IDENTITY AND ACCESS MANAGEMENT- A RISK-BASED APPROACH

Ion-Petru POPESCU[1]
Cătălin Alexandru BARBU[2]
Mădălina Ecaterina POPESCU[3]

ABSTRACT
In this paper we stress out the importance of identity and access management (IAM) when dealing with main business processes. Being able to detect unusual access and outliers forms is absolutely necessary for a manager to be able to address many of the challenges in each of the IAM's major areas. We draw on the fact that identity management implies data analysis, reporting and ongoing monitoring, modelling and efficient decision making processes in order to emphasize the importance of IAM and the necessity for specialized IT solutions. The problem itself is very complicated because the lack of access leads to direct losses of productivity along with other indirect losses.

KEYWORDS: *identity management, access management, risk-based approach, maintenance, reporting.*

JEL CLASSIFICATION: *G30, D23.*

1. INTRODUCTION

In this paper we stress out the importance of identity and access management (IAM) when dealing with main business processes. We draw on the fact that identity management implies data analysis, reporting and ongoing monitoring, modelling and efficient decision making processes in order to emphasize the importance of IAM and the necessity for specialized IT solutions. The problem itself is very complicated because the lack of access leads to direct losses of productivity along with other indirect losses. On the market there are already various specialized solutions that streamline the process of access management and its maintenance.
The literature review in this field, both at national level (Andreica et al. 2014, 2011; 2007) and at international level (Sharman et al., 2012; Osmanoglu, 2014; Scheidel, 2010; Bertino, 2011; Modi, 2011; Anderson et al., 2011; Tipton, 2012), already emphasize on the stringency for systemizing procedures, planning and forecasting models within organizations.

2. A RISK-BASED APPROACH

The levels of information included in Identity and Access Management (IAM) systems and integrated infrastructure can be very extensive: life cycle of user identities, any number of security policies and the user accounts themselves, the entitlements, the roles, and to activities of users and the workflow of data.

[1] The Bucharest University of Economic Studies, Romania, ion.petru.popescu@gmail.com
[2] The National Bank of Romania, Romania, catalin.barbu.alexandru@gmail.com
[3] The Bucharest University of Economic Studies, Romania, madalina.andreica@gmail.com

The downside is, of course the fact that this information is not easily accessible split between systems and department of financial institutions and different data bases. Moreover, the data size itself, can multiply due to:

- **Increased number of identities (people)**: Especially banks can have sometimes millions of identities (active and inactive) due to legal requirements to retain historical data for reporting activities.
- **Applications**: for most of the financial institutions the number of software applications ca be impressive ranging from a few tens of applications to thousands.
- **Different platforms, devices and technologies**: Even if the operating systems are somewhat restricted (Linux, Solaris, Windows, etc.), the number of distributions, versions, compatibilities and integration options can complicate the matter to an exponential degree.
- **Entitlements**: To have millions of entitlements in scope for an IAM solution especially in a bank is not so uncommon.
- **Profiling and Roles**: There are organizations, where one can have thousands of access profiles and roles that need to be maintained at all time. Maintenance is perhaps one of the most difficult issues that an large financial institution can face.
- **User activity data**: With the mobile and internet banking and the ever larger banks, investment funds and insurance companies, the IAM systems can register decision events (that are logged in daily) in the order of millions in regards to authentication and authorization activities. The event correlation systems and repositories are a typical reporting and maintenance issues that need to be handled with very complicated storage algorithms.
- **The transaction data generated by the applications themselves**: Unfortunately, the activities registered by applications themselves, in terms of sheer volume, are actually multiplications of the user activities themselves because of the fact that any user transaction (for example a money transfer from the internet banking application) is processed by several application, data bases and services.

The challenge is however how to solve all these issues in an organized and structured manner. The answer is, of course through a risk based approach, as it is systematically presented in Figure 1.

