionim sistemom treba da bude uređeno na sistematičan način i u tu svrhu usvojena odgovarajuća metodologija.

Uspešno upravljanje informacionim sistemom omogućava postizanje optimalnog učinka IT-a i daje dodatnu vrednost poslovanju.

Upravljanje rizikom informacionog sistema

Rizik informacionog sistema predstavlja mogućnost nastanka negativnih efekata na finansijski rezultat i kapital, ostvarivanje poslovnih ciljeva, poslovanje u skladu s propisima i reputaciju finansijske institucije usled neadekvatnog upravljanja informacionim sistemom ili druge slabosti u tom sistemu koja negativno utiče na njegovu funkcionalnost ili bezbednost, odnosno ugrožava kontinuitet poslovanja finansijske institucije.

Finansijska institucija treba da prepozna rizik informacionog sistema, kao specifičnu i značajnu vrstu rizika, te da sveobuhvatnim sistemom upravljanja rizicima obuhvati i upravljanje ovim rizikom. Proces upravljanja rizikom informacionog sistema obuhvata njegovo identifikovanje i merenje, odnosno procenu, kao i ublažavanje, praćenje i kontrolu. Potrebno je u tu svrhu definisati i koji je prihvatljiv nivo rizika.

Procena rizika informacionog sistema jedan je od osnovnih ulaznih parametara za upravljanje bezbednošću tog sistema i upravljanje kontinuitetom poslovanja. Značajno je da pri tome bude obuhvaćen celokupan informacioni sistem finansijske institucije, kao i da se rizikom informacionog sistema upravlja u svim fazama razvoja tog sistema.

Unutrašnja revizija informacionog sistema

Sve finansijske institucije imaju funkciju unutrašnje revizije, koja bi trebalo da se obavlja u skladu s međunarodnim standardima i domaćom regulativom kojom se uređuje ova oblast. Finansijska institucija treba da

reflected in the reduced trust in certain financial products and, ultimately, in the financial system overall.

Information System Management in Financial Institutions

In order to mitigate the information system risk to which they are exposed during their operations, financial institutions should manage their information systems adequately, implementing sound business practices and following the relevant standards in this field. When it comes to institutions which are members of large groups, many business segments, including this one, are often managed at the group level, meaning that certain policies, standards and practices are being transferred from the parent company. However, given the necessity of establishing a comprehensive and uniform approach at the entire financial sector level, in early 2013, the National Bank of Serbia passed the Decision on Minimum Information System Management Standards for Financial Institutions ("Official Gazette of the RS", no. 23/2013), introducing a set of minimum standards and conditions that each financial institution should meet, naturally, in accordance with the nature, volume and complexity of its operations, i.e. in accordance with the complexity of its information system. Below we present the main areas regulated by this Decision.

Information System Management Framework

The objective of information system management is to support a financial institution's business goals and its strategy, and to provide efficient utilization of information system resources and adequate risk management. A financial institution should establish, supervise, regularly review and upgrade the process of information system management, while sound practices suggest the authorizations and responsibilities in this respect to be assigned to the top management and supervision bodies in the concerned financial institution. Certain authorizations and responsibilities may be further delegated to the lower levels of management, through the establishment of appropriate functions and committees, depending on the size of the institution.

The appropriate information system management framework implies the existence of an information system development strategy, or an IT strategy, which is at all times in accordance with the business strategy and determined business goals. Also, it is necessary to provide adequate organizational structure, with the appropriate distribution (segregation) of tasks and duties, and/or the relevant controls preventing any conflicts of interest, along with the defined internal lines of reporting to the competent bodies about the relevant facts concerning the information system. Managing projects related to the information system should be conducted systematically, for which purpose the appropriate methodology should be adopted.

Successful information system management enables the achievement of optimal IT performance and gives added value to the business.

Information System Risk Management

The information system risk represents the possibility of adverse effects on the financial result and capital, achievement of business goals, operations in line with regulations, and reputation of the financial institution, due to the inadequate information system management or other weaknesses in the concerned system, negatively impacting its functionality or security, i.e. jeopardizing the financial institution's business continuity.

