Evidian

Reduce the operational risk for financial services

Controlling operationnal risks via identity and access management

Reducing operational risks

In the financial sector, data protection is a matter of the utmost strategic importance. In a growing environment characterized by incomplete regulations and close links between market players, with the handling of ever larger amounts of capital and increasingly sophisticated financial products, operational risks have taken on considerable significance.

By rationalizing access to sensitive data and managing access and identities in a structured and coherent way, banks and financial companies can fundamentally reduce their exposure to operational risks.

In a sensitive environment, application access security procedures must be reinforced and simplified. Proactive management of operational risks yields productivity gains and enhances security in all your financial activities.

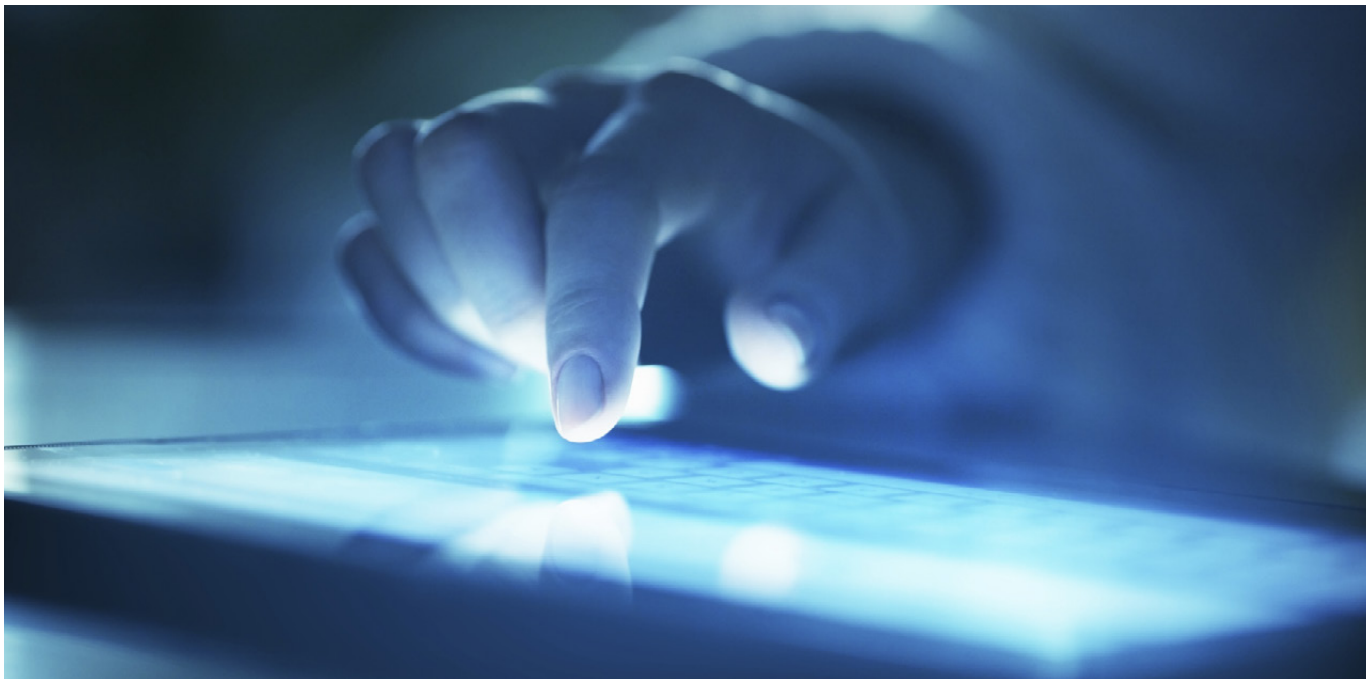
By looking at the legislation, we can refer to the Federal Reserve's Operations and Systems Risk (Management Information Systems) - Internal Control Questionnaire - Section 2040.4 . Is access to the automated systems adequately protected?

