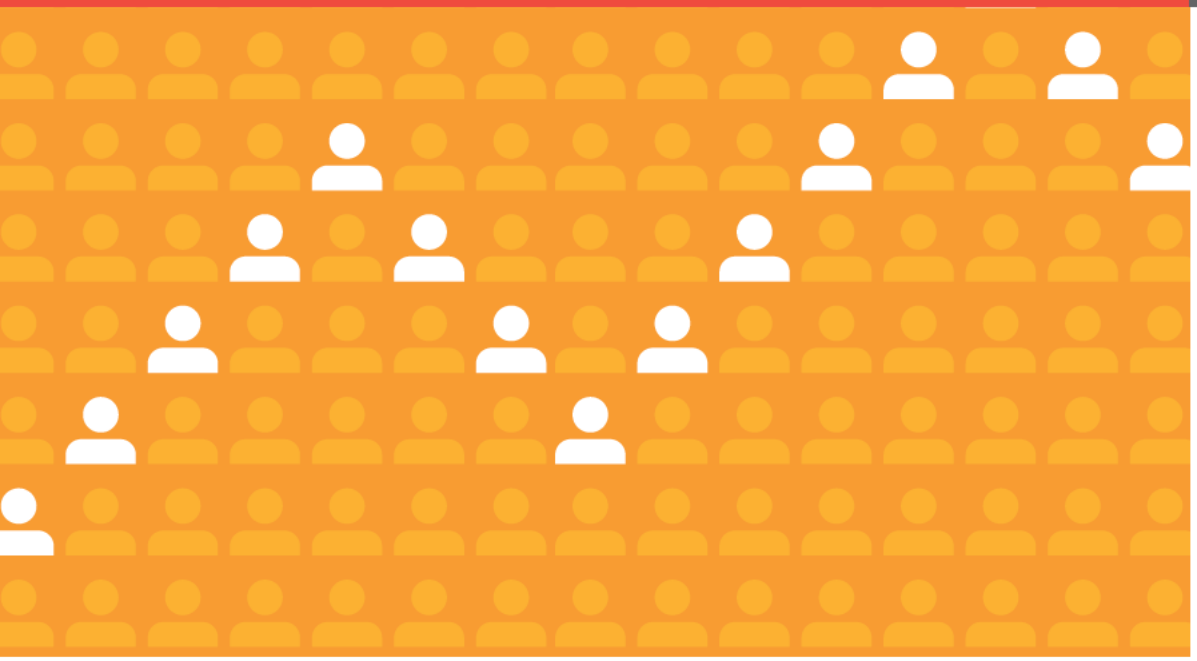
www.pwc.co.uk/cyber

# Transforming access certification

## Simplified access and security based on risk based intelligence

January 2019



pwc

## The danger within

Data, digital resources and systems are the most valuable assets for the majority of organisations today. Protecting them is a priority. Recent research has shown that the biggest security threat comes from within the walls of an organisation, with almost a third of all reported incidents being traced back to current employees[1].

This is why controlling access to systems is critical for organisations – making sure that the right people have the right access, at the right time.

**Source of security incidents**

**Current employees**


**Third parties**


## The challenges with conventional approaches to access certification

Organisations have long struggled to find an effective process that aids the business to determine what constitutes appropriate access. Typically, access should be granted on the principle of 'least privilege' and is only granted to users who need it for a legitimate purpose, with periodic 'snapshot in time' access certification campaigns executed to identify inapproriate access. This essentially treats all access equally and churns it through the same, or a very similar process.

The current approach to access certification often hinders the certifier from being fully informed and productive. Access can often lack a business friendly description and this, coupled with a distinct lack of intelligence regarding certification decisions (e.g. when the last review occured, who performed the review, who approved the initial assignment, if anything has changed, actual access usage) makes it hard for the business to meaningfully certify access. Many organisations simply lack the time or resources to complete a comprehensive access review, leading to the risk of managers bulk approving when they are swamped by too many requests.

In addition to these common certification challenges, business environments today are more demanding and fluid. The adoption of agile workforce demands (permanent or contract staff being more fluid and interchangable), disruptive technologies (cloud, SaaS, AI, IoT), mergers and acquisitions, and many others. These are all adding additional volume to the existing access certification challenge.

This lack of advancement over the last few years means that some organisations rely on a spreadsheet certification model dating back over 20 years. Or even worse, no certification occurs!

### A two tier approach

In many cases, access certification is driven by compliance requirements, resulting in a tick box approach. This places too much emphasis on the progress of the certification itself rather than the quality of the outcome, which is a crucial element in order to best address potential security threats.

Within organisations operating in regulated markets, it's not unusual to see a two tier approach to certification – a mature level for the core applications that fall within the category of being a regulated system or application, and then a 'Wild West' approach for everything else. In non regulated organisations, the maturity of access certification is typically lower and sometimes simply relies on staff 'doing the right thing'.

### Resource intensive

The current access certification process is typically very resource intensive. Several groups of stakeholders are typically involved:

- The certifier performing the review,
- The IT team that defines policies and standards,
- The risk and compliance team; internal audit,
- The service and security operations team who oversee certification campaigns, and
- The end user.

Overall, access certification takes a lot of effort from many people who are already likely to be stretched, with a distinct lack of certification intelligence and insight, to assist and optimise the certification process.

### Cognitive bias

Human beings tend to act in certain ways:

- We simplify and generalise; we favour the familiar and whatever happens to be in front of us when we're making a decision, and
- We are drawn to details that reinforce our existing views.

Access certification reviews are particularly susceptible to this cognitive bias – if a reviewer knows the user, risk may be overlooked. Approval is a repetitive process where important details can easily be lost and the exercise hurried through simply to get it done.

