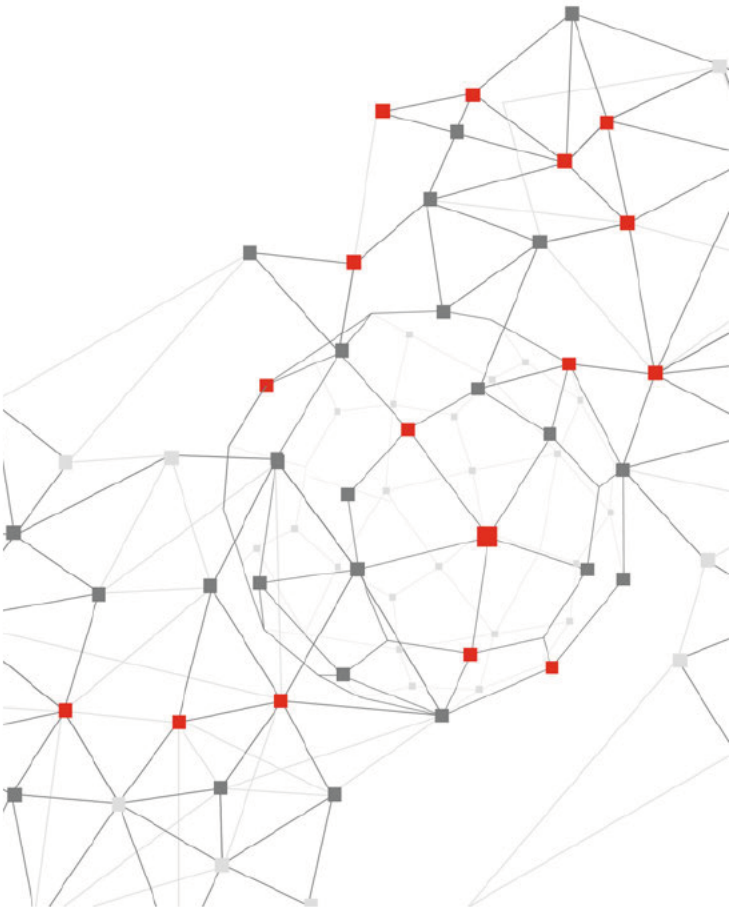
Digital Identity supports a secure remote digital workforce during COVID-19



4 May 2020

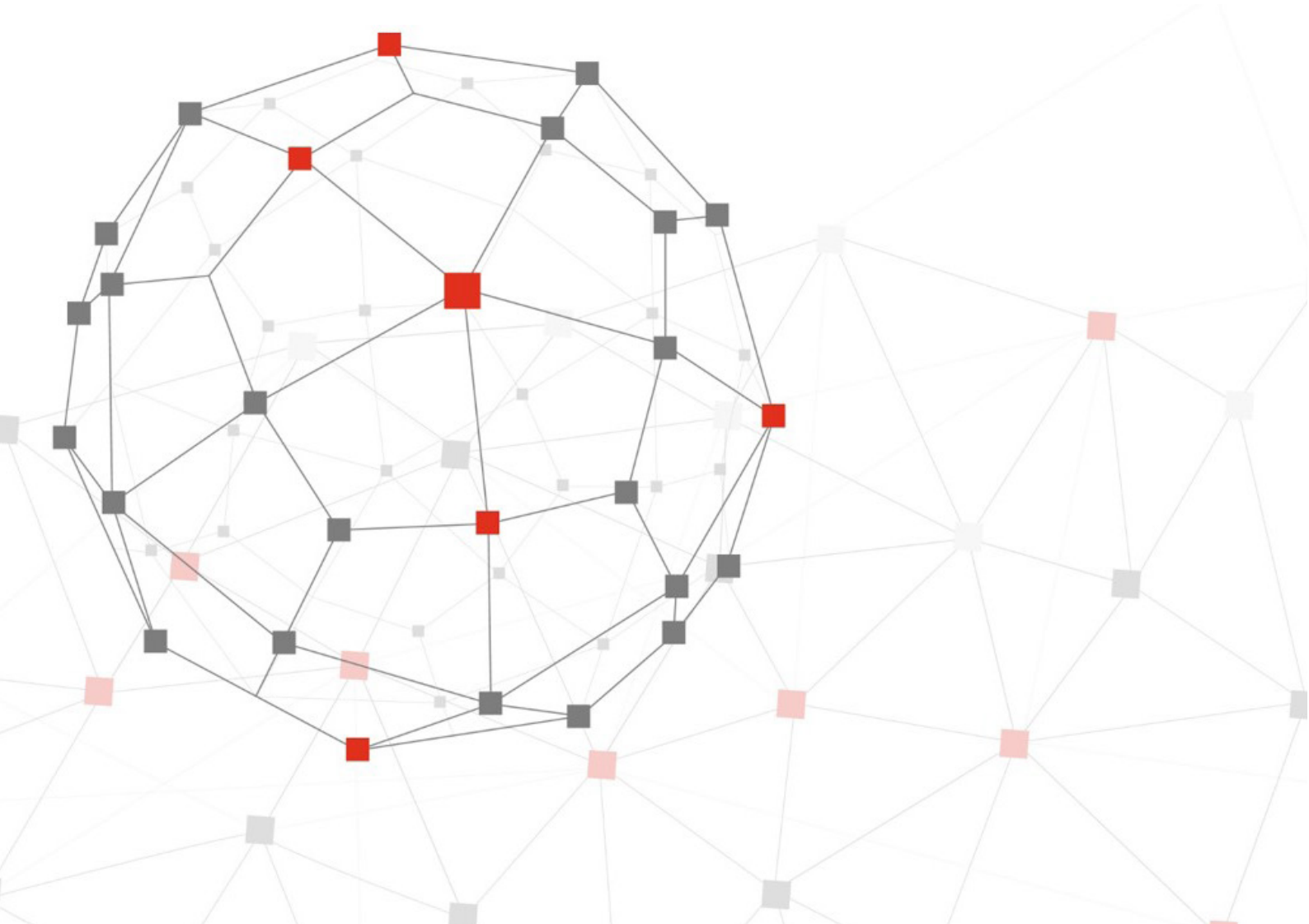
The evolving circumstances around the coronavirus (COVID-19) crisis have dramatically brought remote working to the front of mind for many organisations. For many, the effectiveness with which they have been able to shift to a 100% distributed remote digital workforce has played an important role in maintaining at least some level of business operations.