A financial institution should recognize the information system risk as a specific and significant type of risk, and therefore include the management of this risk within its comprehensive risk management system. The process of information system risk management includes its identification and measurement, i.e. assessment, along with its mitigation, monitoring and control. To this end, the acceptable level of risk has to be defined.

Information system risk assessment is one of the main entry parameters for the system's security management and business continuity management. What is important in the process is for the entire information system of the financial institution to be included, and for the

na odgovarajući način u metodologiju rada unutrašnje revizije uključi i unutrašnju reviziju informacionog sistema, tako da njom bude obuhvaćen i ovaj, neretko zapostavljeni segment revizije. Pri tome je važno da se kriterijumi, način i postupci unutrašnje revizije informacionog sistema baziraju na rezultatima procene rizika.

Dobre prakse nalažu, naročito za veće finansijske institucije sa složenim informacionim sistemima, da se angažuju unutrašnji revizori koji su kvalifikovani za ovu specifičnu oblast. Kao alternativa tome, a što se prevashodno odnosi na manje institucije, mogu se iskoristiti kapaciteti kojima u tom pogledu raspolaže npr. matična kuća.

Bezbednost informacionog sistema

Bezbednost informacionog sistema obuhvata načela poverljivosti, integriteta, raspoloživosti, autentičnosti, dokazivosti, neporecivosti i pouzdanosti. Jedno od najznačajnijih područja celokupnog upravljanja informacionim sistemom svakako je upravljanje bezbednošću tog sistema. Najbolja praksa nalaže da u tu svrhu bude usvojena politika bezbednosti informacionog sistema (ili politika bezbednosti informacija), kao opšti interni akt kojim će se uspostaviti okvir za upravljanje informacionom bezbednošću i utvrditi i urediti osnovni principi, procedure, ovlašćenja i odgovornosti s tim u vezi. Pojedini segmenti detaljnije se mogu obraditi u posebnim aktima, uz odgovarajuće reference u politici. Ovaj akt treba redovno usklađivati sa svim relevantnim promenama u okruženju i u samom informacionom sistemu.

Kako bezbednost informacionog sistema ne može nikada biti apsolutna, potrebno je obezbediti postizanje i održavanje adekvatnog nivoa ove bezbednosti. Koji je nivo adekvatan treba da proceni svaka institucija, i to prevashodno na osnovu rezultata procene rizika informacionog sistema, kao i obaveza koje proizlaze iz propisa, internih akata, ugovornih odnosa i sl. U tom smislu, upravljanje bezbednošću informacionog sistema predstavlja kontinuiran proces identifikovanja i praćenja potreba za bezbednošću informacionog sistema, te postizanja i održavanja adekvatnog nivoa bezbednosti uspostavljanjem i primenom odgovarajućih kontrola. Prema načinu implementacije kontrole obuhvataju upravljačke, tehničke i fizičke, a prema nameni mogu biti preventivne, detektivne i korektivne.

Obezbeđivanje adekvatne zaštite informacija treba da ima polazište u njihovoj klasifikaciji. To podrazumeva da se za informacije utvrdi stepen osetljivosti i kritičnosti s obzirom na moguće posledice narušavanja njihove poverljivosti, integriteta i raspoloživosti, a kako bi se mogao odrediti potreban nivo zaštite tih informacija. Institucija treba da uredi i da dosledno primenjuje klasifikaciju svih informacija u informacionom sistemu. Takođe, potrebno je imenovati vlasnike, tj. odgovorna lica za pojedine informacije.

