Audit Financiar, XXI, Nr. 2(170)/**2023**, *211-219*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Asigurarea securității datelor financiar-contabile stocate în baza de date a sistemelor ERP

Drd. Laura-Eugenia-Lavinia BARNA,
Academia de Studii Economice din Bucureşti, Şcoala Doctorală de Contabilitate,
e-mail: barnalaura15@stud.ase.ro

Prof. univ. dr. Bogdan-Ştefan IONESCU,
Academia de Studii Economice din Bucureşti, Departamentul Informatică de Gestiune,
e-mail: bogdan.ionescu@cig.ase.ro

REZUMAT

Profesia contabilă se află într-un continuu proces de digitalizare, ca urmare a utilizării frecvente a sistemelor informatice cu scopul de a eficientiza şi îmbunătăţii activitatea zilnică a angajaților din acest domeniu. Cu toate acestea, pe lângă beneficiile oferite de aceste sisteme informatice pentru profesioniştii contabili, trebuie avute în vedere şi riscurile la care ar putea fi supuse informațiile prelucrate şi stocate cu aceste sisteme informatice astfel încât calitatea activităților financiar-contabile să nu fie perturbată.

Lucrarea de față îşi propune să analizeze principalele riscuri la care ar putea fi supuse datele financiar-contabile prelucrate şi stocate în baza de date a sistemelor ERP, precum şi modul de asigurare a securității datelor financiar-contabile în cadrul acestor soluții informatice integrate. Acest articol s-a axat pe o cercetare de tip cantitativ, folosind analiza bibliometrică ce se bazează în principiu pe analizarea unui eşantion de 263 de articole care tratează cele două subiecte cheie ale lucrării: "securitatea datelor" şi "sistemele ERP".

Cuvinte cheie: *risc; securitatea datelor; sisteme ERP; soluții informatice integrate; digitalizare; analiză bibliometrică;*

Clasificare JEL: *G32, L86, M15, M40, M41*

Vă rugăm să citați acest articol astfel:
Barna, L.-E.-L., Ionescu, B.-Ş., (2023), Ensuring the Security of Financial-Accounting Data Stored in the Database of ERP Systems, *Audit Financiar*, vol. XXI, no. 2(170)/2023, pp. 291-299, DOI: 10.20869/AUDITF/2023/170/008

Link permanent pentru acest document:
http://dx.doi.org/10.20869/AUDITF/2023/170/008
Data primirii articolului: 23.03.2023
Data revizuirii: 31.03.2023
Data acceptării: 2.05.2023

Introducere

Evoluția tehnologică din ultimii ani a determinat digitalizarea unui număr mare de activități atât în domeniul financiar-contabil, cât şi din alte domenii, facilitând astfel prelucrarea, analiza şi stocarea unui volum mare de informații într-un interval mai scurt de timp ca urmare a utilizării sistemelor informatice. Cu toate acestea, datele trebuie păstrate în siguranță de la momentul introducerii acestora în sistemele informatice până la momentul stocării, prelucrării şi analizei acestora, deoarece în ultima perioadă "utilizatorii au devenit veriga cea mai vulnerabilă a sistemelor de securitate" (Popescu şi Popescu, 2018).

Literatura de specialitate asociază această evoluție tehnologică cu un factor important al creşterii numărului de amenințări ale securității informatice. Însă, realizarea unor controale adecvate şi a unui sistem de protecție ar fi de mare ajutor în asigurarea securității datelor financiar-contabile stocate în sistemele informatice.

Scopul lucrării este de a identifica principalele măsuri care pot fi adoptate, astfel încât informațiile financiar-contabile prelucrate şi stocate în baza de date să nu fie supuse riscurilor apărute din mediul online.

1. Revizuirea literaturii de specialitate

1.1. Importanța sistemelor ERP în activitatea financiar-contabilă

Sistemul ERP (*en. Enterprise Resource Planning*) este un sistem informatic integrat utilizat de companii pentru gestionarea unui volum mare de date şi resurse (Pareek, 2014; Hrischev, 2020; Kitsantas, 2022). Conform Senior Software (2020), sistemul ERP permite "managementul integrat al proceselor şi operațiunilor din diferite arii de business: achiziții, vânzări, contabilitate, producție, managementul relațiilor cu clienții, managementul proiectelor, dar şi alte activități logistice".