- Do access rights, passwords, and logon ID's protect key databases from corruption?
- Are "write or edit" commands restricted to a limited set of individuals?
- Are specific functions assigned to a limited set of individuals? Are access rights reviewed periodically?
- Does the system have an audit report for monitoring user access?
- Is access logon information stored in records for audit trail support?

Solutions to control your operational risks

Managing financial risks means looking beyond the traditional categories of credit risk and market risk. A significant proportion of operational risks involve human beings accessing electronic data.

The Evidian Access Management solution makes it easier to manage operational risks by structuring identities, roles and access to sensitive applications used in the banking IT systems.



Evidian, a provider of secure identity and access management solutions

Evidian is the European market leader in its segment. This offer was rated "Leader" by KuppingerCole Analysts.

With Evidian Access Management, a banking and finance company can achieve end-to-end control over access management, from internal to external user access and from managed to unmanaged terminals. The Evidian solution allows simplifying and controlling the access to the "extended" enterprise for employees, partners and customers.

With Evidian Identity and Access Governance, it is possible to define and apply a role-based policy and risk model, thus segregating tasks and ensuring the confidentiality and integrity of its data. This way, the financial entity can permanently ensure, that only the right people access the right resources with the required rights for the right business reasons. The Evidian solution offers the possibility to certify the compliance with regulations and the involvement of the business individuals using business-aligned processes.

Controlling internal fraud

"The Basel Accord introduces operational risks as a factor to be taken into account when assessing the banks' minimal capital requirements." Evidian offers a comprehensive range of solutions to ideally suit risk management in an investment banking and trading room environment by reducing operational risks with a secure multifactor authentication, Single Sign-On, easy-to-audit and report access.

Trading rooms

Trading rooms are high-risk environments, not only due to the "sensitive" data and applications at stake, but also due to the speculative approach adopted by the traders. The transactions performed are closely monitored and controlled in the back office. But how can you be sure of the true identity of the people carrying out these transactions?

The work of traders is of great strategic importance to a bank. Their key role in the trading room calls for constant focus and stress management. Their work is managed, supervised and controlled in a very precise way. However, identity control is often a weak link, as increasing the number of identification devices would reduce trader productivity.

In the trading rooms, trader desks are characterized by the need to use clusters of workstations with several screens which allow traders to access relevant applications available on-premises and in the cloud.

The most common prominent trader behavior is the sharing of access to applications (accounts) and workstations. This behavior introduces several operational risks.

These main operational risks are:

- Passwords disclosed between users, open access to user sessions: desks, workstations, application accessible without the possibility to identify and restrict privileges, refraining usage of "preventative" systems being the next edge of the risk management.
- Vulnerability of access with weak passwords: although passwords are regularly changed, how many traders in the bank are using #Password1 as a password within most accessed applications, and changing it to #Password2 will not reduce the vulnerability risk.
- Poor auditability of user access to the workstations, applications, accounts: analytical tools use historical and online data to produce KPIs, analyzing and controlling processes, contributing to the optimization of the security policy and procedures. A personal identification and verification allow building a reliable audit without repudiation risks.

Rogue Traders

What measures banks have in place to protect trading room activities against rogue trading?

Among others, the most common requirements are Risk & IT controls, segregation of duties, internal review, audit and reporting, periodic rights certification, strong policies and control, procedures, and monitoring by the top management.