Finansijska institucija treba da kontroliše pristup resursima svog informacionog sistema. S tim u vezi, potrebno je uspostaviti adekvatan sistem upravljanja korisničkim pravima pristupa (evidentiranje korisnika, autorizacija, identifikacija i autentifikacija, nadzor nad korisničkim pravima pristupa). Pored toga, treba obezbediti odgovarajuću fizičku zaštitu resursa informacionog sistema, uključujući i zaštitu od štetnih uticaja iz okruženja. Potrebno je uspostaviti i adekvatan sistem nadgledanja informacionog sistema i obezbediti generisanje logova, njihovu zaštitu i praćenje. Logovi bi morali omogućiti da se identifikuju problemi, rekonstruišu događaji, otkriju neovlašćene aktivnosti i utvrde odgovornosti. Takođe, mora postojati i odgovarajuća zaštita od svih vidova malicioznog kôda.

Upravljanje kontinuitetom poslovanja

Upravljanje kontinuitetom poslovanja treba da obezbedi nesmetano i kontinuirano funkcionisanje svih značajnih sistema i poslovnih procesa, kao i ograničavanje gubitaka u vanrednim situacijama. Ova oblast je šira od oblasti upravljanja informacionim sistemom, ali s obzirom na to da je mali broj poslovnih procesa u finansijskim institucijama koji bi se mogli odvijati bez raspoloživosti resursa tog sistema, jasno je da su ti resursi ključni u planiranju kontinuiteta poslovanja i oporavka u slučaju katastrofe. Dobre prakse nalažu da upravljanje kontinuitetom poslovanja bude zasnovano na analizi uticaja na poslovanje i na proceni rizika. U okviru ovih aktivnosti naročito treba identifikovati resurse i sisteme potrebne za odvijanje poslovnih procesa

information system risk to be managed in all development stages of the concerned system.

Internal Information System Audit

All financial institutions have the internal audit function, which should be performed in accordance with international standards and local regulations regulating this field. A financial institution should, in an appropriate way, include internal information system audit in the internal audit methodology, so that this frequently neglected segment gets included in the audit as well. What is important in the process is for the criteria, methods and procedures of internal information system audit to be based on the relevant risk assessment results.

The sound practices suggest, especially for large financial institutions with complex information systems, to hire internal auditors qualified for this specific field. Alternatively, mostly in case of smaller institutions, one can resort to the capacities that are, in this respect, at the disposal of the parent company, for instance.

Information System Security

Information system security entails the principles of confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability. One of the most significant areas of the overall information system management is certainly the management of that system's security. For this purpose, the best practice suggests the adoption of an information system security policy (or an information security policy), as a general internal act establishing the framework for information security management, and determining and regulating the main principles, procedures, authorizations and responsibilities in this respect. Certain segments can be regulated in more detail in separate acts, with appropriate references to the policy itself. This act should be regularly harmonized with all relevant changes in the environment and in the information system itself.

Given that the information system security can never be absolute, it is necessary to achieve and maintain the adequate level of such security. Which level is adequate is to be assessed by each institution itself, primarily based on the results of the information system risk assessment, and the obligations arising from regulations, internal acts, contractual relations, etc. In this sense, information system security management is a continuous process of identifying and monitoring the needs for information system security, and achieving and maintaining the adequate level of security by establishing and implementing appropriate controls. According to the manner of implementation, controls can be administrative, technical and physical, and according to their purpose, they can be preventive, detective and corrective.

Provision of adequate information protection should be based on its classification. This implies that for each piece of information the level of sensitivity and criticality should be determined, bearing in mind the potential consequences of a breach of their confidentiality, integrity and availability, so that the required level of protection for that information could be determined accordingly. An institution should regulate and consistently implement the classification of all information in the information system. Also, it is necessary to name the owners, i.e. the responsible persons for certain pieces of information.

A financial institution should control the access to its information system resources. In this respect, it is necessary to establish an adequate system of managing user access rights (registering, authorization, identification and authentication of information system users, including the supervision of user access rights). In addition, the appropriate physical protection of information system resources should be granted, including the protection against the harmful influences from the environment. It is required for a financial institution to establish the adequate system of information system monitoring, and to enable generating of logs, their protection and monitoring. The logs must enable the identification of problems, reconstruction of events, detection of unauthorized activities and establishment of related responsibilities. Moreover, there has to be appropriate protection against all forms of malware.