This new working environment has also brought challenges. As their remote workforce log on from a variety of locations, devices and working environments, businesses need to rapidly enable and scale effective, resilient and secure ways of remote working.

Remote workforce requirements have placed new challenges on the existing Enterprise Identity and Access Management (IAM) services and processes, with competing demands for rapidly provisioning and managing access for existing and new applications, accommodating ad-hoc change to processes and controls, all while operating under IAM resourcing and personnel constraints.

pwc

Contents

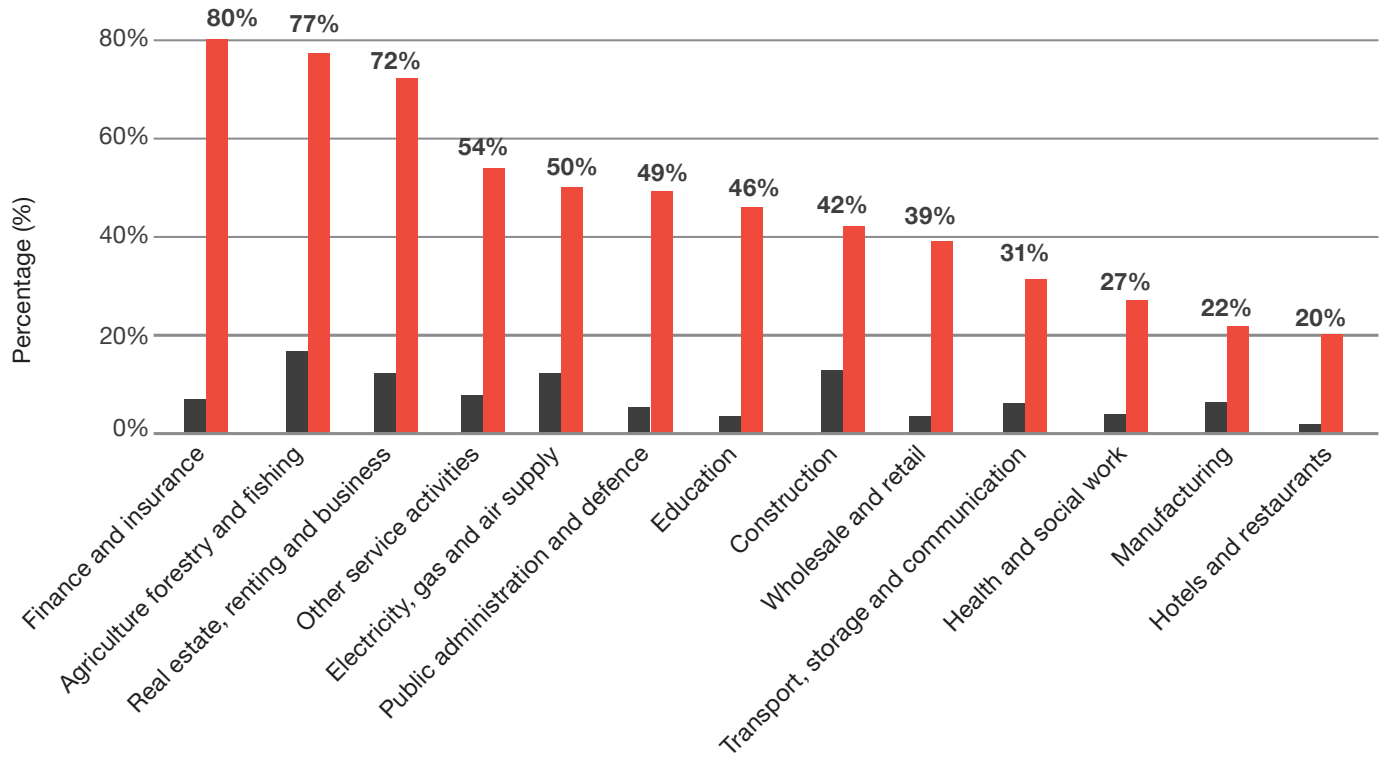


Remote workforce posture

The analysis from our workplace survey augmented with ONS data, shows that previous adoption of remote digital working has been relatively low until COVID-19. It also highlights the market sectors that are best equipped to embrace remote digital working.

The survey highlights the perception that remote digital working for the entire workforce is not possible, mainly based on the fact that it has never been tried and tested. Regardless of their preparations (or lack of), sectors have at best supported remote working to a limited degree by providing the necessary technology, communication, training and support. However, the extent of remote working was never expected to support the entire workforce.

Share of employees that regularly work from home (% of workforce, 2018)



ONS data on workers who regularly work from home

PwC survey on whether the nature of your job allows you to work remotely

Work from home securely

The rapid shift to a remote workforce has presented organisations with many challenges, even those who had significant technology investment with robust policies to support remote working.

At this time, businesses are attuned to the fact that 100% of their digital workforce (where practical and possible) must be enabled to work from home for extended periods of time.

The good news is the majority of the digital workforce, across many industries, can effectively work remotely. As they adopt and transition, it is key that businesses make sure they don't bypass security controls and processes, and succumb to the temptation of shortcuts. For those organisations that provide essential services with on-site workers, the existing IAM services and processes should support any updates required to support new work patterns and system access requirements.