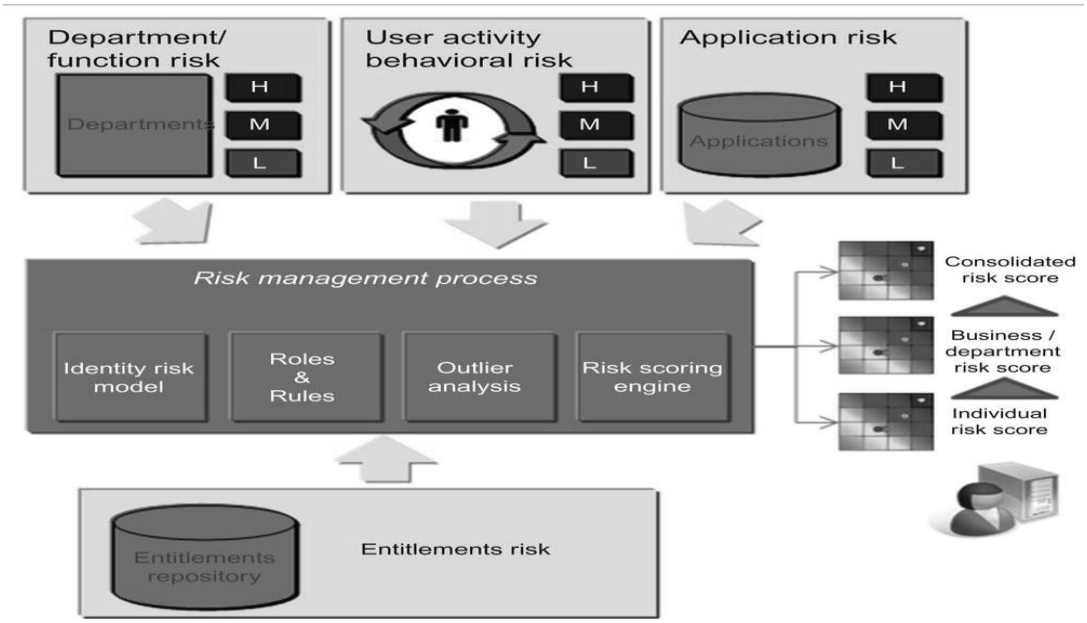

Figure 1. A risk-based approach
Source: authors own representation

With such a holistic view, in concordance with data analysis and optimization engines for the IAM risk portfolio, the improvements in decision-making/allocation of organization's controls over high risk and high impact business areas can result in excellent, long time results. This capability is also known, in the finance industry as **Identity Analytics and Intelligence** (IAI). With the data obtained from the IAM analysis engines, the banks are then able to take informed IAM decisions and concentrate their resources on constantly improving IAM controls around the key financial and operational processes.

Targeted IAI activities can offer a strategic advantages. The recommended approach for the IAI comes with these four steps:

1. Creation of an information framework facilitating fast decision-making. This framework will include a model of data and services based on key IAM data components:
    - Profiling data
    - Entitling data
    - Rules and data (policies, official practices, processes, etc.)
    - Asset profile data (terminals, software, platforms, services, etc)
    - Activity data
2. Correlation and integration of data based on the defined framework
3. Mining data for identification of real value added
4. Exploiting and detecting new opportunities by using predictive analytics.

It is understood that a good IAI analyses will be dependent on the existence good data quality in the organization. Mismanagement of data, poor data maintenance and not having good quality controls will come with significant impact in both cost and risk implications to any financial institution. Before any implementation of IAI capabilities can take place, a set of measures is required for collating, cleaning and verifying al the significant data by:

- Incorporating of data management activities to the project plan
- Choosing the right practices and capabilities for data management
- Identification of the authoritative sources
- Insuring consistency over multiple authoritative sources (if it is the case)

