Access Governance

"Knowing who has access to what information and when can make the difference between peace of mind and uncertainty. Can your business afford the risk of data breaches? How are you managing access to sensitive data and transactions? Does your current access operating model cover all bases and keep your business safe?"

Richard Mardling
Director, PwC

pwc

www.pwc.co.uk

It's no longer acceptable to be in the dark about who has access to what in your organisation. With ever-changing security boundaries, varying staff mix, increasing collaboration, a widening variety of devices and the continued growth of cloud services, it is paramount that only the right people have approved access to your applications and data. Poor access governance and controls can damage your reputation and ultimately profit; a number of high profile organisations have lost significant amounts of money in recent years.

Progressive businesses are solving this problem by adopting a pragmatic approach, implementing revised operating models and technical tools that provide visibility of enterprise-wide access and focusing on cost effective control operations.

What's on your mind?

Knowing who has access to what information and when can make the difference between peace of mind and uncertainty. Can your business afford the risk of data breaches? How are you managing access to sensitive data and transactions? Does your current access operating model cover all bases and keep your business safe?

Do you know your high risk users? Understanding which users pose the greatest risk to your data security is the first step in evaluating your position. Some users will have multiple access rights to support their day to day work and at times this may present an access conflict which breaches your policy. Knowing who has access to what information or critical applications and when, allows you to manage the risk more effectively.

Keeping track of Joiners, Movers, Leavers When staff, contractors and sometimes even third parties, join, move or leave your business, are you keeping track of exactly which systems they can access? How confident are you that their access rights match their job role or status?

Do you know what Segregation of Duties (SoD) need to be managed in your business? Have you hard-coded these into a policy which is regularly updated and how confident are you that the policy is being applied?

Can you justify generic accounts? Is it really enough to know who has access to the account if you cannot identify which individual was accountable in the event of a data breach?

When it matters, can you clearly identify who is employed by you and who is not? Do you understand the difference as this is key to embedding the right access control policies?

Are you monitoring what matters, when it matters? Are you reviewing the most important access areas on a sufficiently frequent basis to allow you to respond quickly before the real damage is done?

Our point of view

'You should be aware of your risks and then manage them, not lock down so tightly that you choke the business.'

Access governance should be considered an area where the three lines of defence model applies.
The first line requires automated, IT dependent or manual controls to be embedded. The second line deploys monitoring and reporting processes and at the third line Internal Audit functions can fulfil their duties.

Conduct independent testing and verification
You need real assurance through an independent testing and verification service. Separate from your 'joiner-mover-leaver' process and controls this service provides you with the assurance that your controls are working or clarifies where there is a deficiency and you need to take action.

Work out what really needs to be locked down
You should be aware of your risks and then manage them, not lock down so tightly that you choke the business. As soon as you do this, users will try to circumvent the controls, resulting in more issues and unmanaged risk.

Access risk is a business mandate, not a function of internal audit or IT
Understanding the risks and presenting them in the right language is essential if this is to happen. You don't want an 'It's English Jim, but not as we know it' scenario.

To reduce cost and disruption, you should automate the management of the critical access controls
These are the ones which provide access to the systems that really matter, and create the foundations for a robust second line of defence which supports the rest of your access governance operating model.

Not all users are equal, therefore employ a risk-based approach to reviewing users' entitlements
High risk users need to be re-certified frequently, whereas users with low impact entitlements can be subject to annual review thereby saving time and money.

Having data in the cloud magnifies the impact of governance flaws
Often, cloud-based access is overlooked in favour of the more tangible on-premise access governance. This has a significant impact when managing leavers and disgruntled employees.

Digital trust is vital in an ever-connected world
Protect what matters and feel confident that you are doing it through strong access control and access re-certification.

Many of the recent cyber security breaches can be traced back to an insider issue resulting from poor access governance.
Failing to address the insider threat will not stand up to scrutiny and could be considered to border on negligence.

When to act

There are logical triggers in your business activities that prompt action. There will almost always be times when you should talk to us. Here are some examples.

- ✓ When you or an organisation similar to you has suffered an access-related breach.
- ✓ If you are impacted by Sarbanes-Oxley and other relevant legislation or regulation.
- ✓ You need to prove who has access to what in the event of a breach.
- ✓ You are considering new operating models, acquisitions, trading relationships or transformation programmes.