In order to support this, heads of IAM need to be able to comprehensively answer the following four key questions:

1 How do I ensure that IAM services support business to enable and scale effective, resilient and secure ways of working?

2 How do I design and implement new IAM processes to implement new appropriate processes and controls to best enable the remote workforce?

3 How do I sustain IAM services and ensure they operate effectively and scale to ensure critical remote workforce services and resources are prioritised?

4 How do I ensure that risk is best managed in the long-term, by reviewing, enforcing and evolving controls to support the remote workforce?

Each of these align to a key IAM principle, as shown below.

Enabling access and services to enable a remote workforce

1 

Adapting IAM processes to support business

2 

Continuity of the IAM Service to the business

3 

Managing access control risk and compliance

4 

The principles needed for robust Enterprise Identity and Access Management (IAM) Services

Enterprise Identity and Access Management is crucial to support and secure the remote digital workforce.

The IAM services provide the core authentication and authorisation services to secure the remote workforce through access management functionality (including Multi-Factor Authentication), and also provide capabilities for identity management (user lifecycle management, access request, automated provisioning, etc.) and access governance (access review and reporting); all of which provide the comprehensive access controls to secure and manage the workforce, remote or otherwise.

These services also support customer access and services, allowing organisations to continue to serve their needs by adapting to shifts in demand and repurposing existing digital channels to scale-up to support customer engagement, experience and trust.

1. Enabling access and authentication services for the remote workforce.

Objective: Support rapid access to key services to enable the mobilisation of a remote workforce, while maintaining security and protection of your digital assets.