To picture the criticality of a good analytics process in relation to IAM decision-making, let's take a simple example applied to a relatively common financial process. Have the simple task of giving access administration to new business application to the administrators. The administration process will require the application manager to know exactly how many of his people will be required to handle access management operations (like add, change and remove access and identities from that particular application). For that, the application manager will need data regarding access management events, like hiring, separation, and new customer, reactivated customer, imported customer. Then an analysis will follow, by summing all the new access support operations for each period or cycle, how many of the users lost access, how many transferred, percentages and promotions, and all other events that may have impacted the application's access. Then the amount of time required to make the changes will need to be divided by the two thousand hours from a normal working year so as to estimate the required number of people that can handle the identity changes requirements. So we can see that also identity management related activities will have an effect on companies' personnel schema and the need to plan for appropriate staffing needs with resources allocated to meet business requirements is imperious. With more sophisticated analysis engines, additional business requirements can be gathered for an improved risk management and important spending cuts.

Banks and other institution of the kind will also use identity and access related data for detection of attacks from within or outside the organization. Advanced data analysis capabilities can be used on examining access rights, identities, and transactions (including but not restricting financial ones) for the organization's most critical applications. Existing security tools will identify high-risk areas and entities for an active threat identification and risk mitigation. Identity and access management practices in the industry should therefore include:

- Peer grouping/outlier analysis
- The classical Role analysis
- System usage analysis/Account analysis
- Resource allocation verifications
- Risk and fraud detection mechanisms.

3. PEER GROUPING/OUTLIER ANALYSIS

As an example we will detail the first of the described practices - that is the peer grouping. This technique will identify deviation in IAM data. In classical statistics, an outlier procedure is defined as the examination of the data for unusual observations that are far beyond from the mass of data. In the particular IAM case, the data in question refers to identities and entitlements. All of the user entitlements that are too different in comparison with other more conform entitlements having a similar profile is referred to as an **OUTLIER**. Figure 2 is a general example that shows more (three) different groups of users:

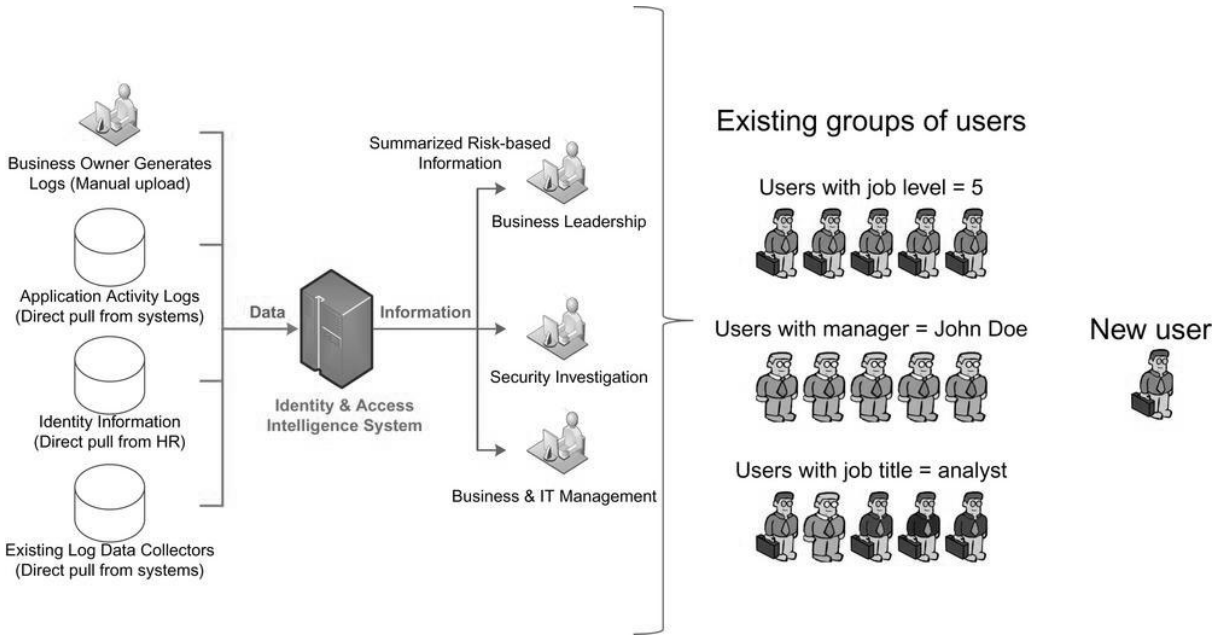

Figure 2. How an outlier analysis will detect a new user (as outlier)
Source: authors own representation

Different attributes will define different sets of user grouping, like, job title, job level or manager. With this representation, a new user is an analyst and he will need to be assigned to the appropriate user groups, so as to have the appropriate entitlements to do perform his specific job activities. Since the lowest denominating access level any one could have is **job level 5** he needs to be assigned to at least that group since it is not clear yet who will be his managers (due to the fact the he is a new resource). If, by any reason, the new users will need to have as manager **John Doe** he or she would become an outlier through the analysis.
Since there are several established methods for performing outlier analysis, each method will come with its fair share of complexity. Since the intention for this article is not to have a deep analysis involving mathematics and statistics, we will present only two methods using easy to relate and to follow examples.

3.1. The Sorting Method

By sorting one can group different groups of users having common attributes, with the tables below we will illustrate a sorting procedure. Figure 1.3 shows an entitlement table, which highlights individual users by their respective departments and job titles, end describes entitlements for each user. Of course the hard part is that these entitlements can be more than one.

User	Department	Job title	Entitlements
A	Finance	AP clerk	Create a PO Receive goods
B	Finance	AR clerk	Create a PO Issue invoice Adjust invoice Receive cash
C	Finance	Director of planning	Open a prior accounting period Approve a PO
D	Finance	VP of finance	Open a prior accounting period Post a PO
E	Operations	Operations analyst	Open a prior accounting period Approve a PO
F	Operations	Director of operations	Manage inventory Approve a PO

Figure 3. The different entitlements
Source: authors own representation

By sorting the data from the above figure (figure 3) by entitlement, we get to see some unusual patterns emerging (figure 4).

As one follows the details presented in figure 4, one can see that an **analyst** from the department of **Operations** has access to "*open a prior accounting period*" entitlement. As this is a *finance role* and could have a potential material impact in regards to the financial statements, an investigation and close monitoring is recommended (this is because a junior analyst should not usually have this entitlement).

Even if a sorting exercise can prove to be useful in highlighting and identifying the outliers, it is still a manual and arduous process. Scaling this up to the multitude of entitlement types (in the order of thousands in any big financial institution) and having a vast number of types of users (ranging from internal – employee type users – to all the customer specific web-service consumer types in a bank, sorting and analyzing the entitlements needs to be automated and sometimes with specific

statistical tools like SAS or R and if the data cannot be normalized, the exercise may prove unpractical and very time consuming.

Entitlement	Department	Job title	User
Create a PO	Finance	AP Clerk	A
	Finance	AR Clerk	B
Receive goods	Finance	AP Clerk	A
Issue invoice	Finance	AR clerk	B
Adjust invoice	Finance	AR clerk	B
Receive cash	Finance	AR clerk	B
Open a prior accounting	Finance	VP of finance	D
period	Finance	Director of planning	C
	Operations	Operations analyst	E
Approve a PO	Finance	Director of planning	C
	Operations	Director of operations	E
	Operations	Operations analyst	F
Post a PO	Finance	VP of finance	D
Manage inventory	Operations	Director of operations	F