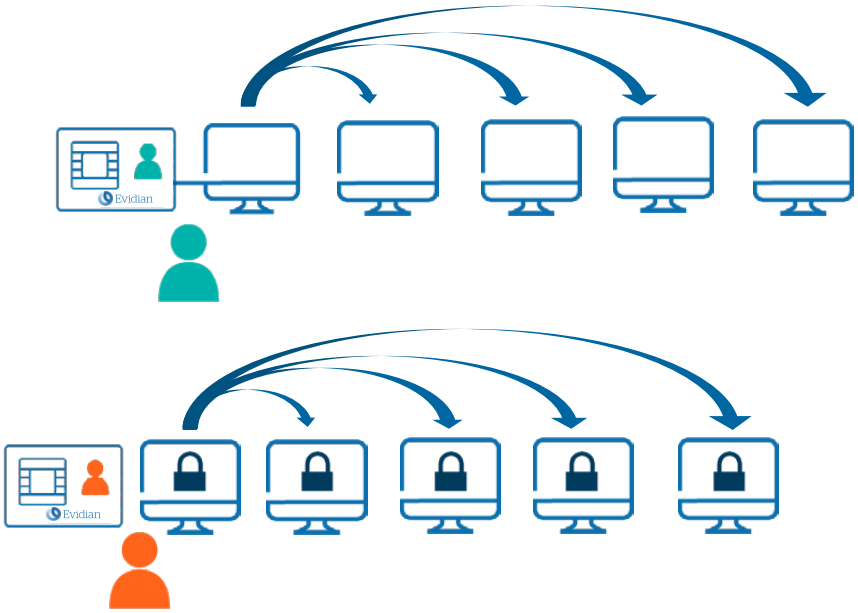
Multifactor Authentication to control and facilitate trader access

Evidian Access Management for trading rooms is specialized in authentication and access management solutions used primarily in large financial institutions, such as banks, stock exchanges and investment firms.

With the Evidian solution, a single, robust means of authentication (smart card, proximity card, biometrics, one-time password, smartphone, etc.) is all that is required for a trader to access all of his displays, monitors, servers and financial applications.

When traders identify themselves, their entire "cluster" of workstations and screens are activated, enabling them to access all their applications. Once they remove their card, their workstations become inaccessible. However, their financial applications can still be monitored by other colleagues thanks to transparent locking.

The Evidian solution provides the same user experience with a biometric authentication, a tap on go authentication with a proximity card and any other supported Windows authentication experience.

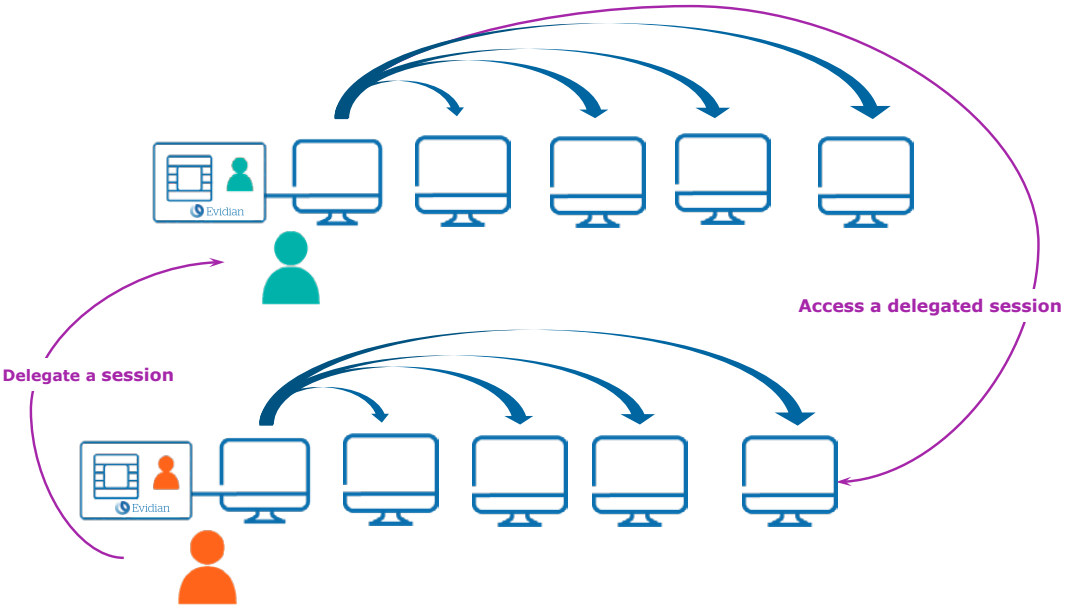


A single authentication with password, smart card, biometrics, one-time password, smartphone, SSPR... to open the Windows session. A single action to lock the Windows sessions on all the workstations.