Multe companii care activează în domeniul financiar-contabil decid implementarea acestor sisteme ERP, deoarece le oferă acces centralizat la date esențiale pentru companie, permițând automatizarea unei game largi de operațiuni care eficientizează fluxul de informații. Mai mult de atât, sistemele ERP oferă posibilitatea utilizatorilor de a introduce datele direct de la tastatură, fie să importe datele, fie să utilizeze tehnologia transferului prin tehnologia EDI (Electronic Data Intercharge).

Principalele funcționalități ale sistemelor ERP care determină companiile să implementeze aceste soluții informatice sunt:

- întregul flux de informații din cadrul companiei este înregistrat în baza de date comună a sistemului ERP;
- asigură automatizarea şi standardizarea diferitelor procese operaționale;
- asigură monitorizarea activităților şi resursele utilizate de companie;
- generarea electronică a diferitelor documente financiare şi contabile (facturi, declarații, note contabile);
- gestionează operațiunile de natură financiară din cadrul companiei;
- generează diferite rapoarte necesare departamentului financiar-contabil, dar şi pentru alte departamente ale companiei.

Principalele beneficii oferite de sistemele ERP pentru companii sunt prezentate în ***Figura nr. 1***.

Kanellou (2013) a identificat trei motive relevante pentru care companiile decid să implementeze sistemele ERP: "cererea crescută de informații în timp real, generarea de informații pentru luarea deciziilor şi nevoia de integrare a aplicațiilor". Nawaz şi Channakeshavalu (2013) au identificat şi alte beneficii: reingineria proceselor de afaceri, standardizarea sistemelor şi proceselor, îmbunătățirea practicilor.

Figura nr. 1. Beneficiile sistemelor ERP

Sursa: Prelucrările autorilor, 2022

1.2. Principalele categorii de riscuri la care pot fi supuse datele financiar-contabile prelucrate şi stocate în sistemele ERP

Conform Popescu şi Popescu (2018), principalele tipuri de riscuri / atacuri cibernetice cu care se poate confrunta o companie sunt:

- atacuri asupra aplicațiilor;
- spionaj cibernetic (accesul neautorizat asupra datelor prelucrate cu ajutorul sistemelor ERP);
- furtul sau pierderea fizică a echipamentelor;
- soft malware;
- erori;
- maparea incorectă a proceselor de afaceri.

1.3. Principalele măsuri pentru asigurarea securității datelor financiar-contabile stocate în baza de date a sistemelor ERP

Principalele nivele de securitate a datelor pe care ar trebui să le aibă orice sistem informatic sunt: securitatea fizică, securitatea logică, securitatea accesului, securitatea

serviciului. Securitatea accesului este definită în literatura de specialitate ca modalitatea de acces la sistem a utilizatorilor. Astfel se poate asigura accesul controlat la datele sensibile din cadrul companiei. Securitatea serviciilor presupune ca funcțiile de detectare şi avertizare în cazul unui potențial atac cibernetic sau a furtului de date să fie activat pe toată durata utilizării sistemului informatic.

Hrischev (2020) şi Parthiban şi Nataraj (2019) au observat că primul pas privind asigurarea securității datelor în baza de date a sistemelor ERP îl reprezintă arhitectura sistemului, altfel spus modalitatea în care este conceput acel sistem informatic. Sistemele ERP prezintă o arhitectură bazată pe trei nivele:

- *nivelul de prezentare* – terminalele, unde sunt introduse datele şi sunt transferate între nivele
- *nivelul aplicației* – serverul sistemului informatic (procesarea datelor pe bază de algoritmi şi funcții de business)
- *nivelul bazei de date* – serverul bazei de date a sistemului informatic (zona de stocare a datelor)

Printre măsurile care pot fi adoptate pentru asigurarea securității datelor financiare stocate în baza de date a sistemelor ERP ar putea fi (Chang ş.a., 2014):

- accesul controlat la date, astfel încât fiecare utilizator are acces doar la datele pe care le utilizează zilnic;
- nivelul de partajare a datelor este strict definit, astfel încât să nu fie încălcată procedura de confidențialitate a datelor;
- comunicarea datelor către clienți se realizează prin canale de comunicare bine definite şi securizate (ex: SharePoint, Google Drive etc.) şi sunt bine criptate

Un alt pas ar fi asigurarea unei conexiuni de internet stabile şi criptate (She şi Thuraisingham, 2007; Sorheller, 2018), astfel riscul de furt al datelor să fie minimizat.