Figure 4. Sorting by entitlement
Source: authors own representation

3.2. Regressions

In IAM data analysis, a very good, alternative method, that may come in handy for highlighting peer groups and outliers is the **logistic regression** which is actually a regression model where the dependent variable (DV) is a binary one that takes only values 0 and 1. By using this method an analyst can build a statistical model that will include data related to the entire user population of an organization to find out whether or not a specific person has the necessary and/or appropriate access. Having, at hand the data set described in the sorting example above, there is a possibility of building a logistic model for each and every entitlement, where the predictor variables are department and job title. A calculus is done in order to estimate a certain probability for each user and each entitlement. A comparison is then made between the actual value - which is binary (1/0) - and the question result, of a given entitlement. When having good probabilities that user should be associated with access, while having low probabilities should result, normally, in no access. Whenever a discord is located, the pairing of probabilities and entitlements will give the outliers. To automate the entitlement process, rules can be implanted for automatic removal or granting of access. The users in question can be "marked" for further investigation and monitoring. With the data above, prediction can be set for users to be a given certain entitlements based on the established patterns seen within the larger tendencies. These activities are done by risk analysts in financial institutions using spreadsheet software like Stata or some other analysis software.
In figure 5 one can see the probability of a particular entitlement to be given to the appropriate user including details on department and job title. There are, of course, some entitlements that appear not to fit, while others are, at least questionable. Figures 6 and 7 point out the concordant pairs as well as the discordant pairs.

Entitlement	Department	Job title	User	Probability
	Finance	AP Clerk	A	0.96
Create a PO	Finance	AR Clerk	B	0.97
Receive goods	Finance	AP Clerk	A	0.90
Issue invoice	Finance	AR clerk	B	0.92
Adjust invoice	Finance	AR clerk	B	0.93
Receive cash	Finance	ARclerk	B	0.91
	Finance	VP of finance	D	0.87
Open a prior	Finance	Director of planning	C	0.82
accounting period	Operations	Operations analyst	E	0.09
	Finance	Director of planning	C	0.75
	Operations	Director of operations	E	0.68
Approve a PO	Operations	Operations analyst	F	0.25
Post a PO	Finance	VP of finance	D	0.98
Manage inventory	Operations	Director of operations	F	0.89

Figure 5. Sorting by Entitlement including the probability scores from the logistic model
Source: authors own representation

Probability Threshold	User Actually Has Access	User Does Not Have Access
Probably user should have access > 0.75	• Concordant data (the probability actually matches the actual access)	• Discordant data (the probability indicates the user should have access but does not
Probability user should have access < 0.25	• Discordant data (the user has access, but the model says the user should not have access) • An example from the table above is user E's ability to open a prior accounting period.	• Concordant data (both the model and the real data agree the user should not have access

Figure 6. Concordant pairs/discordant pairs
Source: authors own representation

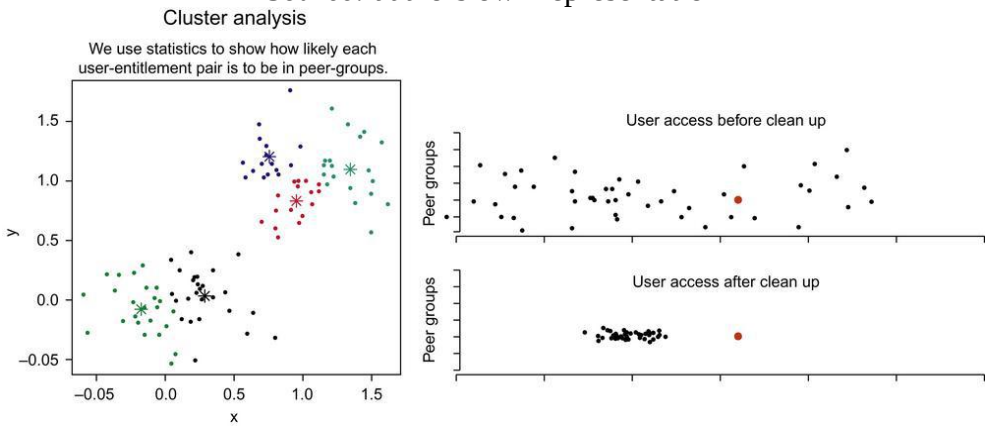

Figure 7. Cluster analysis by Peer group
Source: authors own representation

In the industry, a peer group and outlier analysis is done only when most of the entitlements are actually appropriate. Having outliers will show the failures in the provisioning process which, in turn will allow inappropriate access level for some users. For most companies, these failures are at least uncommon and not really systematic. However, an outlier analysis will not be useful if everyone has all or most of the entitlements or there systematic failures are present in the access granting process.

