The Role of Data Authentication and Security in the Audit of Financial Statements

László Szívós

Faculty of Economics and Social Sciences, Department of Finance
Budapest University of Technology and Economics
Magyar tudósok körútja 2, H-1117 Budapest, Hungary
E-mail: szivos@finance.bme.hu

István Orosz

Doctoral School of Applied Informatics
Óbuda University
Bécsi út 96/b, H-1034 Budapest, Hungary
E-mail: orosz.istvan@arek.uni-obuda.hu

Abstract: Fairly presented financial statements are factual, free from bias and any material misstatements, and reflect the commercial substance of the financial transactions at a company. These statements have a standardized format and should be prepared in accordance with the applicable financial reporting framework. External audits provide reasonable assurance to the owners of the business's on to what extent financial statements are free of material misstatement whether due to error or fraud. There is always a risk (control risk) that the business's internal control system cannot prevent, detect or correct misstatements. The necessary sources of the financial data are handled nowadays by ERP (Enterprise Resource Planning) systems, triggered out the manual handwork. The applied ERP systems are different in companies according to the size and the business flows of the company. When it comes to a small or middle sized company, many of them use one generic system, which operates both the OLAP (analysis) and the OLTP (transaction processing) functions. There is a common risk to overwrite the master data, which can influence the reliability of financial statements. Lot of control procedures assure that the contained data are valid and show the true and fair state of the business. In this paper, we review how control procedures in an ERP system can influence the level of control risk and thus the scope and quantity of the audit procedures performed by the financial auditor.

Keywords: financial audit; control risk; ERP; master data management; data migration; data consistency check

1 Introduction

In the audit of financial statements there is always a risk that a misstatement appears at the assertion level which is material either individually or when aggregated and could not be prevented, detected or corrected by the internal control of the company. This type of risk is called control risk and it plays an important role in the risk assessment of financial auditors.

The accuracy and relevance of master data and master files are essential for the fair presentation of financial statements. Today the application of ERP systems is quite common in business. It also means that ERP provides the platform where master data and master files are managed and maintained. There are transactions which increase the risk of misstatements in the financial statements. Such transactions are e.g. data migration, or unauthorized change of data in master files. These can have an adverse impact on the level of risk perceived by auditors who have to maintain the overall audit risk at an acceptable level.

The article is structured as follows. First, the authors define the risk assessment procedure of the financial auditors and then give a thorough literature review on the impact of information technology applications on the financial audit procedure and on risk assessment. Secondly, they prove the importance of master data management in the accuracy of financial statements and demonstrate an available tool in Microsoft Dynamics AX environment for checking the integrity and consistency of master data across all relations. In the conclusion section they investigate the interrelation between consistency check and the financial audit procedure.

2 The Risk[1] of Auditing Financial Statements

There is always a risk that the auditor expresses an inappropriate audit opinion about the financial statements, this is called audit risk. Risk assessment procedures are conducted by the auditor to understand the entity and its environment, including its internal control, to identify the risk of material misstatement either due to error or fraud. Audit risk is made up of two components: the material misstatement risk and the detection risk.

Material misstatement risk can be split to inherent risk and control risk (Figure 1). Inherent risk is the susceptibility of an assertion to a misstatement that could be material, either individually or when aggregated with other misstatements, assuming that there were no related internal controls. Control risk arises in an assertion that could be material, either individually or when aggregated with other

[1] Definitions are based on ISA 200 [8]

misstatements that will not be prevented, or detected and corrected on a timely basis by the entity's internal control. Detection risk is the risk when the procedures conducted by the auditor will not detect a misstatement. This derives from the fact that the auditor does not, and cannot examine all available evidence. The control risk and the inherent risk are the risks of business and exist independently from the audit procedure.