2. Metodologia cercetării

Metoda de cercetare utilizată de către autori în cadrul acestui articol a avut ca scop definirea conceptului de securitate a informațiilor financiar-contabile prelucrate şi stocate în baza de date a sistemului ERP cu ajutorul articolelor ştiințifice care tratează acest subiect. Articolele au fost colectate în perioada 29 octombrie 2022-5 noiembrie 2022 din diferite baze de date, cum ar fi: Web of Science, Scopus, Emerald, Elsevier şi alte baze de date, utilizând următoarele cuvinte cheie pentru căutare: „securitatea datelor", „sisteme ERP", „date financiar-contabile stocate în sisteme ERP", „securitatea bazelor de date", „securitatea sistemelor ERP".

Autorii au construit şi câteva întrebări ale cercetării prezentate mai jos cu privire la tema articolului, încercând să răspundă cu ajutorul informațiilor colectate din articolele selectate:

Î1. Care este cadrul pentru asigurarea controlului intern?

Î2. Care sunt beneficiile oferite utilizatorilor de sisteme ERP?

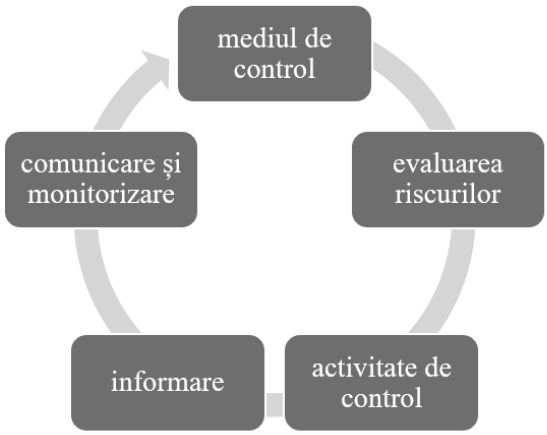
Î3. Care sunt principalele soluții pentru a asigura securitatea datelor financiar-contabile?

Astfel, pentru cuantificarea rezultatelor referitoare la securitatea sistemelor ERP, autorii au utilizat o analiză bibliometrică axată pe gruparea cuvintelor cheie "securitate" şi "sisteme ERP" aflate în relație cu alte cuvinte cheie identificate în articolele selectate din platforma *Web of Science*. Eşantionul a fost format din 263 de articole relevante pentru subiectul lucrării, fiind publicate între anii 1996-2022, cele mai multe articole – după anul 2012, când a avut loc evoluția masivă a conceptului de digitalizare a activităților. Pentru a prelucra datele despre articolele selectate, autorii au utilizat aplicația *VOS viewer*. Rezultatele obținute sunt prezentate în secțiunea următoare.

3. Analiza rezultatelor

Analizând cele 20 de articole selectate din diferite baze de date, autorii au identificat o serie de informații relevante pentru tema articolului. La întrebarea *"Care este cadrul pentru asigurarea controlului intern?"*, autorii Chang (2014) şi Chang ş.a. (2014) au identificat faptul că securitatea sistemelor şi controalele interne din sistemele ERP sunt asigurate de "politica de securitate, modalitatea de autentificare a utilizatorului, securitatea bazei de date". Controalele aplicate mențin fiabilitatea sistemului informatic, dar şi disponibilitatea datelor financiare. Însă, autorii Chang ş.a. (2014) au definit cadrul pentru asigurarea controlului intern prin intermediul a cinci componente prezentate în ***Figura nr. 2***.

Figura nr. 2. Cadrul pentru asigurarea controlului intern



Sursa: Prelucrările autorilor pe baza Chang ş.a. (2014)

Hrischev (2020) afirmă că fiecare utilizator trebuie să aibă un acces controlat la date în cadrul bazei de date. Cele mai multe sisteme ERP folosesc aplicația Citrix care conține o infrastructură ce securizează informațiile pe internet, folosind un portal de acces (Gateway) cu nume de utilizator şi parolă, sporind astfel securitatea datelor.

Baza de date a sistemului ERP este structurată fie prin limbajul SQL (Structured Query Language) sau Oracle DB. Noile versiuni de sisteme ERP folosesc baze de date de tip NoSQL, asigurând un grad mai mare de securitate.

