State of the art

PERSPECTIVES

Basel III Compliance : The contribution of identity and access management

This white paper describes how an identity and access management solution can help master operational risks.

EVIDIAN

A Bull Group Company

Managing your Operational Risks Related to User Accesses

In banks more than in most other industries, the potential for financial damage due to improper access to IT resources is very high.

One way to counter these risks is identity and access management (IAM), a set of solutions that allows fine-grained administration of user access rights. IT access is managed in a rational way, which reduces exposure to losses.

But to take full advantage of identity and access management, a bank can integrate it into its operational risk management system, making it more effective.

The Basel II capital accord introduced the inclusion of operational risk into the evaluation of the minimum capital requirements for banks. It defined operational risk as "*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*". In 2010-2011, the Basel III accord was introduced to strengthen capital requirements in the wake of the 2008 financial crisis.

Among the risk evaluation methods proposed by the accord, the advanced measurement approaches (AMA) authorize banks to evaluate their operational risks themselves.[1]

To do this, a bank sets up an operational risk management system and an organization responsible for managing it. The internal operational risk management system relies in particular on the following data:

- data on the losses actually experienced (loss data).
- data on the operational incidents liable to generate costs.

Identity and access management can be a very effective tool for operational risk management teams. It centralizes information on accesses for the entire bank in a single interface, and makes it easy to quickly enforce controls.

For a bank, the Basel III accord can be an opportunity to significantly improve identity and access management. Such an overhaul can generate important return on investment in terms of productivity among users and IT personnel. It can also allow you to easily deploy procedures that are critical in a banking environment, such as 'de-provisioning', segregation of duties and role-based management.

[1] See the Bank for International Settlements' June 2011 document « *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches* » http://www.bis.org/publ/bcbs196.pdf

IT Access: a Critical Point

A good operational risk management methodology is essential when implementing an advanced measurement approach (AMA). It is also a pre-requisite when implementing a standardized approach.

Many of the operational risks defined by the Basel accords **concern access to computer data by physical persons**. This makes sense, as bank assets are essentially dematerialized and financial streams are digitized.

Evaluating these operational risks presents specific challenges, in particular:

Different types of media

Financial data reside in many different systems and types of applications. These can be accessed either by conventional means or via the Internet.

Diversity of access authorization methods

Although most native authorization methods produce information on the accesses, consolidation and auditing are problematical owing to a lack of standard format.

Technical complexity

The know-how of an operational risk management team is often organizational. That team should not have to focus on advanced IT technical aspects.

Of the seven risk types defined by the Basel capital accord, identity and access management primarily concerns four of them:

Type of risk	Description (*)	Sub-category primarily concerned by identity and access management
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party	✓ Unauthorized activity ✓ Theft and fraud
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	✓ Theft and fraud ✓ Systems security

(*) Source: Annex 9 of the Basel II Accords – "Detailed loss event type classification".

Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product	✓ Conformity, information distribution and fiduciary duty.
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	✓ Input, execution and monitoring of transactions ✓ Customer account

Providing an Identity and Access Management Solution

When setting up an AMA, an identity and access management solution can offer significant advantages:

- **Immediate reduction** in operational risks, by reducing the possibility of computer data access loopholes.
- **Information accessible** and auditable on (a) authorized or illicit accesses and (b) allocation of access rights.
  This information makes it easier to measure the operational risk by the entity concerned and can be directly used by the reporting tools already in place.
- Possibility of **immediate reaction** to detection of a source of operational risk.
  These tools in fact have a centralized console for managing all the access rights. After diagnosing a risk indicator, the detected loophole (over-generous access rights policy, rights allocation error, etc.) can thus immediately be closed.
- **Simplification** of technical concepts. In an identity and access management solution, the technical IT aspects are masked to enable the users to concentrate on the allocation of access rights. The process for allocating these rights is thus simplified and can be audited.

The present document tackles several of these aspects, and gives the optimum characteristics of an identity and access management environment.

The table below summarizes, in a non-limitative way, the possible role that some modules of an identity and access management solution can play in operational risk management. These modules can be deployed in a progressive way.

Type of risks	Sub-category primarily concerned by identity and access management	Identity management	Secure SSO	User provisioning
Internal fraud	Theft and fraud	✓	✓	
	Unauthorized activity	✓	✓	
External fraud	Theft and fraud	✓	✓	
	Systems security	✓	✓	✓
Clients, Products & Business Practices	Conformity, information distribution and fiduciary duty	✓		✓
Execution, Delivery & Process Management	Input, execution and monitoring of transactions	✓		✓
	Customer account management	✓		✓

The diversity of Access Methods is a Source of Operational Risk

When seen from the two-fold viewpoint of the users and the administrators, the absence of a unified method for managing identities and accesses is a source of operational risks.