Authentication and authorisation are crucial to delivering access management capabilities. This includes managing who has remote access to which applications, controlling how access is granted (e.g. using multi-factor authentication) and enhancing the user experience by delivering single sign-on (SSO) and passwordless authentication.

In addition, a novice remote workforce is likely to increase the demand on IT administration services for events such as password resets and requests for applications required for remote working or to cover employee absences.

Remote access and authentication considerations:

- Can you enable flexible remote working arrangements in the event of a full or partial lockdown? Is the infrastructure in place?
- What application access does the workforce require for remote working? What controls are in place to ensure the devices being used for remote access are themselves secure?
- How are staff being deployed across the business? Have you considered the likely access requirements (access request/approve/assign) to support your business?
- Can you rapidly on-board any new applications, tools and utilities required to support remote working? Will they operate with your current IAM processes or will they need to be managed separately?
- What about your suppliers and third parties? To what extent are they impacted, and will this cause issues with authentication (e.g. what if your suppliers can no longer use their own federation service)?

Recommendations

- Make lowered security and disabled access controls the exception, not the norm. Revisit and strengthen your controls to maintain your risk appetite, solving any underlying issues as a priority.
- Leverage existing investments in cloud infrastructure and platforms that provide MFA and SSO.
- Explore any existing IAM tools and services that provide capabilities for the remote workforce. Tools can now initiate secure privileged connections, perform remote password resets and provide IAM services remotely.
- Consider embracing disruptive technology and solutions. Vendors have responded to the COVID-19 situation with free trials and remote, rapid deployment to support adoption.

2. Adapting IAM processes to support new COVID use cases

Objective: Reviewing and revising policies and procedures to enable rapid access and immediate requirements to support critical business operations.

Many organisations have activated their business continuity plans, having anticipated scenarios where physical sites are unavailable and remote working becomes mandatory. However, few, if any, would have anticipated the scale of the current COVID-19 crisis disruption where entire workforces shift to remote working for an extended period of time, potentially many months. These are new scenarios that have yet to be written in any playbook.

IAM services represent Cyber capabilities at the cross-roads during challenging times that can be either seen as a hindrance to be bypassed or an area of improvement that will provide repeat benefit over time. Therefore, it is more crucial than ever to review and, if necessary, update your IAM processes. This may involve:

- Updating access controls such as developing mechanisms to automate, delay or delegate in the instance of a resource absence.
- Incorporating IAM policies and processes with any new technology platforms/tools deployed to support or extend the remote workforce.
- Updating the joiner process to remotely facilitate identity verification, training and also delivering of assets.
- Updating the leaver process to facilitate the return of assets and to provide assurance that access has been completely removed regardless of the leaver's location and device.
- Improving the ability to on-board and integrate new applications so that business operations can continue and grow.

What are some of the IAM process considerations?

- In the instance of employee furlough, will accounts be disabled (and re-enabled as required) and is there an existing process for this?
- How will the joiner process be impacted if offices are closed and the normal training/induction process cannot be followed? Should the process be changed temporarily or permanently (e.g. should there be changes in the ability to remotely issue digital assets, identity verification, training/induction, access assignments or account password issuance)?
- Should the organisation change other IAM BAU policies (i.e. temporarily disable password expiration policy) to support the wide-scale temporary workforce change?
- How will the leaver process be impacted if offices are closed and line managers unavailable? Will the operations team be more involved, contacting leavers and arranging for the return of digital assets (e.g. in the case of a person who is no longer employed; will the asset still be insured)?
- In the instance where changes are applied to processes, what hygiene operations will be considered to tidy up any temporary access or approved exceptions once normal operations are resumed?
- Have your administration and emergency (break-glass) processes been tested and are they ready for the change in working environment, context and risk?

Recommendations

- Refactor the joiner and leaver processes to extend management of the remote workforce use cases, including the ability to provide secure remote asset delivery/pick-up, user verification and minimise disruption.
- Ensure that you consider as many of the potential impacts on IAM processes as possible before they occur.
- Review your overall readiness to rapidly deploy edge IAM processes, preferably in bulk (e.g. disable users with a furlough status).
- Prioritise IAM process changes, consider any short-term risk factors and create a log of all changes to allow for retrospective update and review.
- Review and consider other areas of cyber defence that may compensate if access controls need to be weakened (e.g. enhance end-point management and threat detection).

3. Continuity of the IAM service against fluid priorities and resourcing constraints

Objective: Support business operational resiliency in a time of uncertainty.