Business Continuity Management

The objective of business continuity management is to ensure smooth and

i utvrditi njihove međuzavisnosti, proceniti rizike, utvrditi koji su to kritični/ključni poslovni procesi i aktivnosti čije neadekvatno funkcionisanje može značajnije ugroziti poslovanje finansijske institucije, usvojiti prioritete oporavka poslovnih procesa i resursa i sistema potrebnih za njihovo odvijanje, kao i ciljne nivoe aktivnosti, ciljna vremena oporavka itd.

Na osnovu izvršene analize uticaja na poslovanje i procene rizika, potrebno je doneti plan kontinuiteta poslovanja i plan oporavka aktivnosti u slučaju katastrofa. Plan oporavka treba da obezbedi oporavak i raspoloživost resursa informacionog sistema potrebnih za odvijanje kritičnih/ključnih poslovnih procesa. Pri tome je važno obezbediti da sva lica budu upoznata sa svojim ulogama i odgovornostima u slučaju nastupanja okolnosti koje bi zahtevale aktiviranje ovih planova. Navedene planove treba redovno usklađivati sa svim relevantnim promenama, kao i obezbediti njihovo periodično testiranje.

Sastavni deo upravljanja kontinuitetom poslovanja jeste i upravljanje incidentima, kao neplaniranim i neželjenim događajima koji mogu narušiti bezbednost ili funkcionalnost informacionog sistema, a radi blagovremenog i efikasnog odgovora na te incidente.

Takođe, potrebno je definisati procedure i odgovornosti u vezi sa izradom, čuvanjem i testiranjem rezervnih kopija podataka, kao i oporavkom podataka na osnovu tih kopija. Na osnovu analize uticaja na poslovanje i procene rizika treba obezbediti i raspoloživost adekvatne rezervne lokacije za slučaj nemogućnosti odvijanja poslovnih procesa na primarnoj lokaciji, kao i rezervnog računarskog centra.

Razvoj i održavanje informacionog sistema

Kako bi se obezbedilo da informacioni sistem u svakom trenutku pruža adekvatnu podršku poslovnim procesima finansijske institucije, trebalo bi da postoji kontinuirani proces njegovog razvoja, u skladu sa svim relevantnim promenama, uzimajući pri tome u obzir funkcionalne zahteve i potrebe za bezbednošću. Taj proces mora biti dokumentovan i u skladu s napred pomenutom strategijom razvoja informacionog sistema i metodologijom upravljanja projektima, a potrebno je obezbediti i da razvojno, testno i produkciono okruženje budu na odgovarajući način razdvojeni.

Dobre prakse nalažu uspostavljanje procesa upravljanja hardverskom i softverskom imovinom u svim fazama njihovog životnog ciklusa, uključujući pored ostalog i održavanje odgovarajućih inventara, imenovanje vlasnika, tj. odgovornih lica, definisanje pravila prihvatljivog korišćenja i bezbednog odlaganja i sl.

Uspostavljanjem adekvatnog procesa upravljanja promenama hardverskih i softverskih komponenata informacionog sistema može se izbeći da one dovedu do neočekivanog i neželjenog ponašanja ovog sistema, odnosno naruše njegovu bezbednost ili funkcionalnost. Pri tome je ključno da sve promene hardverskih i softverskih komponenata, uključujući i nove komponente i sisteme, budu testirane i odobrene pre puštanja u produkcijski rad.

Ako se planira migracija podataka na novi sistem glavnih poslovnih aplikacija, potrebno je prethodno sagledati i proceniti sve rizike i definisati kontrole koje će biti primenjene radi ublažavanja tih rizika. Takođe, nužno je sprovesti adekvatno testiranje i definisati „plan B“. Treba imati u vidu da neadekvatno testiranje, neuspeh da se očuva poverljivost, integritet ili raspoloživost podataka, odnosno drugi propust u realizaciji ovakvih projekata može ozbiljno ugroziti interese klijenata i dovesti u pitanje čitavo poslovanje finansijske institucije.