A very famous case of a very large insurance company, that is also present in Romania, has recently performed an outlier analysis and the results have revealed that everyone had access to critical systems of the company. To come to this conclusion, this company has actually done a rigorous role definition exercise before the outlier analysis itself so as to come with any meaningful results afterwards.

In practice, most established IAM products on the market (like Identity IQ and Oracle Identity Management) have analytical functions that can perform peer group and outlier analysis in an automated way. Peer group and outlier analysis should be always integrated with key IAM process areas such as requesting access and approving access, reviewing access and certification along with provisioning/deprovisioning so as to provide business value during key managerial decisions like designing workflows.

4. CONCLUSIONS

Being able to detect unusual access and outliers forms is absolutely necessary for a manager to be able to address many of the challenges in each of the IAM's major areas. Bad provisioning practices, for example, causes managers to have a limited understanding of the needed entitlement level for their subordinates (so as for the subordinates, in question, to meet business requirements) and over-assignation of entitlements occur. Therefore, the ability of an IAM team to provide a manager a risk-based report view showing the access requested is critical for the stakeholder of an application/service/department to understand the risks associated with the requested access.

Like so, the process of access review and certification, involving the review and approval of existing entitlements by business managers, usually becomes nothing more than a routine exercise that no one care about in management, unless information about outliers and associated risks is provided. This process of access review and certification is performed on a regular basis, especially in financial institutions, often quarterly. When considering the volume of hardware software and services involved the **maintenance** of the IAM systems becomes critical. Having an outlier or risk-based view, a bank can focus a manager's activity in spotting on the most questionable entitlements.

REFERENCES

Anderson, B. & Mutch, J. (2011). *Preventing Good People From Doing Bad Things: Implementing Least Privilege*, Dublin: Editura Apress.

Andreica, C., Andreica, M., Andreica, R., Miclăuş, I. & Ungureanu, M. (2007). Conclusions on Using the Statistical Methods in Forecasting the Structure Evolution of an Economic Indicator System, *Economic Computation and Economic Cybernetics Studies and Research*, Nr. 1-2.

Andreica, M., Popescu, M. E. & Micu, D. (2014). Proposal of a SMEs Forecast Management Support System, *Review of International Comparative Management*, Vol. 15(2), pp. 237 -243

Andreica M., Pârţachi I., Andreica C. & Andreica R. (2011). *Previziunea în afaceri*, Bucureşti: Editura Cibernetica MC.

Bertino, E. & Takahashi, K. (2011). *Identity Management: Concepts, Technologies, and Systems*, New York: Editura Artech House.

Modi, S. K. (2011). *Biometrics in Identity Management: Concepts to Applications*, New York: Editura Artech House.

Osmanoglu, E. (2014). *Identity and Access Management: Business Performance Through Connected Intelligence*, Istanbul: Editura Syngress Publishing.

Scheidel, J. (2010). *Designing an IAM Framework with Oracle Identity and Access Management Suite*, Vancouver: Editura Oracle Press.

Sharman, R. & Smith, S. D., Gupta M. (2012). *Digital Identity and Access Management: Technologies and Frameworks*, Chicago: Editura IGI Global.

Tipton, H. F.& Nozaki, M. K. (2012). *Information Security Management Handbook, Sixth Edition, Volume 5*, London: Editura Auerbach Publications.