Operational Risks Linked to the Users

These risks are primarily linked to the large number of passwords an employee has to use in his day-to-day work. For example:

- If a source can only be accessed by a password, the user will tend not to refer to it. This is a source of the "process management" type operational risk: poor monitoring of reference data, accounting error or assignment of an entity, etc.
- If the passwords are too many, the user will tend to write them down on an easily accessible medium (Post-It™ for example). This facilitates internal fraud.
- A frequent alternative is passwords common to a whole team, enabling an employee to access client data that do not concern him. This is a potential source of "Client, products and commercial practices" type risk.

Some solutions propose that the user have a single password for all the resources he or she accesses. This is an evident source of "internal fraud" type operational risks, as someone need only break the security on a single system (old application for instance) to gain fraudulent access to all the resources with the password obtained in this way. The policy for choosing the passwords used may also not be compatible between the applications in the bank.

How to reduce these risks?

Those risks can be significantly reduced by use of a secure single sign-on (SSO) solution such as the one included in Evidian IAM Suite.

With a secure SSO solution, the users need only remember a single identifier/password pair, with all the others being entered invisibly at each access to an application. Biometric and/or smart card-based authentication methods can reinforce a single sign-on solution.

For a given application, Evidian IAM Suite hides the real passwords from the user. These passwords can therefore all be different and non-intuitive; so breaking the security of an application does not compromise the other resources. Moreover, Evidian IAM Suite enables the bank to define and deploy a specific password policy.

Operational Risks Linked to Administration of Access Rights

It is increasingly difficult to manage allocation of access rights satisfactorily. Although the numbers of administrators are stable or falling, as a result of cost reductions, their work is increasingly complex:

- Access rights concern a wide variety of resources such as web sites, mainframe applications and so on,
- At the same time, personnel movements (turnover, reassignment, bank mergers, etc.) imply regular, constant updating.
- This creates operational risks, for example:
- Access rights allocation is often delegated to the systems engineers, who consider this to be a secondary task. This manual step is thus sometimes delayed or subject to operator errors. This is a source of "process management" type operational risks.
- When an employee leaves the bank, his or her rights are often not cancelled, the problem being that it is hard to make a complete inventory of all the authorizations granted to him during the course of his or her career. He or she will therefore still have access to systems even though no longer employed. This is a source of external fraud.
- Finally, having too many passwords means that they are often lost or forgotten, generating calls to the help-desk. Faced with the volume of these calls (up to 30% according to Gartner Inc.) a large number of people have to be given the powers to change a password. This can be a source of internal fraud risk.

How to reduce these risks?

These risks can be significantly reduced by using a "provisioning" solution with identity management. Granting (and revoking) access rights is easily done from a central console, without any manual intervention on the resources themselves. This allocation of rights is done on the basis of organizational criteria by trustworthy persons and with no technical know-how required. All these administrative operations must of course be logged so that they can be audited.

Ideally, it must be possible to integrate this solution natively with the company directories, so as to reduce the number of manual operations, all of which are potential sources of error. User data will then be updated by the Human Resources department rather than by the access security managers.

Identity and Access Management Must be Technology-independent

The rapid development of information systems shows that an identity and access management system must be extremely adaptable.

- Permanent evolution of technologies (J2EE, certificates, etc.)
- Need to integrate a new information system, in the event of a bank merger
- Development of new applications, purchase of software licenses

The means of managing identities and accesses must therefore be independent of the technologies and applications. If not, the proliferation of access rights management consoles makes the process very hard to define, implement and audit.