Pored navedenog, od značaja je i upravljanje dokumentacijom koja se odnosi na informacioni sistem, na način da se obezbedi njena tačnost, potpunost i ažurnost, kao i adekvatno, kontinuirano stručno osposobljavanje i obučavanje zaposlenih za korišćenje tog sistema i očuvanje njegove bezbednosti.

Poveravanje aktivnosti trećim licima (IT outsourcing)

IT outsourcing označava eksternalizaciju određenih aktivnosti u vezi sa informacionim sistemom i njihovo poveravanje trećem licu. Osnovni pokretači za to su kvalitet usluge, tj. nedostatak specifičnih znanja unutar institucije, snižavanje troškova usled efekta ekonomije obima, pristup novim (boljim) tehnologijama, mogućnost fokusiranja na osnovnu delatnost finansijske institucije i dr. Međutim, dok s jedne strane *outsourcing* umanjuje određene

continuous functioning of all important systems and business processes, as well as to limit the losses in emergency situations. This field is wider than information system management, but given that only a few business processes in financial institutions could be performed without the available resources of this system, it is clear that these resources are crucial in business continuity and disaster recovery planning.

Sound practices suggest that business continuity management should be based on business impact analysis and risk assessment. Within these activities, a financial institution should particularly identify the resources and systems required for the performance of business processes and their interdependence; assess the risks; establish the critical/key business processes and activities whose inadequate functioning may considerably jeopardize the financial institution's operations; adopt the priorities of recovery of business processes, as well as resources and systems needed for their implementation, along with service delivery objectives, recovery time objectives, etc.

Based on the conducted business impact analysis and risk assessment, it is necessary to adopt a business continuity plan and a disaster recovery plan. The disaster recovery plan should ensure the recovery and availability of information system resources, needed for the performance of critical/key business processes. It is significant to ensure that all employees are familiar with their roles and responsibilities in case of emergency situations that would require the activation of these plans. The plans referred to above should be regularly harmonized with all relevant changes, and submitted to periodical testing.

An integral part of business continuity management is the management of incidents, as unforeseen and unwanted events that could jeopardize the security or functionality of the information system, with a view to providing a timely and efficient response to the concerned incidents.

Moreover, a financial institution should define the procedures and responsibilities concerning the creation, storage and testing of backup copies, as well as the restoration of data based on these copies. Based on the business impact analysis and risk assessment, a financial institution should also ensure the availability of an adequate alternate site, in case of an interruption of business operations on the primary site, along with a secondary data center.

Information System Development and Maintenance

In order to ensure that the information system at all times provides adequate support to its business processes, a financial institution should implement the continuous information system development process, in accordance with all relevant changes, taking into account the functional requirements and security needs. This process has to be documented, and in line with the above mentioned information system development strategy and project management methodology, with the development, testing and production environments being appropriately separated.

Sound practices suggest the establishment of the process of hardware and software asset management in all stages of their life cycle, including, among other things, the maintenance of appropriate inventory, appointment of owners, i.e. responsible persons, definition of rules for acceptable usage and secure disposal, etc.

By establishing the adequate change management process for hardware and software components of the information system, a financial institution can avoid the unexpected and unwanted behavior of this system, and/or avoid jeopardizing the system security or functionality. To this end, it is critical for all changes in hardware and software components, including new components and systems, to be tested and approved before becoming operational.

If a financial institution is planning data migration into the new core business applications, it is necessary for it to first review and assess all risks and define the controls to be implemented in order to mitigate those risks. Also, it is necessary to conduct adequate testing and define the "Plan B". A financial institution should bear in mind that inadequate testing, failure to preserve confidentiality, integrity or availability of data, along with other oversights in the implementation of such projects may

rizike, istovremeno mogu nastati novi, i to usled propusta u izboru pružaoca usluga, neadekvatnog nadzora nad obavljanjem poverenih aktivnosti, nepostojanja adekvatne izlazne strategije ako dođe do prekida pružanja usluga, nemogućnosti pristupa podacima i sl. Posebno se napominje da *offshoring*, kao prekogranični *outsourcing*, može dodatno otvoriti i neka pravna i ekonomska pitanja, naročito ako se radi o aktivnostima koje uključuju čuvanje i/ili obradu podataka finansijske institucije izvan granica zemlje.