What good looks like

Characteristics of organisations that have a successfully access governance programme include:

- ✓ Boards and Audit Committees actively and regularly discuss access governance.
- ✓ A baseline of access control data to support good decision making. This requires you to get the data clean and then ensure that you have the processes in place to keep it clean. Too many times organisations have spent good money cleaning up their user data only to have poor processes which ultimately result in the destruction of the initial investment, and the loss of confidence in the service.
- ✓ A deep understanding of who has access to what, today or for some defined period. You have visibility of the differing user communities including employees, contractors and third parties.
- ✓ Clear understanding of Segregation of Duties (SoDs) concerns for all of your user communities, whether internal or external, customer, partner or supplier, on premise or in the cloud.
- ✓ Corporate agreement on how SoDs are managed. Do you immediately revoke one or more entitlements, do you manage and monitor them or do you employ an agreed set of techniques to manage specific types of access risk across your business?
- ✓ An independent second line of defence is actively testing and reporting the status of your access polices and controls.
- ✓ Access governance is a corporate responsibility and not owned by IT. A cross-discipline operating model will involve the whole organisation and allow the business to set the pace and focus areas.
- ✓ Application owners, typically from the business rather than IT, play a key role in defining and managing access rights.
- ✓ Business language is used when access governance is discussed to make it accessible and understood by all key parties.
- ✓ Defined process are in place for evaluating the risk posed by your users to determine how often they should be re-certified, targeting a greater frequency for those who pose a higher risk.
- ✓ Simple dashboards and reports are available and written in business language.

How we can help

We help you to assess where you are, where you want to be and how you can get there. Our wealth of experience can help you to manage risk effectively and improve the security of your information. We can help you by:

- advising on the structure of your first and second lines of defence in order to allow internal audit to efficiently deliver the third line.
- designing and deploying an Access Governance Operating Model as an enduring function within your business. As part of this activity we will:
  - help you to ensure that ownership of access governance is with the right people.
  - design the processes to clean your data and keep it clean.
  - assist you with defining the necessary controls and matching your needs with the appropriate technology.
- providing clear guidance and education on why managing entitlements is central to a secure business.
- identifying segregation of duties, both within an application and across applications.
- developing a roadmap to ensure that you fully exploit the technology available to you.
- selecting and deploy technology (on premise or on cloud) that can help support your access control objectives.
- delivering additional services to reassure your board or audit committee if they are concerned about the level of confidence provided by your lines of defence.
- providing experts in the event of an access control breakdown or breach, to identify the source of the issue and support you in making sure it does not re-occur.

What you gain

Risk-managed access

Having a second line of defence to identify what needs to be controlled and who owns it lowers your operational costs, while taking a risk-based approach ensures greater reporting efficiency.

Greater value from internal audits

Keeping a close eye on regular access issues and allowing your internal auditors to identify anything extraordinary improves your security.

Reputation protection

Reducing the risk of major losses through data breaches and protecting your reputation.

Improved security

Minimising the opportunity for inside attacks through mistakes, misuse or malicious activity by managing user access and using effective controls.

Reduced management overhead

Taking advantage of simpler access governance processes tied to automated management and reporting tools delivers greater security at lower cost.

Contact us

Cyber security partner

Richard Horne
+44 (0)7775 553373
richard.horne@uk.pwc.com

Cyber security director

Richard Mardling
+44 (0)7711 589047
richard.w.mardling@uk.pwc.com

Delivering value

Putting a project back on track for success

Our client, a top 25 UK higher education institution, invited PwC to assist them as part of a large digital transformation programme. Prior to PwC being engaged, they had tried for six years, and ultimately not succeeded, in delivering an identity management solution.

What did we do

- Developed an IDAM strategy and roadmap
- Performed vendor selection
- Re-designed staff joiner, mover and leaver processes
- Created high-level and low-level technical designs
- Implemented the solution (Joiner-Mover-Leaver and Access Governance)
- Designed and prototyped a federated SSO solution

Outcomes

- Improved reputational value of the client team and transformation ability within the university, by supporting the client team tackle a large IDAM project which had repeatedly failed in the past
- Built and tested an identity management and access governance platform
- Designed the subsequent phase of the platform to on-board additional users and applications
- Delivered a prototype enterprise SSO solution
- Advised the university on improving several business processes that will realise efficiency gains
- Streamlined several IT processes including test management, release management and development architecture to get the maximum from cross-organisation teams

Implementing a consistent access governance framework and culture change

The client, which had a large number of retail banking branches and a network of business and private banking centres, had an increased senior management focus to remediate known access governance and control issues. This was due largely as a result of audit findings around the management of access rights, coupled with deficiencies identified by the Identity Management and Information Security teams within the bank

What we did

The work was split into three workstreams:

- **Access Governance** – Provisioning of a consistent access governance framework
- **Application Categorisation** – Identifying the application landscape and drive business ownership
- **Recertification of User Access** – Defining recertification procedures and executing a review of user access for seven of the Bank's critical applications for over 6,000 users.

Outcomes

- As a result of our work the client was able to identify business owners for applications and begin to change the culture, so that wider responsibility and accountability is taken in the business. They were able to identify critical applications through a measurable process, and manage these effectively through the access governance processes designed by PwC.
- The value of the work delivered has facilitated a change in the culture to drive consistent processes, visibility of assets, and impact analysis which will ultimately allow the client to make improved management decisions.

www.pwc.co.uk

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

160106-160723-CU-OS