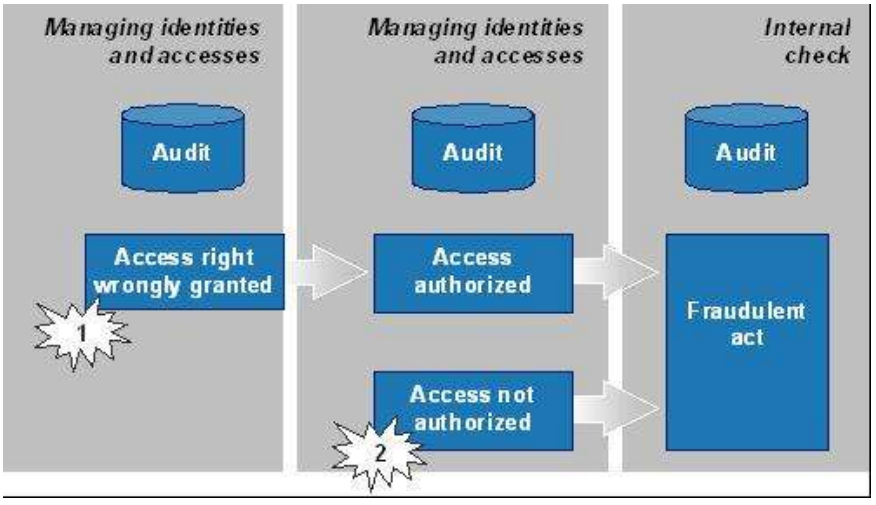
The Separation of Roles in the Access Rights Allocation Process

In order to be easily auditable, the access rights allocation process must be clearly defined and comprise as few manual operations as possible.

Evidian IAM Suite relies on the user and organization definitions already in place in the bank. It in fact uses the company's LDAP directories directly, without requiring any import. The roles are thus clearly defined and the information auditable:

Role	Who?	Where to audit?
Definition of the organization, creation, modification and cancellation of the users	Existing organization. Generally the human resources department	LDAP directories
Allocation of rights to users thus defined	Management of user rights; centralized organization with possible delegation	Evidian IAM Suite repository
Definition of technical resources for which the access rights are to be managed	IT department	Evidian IAM Suite repository
Generation of audit data on the accesses and administration operations	Done automatically by Evidian IAM Suite	Evidian IAM Suite audit base

The rights allocation processes (request, qualification, approval, etc.) can thus be easily defined and audited, even if highly detailed and complex.



In this way, the information needed for the audit, such as an inquiry into the origin of an operational incident, is clearly localized.

In the above diagram, we can see that a fraudulent act can be the result either of an unauthorized access (password theft for example), or incorrect allocation of access rights (intentionally or otherwise).

The identity and access management audit data must thus cover both aspects:

1. audit of rights allocations and
2. audit of accesses

Return on Investment

An Opportunity for Cost Reduction

Installation of an advanced measurement approach (AMA) is generally decided on at general management level for business reasons:

- Reduction and control of capital
- Reduction of insurance costs,
- Demonstration of good risk control to customers and investors.

AMA is necessarily costly in terms of organization and processes, but identity and access management can alleviate some of that cost.

First, identity and access management can reduce the number of loss-generating operational incidents. Through its AMA operational risk measurement processes, the bank can measure that impact.

Second, identity and access management allows banks to improve staff productivity. Indeed, when companies in other business sectors (therefore not concerned by Basel III) deploy identity and access management, they generally do so, not only to reduce operational risks, but also to get a direct return on their investment.

This second source of cost reduction can be easily demonstrated in terms of productivity gains by three types of populations:

1. Users,
2. Help desk,
3. System administrators.

For a bank, an identity and access management solution can thus pay for itself, even without taking account of the drop in the number of operational incidents.

Measuring Return on Investment in Productivity Terms

Evidian has developed a methodology for evaluating the return on investment of an Evidian IAM Suite solution in productivity terms. Here are a few examples of the areas concerned:

On the market, you can find three basic architectures for making available SSO information such as logins, passwords and access rights.

Users	Time saved by no longer having to enter multiple passwords. As there is only one password to remember, a significant drop in the number of forgotten passwords - and the time lost in contacting the help desk. A new user or a user changing functions immediately has his or her access rights. That user no longer has to wait a few days to receive them.
Help desk	Lost passwords account for up to 30% of calls to the help-desk. Setting up an identity and access management solution, such as Evidian IAM Suite, considerably brings down these costs.
System administrators	The procedures for declaring a new user are extremely fast and only involve a simple operation on the Evidian IAM Suite console. Deleting all the accounts of a user who leaves the bank also only takes just a few seconds.

For a personalized ROI evaluation for your organization, contact Evidian at info@evidian.com.

Audit Data

The Basel Accord (paragraph 669 c) requires high granularity of the operational risk measurement system.

The audit data generated by Evidian IAM Suite are extremely detailed. They cover the following domains, among others:

Audit of user activity

- Access to an application granted
- Access denied because of password/identifier
- Access denied because outside authorized times and dates (configurable)
- Account blocked because too many attempts refused, etc.