Odredbe Odluke kojima se uređuje poveravanje aktivnosti u vezi sa informacionim sistemom trećem licu odnose se na sve aktivnosti koje obuhvataju obradu, čuvanje i/ili pristup podacima kojima raspolaže finansijska institucija a odnose se na njeno poslovanje, kao i na aktivnosti razvoja i/ili održavanja glavnih poslovnih aplikacija. Pri tome, poveravanje aktivnosti uključuje i poveravanje licima povezanim s finansijskom institucijom imovinskim i upravljačkim odnosima.

Zbog mogućih posledica u slučaju propusta u radu pružalaca usluga ili neadekvatnog upravljanja rizicima koji proizlaze iz tog poveravanja, neophodno je da finansijske institucije na odgovarajući način urede ovu oblast, i to naročito proces odlučivanja o poveravanju aktivnosti i kriterijume za donošenje odluke, uključivanje tih aktivnosti u proces upravljanja rizicima i u planiranje kontinuiteta poslovanja, kao i nadzor nad obavljanjem poverenih aktivnosti. Svako poveravanje aktivnosti mora biti uređeno odgovarajućim ugovorom s pružaocem usluga.

Neophodno je obezbediti da se poveravanjem aktivnosti ne ugrozi bezbednost ili funkcionalnost informacionog sistema, kao i da podaci finansijske institucije ostanu u njenom posedu, a sa aspekta supervizora od značaja je istaći i da poveravanje aktivnosti ni na koji način ne sme biti prepreka za nesmetano vršenje kontrole tog dela poslovanja. Važno je napomenuti da odgovornost za aktivnosti koje su poverene trećem licu u celini ostaje na finansijskoj instituciji.

Elektronsko bankarstvo

Elektronsko bankarstvo označava sisteme koji klijentima banke omogućavaju korišćenje usluga koje banke pružaju (pristup finansijskim informacijama, elektronsko plaćanje i sl.) sa udaljene lokacije preko elektronskih interaktivnih komunikacionih kanala (npr. internet bankarstvo, mobilno bankarstvo, telefonsko bankarstvo i dr.). Banke bi trebalo posebnu pažnju da posvete elektronskom bankarstvu, zbog povećanih rizika koji proizlaze iz ovih aktivnosti.

Neophodno je primeniti sigurne i efikasne metode za proveru i potvrdu identiteta i ovlašćenja lica, procesa i sistema. Jednofaktorska autentifikacija više nije dovoljna. Banka treba da, naročito pri izvršavanju platnih transakcija, obezbedi najmanje dvofaktorsku autentifikaciju korisnika, tj. potvrdu njegovog identiteta pomoću najmanje dva različita elementa (nešto što samo korisnik zna; nešto što samo korisnik poseduje; nešto što samo korisnik jeste). Takođe, banka treba i da obezbedi odgovarajuću potvrdu svog identiteta na distributivnom kanalu elektronskog bankarstva, kako bi korisnici mogli da provere autentičnost banke, tj. da se uvere da nije u pitanju pokušaj prevare. Pored toga, da bi se mogla u odgovarajućoj meri obezbediti neporecivost i dokazivost radnji u vezi sa elektronskim bankarstvom, neophodno je obezbediti i postojanje odgovarajućih logova.