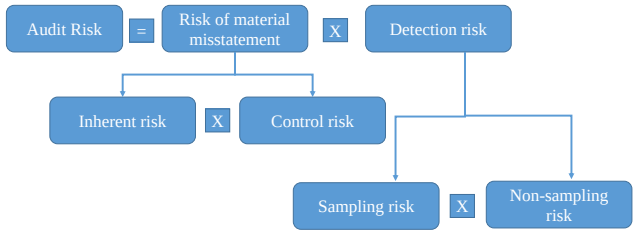

Figure 1
The components of audit risk

ISA 200 [8] states that in order to provide reasonable assurance the auditor should gather appropriate and sufficient audit evidence to keep audit risk at an acceptable level.

Our study investigates the control risk, which is one of the three above mentioned risk factors. Control risk depends on the effectiveness of internal control designed and implemented by the management of the entity. Efficient internal control, however, can only decrease but not totally eliminate the existence of control risk. This means that a certain level of control risk will always exist. The most common examples are human errors and mistakes, and examples when the management and those charged with governance override control.

Based on ISA 315 [8] definition, internal control is the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations and compliance with laws and regulations. Through a financial statement audit the auditor should acquire a reasonable understanding of the relevant aspects of the client's internal control system. This covers the identification of potential misstatements, the consideration of the factors that affect the risks of material misstatement, and based on the first two the design of the nature and timing of further audit procedures.

2.1 The Impact of Information System Applications at the Level of Control Risk

Companies can gain substantial benefits from using IT systems, however, this can also bring significant risks. The financial statement can be prepared based on IT systems which inaccurately process data or process inaccurate data, or in certain

cases both at the same time. If users have unauthorized access to data it might result in improper changes in data or in the record of unauthorized or non-existent transactions, or inaccurate recording of transactions.

ISA 315 [8] says that the auditor should understand the information systems applied by the company and all the related issues relevant to financial reporting. ISA 315 also says that the auditor shall overview the related accounting records, supporting information and specific accounts that are used to initiate, record, process and report transactions. It is also important for the auditor to understand the way the information system captures transactions and events that are significant to the financial statement.

Furthermore the auditor should understand how the company responds to the risks arising from the application of IT systems. The expected control an entity shall conduct can be split into two categories: 1) General IT controls and 2) Application controls. General IT controls are those policies and procedures which support the appropriate operations of an information system. General IT controls cover the following: 1) data centre and network operations, 2) system software acquisition, change and maintenance, 3) program change, 4) access security and 5) application system acquisition, development and maintenance. Application controls are procedures, either manual or automated, that run at business process level. The purpose of these controls is to maintain the integrity of accounting records. They are either preventive or detective. Most common application controls are: 1) controls over input: completeness, accuracy and authorization, 2) controls over processing, 3) controls over master file and standing data. The application of general IT controls and application controls are strictly interrelated in a way that they can either support or undermine each other. The strength of general controls can increase or decrease the reliability of application controls. For example the weaknesses in general control procedures, e.g. system development or software maintenance, or the authority of system users to sensitive data or system functions might result in a higher control risk as it can deteriorate the efficiency of application controls.

The level of control risk depends on the nature and characteristics of the company's information system. The company must manage the risk of using IT applications by setting up effective controls in respect of the nature of the information system.

2.2 The Response of Auditors to Increased Control Risk

As stated in ISA 200 the auditor is responsible for maintaining the audit risk at an acceptable level. As the audit risk is the function of the risk of material misstatement and the detection risk, if the internal control system fails to operate efficient and effective controls over the IT system it necessarily results in increased control risk and thus in increased material misstatement risk. In order to maintain the acceptable level of audit risk the auditor should outweigh this effect

by reducing the risk of detection. In this part we review what ISA 330 says about the auditor's required responses.

Based on ISA 330 [10] the auditor must design and apply appropriate responses to the assessed risk of material misstatement at the financial statement level. If the auditor reveals that the risk of material misstatement (including the control risk) is high, substantive procedures that respond to the assessed risk shall be conducted. The auditor can respond the assessed risk of material misstatement by means of:

- maintaining the professional scepticism in the engagement team,
- more experienced staff with more sophisticated skills should be appointed,
- the use of the work of experts,
- higher supervision over the audit process,
- higher unpredictability in the selection and application of audit procedures,
- general changes in the nature, timing and scope of the audit procedures.

