Madigan
Solutions

SIX SPRINTS TO IAM SUCCESS

Most organisations have embarked on a journey towards Identity & Access Management maturity – few have come close to achieving it. These six sprints can re-energise your identity programme.

SIX SPRINTS TO IAM SUCCESS

All organisations have embarked on some form of journey towards Identity & Access Management maturity – few have come anywhere close to achieving it.

Time, money, and effort have been expended in vast quantities over many years attempting to address what are seemingly resolvable issues. For many organisations, too much time has been spent in the **trough of disillusionment**. However, now is the time to climb that **slope of enlightenment** and reboot your IAM programme and there are many reasons to do so:

- **Audit:** "we suffered a breach and now we have to remediate a bucket-load of weaknesses"
- **Risk Reduction:** "we need RBAC because we have a high turnover of staff"
- **Time to market:** "we need to automate and accelerate the onboarding (and offboarding) process"
- **Integration:** "we love M&A activities, but our IAM platforms don't offer enough support in that arena"
- **Costs:** "have you seen our insurance premiums?"

> While these drivers can certainly renew enthusiasm for your IAM strategy, it should be noted that the cybersecurity world is currently dominated by one phrase: **Zero Trust.**

Madigan Solutions

Zero Trust is the idea that all users, regardless of physical or network location, should have their security posture continuously validated while attempting to access applications and data. And at the core of a Zero Trust strategy is Identity & Access Management.

Indeed, Dr. Zero Trust himself, Chase Cunningham, said:

> "IAM is the gear around which Zero Trust revolves"

Software vendors are clamouring to declare their latest widget to be Zero Trust accredited. But almost everyone agrees that the primary capability of a Zero Trust architecture is focused on **identity** regardless of whether that is a person, service, or device.

The following six short sprints can help push you along your Zero Trust roadmap and re-energise your Identity & Access Management capability:

1. Switch on Multi-Factor Authentication (MFA)
2. Deploy password vaulting & privileged session management
3. Enable comprehensive third-party user management/governance
4. Gain deeper understanding with identity analytics and metrics
5. Finally enable access requests that work for users
6. Take control of risks effectively

Completion of these sprints should, in theory, help you finally reach the **plateau of productivity** and ensure that your IAM capability delights and engenders trusts from your stakeholders.

MULTI-FACTOR AUTHENTICATION

The vulnerability of passwords is well understood. In fact, an oft-quoted statistic states that 80% of breaches in 2019 were password related. Fortunately, one of the best solutions to this problem is also one of the most efficient – the introduction of an additional authentication step.

Multi-Factor Authentication (MFA) can be simple and straightforward. But it is reliant on you choosing the most appropriate method of securing that second step which does not impinge on usability. The key is to ensure that users do not perceive any additional friction in their logon journey.

What will you use to verify that additional authentication step? This will depend on your business model and what works best for your users. Smartphones are almost ubiquitous, but they are not always appropriate for each user type.

This sprint will reveal how you can best leverage MFA to make your business systems more secure.

WARM-UP

Think about what kind of authentication factors would be acceptable to your user community. Comprehensive authentication will validate a combination of something you know, something you have, and something you are.

SPRINT

Roll-out a Multi-Factor Authentication solution for a subset of users accessing some key critical assets.

WARM-DOWN

Review what worked well, what was problematic for your user community, and how you can best tailor your MFA provider solution to meet your stakeholders' requirements.

Madigan Solutions

THE WARM-UP

To lay the groundwork for your MFA roll-out you will need to consider the following:

Where is your greatest risk of exposure?

Determining your current risk posture will involve a conversation with your risk management team (or equivalent). They will confirm any regulatory or compliance requirements for your industry and where your biggest risks lie. Factors that determine your exposure to risk include having a high number of remote workers or a requirement for secure access to data in the cloud.

Employee or consumer?

There may well be a recognised (and pressing) business requirement or risk that will dictate which user community your address first but, in general, your consumer community will be an easier sell to the powers that be. Consumers generally have their own smartphone device, and their authentication journeys are much more straightforward than those that employees have to endure.

How 'computer literate' is your user group?