Koncepcija nove regulative i očekivani efekti

Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije zasnovana je na najboljoj međunarodnoj praksi, uz primenu pozitivnih iskustava stranih regulatornih, odnosno supervizorskih tela. Njom se prvi put sveobuhvatno i jedinstveno za sve finansijske institucije pod supervizijom Narodne banke Srbije uređuju oblasti upravljanja informacionim sistemom i kontinuitetom poslovanja. Uvažavajući činjenicu da postoje razlike među institucijama (u pogledu prirode, obima i složenosti poslovanja, odnosno složenosti informacionog sistema), primenjen je u određenim odredbama princip proporcionalnosti. Takođe, većina odredaba Odluke konceptualno su definisane, što omogućava primenu pristupa zasnovanog na riziku, koji je ključan za prevenciju neželjenih

seriously jeopardize the interests of the clients and bring into question the entire business of the concerned financial institution.

In addition to the above mentioned, it is important to manage the documentation related to the information system in such a way so as to ensure that it is accurate, comprehensive and up-to-date; and to organize adequate, continuous professional development and training of employees to use the information system and preserve its security.

Outsourcing of Activities Related to the Information System (IT Outsourcing)

IT outsourcing refers to externalizing certain activities related to the information system, and entrusting them to the third parties. The main drivers for outsourcing are quality of service, i.e. the lack of specific competencies within the institution; reduction of costs due to the effect of economies of scale; access to the new (more advanced) technologies; possibility of focusing on core activities of the financial institution, etc. However, while on the one hand outsourcing reduces certain risks, at the same time it may cause some new ones, due to the oversights in choosing the service provider; inadequate supervision of conducting the outsourced activities; lack of an adequate exit strategy in case of interrupted provision of services; inability to access data, etc. What is also worth mentioning is offshoring, as the cross-border outsourcing, which may open some additional legal and economic issues, especially if it concerns activities including the storage and/or processing of a financial institution's data outside the country's borders.

The provisions of the Decision regulating the outsourcing of activities relating to the information system to the third party refer to all activities which include processing, storage and/or access to data which are in possession of a financial institution and which relate to its operation, as well as the activities of development and/or maintenance of core business applications. Outsourcing of activities also includes outsourcing to the parties linked to a financial institution through ownership and management relations.

Due to the possible consequences in case of oversights in the operations of service providers or inadequate management of risks arising from outsourcing, it is necessary for financial institutions to appropriately regulate this field, particularly the decision-making process regarding outsourcing of activities and the criteria for making such decision; integration of these activities into the risk management process and business continuity planning, along with the supervision of conducting the outsourced activities. Each outsourcing of activities must be regulated by means of an appropriate contract with the service provider.

A financial institution should ensure that the outsourcing of activities does not jeopardize the information system security or functionality, and that the data of the financial institution remain in its possession. From the perspective of the supervisor, it is important to underline that the outsourcing of activities must in no way be an obstacle for unhindered control of that business segment. Another significant aspect is that a financial institution remains fully responsible for the activities outsourced to a third party.

Electronic Banking

Electronic banking refers to the systems which enable the bank clients to use the services offered by the bank (access to financial information, electronic payments, etc.) from a remote location by means of electronic interactive communication channels (e.g. Internet banking, mobile banking, phone banking, etc.). The banks should pay particular attention to electronic banking, due to the increased risks arising from such activities.

It is necessary to apply secure and efficient methods for verification and confirmation of the identity and authorizations of persons, processes and systems. Single-factor authentication is no longer enough. A bank should, especially when conducting payment transactions, ensure at least two-factor authentication of users, i.e. confirm their identity by means of at least two different elements (something that only the user knows; something that only the user has; something that only the user is). Moreover, a bank should ensure the appropriate confirmation of its identity on the electronic banking distribution channel, so that the users can verify the bank's authenticity, and be certain

događaja. To podrazumeva da su finansijske institucije u obavezi da kontinuirano upravljaju rizikom informacionog sistema i unapređuju sistem kontrola koje primenjuju radi ublažavanja tog rizika. Ovakvim pristupom propisivanja šta mora da bude zadovoljeno a ne kako to postići obezbeđuje se i određeni stepen fleksibilnosti, što je neophodno imajući u vidu dinamičnost oblasti informacionih tehnologija koju karakterišu stalne inovacije i brzo zastarevanje, kao i neprestana evolucija pretnji po informacionu bezbednost.