IAM services are crucial to allow response to the circumstances brought about by COVID-19 where staffing and access changes will increase beyond normal levels. Given the fluid and uncertain nature of the situation, the demands on IAM services will at times surge. This may put strain on the IAM team, which may also be facing limited resources and reduced staffing levels.

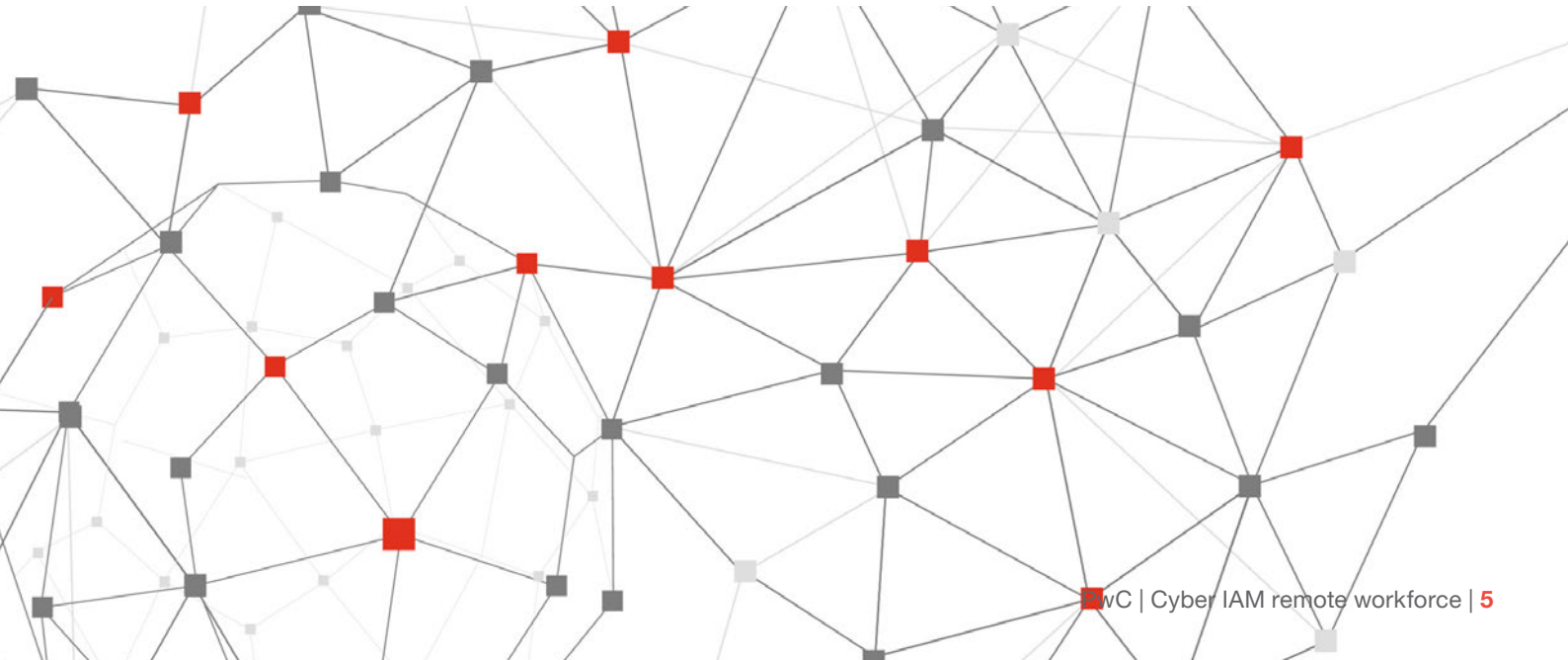
It is important to determine what is essential for your organisation and to prioritise resources. This self-assessment is always a good exercise to undertake periodically, but now it is crucial.

What are key IAM service continuity considerations?

- What is the plan to support the business during any short-term operational changes? After the initial phase of supporting remote working with the required setup of any new access, will there be any IAM service changes (e.g. more focussed access review and monitoring, on-boarding of new assets and identities, improving processes for automation and bulk changes)?
- Are there coordinated activities between the business teams and IT operations to assess any priority IAM demands (e.g. fulfilment for any priority temporary access to applications and data)? Should SLAs for non-essential application access request/approval/fulfilment be relaxed?
- Is there an opportunity to reskill and repurpose resources to support any short-term IAM tasks? Are your run books, tools and guides reflective of any temporary changes?
- Given the increased use of devices and access from outside the corporate network, what measures are being taken to enforce (or retrospectively update) least privilege for the 'essential' access that remains?
- Does the business require a change in control layers (e.g. are preventative controls no longer sustainable with the change in working environment)? Are changes to monitoring and detective controls required?
- How is the business going to address movement (or restriction) of people en masse (due to restrictions on cities/countries) that may effectively prevent key business operations across all parties (onshore/offshore/third parties)? Does this require out-of-the-box thinking to provide alternative approaches?