The response of the auditor to the assessed risk highly depends on the auditor's opinion of the control environment. If the control environment is effective the auditor might put higher confidence in the internal control and the audit evidence gathered internally. Inefficiencies of the control environment, however, have the opposite impact on the procedures conducted by the auditor. The auditor's responses to the ineffective control environment are as follows:

- more audit procedures shall be conducted,
- gathering more audit evidence from substantive procedures,
- greater number of locations shall be included in the audit.

Any material misstatement revealed by the auditor is an indicator of the weakness in the internal control system. The auditor may decide to:

- perform only substantive analytical procedures as they are sufficient to reduce audit risk to the required level,
- conduct test of details only,
- use a combination of substantive analytical procedures and test of details.

As the assessment of the risk of material misstatement considers the characteristics and reliability of the internal control system, the extent of the substantive procedures should be increased if internal control turns to be inefficient.

However, it should be highlighted that the auditor's risk assessment is a matter of professional judgement, so might not take into consideration all risks of material misstatement and there are inherent limitations to internal control, i.e. management can override controls.

3 Literature Review

Both the function of audit and the required audit procedures (analytical and substantive) went through significant changes as a consequence of more intensive ERP system application among businesses. The research conducted by Wright and Wright (2002) [18] evidenced the fact that the application of ERPs significantly increases the control risk. They also stated that many of the risks come from inadequate training of personnel. However, efficient internal control procedures can outweigh the risk arising from the application. The companies must manage the control procedures properly as it costs approximately 50 to 100 times more to add functionality or to correct an error post-implementation that it would have cost to provide the proper functionality during the implementation (Goldberg and Godwin 2003) [6].

Bae and Aschroft (2004) [2] stated in their article that external auditors shall focus on two issues, on control activities and on information and communication, out of several components of an internal control system. Control activities are procedures to protect the company's assets and prevent the manipulation of accounting records. Information and communication are the timely identification, collection, processing and reporting of relevant data in a useful format, such that employees can effectively meet their responsibilities. It is essential for an external auditor to understand and document how the ERP system collects and processes data and what are the controls implemented in relation to the ERP system.

The research conducted by Messier et al. (2004) [14], surveying the six biggest public accounting firms in Norway, investigated the impact of IT on the audit procedures performed by external auditors. The research also examined whether the origins of misstatements revealed by the audit are different for computerized and non-computerized business processes. They found that control procedures were missing more often in computerized rather than non-computerized business processes and there is an increase in the cause of misstatements resulting from missing and poorly designed controls and audit test. They also found that as IT emerged in business, a deterioration of the control environment and excess workload of accounting staff could be observed. The authors identified that the main reason auditors could not rely on the internal control was their belief that substantive testing was more effective.

Some earlier researches indicated (e.g. Hunton et al., 2004 [7]) that financial auditors recognize the risk associated with the ERP systems differently than IT auditors. Only certified public accountants were included in the research and the survey found that financial auditors were less concerned then IT auditors with the increased risk of the ERP implementation (e.g. business continuity, database security, application security). Financial auditors had a higher belief in their capabilities to evaluate risk in both computerized and non-computerized information systems. Financial auditors need the expertise of IT auditors and a strong cooperation between them is required. A study conducted by Brazel and

Agoglia in 2007 [3] showed that auditors having a higher information system expertise assessed higher control risk in the case of new information system (e.g. ERP) implementation than those not having previous IT experience and when internal control and computer assurance specialist competence was low, financial auditors planned more extensive substantive testing. As we evidenced above the relevant standard on auditing (ISA 315) requires the financial auditors to change their audit procedures and strategies in response to changes in the audit clients' information systems. However, some researches indicated (e.g. POB 2000 [16]) that the level of and the change in control risk sometimes are not reflected in the audit procedures performed by financial auditors.