### What does good look like?

Good access certification is a seamless, continuous process that causes the least possible disruption to users and to the organisation as a whole whilst conforming to robust security controls. It is driven by an informed assessment of risk.

Good access certification takes into account important contextual information such as:

- **Historical data** – Has there ever been a previous review decision? When and by whom? Are there notes available from a previous certification?
- **Peer data** – How does this access assignment profile compare to others in the peer group? Or is it an outlier?
- **Risk** – Does the user have access to sensitive applications or multiple accounts?
- **Change** – What has happened since the last certification? Has the job changed? What access has been added?
- **Usage** – Whilst not available for every application or system, some do provide transaction or event data detailing when the account and access assignments were last used? Does this appear to be abnormal usage?

Good access certification also sees the value in the process rather than treating it as an administrative burden. It measures risk well, benchmarking data to track whether access risk is increasing or decreasing and feeds the outcomes into governance decisions. The access certification process generates valuable information – so why not use it? In addition, organisations struggle to even understand their own end to end processes. Having these documented and understood will in itself lead to better outcomes.

[1] PwC, CIO and CSO, The Global State of Information Security Survey, 2018

## A new, dynamic approach

Advances in analytics have brought a new and valuable approach to access certification within reach. Access analytics can be utilised to better inform the process, to focus more closely on risk and change, and to transform certification from a periodic exercise to a dynamic, continuous review.

Access governance tools, such as our own cloud based service, AccessAble, are already greatly enhancing the access certification process by leveraging access analytics, reducing certification clicks and improving outcomes.

Integrating access analytics into these tools provides organisations with more dynamic, risk based options or 'focus filters' for certifying access, increasing efficiencies and productivity and generating valuable information for the organisation. Access certification becomes easier, more robust, less risky, and better informed. In addition, the success of your access policies can be seen and measured.

## The future of managing access

It is evident that the future of how access governance is performed will change to take advantage of technology tools and data analytics capabilities. These capabilities provide a richer 'identity context' view that provides focus areas for access certification.

As organisations drive for a zero trust security model, they will need to manage their hybrid (On-Premise, Cloud and SaaS) IT assets to improve their risk posture and leverage machine logic to provide certification focus. This allows the human certifiers to more intelligently review access and means that access certification will be dynamically and actively managed in real time.

**More specific risk based views are vital to allow organisations to make more informed decisions, to reduce the human time investment and improve the overall outcomes as well as the experience of performing the access review.**

We are challenging clients to think differently about how to do access governance more intelligently. The evolution of how we manage access with access analytics will not only improve the certification outcomes, it can also proactively be used as part of the access assignment process.

Many access governance tools can proactively identify unused accounts/ access with the ability to automatically deprovision after a predefined time period. However many opt not to use this capability because of poor access request experience. Imagine what difference it would make if removed access could be reprovisioned in real time with automatic approval when requested after a certain period of time? Would that convince more people to enable self maintainance of unused access?

**Improving the access request process**

Access request and approval governs how users gain access assignments in the first place. Access analytics can play a significant role to improve this process also, using risk scores, historical certification data and peer group data to highlight which access or roles are likely to be required or missing, therefore providing greater intelligence and insight across the request and approval process.

The future will simplify and better inform all stakeholders, providing enriched access management and governance processes. The day when tools provide requesters with a percentage chance of approval and an estimated timescale for approval or assignment is fast approaching. This could challenge the requestor to think twice about the request, with perhaps the ability to escalate requests for emergency access. If so, could this justify the need for a tool that also suggests a default action to the approver based on this intelligence?

## Using analytics to inform access governance

### Risk lens

Not all users are equal – providing a risk lens helps you ensure the focus is right.

Risk scores can be applied to users, informed by the access they hold, violation history, date of last certification etc. Filters can then identify particular sets of users, such as high risk users, or users whose access has changed since the last review.

### Outlier lens

Comparing access anomolies across peers. Vital for keeping you secure.

Analytics can be used to identify users with access rights that vary from those granted to their peers by highlighting any access anomalies. This can also identify 'key person reliance' based on access profiles.

### Change and usage lens

Preempting certification by spotting key events (e.g. movers and leavers) dynamically performed outside of the normal periodic model.

Context for access certification is vital information. Has the user changed jobs? What is new since the last review? Has the user utilised the access or account? Access analytics captures this information to explain what has changed.

## Conclusion

The current approaches to access governance are not overly smart and continue to create too much complexity and effort to comprehensively review and certify legitimate user access. **This complexity often leads to human errors that result in costly breaches to confidential data or intellectual property, as well as the cost of supporting ongoing audit remediation activities.** Therefore, these processes need to be more productive.

Now is the perfect time to reimagine the processes for access management and governance. By taking advantage of an intelligent digital identity through access analytics, the existing access governance processes can evolve to a new level; one where risk is consistently and reliably identified, tracked and measured across both inter – and intra-application levels. The unlikely two bedfellows of convenience and security can finally coexist.

## Contacts


**Colin Slater**
Regional – Cyber Security Lead Partner
M: +44 (0)7711 589065
E: colin.slater@pwc.com

**Derek Gordon**
Identity and Access Management – Director
M: +44 (0)7843 333935
E: derek.gordon@pwc.com


### Intelligent Digital

At PwC, we are harnessing the power of Intelligent Digital, helping our clients rethink their futures and reshape their own world.

We're using cutting edge technology, formidable human insight and industry expertise to protect what matters most to you.

Fear cyber attack? Attack cyber fear. With a risk based mindset we can build a secure digital society together.

pwc.co.uk/intelligentdigital

#IntelligentDigital

www.pwc.co.uk/cyber




190124-130107-BC-OS