La întrebarea *"Care sunt beneficiile oferite utilizatorilor de sisteme ERP?"*, autorul Kanellou (2013) afirmă că sistemele ERP oferă utilizatorilor o creştere a flexibilității informațiilor, îmbunătățirea calității rapoartelor, dar şi îmbunătățirea procesului decizional. Kitsantas (2022) a identificat faptul că sistemele ERP asigură informații mai bune într-un timp mai scurt, la un cost cât mai redus. Alți autori sunt de părere că implementarea sistemelor ERP este destul de costisitoare, însă pe parcurs această investiție realizată de companie se amortizează. Nawaz (2013) consideră că sistemele ERP oferă posibilitatea utilizatorilor de a procesa mult mai rapid informația, dar şi de a centraliza datele mult mai eficient, ca urmare a integrării unui număr mare de funcții pe care le dețin sistemele ERP, funcții utile pentru diferite departamente din cadrul companiilor.

Autorii Pareek (2014), Onyshchenko (2018), Rîndaşu (2018) şi Parthiban şi Nataraj (2019), consideră că principalele măsuri pentru securitatea datelor din sistemele ERP sunt: securitatea rețelei de internet (aplicând un protocol HTTPS, asigurând autentificarea utilizatorilor pe bază de certificate digitale), securitatea bazei de date (izolarea serverului de restul infrastructurii IT a companiei), securitatea serverului aplicației, securizarea informațiilor pe terminalele utilizate şi securitatea sistemelor ERP.

She şi Thuraisingham (2007) şi Sharma şi Maheshwari (2014) sunt de părere că securitatea datelor financiar-contabile ar trebui mai întâi asigurată din interiorul şi exteriorul companiei şi ar trebui asigurat un control intern adecvat al sistemului ERP. De asemenea, ar trebui conceput şi un plan de recuperare în cazul apariției unui atac cibernetic sau a furtului de date (Xu ş.a., 2002; Weng şi Hung, 2014).

FBI (2012, citat de Mangiuc, 2016) a identificat principalele origini ale riscului de securitate informatică ca fiind angajații nemulțumiți, apoi hackerii independenți sau spionajul economic şi business intelligence.

La întrebarea *"Care sunt principalele soluții pentru a asigura securitatea datelor financiar-contabile?"*, autorul Rădulescu (2016) a identificat următoarele soluții de securitate a datelor unei companii pe următoarele planuri:

- logice: criptare, backup, monitorizare, antivirus, audit, firewall
- fizice: securizarea echipamentelor gestionate

- operațional-administrativ: crearea unor proceduri de lucru, training-uri cu angajații etc.

Conform studiului realizat de Rîndaşu (2019), majoritatea profesioniştilor contabili care au fost ținta unui atac cibernetic se adresează de cele mai multe ori departamentului IT al companiei. Alți profesionişti contabili se adresează superiorului ierarhic, responsabilului cu protecția datelor, autorităților sau colegilor pentru a rezolva problemele apărute ca urmare a atacului cibernetic.

Analizând în detaliu informațiile identificate, autorii articolului de față consideră că securitatea datelor financiar-contabile ar trebui asigurată atât din interiorul companiei, cât şi din exteriorul acesteia.

În ***Figura nr. 3***, datele despre cele 263 de articolele selectate din Web of Science pe baza cuvintelor cheie "securitate" şi "sisteme ERP" aflate în relație cu alte cuvinte cheie, arată că multe articole prezintă securitatea sistemelor ERP din perspectiva noilor tehnologii, cum ar fi: cloud computing, Big Data, e-business, SaaS.

Figura nr. 3. Relația dintre cuvintele cheie "securitate" şi "sisteme ERP"

Sursa: Prelucrările autorilor pe baza informațiilor colectate despre articole din platforma Web of Science (2023)

Autorii au identificat 7 grupări de cuvinte cheie (clustere), acestea fiind prezentate detaliat în **Tabelul nr. 1**. Grupările de cuvinte care au înregistrat cele mai multe elemente prezintă nuanțe de negru intens, urmând ca treptat, odată cu scăderea numărului de elemente, această nuanță să predomine în nuanțe de gri închis şi gri mai deschis. Astfel, grupările de cuvinte care conțin cele mai puține elemente, prezintă o nuanță de gri foarte deschis.