As the consequence of using IT applications and ERP systems in businesses, the auditors were forced to cope with the challenges of providing audit in IT environment. Many professional bodies (IFAC – International Federation of Accountants, ISACA – Information System Audit and Control Association, AICPA – American Institution of Certified Public Accountants) have issued standards in this area. The survey of Yang and Guan in 2004 [19] examines the importance and advantages of using these standards in financial statement audits and emphasizes the importance of having a thorough understanding of these guidelines, standards by the auditors. Vendrzyk and Bagranoff in 2003 [17] investigated the impact of information system audit on the work of financial auditors. They found that in the last couple of decades the role of IT audit has shifted from a support tool towards an important pillar of financial audit. They also revealed that financial auditors found the test of general and application controls very important and the weaknesses of these controls have an impact on the scope of the audit procedures performed by financial auditors.

Based on reviewing all relevant literature Kanellou and Spathis 2011 [11] stated that ERP systems exert a significant impact on financial audit and internal audit. According to Kuhn and Sutton 2010 [12] in ERP environment errors might be undetected if there are no sufficient audit procedures performed, so internal control procedures shall be improved. Several risks appear and the most significant ones are related to information integrity, transaction errors, transparency of data and fraud.

4 Master Data Management

One of the first steps of keeping the system data validation is to secure the integrity and consistency of the Master Data. If Master Data records can be overridden, like the legal entity, this could lead to a serious problem. The area of the Master Data has to be first identified, and rules must be declared on how the change process will look like in this area. The area which will be called Master Data can be described on its way by interacting with other data areas. In ERP systems, the generally called Master Data is usually involved in each transaction

[5] [13]. For instance a customer can buy a product; a vendor can sell an accessory. Between the master data and the transactional data, these relationships can be examined. These are the main areas, which can be covered by this definition:

- Vendor and customer core data
- Global Address Book
- General Ledger
- Inventory
- Fixed Assets
- Open Financial Transactions (e.g. open purchase order, open sales orders etc.)
- Warehousing and transportation data
- Production data

There is another way of defining Master Data by its life cycle. These functions describe the following operations: create, read, update, delete, search, generally called SCRUD. When we define the Master Data this way, it will slightly change from company to company. It is a common experience that Master Data generally tends to be more volatile than transactional data, which means that it is important to keep the validity. The key usage of Master Data is reusability; we want to use the valid data as a basic of the transactions entered in the system. ERP's role is becoming more and more complex and the need is common for storing the Master Data only in one place and reuse it via a common channel. Proper Master Data Management could be vital (Figure 2), for instance a typing mistake in an invoice ship-to or bill-to address may cause loss of money. But we also mention the possibility of a mistyped price in the item master, an incorrect account number in account master – these actions can lead to even fraud-like actions. So maintaining the Master Data, and keeping the validity and consistency is very important to avoid these kind of issues when operating an ERP system.

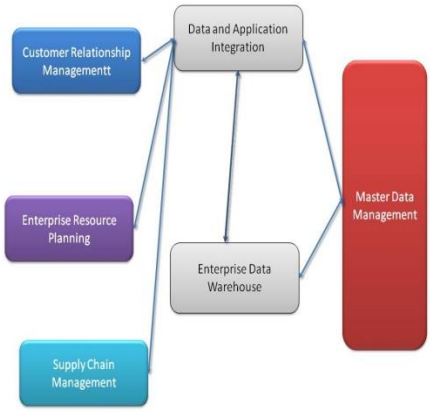

Figure 2
Data flow in the area of Master Data Management

Suppose that the current status of the Master Data does not contain any error. In this case, we should secure, that only one used entity exists, and no one uses local copies from cache, etc. An older and not up-to-date version of Master Data could cause exactly the same issues as mentioned in the previous section.

There are many companies, which are growing through mergers and/or acquisitions. Each time they acquire a company, the following problem occurs: the acquired company has its own Master Data and transactional data. This fact can lead to issues at merging: the structure of the data is different, sometimes came from different ERP, and there are possible duplicates. When the company acquired comes from a corresponding area of business, which is a possible situation, they likely to have the same customers, vendors. Transactional data have to be checked one by one for all of these vendors and customers. Items, attributes and inventory Master Data could be even harder to reconcile, when the corresponding parts were supplied by the same vendor, but probably with different item and vendor identifiers. Handling these kind of problems can be a part of the company's change management process (Figure 3).