Recommendations

- Reskill and repurpose resources to support any IAM administration or operational surges and to enable coverage of individuals becoming unavailable.
- Define plans for countries and operations to be suddenly impacted, re-evaluating scenarios to consider a more disruptive impact than before.
- Analyse the impact on any wider IAM resources, including third parties and contractors, and the impact of any lost operations (e.g. first-line call centre, etc.).
- Consider 'pausing' and 'restarting' non-essential IAM processes, such as delaying any new recertification activities, to best support changes to business operations.
- Prepare for the impact of a proportion of the workforce (e.g. 20%) being off due to illness or a large portion of the workforce being largely unresponsive due to other priorities.
- Review the privileged access management (PAM) process. Break-glass processes may rely on physical access to information (e.g. written keys). Consider adapting these processes for remote management.



4. Managing access control risk and compliance

Objective: Managing the potential changes to risk posture as controls are relaxed or new technology is rapidly deployed.

A sudden change often means there is little time to apply your organisation's standard security architecture and controls. In the face of a workforce being unable to perform critical functions, risk and compliance is no longer the top priority.

It is therefore critical to consider the retrospective application of access controls and bring any new technology into the scope of IAM services.

Key access control risks and compliance considerations:

- How and when are you proposing to manage any increased risk that has been introduced as a result of the adoption of 'emergency' technology and tools (e.g. MFA, VPN, collaboration)?
- Are there any relaxed security controls applied to applications or systems for this 'emergency period'? Have the conditions and plans to reapply these controls been defined?
- Are there any operations that typically rely on physical location-based authentication (e.g. password reset operations that rely on validation to verify the user or internal extension callback to communicate the password to the user) that will need to be updated?
- Are there any third party suppliers accessing services from unusual remote connections? Do any risk assessments need to be considered?
- Are there any additional risk impacts associated with fraud or asset loss as a result of the remote operations?
- Are there any increased threats associated with the remote working model?

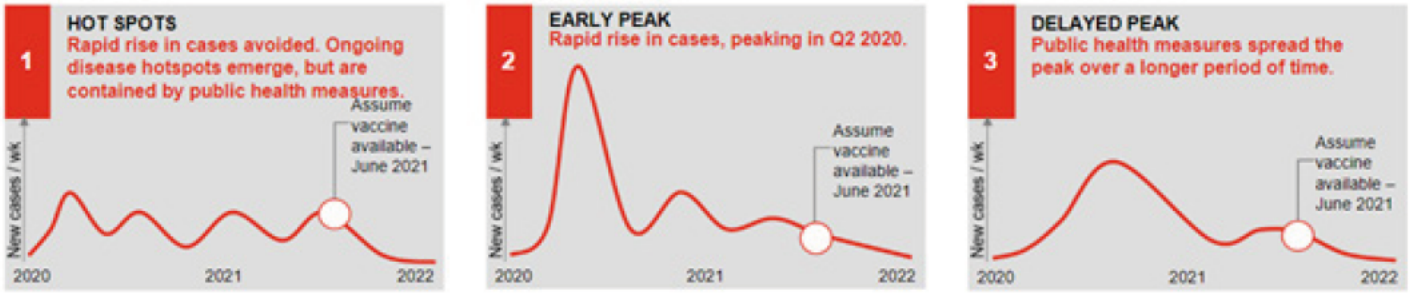
Recommendations

- Cyber threat actors are likely to attempt to exploit any weaknesses presented by relaxed security controls. Therefore, review and retrospectively apply appropriate controls and access management to any new technology deployment, integrating them with the existing IAM services and processes.
- Consider other areas of cyber defence that can help compensate and mitigate where access controls are weakened (e.g. enhance end-point management and threat detection).
- Deploy and/or leverage IAM Cloud architecture to provide authentication and authorisation services to support MFA across critical services, enhance application access management, improve performance and user experience, and reduce costs.

What will be the lasting impact of COVID-19?

The COVID-19 crisis has seen a rapid adoption of remote working. This rapid shift has highlighted the importance of technology investment in supporting a dispersed workforce or, perhaps, highlighted the need for improvements in that investment.

