

## Case Study: User Access Review

### Industry Sector: Finance

In large multi-user environments it is often difficult to establish exactly who has access to data, systems or applications. Historical user accounts and group memberships along with various generations of internal architectures further complicate matters.

Through a User Access Review engagement IRM identifies user access models throughout the corporate environment. Such reviews can be tailored to meet specific internal or external compliance requirements. IRM has built custom tools such as PRESQL<sup>†</sup> to help organisations graphically view the role and privileges of users across resources; this has proved invaluable with respect to identifying excessive or redundant accounts and roles, which can then be removed to minimise the potential for unauthorised access.

#### Case #1 – Streamlining the compliance process

IRM was asked to help a global fund management company meet the requirements of their internal compliance programme by identifying all users with access to mission critical systems and applications, particularly those with administrative privileges. Over the course of three months, IRM conducted audit interviews with key systems administrators and business stakeholders, supplementing this with a hands-on technical investigation. This allowed IRM to accurately establish the user access models present across the wide variety of technologies in use.

The result of the assessment was a documentation set identifying where current system management practices deviated from the organisation's internal policy requirements, including the identification of unnecessary access privileges, poor password management, areas where obsolete accounts had been left active and areas where system management did not conform to best practices.

IRM also produced an access control framework report for each of the organisation's most critical applications, documenting exactly which employees had access to what, and what processes and procedures were in place to control access.

IRM's involvement was instrumental in allowing our client to focus their remediation effort on the most adversely affected systems in preparation to meet the requirements of their own group policies and an impending internal audit.

#### Case #2 – Understanding your business

IRM was asked to perform a SQL Server Database User Access Review for a large financial institution. The client utilised various Microsoft SQL Servers for storing sensitive client details, and sought information on all user accounts and privileges across the database estate. Through a combination of bespoke scripts and the PRESQL tool, IRM consultants were able to identify all user accounts across the database estate, their roles and corresponding privileges. The review identified a number of redundant accounts belonging to former employees, and a handful of accounts configured with full execution rights on the databases.

The result of this engagement was a full understanding for the client of the number of users with access to confidential data stored across the database estate. IRM was able to formally present these results to the client, facilitating the removal of unnecessary accounts and privileges. IRM was also able to provide the client with best practice procedures for future user account management across the databases, suggesting changes to policies and procedures for the addition, modification and deletion of accounts.

#### About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.

---

<sup>†</sup> PRESQL - the *Pictorial Representation of Enterprise SQL* – an in-house developed IRM tool to assist enterprises in mapping out diagrammatically user roles, groups and privileges across multiple systems.