Common data cleansing issue is to consolidate the different versions of the same data element. Let's get an example, the same vendor, who can have several business names, site addresses, phone and fax numbers. The name of the business responsible can be written as Mátyás Gábor, Gábor Mátyás, Gabor Matyas, Matyas Gabor, and in a lot of other versions. The data cleansing in this case needs a lot of manual handwork, because normal database data update queries cannot resolve this issue correctly [15].

Figure 3
Change management structure

At this stage it is important to estimate the amount of fully or partly invalid data. There are only limited tools for this estimation, only fot the syntax issues. Right now the exact estimation needs a lot of handwork beacuse of the hardnesses in semantic comparison automatization.

There are a lot of advantages, when a company has a clean, up-to-date and valid Master Data:

- can improve customer satisfaction,
- could save time and money in business operations,
- could reduce the danger of loss of revenue,
- could reduce the possibility of legal issues when preparing financial statements,
- reduces the time need of the database maintenance,
- minimizes the possible impact of having a corrupt database.

It is clear about these reasons, that having a real consistent and valid set of Master Data is vital for every ERP systems. All the policies, processes and systems, which are needed to achieve this is known as Master Data Management.

If Master Data Management is well defined, we should note, that it is just partly a technological problem, but the most difficult things to solve in this area are related to business processes and internal data flows.

Standardizing the data is often the most difficult part of making the right Master Data. On the technical side, at first the data structure has to be normalized to 4^{th} normal form. After normalization the missing values have to be inserted, for instance the default values and the initial setups. Often there is a next step when standardizing the values, e.g. convert all dimensions to metric, all prices to a common currency. In this case at multinational companies there is a need to have a solution for cross-converting.

The future research direction will focus on the validation of Master Data. What kind of algorythms can be used to automatize the validation process, and how can the human factor be minimized? Future research efforts are needed on how can be determined the amount of invalid data, how can it be estimated?

5 Consistency Check, a Proposed Methodology to Reduce Control Risk

Consistency Check is one of the strongest tools in Microsoft Dynamics AX to secure the validity and consistency of the transactional data. Technically it is a batch processing tool, which validates every transactional data in the system, and checks the connections between the other transactions and Master Data as well.

The running time of this tool can be extremely long, depending on the number of the transactions in the system.

Tables in Dynamics AX can be divided into three categories: 1) master data tables like Customers, Ledger Accounts, Vendors, etc.; 2) transaction headers like Sales Orders, Purchase Orders and 3) transaction details like Sales Lines, PO Lines, etc. When a transaction is entered into Dynamics AX, the necessary indexes and keys are updated for connecting Sales Orders and Lines.

Sometime these records can be abandoned, which means, that the parent record was deleted while the child records still exist. These are called orphan records[2], because the transaction still exists, but either the parent or the child does not exist anymore.

If we have numerous orphan records, it can slow down the performance. To avoid these situations, AX2012 has a tool, which is called consistency check. The basic idea behind this tool is to go through the whole database and scan for orphan records. Keeping the transactional data up-to-date is vital for every ERP system, no matter what was the scenario because these records remained orphaned.

The ConsistecyCheck framework is the core of the Dynamics AX data migration process. If we want to use it as a whole integrity check for the database, more tables and rules can be inserted into the validation process. These modifications should be derived from the SysConsistencyCheck base class, and should make the following methods: executionorder(), run(), description(), helptext() (Figure 4). All the derived classes should overwrite these methods to specify the related tables and methods. The kernelCheckTable and kernelCheckRecords methods check the relation between these tables. The modifications are essential, because the standard consistency check which comes out of the box with dynamics AX does not contain the necessary areas for a specific implementation.

These customizations enable for example an Independent Solution Provider (ISV) to include their data area in the consistency and integrity check. This also prevents users from false positive checks.