While we hope for a quick resolution to the COVID-19 scenario with minimum disruption, a proper analysis of possible business impacts means we have envisaged three potential scenarios, based on 1) Hot Spots (best case), 2) Early Peak (relatively short period of disruption) and 3) Delayed Peak (longer period of disruption and uncertainty).



The impacts to IAM vary depending on each scenario and are expanded on in this section.

Our approach uses a 3-phase response model regardless of which scenario comes to pass:

- Mobilise – Establishing services.
- Stabilise – Ensuring security controls are effective and new applications hardened.
- Prepare for the future – Embracing disruption in the future.

Stage 1 – Mobilise

Stage 2 – Stabilise

Stage 3 – Prepare for the future

IAM planning and wider priorities to address the COVID-19 scenarios

	One-Off	Rapid Flex	Shift to increased remote working
Mobilise	1. Implement IAM services to support/expand remote access options (MFA/SSO). 2. Acquire **short-term** licenses, perform training and issue communications.	1. Implement IAM services to support/expand remote access options (MFA/SSO). 2. Identify and prioritise **essential assets** and their controls. **3. Disable non-essential access** to minimise threat impacts. 4. Update **view of privileged access for new technology.** 5. Short delay/pause for non-essential controls to support business ops.	1. Implement IAM services to support/expand remote access options (MFA/SSO). **2. Tighten access controls** (e.g. MFA) for untrusted devices. 3. Identify and modify key processes and **streamline or automate.** 4. Perform **access reviews** of key assets (new technology) and revoke access. 5. Short delay/pause for non-essential controls to support business ops.
Stabilise	1. Convert processes and tools to process large **batches of users or unusual loads/use cases.** 2. Define policies, processes and controls for **'Remote' and 'Non-Remote'** Identities as part of workflow.	1. Convert processes and tools to process large **batches of users or unusual loads/use cases.** **2. Review and revoke access** after Initiate phase, retroactively approving access if assigned outside of process. 3. Update access controls for devices, apps & data (e.g. MFA). 4. Permanently update processes (e.g. leavers) to function remotely.	1. Convert processes and tools to process large **batches of users or unusual loads/use cases.** 2. Build **persistent extra operations capability** (e.g. cross train IAM team to perform each other's function). 3. Review plans to expedite usage of **IAM cloud service** (strategic initiatives). 4. Permanently update policies and processes (e.g. joiner/leaver) to **function remotely.** 5. Role management for Remote Workforce.
Stand Down	1. Review and Remediate **temporary access** granted during the operate phase. **2. Stand down** access controls specific for remote working (e.g. conditional MFA).	**Prepare for the future** 1. Define official process for **access** request/approval. **2. Maintain** increased access controls specific for remote working. 3. Review IAM Strategy.	1. Adopt zero trust architecture as overall IAM strategy and architecture. 2. Define official BAU process for remote **access role** request/approval as BAU. **3. Maintain** increased access controls specific for remote working. 4. Define PAM processes and services for remote workforce.

Note: In the case of returning to the old way of working (One-Off), the third phase is based on Stand-Down activities.

Conclusion

Unpredictable and unprecedented events do occur. We've seen that time and again. Such events always have an instant and significant impact on the business, the workers and the processes. Initially there is shock and then a surge of activity, undertaken to simply allow the business to operate; it is important that security controls are retrospectively applied to maintain and improve security on existing and new technology platforms.

Organisations that have invested in cloud-based IAM tools and services, and significantly invested in cyber transformation, are likely to be in a stronger position and experience less disruption. However, regardless of starting position, there are lessons and opportunities for the future.

Lessons and opportunities for improvement

There are a number of lessons to be learnt from this unprecedented disruption.