This may seem an odd question in the second decade of the twenty-first century. However, it is well documented, if not widely acknowledged, that there are user groups who either do not have the means or the inclination to be part of the information 'revolution'. Should they be denied access to your services? You may find yourself in legal hot water if you do deny them access. Therefore, consider how you might provide alternative means of continuing to do business with your organisation for those users for whom a Multi-Factor Authentication mechanism will seem like a barrier.

What device?

If you are to use the 'something you have' approach to stronger authentication then you need to think carefully about what that thing actually is. Despite the ubiquity of smartphones, you may have users who do not own one or who will be reluctant to use a personal one for work purposes. Therefore, will you issue devices? And if so, you will need to consider how to handle lost devices and how a user should be able to reset their second factor.

OTP or authenticator app?

OTP to SMS or email is not as secure or reliable as the use of an authenticator application, which should be encouraged, if possible. Some of the 'big players' who provide an authenticator application include Microsoft, Google, IBM, and Duo and they mostly operate and behave in a consistent and intuitive manner.

Allow choice?

Some users, particularly the more tech savvy will welcome being able to choose which authentication method they use for their second factor. Tools such as IBM Security Verify allow administrators to open up (or limit) a wide range of possible MFA mechanisms including the use of FIDO2 devices such as Windows Hello.

Biometrics?

Many people are still sceptical about sharing biometric data. If you decide to go down this path, then you will need to understand where the data will be stored and how will it be accessed. If you are relying on the use of personal devices, you will need to consider whether your users have a device compatible with using this technology.

THE SPRINT

Now you have answered the questions above, what subset of users did you choose for your sprint? Often, IT managers will start with remote workers or those accessing high risk applications.

Tools like IBM Security Verify allow you to pilot with a clearly defined subset. The wizard-based setup will allow you to tailor the user authentication journey in line with the points considered above. Defining a policy enforcement rule is simply a matter of selecting your user community, picking the application they are attempting to access, and presenting them with a list of appropriate MFA methods to help them fulfil their authentication requirements.

But policy definitions can go much further than this. You can create a policy that will take a context-based approach to enforcing MFA. For example, if a user is attempting to access a critical application from a trusted device, on a trusted network, you may decide that MFA is not required and adding friction to the user journey is unnecessary. If the user, however, is using an unknown device in a geographical location that is outside your normal jurisdictions, then you probably want to mandate a stronger level of authentication.

The days of having to code this logic are no more. Point-and-click operations are all that are required to implement your policies.

And there's more. Existing access management systems can play nicely with your MFA provider. In other words, you can deploy MFA capability to your legacy applications and give them a modern authentication mechanism without the need to completely rip out your existing access management service.

Providing you've managed to get all the answers you needed in the 'warm-up', your MFA tool of choice should be capable of doing all the heavy lifting when it comes to configuring your policies and workflows.

THE WARM-DOWN

Your sprint will have been a success and now is the time to consider to whom you next rollout your service or for which applications you want to add an additional layer of protection.

If you're feeling really confident (and why wouldn't you), then setting up adaptive access controls is a logical next step. Not only is this flexible but it enables a better user experience. Adaptive access controls look at a number of contextual parameters and automatically make a decision based on predefined criteria such as geography, IP routing, time of day, device, behaviour.

In short, a context and risk-based approach to introducing friction to the logon journey can be appropriate. Removing friction when you are confident that the context suggests low risk will be greatly appreciated by your end users. If the user is presenting a scenario that is the same as every day for the last six months, then it's highly likely they are who they say they are and it is low risk to allow them to go about their business without further interruption.

TAKE CONTROL OF PRIVILEGED CREDENTIALS

Could you say how many privileged systems and accounts exist in your organisation right now? Do you know who has access to what, when and (more importantly) what they are doing when they are in there?

Passwords are vulnerable and shared passwords are an accident waiting to happen. How can you protect your most privileged accounts and how do you mitigate against the potential threat posed by inside users?

Within this sprint, you should aim to:

- Create a centralised view of privileged credentials via discovery
- Vault those privileged credentials
- Identify privileged users who require access to those credentials
- Optionally, switch on session recording for privileged credential usage

Ultimately, taking control of your privileged credentials can provide a tick in the audit box by demonstrating you are heading in the right direction with regards to establishing a principle of Zero Standing Privileges (ZSP).