There are standard tools for maintaining transaction integrity in Dynamics AX, like ttsLevel (SQL transaction level) checking and forUpdate checks within data manipulation codes. Although these are low level tools, we should mention them, as the right usage of them makes the consistency check cleaner on the technical side. If we check the functionality of forUpdate, we can see that it ensures that a record can be deleted or updated only if it was first selected for update.

[2] Orphan records are records of data that have no longer connection to other data.

```
Query                          query;
QueryBuildDataSource           qbds;
QueryRun                       queryRun;

// LedgerTable
this.kernelCheckTable(tableNum(LedgerTable));

// LedgerJournalTable
query   = new Query();
qbds    = query.addDataSource(tablenum(LedgerJournalTable));
qbds.addRange(fieldNum(LedgerJournalTable,posted)).value(enum2
queryRun  = new QueryRun(query);
this.kernelCheckRecords(queryRun);

// LedgerTableAlterntive
this.kernelCheckTable(tableNum(LedgerTableAlternative));

// LedgerTableAlternativeTrans
this.kernelCheckTable(tableNum(LedgerTableAlternativeTrans));
```

Figure 4
LedgerConsistencyCheck.run() method

The ttsLevel check works similarly, ensures that a record can be updated or deleted only in the same transaction scope as it was selected for update. The transaction scope is bordered by the ttsBegin and ttsCommit. The first marks the beginning of the scope, and guarantees that all updates are consistent which are performed until the transaction ends. The second marks the successful end of a transaction, and commits all the changes. If there are any circumstances which deny the transaction to be consistent, the ttsAbort can discard all the changes and rolls back the database in the previous state. Maintaining referential integrity is a vital point for any ERP applications. In Dynamics AX 2012, we can model table relations with rich metadata content and express referential integrity. Dynamics AX 2012 does not represent table relations as SQL foreign table key constraints, because of the huge performance overhead in the SQL server. The application code can also violate referential integrity. In this case, referential integrity maintenance means that the data manipulating operations have to be performed in correct order. This is most vital when records are deleted and created. The parent record must be created first, before the child records can get the correct foreign key. And the following is also true; the child records must be deleted first before the parent records. Ensuring this from code can be hardly maintained, especially with the strongly normalized data structure of Dynamics AX 2012. That is the reason, why Dynamics AX 2012 provides a new programming concept, which is called Unit Of Work. This is basically a set of data manipulation methods, which are performed on the related data. The application code establishes the connection within the data in memory, modifies them, registers the modifications and then requests the Unit Of Work to perform the necessary operations in the correct sequence. For example, if the RecId of the header comes as a foreign key to the lines, we cannot insert lines first because we need the RecId of the header record.

Also we cannot insert the header first, if we need SUM from the lines. If we use the Unit Of Work class, all these are handled by the AX kernel itself.

Troubleshooting these data consistency issues during upgrading to a newer version of Dynamics AX or migrating to / from a different ERP system is vital part of the Data Migration process. In the first test after the migration, it is natural to have consistency errors both during and after the process. There are some guidelines to follow which can help quickly to find the root cause of the issues. At first, one has to check the generate mapping form to see if there are any mapping errors. After this it has to be determined if the issue is on the source or the target side of the process. Data Consistency Check can help this decision. There are two options:

- The data looks corrupt: which means that the issue occurred in the source side. We have to determine the source table and the transformations made on this table. If the table is part of a transformation, one has to be sure which tables were populated and with what kind of outcomes?
- The data is ok: the issue is on the target side. If the data were copied correctly during the bulk copying, the script, which was used during the data migration, has to be determined. From this point, we can debug the script to determine the critical operation. It is also useful to check the dependencies of the script.

After this decision, the data migration process has to be corrected, rerun, and the consistency should be checked again. After the check, we can quickly determine if there are any modifications needed for the process.

The most important usage of the Data Consistency Check is carried out after a successful import of data, thus after the Data Migration. It assures that data are consistent through different relations and cross references. It prevents the system from becoming corrupted, and can warn for the underlying problems under the hood. If we cannot pay enough attention to these issues, they can seriously jeopardize the stability of the system.