Audit of allocation of user rights

- Creation, modification and deletion of a user, a resource, a group of users or resources
- Inclusion of a user or resource inside a group
- Allocation of access rights (to a resource or group of resources) for a user or group of users
- Creation and modification of profiles
- Allocation of rights specific to a security administrator (based on roles).
- Password change operations, etc

To better document loss events, logs should store "user identification" and "origination of event" for application access. This information is typically not present in application logs. However, it is present in the Evidian IAM Suite log.

Application Log:	" Somebody accessed account **GMAR_01** on **02/03/2009** at 1:02am "
IAM Suite Log:	" User **George Martin** accessed account **GMAR_01** from station **PC_027** on **02/03/2009** at 1:02am ".

Reducing Operational Risks with Evidian IAM Suite

Modular Approach

The Basel III accord makes it possible to implement advanced measurement approaches in specific geographical areas or specific functional domains.

Similarly, the modularity of Evidian IAM Suite makes it possible to deploy it to selected areas of a bank (region, subsidiary, type of business, etc.). It is also possible to activate only certain functions, such as single sign-on, provisioning or identity management.

Evidian IAM Suite can be implemented in a modular way, through a multi- phase project. Thus, a bank can implement identity and access management functions and gradually integrate them into its operational risk management infrastructure.

Integration within an Operational Risk Management Hub

By making it possible to efficiently manage identities and accesses, Evidian IAM Suite can immediately reduce the operational risks linked to IT resource access.

Evidian IAM Suite consolidates audit data concerning allocation of access rights and their use within the bank. This significantly simplifies audit, reporting and diagnostic.

Moreover, the operations involved in allocating access rights are consolidated on the same console, whatever the platforms concerned (servers, applications, web, etc.). It is therefore possible to take corrective action immediately if an operational incident is discovered.

Evidian IAM Suite thereby makes it easier to take account of the information access related risks by the operational risks management hub defined by the Basel III accords.

Appendix A: Coverage of Requirements of the Basel Accord

The following tables, which are not exhaustive, mention some of the qualitative criteria needed to implement the advanced measurements approach (paragraph 666). They describe which Evidian IAM Suite features help master operational risks related to identity and access management.

Requirement (a):

"The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk measurement methodology; for the design and implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk."

Coverage (a):

Codifying firm-level policies and procedures concerning operational risk management and controls	Installing Evidian IAM Suite gives the operational risk management team a single place to consult data access procedures and historical data concerning accesses and rights allocations. Moreover, this environment can be used to define and enforce all IT access policies. This facilitates and speeds up implementation of policies and procedures.
Design and implementation of the firm's operational risk measurement methodology	Evidian IAM Suite produces historical data on access to the IS and the allocation of rights, whatever the technical platform. The work involved in synthesizing these data for operational risk measurement purposes is thus made significantly easier. Moreover, the measurement methodologies put in place with Evidian IAM Suite are independent of the underlying IT technologies.

Design and implementation of a risk-reporting system for operational risk	Evidian IAM Suite has configurable alert procedures should a critical situation arise (intrusion attempt, etc). This is a useful supplement to the notification system installed within the bank.
Implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk	The operational risk linked to IT data access is measurable through the audit information produced by Evidian IAM Suite. Using Evidian IAM Suite, administrators can intervene immediately to remedy a newly discovered operational risk. It has centralized consoles for modifying the access rights policy across the entire bank, regardless of the technical platforms.

Requirement (b):

"The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis. The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm."

Coverage (b):

The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank	Daily management of the risks linked to IS access is handled by Evidian IAM Suite. Access rights policy, account cancellations and allocations and other operations are performed from the management console. This is valid for all parts of the bank in which Evidian IAM Suite is deployed.
Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile	The audit data produced by Evidian IAM Suite are used directly by the operational risk management function.

Requirement (c):

"There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports."

Coverage (c):

Evidian IAM Suite can be used as an information source for management notification procedures. It regularly produces audit data usable by the measurement and reporting tools.

Evidian IAM Suite makes it possible to rapidly enforce the access rights allocation measures needed to counter a newly detected operational risk.

Requirement (d):

"The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of noncompliance issues."

Coverage (d):

As Evidian IAM Suite is independent of the underlying IT technologies, the procedures intended to counter the breaches linked to fraudulent access are easy to document. They are all produced using the same interface, that of the Evidian IAM Suite console.