WARM-UP

The warm-up phase to this sprint should be used to discover privileged servers and privileged credentials. It should also be used to identify those individuals who require access to privileged credentials as part of their job function.

SPRINT

Within the sprint, you will be able to deploy a PAM solution, automate the discovery of your assets, construct business processes for requesting access to privileged credentials and enable session recording for privileged access.

WARM-DOWN

The warm-down phase allows you to bed in your new processes ready for a BAU approach to privileged access management including: ongoing monitoring, education, and adoption across your organisation.

Madigan Solutions

THE WARM-UP

Even without a privileged access management tool, there is a certain amount of discovery that should be undertaken. Who is a privileged user? What is a sensitive system? What are privileged credentials? How are privileged credentials currently assigned and used? What regulatory compliance are you subject to?

With the right tool, the discovery of servers, applications, privileged credentials, and privileged users can be automated. You may even unearth some sensitive access rights that have been granted without your prior knowledge!

With the discovery information at your fingertips, you will be able to identify where the highest business risk exists and establish a priority list for switching on privileged access management controls.

You should also consider the kind of access request rules you want to enable. Most tools will have a rules-based wizard with best practice rule definitions provided out-of-the-box. These will cover things like: who has access to vaulted credentials, how are vaulted credentials checked-out by a privileged user; how are privileged credentials to be used; how are sessions initiated; how are sessions recorded and retained.

THE SPRINT

A tool such as IBM Security Verify Privilege Vault (ISVPV) provides the necessary functionality to address the needs of a PAM sprint and the SaaS version is perfect for a Proof of Concept.

Discovery is a point-and-click affair and can be as targeted as you need for the purposes of your sprint. Ideally, you will tackle a service and a set of privileged credentials that are used by a team of users who are sympathetic to your goals and can help you derive value and a base line for a suite of BAU processes.

You should vault credentials, define credential rotation rules, and enforce password complexity rules which go beyond any default policy you may have for end users.

The sprint should also define credential check-out rules including any approval processing required. You could switch on integration with your favourite service management tool to ensure tickets have been raised in advance of any request for check-out.

And of course, there is the session launch sequence that should be defined. Most PAM tools provide launchers, such as SSH Terminals or RDP handlers. These can even be configured in a manner that forces recording of privileged sessions for future forensic analysis.

A comprehensive suite of reporting tools is normally provided out-of-the-box – ISVPV has almost 100 such reports plus a comprehensive engine for developing custom reports, should they be required. The sprint should identify a core set of useful reports and have those shared with key stakeholders.

THE WARM-DOWN

The warm-down should analyse the success of the sprint, garner feedback from the key stakeholders involved in the sprint, and work out a plan for rollout to a wider community.

Don't underestimate the impact a PAM solution will have on privileged users. It is only natural for people to be resistant to any programme of change, but the barriers that will be placed in the way of privileged users will result in significant grumbling. Every effort must be made to ensure that the privileged users truly understand the need to put those barriers in place. They need to understand that control and risk reduction are imperative.

The warm-down process should also attempt to identify any future third-party system integrations that would be beneficial such as:

- Security Incident & Event Monitoring (SIEM) integration of security event monitoring
- Multi-Factor Authentication (MFA) provider integration for strong authentication into the PAM service
- User Behaviour Analystics (UBA) integration for AI analysis of user behaviour
- Identity Governance & Administration (IGA) integration for formal processing of the creation of privileged user accounts

Finally, most organisations fail to produce a response plan should a privileged account be compromised. Many organisations are even unaware of the risks of such a compromise. The implementation of a PAM solution can go a long way to preventing such a compromise, but that certainly does not negate the need for a response plan. Write one now!

THIRD PARTY USER MANAGEMENT

It is hard to imagine these days, but there was a time when access to enterprise systems was restricted to staff only. Today, enterprises expose their systems, applications, and platforms to trusted third parties on a regular basis. But those third parties need to undergo some form of vetting, periodic review, and ultimately, have their access denied when it is no longer appropriate for them to interact with your enterprise systems.