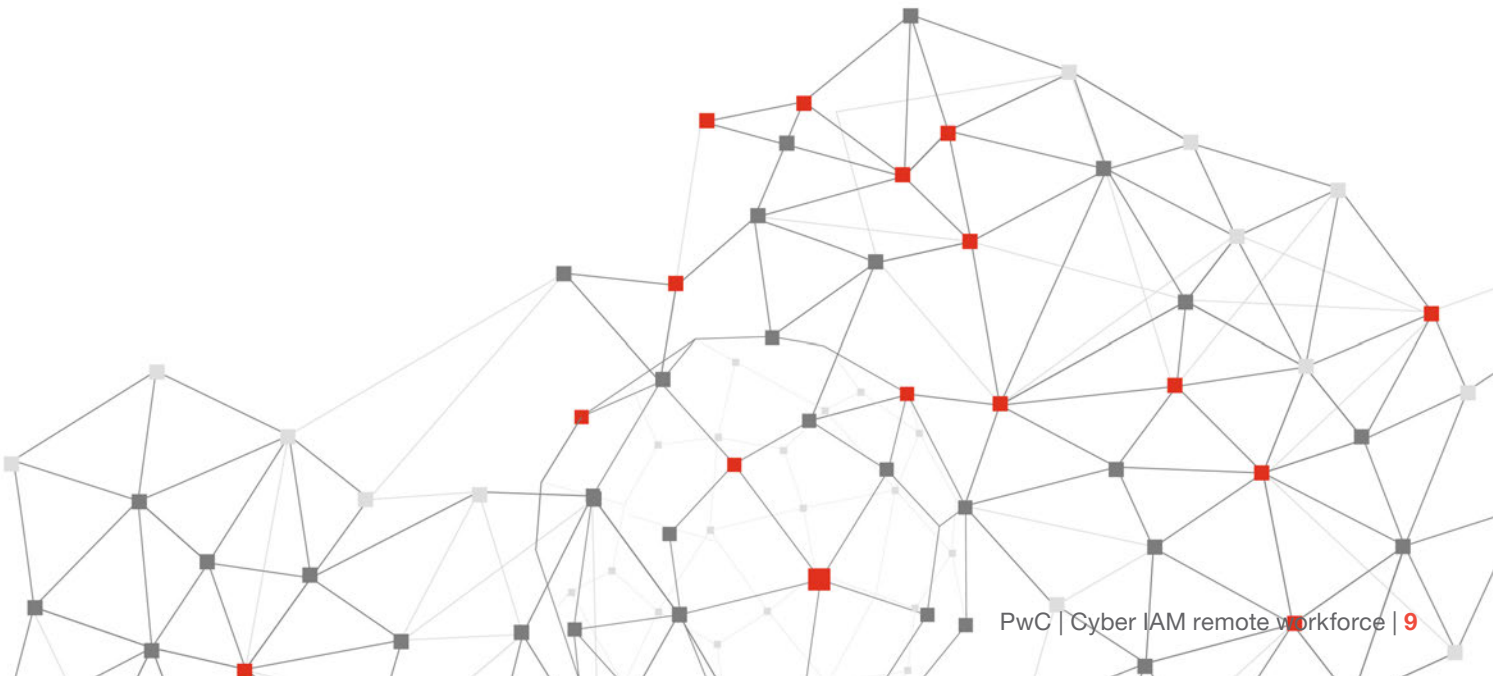
The strategic shift in ways of working, including the remote workforce, are now easier to envisage and the real-world requirements of such an option are becoming clear. Organisations will be better prepared to flex to an entirely remote workforce where and when required (i.e. mandatory controls imposed by Government). It may be possible to transition certain business operations to a higher degree of remote working than had previously been the case. This could reduce office space requirements and costs while potentially improving collaboration across locations and breaking down silos.

The adoption of cloud services and tools can reduce the reliance on internal systems and infrastructure, improving scalability and performance. This new world could expedite the adoption of zero-trust architecture and provide positive disruption, supporting digital transformation and enhanced digital services.

When disruption forces change, lead the change

The unprecedented events have forced change on to many organisations. However, with the disruption comes the opportunity to update Identity and Access Management (IAM) controls, using new capabilities and approaches to not only operate through this disruption but also to provide the foundations for resilient and business enabling access controls.

Whether the remote workforce is the exception or the new normal, a zero-trust approach to security services gives the ability to choose, providing security services capable of supporting either decision. Developments in IAM capabilities are the key to enabling this approach, maintaining security posture while enabling business agility and expansion. It is now possible to automate and streamline access controls and compliance while using risk based analysis to minimise the impact to usability and business activity.



Contact us

Derek Gordon
Identity and Access Management Territory Leader, Cyber Security

E: derek.gordon@pwc.com

Sean Sutton
Partner, Cyber Security

E: sean.sutton@pwc.com

www.pwc.co.uk/issues/cyber-security-data-privacy/services/identity-and-access-management

To find out how PwC UK is responding to COVID-19, please visit:
www.pwc.co.uk/COVID19businesscontinuity

For our latest insights and resources, please visit:
www.pwc.co.uk/COVID-19

2020-05-04_RITM2962456