There are some challenges with customizing complex business rules in integrity checks but the need for avoiding the manual checks is always stronger. Using Consistency Check with Data Migration is an essential step for a successful migration (Figure 5).

This tool provides a wide range of information, which needs to be evaluated by the data steward or master data track lead, because of the complexity of the field.

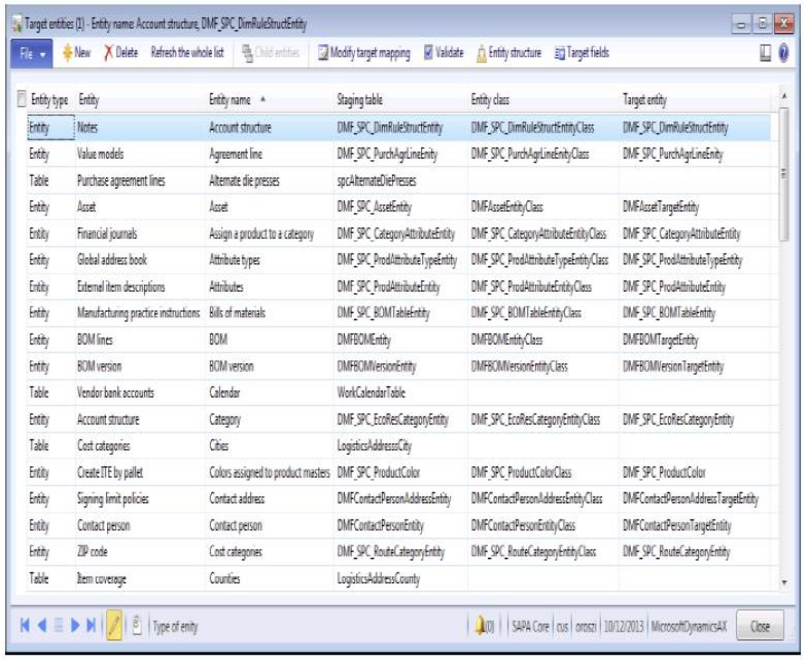

Figure 5
Data Migration Framework entities

Conclusion

The aim of the Data Consistency Check is similar in every ERP system. With this tool, the system can guarantee that the master data is valid in all respects. If we develop the necessary parts for the customized code, it will also be true for those parts as well. The outcome of this function is a report, which contains all the table records with issues. If the report is empty, than it is a theoretically perfect database. Based on practical experience usually it is not the case, so after a migration cycle there are always consistency issues arising, so data inaccuracies and corruptions can be fixed immediately before transactional records start to use the corrupt data.

The application of Data Consistency Check is optional but not mandatory after data migration. Data migration carries the risk of data corruption and inconsistencies in master data and transactional data. In the absence of effective control procedures the reliability of the data from which the amounts in the statements are calculated is highly questionable. As a consequence, auditors should perform more extensive substantive procedures to check master data and transactional data accuracy in order to detect material misstatements at financial statement level. As many researches proved that it is 50 to 100 times more expensive to correct mistakes than to prevent them, the usage of control

procedures becomes more important. If effective general and application IT controls are in place, after these controls having been tested, financial auditors can rely on them. So the application and proper documentation of Data Consistency Check and other similar control procedures would decrease the control risk and as a consequence would result in:

- lower level of audit risk,
- less extensive substantive procedures,
- lower sample sizes,
- shorter audit procedure.

We can also conclude that the current methodology of the consistency check in Dynamics AX is useful for providing necessary information about the validity of transactional data, but it needs to have a broader validity area to be useful enough. We need to make a detailed description of the validity of a business rule, not just white and black. When it comes to enhancing the possibilities of this tool, we need to focus on advanced machine learning and intelligence techniques, e.g. fuzzy logic [4] [1]. Master Data management needs extensive standardization as it is heavily dependent on the methodology of the project.