HR do a pretty good job of managing the state of employees. In most organisations, however, the HR function refuse to take on the management of non-employees. In other words, for most organisations, there is no such thing as a single authoritative source of identity information for non-employees.

How can these third parties be managed in an effective way for my business? This is becoming a more pressing question as demands for access, streamlined procurement, and management increase.

Madigan Solutions

WARM-UP

Work out the type of relationships you have with non-HR managed users. Who are they? What identity types or persona need managing? Where do they come from? What rules govern the life-cycle of their relationship with you?

SPRINT

Get access to a third-party User Management Tool hosted as a SaaS offering with many out-of-the-box features to help you take control of those users for whom an authoritative source of identity information may not be available.

WARM-DOWN

Reflect on your PoC and work out how the tooling can be integrated into your existing BAU processes for identity governance and management.

THE WARM-UP

How many non-HR managed users do you have in your organisation? What type of user are they? Which departments are responsible for the various user types? The following persona definitions may help you answer these questions.

Staff Augmentation Suppliers

Many organisations outsource certain aspects of their business operations to suppliers who are trusted third parties. Contracts will be in place; due diligence will have been completed; and those suppliers will be included on the Preferred Suppliers List or PSL.

It is commonplace to find business operations such as HR, Call Centre, IT Infrastructure & Hosting, or IT Development being outsourced to third parties. In many cases, those third parties are supplying a significant number of people to address the tasks at hand.

Similarly, many organisations regularly dip into the contractor market to augment their staff.

B2B - Purchasers

As part of the B2B purchasing and service consumption process it is now common for buyers of your services to need to interact with some of your critical assets. They may need access to re-ordering systems, for example.

Tenants

There are organisations who have prime real estate, elements of which they may sub-let to tenants. In many cases, those tenants may require access to the letting organisation's network, systems, and/or physical security platforms. Universities are a great example of organisations that will have commercial enterprises taking up tenancy agreements to get access to research students.

Guests & Work Experience

Many organisations offer short-term work experience placements to students in secondary education. These placements may require both physical and logical access to systems meaning a requirement exists to manage the extremely short-term life-cycle of such users.

Students on a work experience placement programme are limited to a maximum of 2 weeks of experience under UK law. While this may be deemed short-term, it isn't quite as short as the access required by guests, i.e., those people who turn up for a conference or a meeting. In these instances, an organisation may want to offer access to a guest network and potentially restrict that access to specific locations throughout their premises such as meeting and conference rooms.

Non-Human Entities

The point of the HR system is that it manages the life-cycle of Human Resources who are directly employed but non-human identities already outnumber human identities- and by quite a multiplier. Taking control of your system and service accounts, robots, and Operational Technology (OT) has become more relevant as bad actors turn their attention to these identity types in their attempts to find a back door route into your systems.

Once you have established the user types you are dealing with you will need to review their existing access arrangements.

And finally, are there any persona-specific life-cycle rules you need to adhere to? Your risk and compliance team may have something to say about this.

THE SPRINT

Third party user management functionality is rarely provided as an out-of-the-box feature of Identity Governance & Administration software. Configuring IGA tools to add the necessary data input screens and life-cycle rules is something that needs to be accounted for from a total cost of ownership perspective. Worse still, some of the big players in the IDM/IGA space don't provide a means of configuring their software to address third party needs at all!

But a dedicated third-party management tool does exist in the marketplace – and it is offered as Software-as-a-Service. Madigan's UMT is available as a free trial, specifically to fit into a sprint that can address the following use cases.

Use Case 1 – User Creation

Who in your organisation should be capable of creating a user record for a third-party user in your systems? And should the distribution of this administrative capability be identity type specific?

Ideally, Department Managers should undertake the administration of contractors/consultants who report to them. However, some form of approval process might be needed to ensure a relevant purchase order is in place, for example.

For tenants who rent office space in your buildings, it might be more prudent to delegate that responsibility to a tenant administrator.

Use Case 2 – Continuous Review

When we talk about continuous review, we are not necessarily talking about the periodic certification of access rights. Instead, we are reviewing whether the user should continue to be regarded as an active resource.