Requirement (e):

"Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function."

Coverage (e):

Review of the operational risk management processes concerning access rights is simplified: on the same platform, Evidian IAM Suite concentrates the management of access to a wide variety of environments (web, Windows applications, mainframes, client/server environments, etc.) Access rights management therefore involves a limited number of players (such as the HR or security departments). This makes auditing far easier.

The measurement chain for access rights-related operational risk is simplified as data is concentrated in one point. Reviews are thus easier.

Requirement (f):

"The validation of the operational risk measurement system by external auditors and/or supervisory authorities must include the following:

- *Verifying that the internal validation processes are operating in a satisfactory manner; and*
- *Making sure that data flows and processes associated with the risk measurement system are transparent and accessible. In particular, it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the system's specifications and parameters."*

Coverage (f):

The access rights to all the IT resources in the bank are entirely managed from the Evidian IAM Suite console. It is therefore possible for the auditors to access this console at all times and check that it is correctly configured and parameterized.

Appendix B: National implementation of the Basel accords

Member countries are expected to use the Basel Capital Accords as a basis for overhauling local regulations. We give hereafter one example in Europe.

In 2003, the French national banking commission issued a questionnaire to enable financial establishments to evaluate their preparation for the new Basel Capital Accord's criteria. The following table presents the answers that an identity and access management (IAM) tool could provide to a number of questions.

Management, Identification and Evaluation

(1) Has the board of your establishment approved installation of a system dedicated to supervision of the operational risk?	Installation of Evidian IAM Suite makes it very easy to supply the supervision system with pertinent information concerning information access.
(4) Is the General Management provided with appropriate summary statements allowing supervision of the operational risk?	The supply of summary statements cannot be dependent on the source of information. Consequently, Evidian IAM Suite does not aim to produce immediately usable reports. However, the data produced can be easily integrated into an existing reporting infrastructure.
(27) Did these analyses lead to production of an operational risk typology conforming to the 7 risk factors defined by the Basel Committee?	The operational risk data supplied by Evidian IAM Suite concern four of the seven types of risk factors: ✓ internal fraud, ✓ external fraud, ✓ customers, products and commercial practices, ✓ process execution, delivery and management.
(31) Does your establishment have a historical database recording losses and incidents?	Evidian IAM Suite can provide data about operational incidents in relational or export form readable by standard report tools. These extracts can be stored for several years.

Internal Reporting

(33) Has your establishment set up internal reporting of the operational risk?	Evidian IAM Suite can manage access security and produces audit data concerning accesses and rights allocation operations. The data produced by Evidian IAM Suite are directly usable by standard reporting tools.
(35) Does this reporting reflect and identify all the areas at risk?	The data produced by Evidian IAM Suite concern: ✓ incidents linked to unauthorized access attempts (incorrect password, access outside working hours, etc.), ✓ data about authorized accesses, allowing subsequent diagnosis following an operating incident, ✓ rights management data, identifying incorrect or fraudulent administrative operations.
(38) Does this reporting include alert indicators highlighting any rise in the risk or any possibility of future losses?	Evidian IAM Suite produces alerts for a range of events concerning unauthorized access attempts.

Reduction System

(45) Does your IS supervision system guarantee maintained secure access to the assets and data along with the corresponding backup procedures?	The servers offering secure access to the resources can be installed in fault-tolerant configuration. This guarantees high-availability access to the servers and critical applications.

Appendix C: Identity Management and Intrusion Detection

Centralized management of identities and accesses significantly simplifies the work of the operational risk management team. Basically, it complements the work done by the intrusion detection tools, which on their own are insufficient to offer complete coverage of the IT risks:

- A large part of operational incidents concern access using stolen or incorrectly used passwords. They are not therefore due to technical intrusion. An identity and access management solution such as Evidian IAM Suite is able quickly to identify the source of the access and the conditions in which the access rights were wrongly granted.
- Many operational incidents are attributable to persons working inside the company and taken place in the bank's intranet. There is thus no external access attempt.
- An intrusion detection tool can centralize the alert data but not the means of remedying these alerts. After detecting an operational incident, a precise tool (firewall, router, etc.) has to be reconfigured with its own administration tools.

Evidian IAM Suite, on the other hand, allows immediate correction of the source of the incident from a single console, whatever the platform concerned (mainframe, web site, etc.).

For more information, please visit our website: www.evidian.com

Email: info@evidian.com

This white paper is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001).

39 A2 10LS 04