References

[1] Anil Kumar Gupta, "Quality Assurance for Dynamics AX-based ERP Solutions: Verifying Dynamics AX customization to the Microsoft IBI Standards Studies". Packt Publishing, 2002, ISBN-10: 1847192912

[2] Bae, N. and Aschroft P.: "Implementation of ERP Systems: Accounting and Auditing Implications", Information System Control Journal, 2004, Vol. 5, pp. 43-8

[3] Brazel, J. F. and Agoglia, C. P.: "An Examination of Auditor Planning Judgements in a Complex Accounting Information System Environment", Contemporatry Accounting Research, 2007, Vol. 24, No. 4, pp. 1059-83

[4] Fodor, J., Ősz, R., "Possible Applications of Fuzzy Methodology in the Educational Process", IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI), DOI: 10.1109/SAMI.2013.6480992, ISBN: 978-1-4673-5927-6, pp. 37-40, 2013

[5] Forrester, Jay Wright, "Industrial Dynamics". Waltham, MA: Pegasus Communications, 1961

[6] Goldberg, S. and Godwin, J. H.: "Operational Reviews on Auditing ERP", The Journal of Corporate Accounting and Finance, 2003, Vol. 14, No. 4, pp. 63-5

[7] Hunton, J. E., Wright, A. M. and Wright, S.: "Are Financial Auditors Overconfident in Their Ability to Assess Risk Associated with Enterprise

Resource Planning System?", Journal of Information Systems, 2004, Vol. 18, No. 2, pp. 7-28

[8] International Standard on Auditing 200: Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing, IFAC. http://www.ifac.org/sites/default/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf

[9] International Standard on Auditing 315: Identifying and Assessing the Risk of Material Misstatement through Understanding the Entity and Its Environment, IFAC. http://www.ifac.org/sites/default/files/downloads/a017-2010-iaasb-handbook-isa-315.pdf

[10] International Standard on Auditing 330: The Auditor's Response to Assessed Risks, IFAC. http://www.ifac.org/sites/default/files/downloads/a019-2010-iaasb-handbook-isa-330.pdf

[11] Kanellou, A. and Spathis, C.: "Auditing in Enterprise System Environment: a Synthesis", 2011, Journal of Enterprise Information Management, Vol. 24, No. 6, pp. 494-519

[12] Kuhn, J. R. and Sutton, S. G.: "Continuous Auditing in ERP System Environments: the Current State and Future Directions", 2010, Journal of Information Systems, Vol. 24, No. 1, pp. 99-112

[13] Maedche, Alexander, "An ERP-Centric Master Data Management Approach" (2010) AMCIS 2010 Proceedings. Paper 384. http://aisel.aisnet.org/amcis2010/384

[14] Messier W. F., Eilifsen, A. and Austen, L. A.:"Auditor Detected Misstatements and the Effect of Information Technology", International Jounal on Auditing, 2004, Vol. 8, pp. 223-35

[15] Osz, Rita; Fodor, Janos: "Possible Connecting Areas of Education and Intelligent Systems", 2013 IEEE 9th International Conference on Computational Cybernetics (ICCC), Digital Object Identifier: 10.1109/ICCCyb.2013.6617560, Print ISBN:978-1-4799-0060-2, pp. 51-56

[16] Public Oversight Board (POB): Panel on Audit Effectiveness: Report and recommendations, 2000, AICPA, Stamford, CT

[17] Vendrzyk, V. P. and Bagranoff, N. A.: "The Evolving Role of IS Audit: a Field Study Comparing the Perceptions of IS and Financial Auditors." 2003, Advances in Accounting, Vol. 20, pp. 141-63

[18] Wright, S. and Wright, A. M.: "Information System Assurance for Enterprise Resource Planning Systems: Unique Risk Considerations", Journal of Information Systems, 2002, Vol. 16, pp. 99-113

[19] Yang, D. C. and Guan, L.: "The Evolution of IT Auditing and Internal Control Standards in Financial Statement Audit. The Case of the United States", 2004, Managerial Auditing Journal, Vol. 19, No. 4, pp. 544-55