Contractors normally have both contract start and end dates, but contractors (and organisations) can terminate such contracts early. Any system put in place to manage third-party users should have the ability to constantly ask the question of third-party user administrators: "does this person still have a contract?"

Use Case 3 – Off-Boarding Process

A contract end date is a great date to flag a third-party user as no longer existing and it can be used to trigger the process of removing that user's access rights. Similarly, a contract end date with an over-arching supplier (like a staff augmentation provider) can also be used to trigger the automatic removal of access rights for all identities associated with that supplier.

Supplementary Use Cases - Life-Cycle Rules & Automation

Why should life-cycle rules require development by someone with a degree in Computer Science? There is very little excuse for a modern-day platform to require an administrator to develop a life-cycle rule in Java or JavaScript or VB Script or PowerShell. Therein lies the path to technical debt, after all.

What do life-cycle rules look like and what should you consider implementing? Here are some simple examples that can provide instant benefit:

Trigger or Event	Action
User contract start date has been reached	Set user status to ACTIVE Send alert to Department Manager or Owner
User contract end date approaching	Send alert to Department Manager or Owner
User contract end date reached	Set user status to INACTIVE Send alert to Department Manager or Owner
Organisation contract end date approaching	Send alert to Organisation Owner
Organisation contract end date reached	Set all associated users' status to INACTIVE Set organisation status to INACTIVE Send alert to Organisation Owner

The UMT service provides these rules out-of-the-box, but the platform will allow a suitably authorised administrator the ability to create their own rules.

WARM-DOWN

After running a successful PoC, it is time to reflect on what has been achieved; what worked well; how rules and the creation of third-party entities and user types can work for your business; and crucially, work out how the tool can augment your existing identity governance solution.

Remember, HR is authoritative for employees. There's no reason why a Third-Party Management tool can't be authoritative for all those users that fall outside of the HR processes.

IDENTITY ANALYTICS

Everyone loves a dashboard. They look pretty and a picture tells a thousand words. Apparently.

Your identity governance platform should allow you to automate your user onboarding, provisioning, and life-cycling but this is not enough. You need to prove how effective those processes are and how that effectiveness can be compared against your Key Performance Indicators (KPIs).

Out-of-the-box reporting ought to go a long way in helping you better understand your identity posture. The IBM Security Verify Governance platform ships with over 100 such reports out-of-the-box with a Report & Dashboard Designer module enabling you to create bespoke reports.

With this you should have all the data that you are likely to require to produce effective reporting against your KPIs.

WARM-UP

Review of the current reporting and analytics. Validation of mandated default suite of reports – are they configured, published, and scheduled?

SPRINT

Get more relevant information from the data you have at your disposal. Expand upon your default set of reports. In addition, introduce mechanisms to glean more meaning from the information allowing you to better understand your risk exposure.

WARM-DOWN

A review of your new analytical posture and definition of a roadmap for pushing adoption of the new-found information to your key stakeholders.

Madigan Solutions

THE WARM-UP

What information might you need to delight your key stakeholders and auditors?

What information are you currently exposing to your stakeholders? It is likely that the following reports are being generated:

- **User Metrics:** Number of active/inactive users by user type
- **Orphan Metrics:** Number of unmatched or orphan accounts by provisioning target
- **Dormancy Details:** Active accounts that are seemingly no longer used
- **Status Mismatches:** Details of inactive or suspended users who continue to have active accounts
- **Entitlement Details:** A breakdown of entitlements and the business unit within which they are available
- **Expiring Users:** A list of those users who will shortly have no further relationship with your business

If you find that you are not currently generating these reports, then do so immediately. They ought to be very straightforward to create, publish, and act upon.

These reports should be considered a baseline, and ought to be available in your identity arsenal by default.

THE SPRINT

Re-enforcing your identity armoury over a two-week sprint should be within your capabilities. For most IGA tools reporting can be added to as a BAU process. You should think seriously about tackling the following:

Timeliness KPIs

- **Average time to onboard:** the time it takes between an identity record appearing, the relevant downstream accounts being created, and the correct entitlements being assigned should be captured and reported on. For a fully automated platform, the timeliness is likely to be recorded in minutes and seconds. More important, however, is the capture of the time taken for those processes requiring manual intervention.
- **Offboarding effectiveness:** the time it takes to ensure that all downstream accounts have been either disabled (and entitlements removed) or deleted following a user's end date being reached. Access should, in theory, be revoked on the same day that the user leaves the organisation.