Kao što je napred već pomenuto, neke od najboljih praksi iz ove oblasti sistematizovane su u vidu različitih opšte priznatih i prihvaćenih standarda i okvira. Iako Odluka ne insistira ni na jednom konkretnom standardu ili okviru, oni svakako mogu poslužiti kao dobar vodič i pružiti usmerenje pri ispunjenju njenih odredaba.

Odluka počinje da se primenjuje 1. januara 2014. godine na banke, a 1. jula 2014. godine na ostale finansijske institucije. Imajući u vidu da određene obaveze za banke već postoje, obezbeđen je kontinuitet i potreban nivo kompatibilnosti s važećim propisima.

Očekuje se da će primena Odluke značajno doprineti unapređenju postojećih praksi u domenu upravljanja informacionim sistemom, što je neophodan preduslov za stabilno i sigurno poslovanje finansijskih institucija.

Literatura / References

1. Pantović, Vladan; Dinić, Slobodan; Starčević, Dušan. *Savremeno poslovanje i internet tehnologije: Uvod u digitalnu ekonomiju*. Beograd: InGraf, 2002.
2. Westerman, George; Hunter, Richard. *IT Risk: Turning Business Threats into Competitive Advantage*. Boston: Harvard Business School Press, 2007.
3. Cannon, David. *CISA Certified Information Systems Auditor Study Guide, 3rd ed.* Indianapolis: Wiley Publishing, 2011.
4. Van Grembergen, Wim; De Haes, Steven. *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value*. New York: Springer, 2009.
5. Stojanović, Gordana; Pantović, Vladan. *"Standardizacija sigurnosti finansijskih transakcija"* Prvi stručni skup - Zaštita podataka u računarskim sistemima, Zbornik radova, 163-180. Beograd: Savez inženjera i tehničara Srbije, 1995.
6. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows: ISACA, 2012.
7. Pantović, Vladan. *"COBIT 5: Referentni model procesa za korporativno upravljanje i menadžment informacionih tehnologija"* XXVII naučno-stručni skup Infotech 2012, CD Zbornik radova. Vrnjačka Banja: 2012.

that they are not part of an attempted fraud. In addition, a bank should warrant the existence of appropriate logs so as to ensure the appropriate non-repudiation and accountability of actions concerning electronic banking.

New Regulatory Concept and its Expected Effects

The Decision on Minimum Information System Management Standards for Financial Institutions is based on the best international practice, and implements the positive experiences of foreign regulatory and supervisory bodies. This Decision for the first time regulates the fields of information system management and business continuity management comprehensively and uniformly for all financial institutions under the supervision of the National Bank of Serbia. Taking into account the fact that institutions differ among themselves (in terms of the nature, volume and complexity of operations, i.e. the complexity of their information systems), the Decision in certain provisions implements the principle of proportionality. Also, most of the provisions of the Decision are conceptually defined, enabling the risk-based approach, which is crucial for the prevention of undesired events. This implies that financial institutions are obliged to continuously manage the information system risk and upgrade the system of controls implemented in order to mitigate that risk. This kind of approach - prescribing what has to be met, but not how to achieve it - provides a certain level of flexibility, which is necessary bearing in mind the dynamics of information technologies, characterized by constant innovations and quick obsoleteness, along with the never-ending evolution of threats for information security.

As was already mentioned above, some of the best practices in this field have been systematized in the form of various, generally recognized and accepted standards and frameworks. Although this Decision does not insist on any concrete standard or framework, they can certainly serve as excellent guidelines and provide direction in respecting its provisions.

The Decision will be implemented as of January 1st 2014 for banks, and as of July 1st 2014 for other financial institutions. Given that certain obligations in this respect have already been in place for banks, the relevant continuity and required level of compatibility with the existing regulations has been provided.

The Decision's implementation is expected to contribute considerably to the advancement of existing practices in the field of information system management, as the necessary precondition for stable and secure operations of financial institutions.