Tabelul nr. 1. Grupările de cuvinte cheie identificate în articolele selectate

Grupare (Cluster)	Cuvinte cheie specifice
Cluster 1 (9 elemente)	Big Data, Blockchain, Cybersecurity, Information security, Internet, Management, Privacy, Security, Systems
Cluster 2 (10 elemente)	Adoption, Cloud, Cloud computing, Determinants, E-business, Information-technology, Performance, SaaS, Smes, User acceptance
Cluster 3 (7 elemente)	ERP implementation, Information systems, Integration, Model, Optimization, Success, Technology
Cluster 4 (7 elemente)	Business, Challenges, Cloud ERP, Critical success factors, Enterprise, Network, Network security
Cluster 5 (7 elemente)	Authentication, Classification, Data security, EEG, ERP, P300, RFID
Cluster 6 (6 elemente)	Enterprise systems, Framework, Impact, Implementation, Internal control, Software
Cluster 7 (1 element)	Services

Sursa: Prelucrările autorilor

După cum se poate observa în **Tabelul nr. 1**, cuvintele cheie identificate prezintă legătură între ele, toate cuvintele fac referire la tehnologiile noi din domeniul IT. Astfel, corelația identificată de autori ar fi în cea mai mare măsură între sistemele ERP, securitate, autentificare şi implementare.

Tabelul nr. 2 prezintă distribuția publicațiilor şi citărilor acestora în funcție de regiunea geografică.

Tabelul nr. 2. Distribuția publicațiilor şi citărilor acestora în funcție de regiunea geografică

Țara / Regiunea geografică	Număr lucrări scrise în fiecare țară / regiune	Numărul de citări ale articolelor care provin din regiunea respectivă
SUA	45	996
China	47	314
India	34	198
Anglia	17	693
Arabia Saudită	9	142
Taiwan	19	97
Germania	16	203
Italia	5	46
Australia	6	171
Canada	8	204
Africa de Sud	8	44
Coreea de Sud	8	138
Pakistan	5	29
Spania	6	68
Republica Cehă	5	11
Indonezia	6	3
Polonia	7	20
România	7	16
Ucraina	5	9
TOTAL	263	3402

Sursa: Prelucrările autorilor

Cele mai multe lucrări provin din țări dezvoltate din punct de vedere al digitalizării, cum ar fi: China, SUA, India, Taiwan, Anglia şi Germania. Celelalte țări, cum ar fi Italia, Australia, Canada, Africa de Sud, Coreea de Sud, Pakistan, Spania, Republica Cehă, Indonezia, Polonia, România, Ucraina, înregistrează un număr mic de articole, cuprins între 5 şi 8 pe țară sau regiune.

4. Concluzii

Chiar dacă procesul de digitalizare a luat amploare în ultimii ani, trebuie avută în vedere şi asigurarea unei securități adecvate a datelor prelucrate şi stocate cu aceste sisteme ERP.

Digitalizarea activităților din domeniul financiar-contabil a apărut ca urmare a necesității utilizatorilor de a avea acces rapid la informații relevante şi în timp real.

Ca urmare a efectelor post-pandemiei de COVID-19, s-a observat creşterea numărului de incidente de securitate atât la nivel național, cât şi la nivel global, conform raportului emis de CERT. Încă se află în cercetare modul prin care se poate reduce apariția unor astfel de incidente. Progresul tehnologic a influențat apariția unor noi categorii de vulnerabilități în asigurarea securității datelor.

Având în vedere articolele selectate pentru a fundamenta baza teoretică a articolului de față, autorii au ajuns la concluzia că o cultură organizațională stabilă şi puternică poate preveni apariția unor incidente de securitate, deoarece fluxul de informații este mult mai bine gestionat de membrii unei astfel de organizații, iar activitățile sunt mult mai bine definite în cadrul organizației.