Cost Reduction KPIs

- **Automation v Manual Fulfilment:** The automatic assignment of entitlements because of some birth-right entitlement rule is much more cost-efficient than having someone on the Service Desk responding to an entitlement request ticket. Now is a good time to gain insight into how entitlement fulfilment is being achieved. Break down the analysis by automatic fulfilment, manual fulfilment via the IGA tool, or (heaven forbid) manual assignment in the provisioning target.

Risk Analysis KPIs

- **Entitlement drag analysis:** Many organisations have historically allowed users to move around the organisation without reviewing the entitlements they take with them. It should be easy to run analysis on the effect of that drag and at least begin the process of drag remediation. For example, why is there someone in the Marketing Division entitled to 'Close the General Ledger'?
- **Peer analysis:** The ability to identify those people who have unusual assignments compared to their peers could be crucial in minimising the attack surface in your organisation.
- **Approver analysis:** Was access to systems approved by someone who no longer works in your organisation? If so, maybe it is time for that access to be reviewed.
- **Status mismatch analysis:** Just because an identity record is flagged as being inactive doesn't mean that the accounts associated with that identity record are also inactive. They ought to be. But what happens if they are not?
- **Entitlement assignment frequency:** If someone is having their assigned entitlements updated frequently, should that sound the alarm bells? Probably. Most users in an organisation ought to have a consistent set of entitlements after all.

The IBM Verify Identity Analytics platform can rapidly add comprehensive dashboarding capabilities regardless of the IGA suite that you have managing your identities. In other words, you don't have to be an IBM Security Verify Governance customer to get benefit from the analytics platform.

The dashboarding includes:

- Recommended actions
- Top Violations
- Top Risky Users
- Top Risky Applications

THE WARM-DOWN

With the relevant reports to hand, now is the time to review the information you have and determine its relevance. You can make tweaks as needed and work out a mechanism of delivering the information to your key stakeholders, equipping them to make better informed decisions.

ACCESS REQUESTS THAT WORK

Several years ago, identity governance tools were seen as a panacea for enterprises. These tools were sold as a silver bullet to the problem of who has access to what. The truth of the matter is that while the tooling did have that technical ability, it required a little more business analysis and configuration effort than organisations could spare. Automation of joiner and leaver processes was successful, but the well of enthusiasm was often dry by the time it came to enabling end user access requests. The Service Desk were left to pick up the pieces.

What end users really want is frictionless access to the platforms and systems they need to access to fulfil the requirements of their job. No blockers. No painful processes. Business owners want to ensure access requests are fulfilled smoothly and efficiently and there is no risky over-entitlement.

Madigan Solutions

WARM-UP

Determine your current entitlement estate, and the business processes you have in place for requesting entitlement assignment.

SPRINT

Perform a role discovery exercise followed by publication of those roles. As part of the publication process, you should determine whether the roles (or any other lower-level entitlement) can be automatically assigned to users to streamline your processes or if manual request processes need to be built. For the latter, re-certification of access rights needs to be deployed.

WARM-DOWN

Establish a set of BAU processes for ongoing role discovery; management of roles and entitlements; a means of re-certifying the structure of entitlements; and re-certifying their assignment to users.

THE WARM-UP

Review your current suite of entitlements and the existing processes for requesting and assigning those entitlements.

Users want access when they need it. They don't want to request access only to find that the approval process injects unnecessary delay and is then followed by a vexatious manual entitlement assignment process.

Manual processes may be fine for micro-organisations, but at scale, they fail. Failure results in frustration. Frustration results in people trying to find a way around processes. By-passing processes results in increased risk. Everyone's a loser – contrary to what Hot Chocolate had to say in the 1970s.

A clearly defined role model with a means of requesting, approving and (ideally) automatically provisioning access above and beyond birth right entitlements is achievable!