A solution designed with trader efficiency in mind

Evidian has developed its access security and risk management solutions in partnership with a number of international corporate investment and wealth management banks. Evidian's experience enabled it to take into account real-life everyday scenarios, allowing traders to work securely while improving their efficiency and productivity with a proven enhancement of user experience.

Thus, Evidian software authenticates the user's identity and displays his application environment. This simplifies the day-to-day organization of the trader's work and makes it possible to monitor the identity and location of anyone attempting to access the system and applications.



A single action to delegate one of the sessions within the cluster.

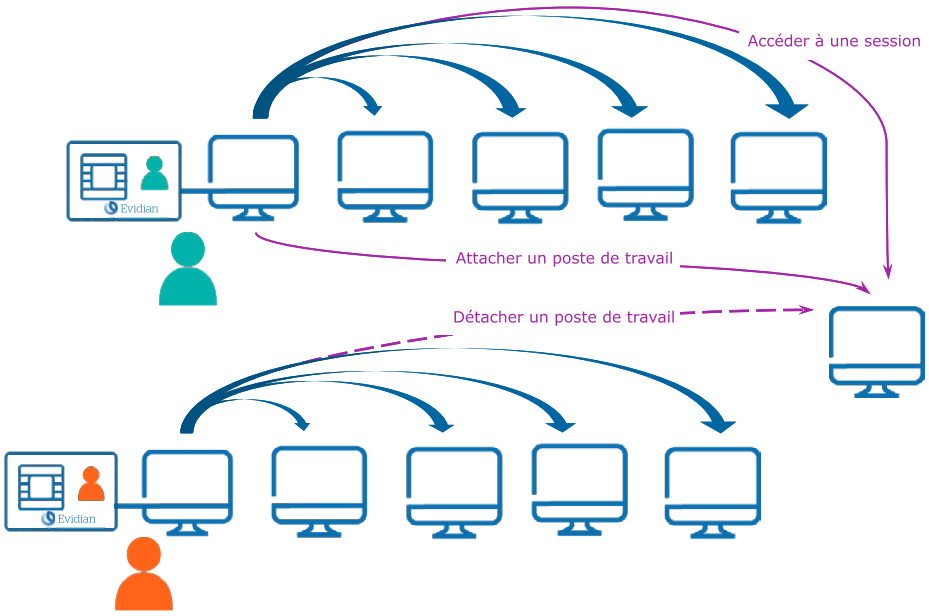
Moreover, a trader can delegate or share a part or the whole set of his cluster of PCs securely with an assistant, a colleague or support, without having to close and reopen Windows sessions.

Access to the Windows session and applications can be delegated, permanently or temporarily, with restrictions to account(s) of application(s).

Moreover, a trader can detach a part or the whole set of his cluster of PCs securely. A colleague can dynamically attach available PC(s) to his cluster of PCs and open new Windows session(s).

All access events are stored in a central database, which can be used to audit access to the PCs in the cluster and to applications. The Evidian solution helps to reduce the number of loss-generating operational incidents. Relying on Microsoft Active Directory repository, the solution is cost-efficient and doesn't need to introduce a specific repository.

The Evidian solution is based on a standard configuration of the software, avoiding development, modification of the applications and introduction of hardware components and appliances in your domain.



A single action to detach a workstation and allow access to a colleague

Internet Financial Services and Branch networks

The growing number of internet Financial Services and Branch networks spanning several geographical areas imposes constraints in terms of employee, partner and customer access management.

- How can you make sure your security policy is applied?
- How can you manage the application accounts of thousands of employees?
- How can you let branches manage their own users in a secure way?
- Which procedure to implement to secure and facilitate new user arrivals?

Managing access in branches

Internet Financial Services and Branch staff often find restrictive the increasingly demanding security rules. With these concerns in mind, Evidian Access Management simplifies and rationalizes access security by managing the application authentication process on the user's behalf. Therefore, employees naturally comply with the security policy.

Administrators modify, delete or adjust access rights from a central console. They assign rights based on the role of the employees within the branch, thus complying with task segregation rules.