BIBLIOGRAFIE

1. Chang, S.I. (2014), Internal control framework for a compliant ERP system, *Information & Management*, vol. 51, pp. 187-205, DOI: http://dx.doi.org/10.1016/j.im.2013.11.002
2. Chang, S.I., Yen, D.C., Chang, I.C., Jan, D (2014), Internal control framework for a compliant ERP system, *Information & Management*, vol. 51, pp. 187-205, DOI: http://dx.doi.org/10.1016/j.im.2013.11.002
3. Hrischev, R. (2020), ERP systems and data security, *IOP Conference Series: Materials Science and Engineering*, vol. 878, pp. 1-8
4. Kanellou, A., Spathis, C. (2013), Accounting benefits and satisfaction in an ERP environment, *International Journal of Accounting Information Systems*, vol. 14, pp. 209-234, DOI: http://dx.doi.org/10.1016/j.accinf.2012.12.002
5. Kitsantas, T. (2022), Exploring Blockchain Technology and Enterprise Resource Planning System: Business and Technical Aspects, Current Problems and Future Perspectives, *Sustainability*, vol. 14, DOI: https://doi.org/10.3390/su14137633
6. Mangiuc, D.M. (2016), Auditing security for the Cloud, *Audit Financiar*, vol. XIV, nr. 3 (135) / 2016, pp. 302-311, DOI: 10.20869/AUDITF/2016/135/302
7. Nawaz, M.N., Channakesshavalu, K. (2013), The impact of Enterprise Resource Planning (ERP) systems implementation on business performance, *Asia Pacific Journal of Research*, vol. 2, nr. 4, pp. 30-47
8. Onyshchenko, O. (2018), Introducing ERP system as a condition of information security and accounting system transformation, *International Journal of Engineering & Technology*, vol. 7, nr. 4.3, pp. 530-536
9. Pareek, R. (2014), Analytical Study of Cloud ERP and ERP, *International Journal of Engineering and Computer Science*, vol. 3, nr. 10, pp. 8710-8717
10. Parthiban, K., Nataraj, R.V. (2019), An efficient architecture to ensure data integrity in ERP systems, *5th International Conference on Advanced Computing & Communication Systems*, pp. 236-241, DOI: 978-1-5386-9533-3/19/$31.00
11. Popescu, C.R., Popescu, G. (2018), Risks of cyber attacks on financial audit activity, *Audit Financiar*, vol. XVI, nr. 1 (149) / 2018, pp. 140-147, DOI: 10.20869/AUDITF/2018/149/006
12. Rădulescu, M.C. (2016), Considerations on the selection and prioritization of information security

solutions, *Audit Financiar*, vol. XIV, nr. 5 (137)/2016, pp. 564-574, DOI: 10.20869/AUDITF/2016/137/564

13. Rîndaşu, S.M. (2018), Information security challenges – vulnerabilities brought by ERP applications and cloud platforms, *Audit Financiar*, vol. XVI, nr. 1 (149) / 2018, pp. 131-139, DOI: 10.20869/AUDITF/2018/149/005
14. Rîndaşu, S.M. (2019), The Security of Accounting Information – A Perception-Based Analysis of the Practitioners from Romania, *Audit Financiar*, vol. XVII, nr. 2 (154) / 2019, pp. 298-305, DOI: 10.20869/AUDITF/2019/154/012
15. Senior Software (2020), What is ERP?, disponibil la: https://www.seniorsoftware.ro/erp/ce-inseamna-erp-software-erp-sistem-erp-soft-erp-romania/?gclid=EAIaIQobChMIu_KCr_-W-wIVZI9oCR2tZgyVEAAYASAAEgLVD_D_BwE, accesat la 10 Noiembrie 2022
16. Sharma, C., Maheshwari, S. (2014), Ten security practices to a formidable ERP system, *International Conference on Smart Structures & Systems India*, pp. 41-50, DOI: 978-1-4799-6506-9/9
17. She, W., Thuraisingham, B. (2007), Security of Enterprise Resource Planning Systems, *Information Systems Security*, vol. 16, pp. 152-163, DOI: 10.1080/10658980701401959
18. Sorheller, V.U., Hovik, E.J., Hustad, E., Vassilakopoulou, P. (2018), Implementing cloud ERP solutions: a review of sociotechnical concerns, *Procedia Computer Science*, vol. 138, pp. 470-477
19. Weng, F., Hung, M.C. (2014), Competition and challenge on adopting Cloud ERP, *International Journal of Innovation, Management and Technology*, vol. 5, nr. 4, pp. 309-313
20. Xu, H., Nord, J.H., Brown, N., Nord, G.D. (2002), Data quality issues in implementing an ERP, *Industrial Management & Data Systems*, vol. 102, nr. 1, pp. 47-58, DOI 10.1108/02635570210414668