THE SPRINT

If you already have a well understood suite of entitlements and you have managed to roll them up into Business Roles, give yourself a pat on the back. Not many organisations have achieved that!

If you haven't, the first step in your sprint ought to be running a role mining activity. Many governance tools are provided with such capability and with good quality datasets, they can unearth candidate roles very quickly.

Once the roles have been mined, it's time to publish them. Optimally, you will do so in a way that means that many are automatically assigned to users because of attributes associated with those users.

Birth-right entitlements are fabulous, but a process should be put in place to periodically review those entitlements to assure they continue to be appropriate.

For the next stage you will need to build request workflows for entitlements that cannot be automatically assigned. The key here is to keep it simple! Often, there is a temptation to build overly complicated workflows and approval processes. In most cases, this is unnecessary. Keep those steps to a minimum, otherwise fulfilment time-scales are going to look a little crazy.

Just as birth-right entitlements can be automatically assigned to users, they can also be automatically unassigned. The same rule could potentially be applied to requestable entitlements. However, these requestable entitlements will need some form of periodic review. Now is the time to configure an Access Certification review which will enable you to demonstrate how recurrent certification campaigns can be used to limit entitlement drag.

THE WARM-DOWN

Role mining should not be considered a one-off exercise. It should be repeated regularly to ensure there are no candidate roles lurking about in your infrastructure.

Delegate the process of access request and approval workflows to an appropriate service management tool, such as Service Now. The APIs in your Identity Governance tool ought to allow for such externalisation to provide a consistent IT Service Request process to your users.

And finally, now you have your access recertification review in place you should also establish a BAU process for looking at the structure of entitlements. Business roles evolve over time and should be reviewed regularly to ensure that they are still relevant.

EFFECTIVE RISK MANAGEMENT

Do you understand your current risk exposure? Do you know what your users are entitled to do with your systems and data? Do you know which users and departments carry the most risk? Do you have a Zero Trust approach to run-time verification of access rights?

One of the primary drivers of an identity programme is the concept that risk can be dramatically reduced, but is such a reduction ever realised?

WARM-UP

We have six questions that you need to ask yourself and your stakeholders.

SPRINT

You will determine risk at runtime and enforce adaptive authentication & authorisation controls. Determine risk at provisioning/discovery time by analysing your entitlement assignments and apportioning mitigating controls.

You will need help from your friendly auditors and the CEO's office although starter-kits are available to get you going.

WARM-DOWN

Having demonstrated that an effective risk management strategy can be applied to your identity governance processes, work out a plan to extend that strategy to cover your entire organisation – or at least those divisions and departments that would most benefit from the process.

Madigan Solutions

THE WARM-UP

Perform a quick inventory of your estate and ask yourself these questions:

- What sensitive applications and data do we have in our organisation?
- What user types do we have that access those applications and data?
- What networks do those users traverse?
- What end points do those users use to access our services?
- Can we adequately classify our applications and data and rank them by risk?
- Can we assign ownership of those risks to someone who has the authority to define mitigating controls?

THE SPRINT

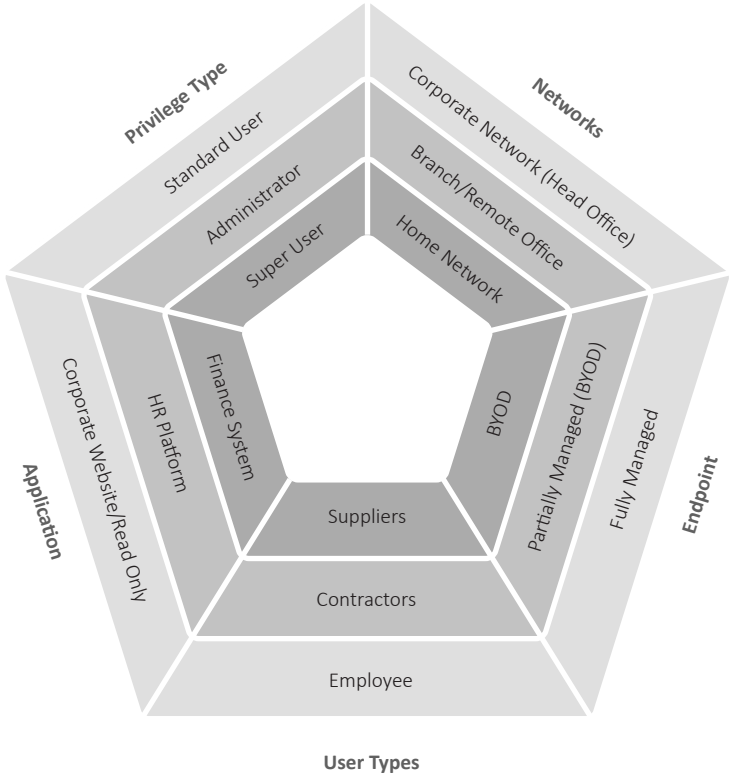
Enforce adaptive authentication & authorisation controls