An approval workflow integrated with application provisioning automates the authorization process and makes financial services available faster.

Since all access events are audited, traceability and generation of reports are facilitated.

Increasing employee efficiency

Within the branches, employees use several applications, each protected by a password. Forgotten passwords increase the number of calls made to the help desk, damaging the company's image and reducing customer satisfaction.

Evidian Access Management eliminates this problem while increasing the user productivity. A single means of identification (password, smart card, proximity card, biometrics, One-time-Password, Smartphone, etc.) gives access to the Windows session. Enterprise SSO transparently allows access to all authorized applications and eliminates the need to remember or to type various identifiers and passwords. Moreover it supports any type of application without modification. Mobile employees can still have secure access to corporate web applications, even from outside the company.

Secure Online services and Mobile accesses

With Evidian Access Management, users have a secure access to the extended enterprise including on-premises, Cloud and SaaS applications, using Identity Federation based on industry standard protocols such as SAML, OAUTH, OpenID Connect and Social Identity.

The solution natively allows the definition of adaptive authentication policies with out-of-the-box authentication methods increasing the level of security required for the authentication to sensitive services.

Supported authentication methods are: password, certificates, smart card, proximity card, One-time-Password (OTP) via SMS, OTP via email, Grid card, OTP via Apps on Smartphone, Evidian QRentry...

Simplifying and strengthening your security policy

With the Evidian IAM Suite, identity and access management becomes standard and systematic; this makes control procedures easier to maintain and document.

When staffing changes occur (new recruitments, transfers, departures), the Evidian IAM Suite can trigger the creation or deletion of accounts. The latter are allocated in such a way that convergence between application rights and your security policy is facilitated. The application managers are relieved from repetitive tasks in which errors can easily occur.

The Evidian IAM Suite implements critical procedures such as account removal and role-based task segregation. Unused accounts are detected and, if necessary, deleted. Moreover, the central access audit can also tell you precisely who in the branch has used a generic account.

In the event of a staffing change, the relevant line managers are informed through notifications (sent by an integrated approval workflow). These managers can then approve or reject the assignment of new rights with just a few clicks. Once the manager has approved, the account is activated automatically for the required period of time.

The Evidian solution allows the organization to have end-users, operational managers and security officers accountable for the identity and entitlement management processes.

The efficiency of the security policy can be measured at any time, for example, by determining the applications currently used by an employee profile. As a result, you can regularly optimize your security procedures.

Delegating to Branches & Partners the management of their users in a secure way

Opening Internet Finance Services to Branches and Partners implies managing the users and their rights of the organizations that will access the Services. The Evidian IAM Suite lets you delegate, in a secure way, this management to the appropriate individual in each organization.

By implementing a user management security policy, each request will have to be validated by the identified correspondent in each organization and, when defined, even be validated by a central manager.

With this procedure, Branches and Partners user management may be delegated to the nearest manager without taking any risk.

Facilitating the arrival of new users in a secure way

In order to ease the planned arrival of new employees or users in branches or partners, accounts can be created in advance in deactivated mode. At the planned date for the arrival or even some time before, the activation process proposed by the Evidian IAM Suite will inform the person that he has to activate his account via a temporary link sent by email. By clicking this link, the user can then define his password to access the system, activating at the same time his account and applications. The user is ready to start working.

Of course, this password must respect a given format defined by the company. Alternatively, this process can also be linked to the activation of a strong authentication device, previously given to the user.

Evidian

Evidian is the Identity and Access Management Atos.

Evidian is a software publisher that has specialized for over 20 years in identity and access management (IAM) solutions. Every day, more than 5 million users access their applications with Evidian solutions.

Evidian is the identity and access management solution of dozens of banks and insurance companies in the United States, Europe, Africa, Asia and the Middle East. It enables these organizations to comply with their legal confidentiality and data integrity obligations, make their employees more efficient and autonomous, and improve the service they provide to their customers.

Brochure

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

For more information: **evidian.com**

CT_191021_LPM_Evidian_BR_Finance_Banking_en