These days, configuring the access controls necessary to adequately manage your risk posture is much more feature-rich. Adaptive authentication features, such as those provided by IBM Security Verify, are commonplace and provide a means of taking context into consideration when applying security controls.

During authentication, consider the following contextual factors:

- the user or user type initiating the request
- the endpoint device being used
- their network location (including geography)
- the privileges they carry
- the application or data elements they are trying to access.

Each metric will affect the risk associated with the access request. That risk can then be used to determine whether the access request can be approved or denied; whether the access request needs stronger authentication controls to be applied; or whether the session needs to be monitored/recorded for future forensic analysis.



It used to be that writing a strong authentication policy and chaining authentication policies together required significant coding or redirection handling. But modern access management services make it easy. Wizard-based services allow for policy definition in a natural language format. In short, a computer science degree is no longer required to define authentication policies.

Your goal should be to implement a simple Multi-Factor Authentication flow for a subset of users accessing legacy systems. An authenticator app, FIDO2 device or even TOTP delivery via SMS or email should suffice.

Define entitlement risks and mitigating controls

An entitlement is any data object assigned to a user/account which grants them the ability to perform a system function or access a data object. For many systems, such an entitlement will be a group or a role. For others, the authorisation decision may depend on other attributes associated with the user/account such as the security clearance held by the user, their department details, or in the case of certain government departments, their nationality.

To complicate matters further, it might be a combination of group memberships and attributes that creates the entitlement.

Many IGA tools have struggled with this concept in that the definition of risks and the definition of toxic combinations of permissions has been limited to business roles. However, business roles evolve over time and users in your systems may be assigned entitlements that generate a risk without ever having been assigned the business role.

Defining at least one entitlement risk and an associated mitigating control is achievable within a sprint. To do that, however, you need to speak to your friendly Risk Analyst to get a real-world example of a risky business function and what a mitigating control might look like.

You then need to speak to your friendly System Administrators to work out which set of permissions on their systems provide a user with the ability to perform that function.

Then you need to map the risk and the permissions together. Take note, though, we aren't talking about business roles here because the intention of a business role in 2022 may have no bearing on what it is being used for in 2023, despite your best intentions. In other words, risk assignment should be based on what a user can do rather than what you intended them to do.

If you already have IBM Security Verify Governance, your life is made easier when it comes to defining risks and mitigating controls. If not, speak to someone to arrange for a live demo using a dataset that you provide to see how it can work for you.

THE WARM-DOWN

The American Productivity & Quality Centre (APQC) have developed a wide range of business activities for many vertical industries. It's a great place to start when defining the tasks that can be undertaken within your business. Now is the time to work out how best to extend your risk management process to cover all those risky tasks, assign ownership to those risk definitions, and work with those owners to help define mitigating controls that are meaningful.

THESE SIX SPRINTS, SPREAD OVER A SIX-MONTH PERIOD, WILL BREATHE NEW LIFE INTO YOUR IDENTITY & ACCESS MANAGEMENT PROGRAMME.

For a demonstration, more information, or assistance, speak to the team at Madigan Solutions:

- **Email:** sixsprints@madigansolutions.com
- **Phone:** +44 333 242 2889
- **Web:** www.madigansolutions.com
- **LinkedIn:** mdgn.me/linkedin
- **Twitter:** mdgn.me/twitter

Madigan Solutions