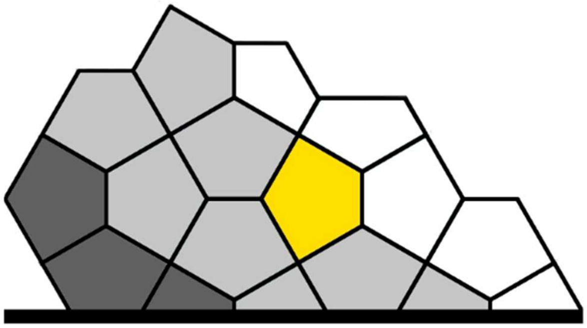
Identifying and Managing Risk with an Identity Governance Platform



A Madigan Solutions White Paper

ABSTRACT

The ability to quickly identify segregation of duty access risks and manage/mitigate against them is a key consideration for any organisation aiming to ensure compliance regulations and governance standards are met.

All major enterprises have some form of risk management process and controls in place. If a business wants to be sustainable, have a future and grow, then it needs to be able to identify various types of risk and act on them accordingly. Access to IT systems and applications that perform business critical processes, so employees, end-users, etc can perform job functions also present a risk to the business if the wrong access has been granted.

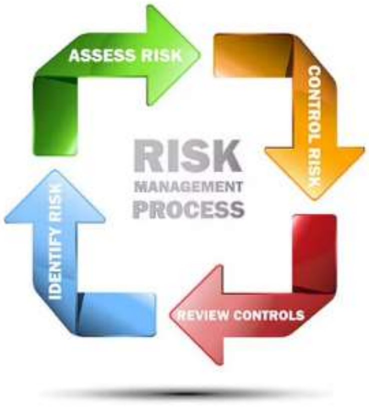
This white paper will review Risk Management and Segregation of Duties compliance, how they pertain to IT systems and application access, and the challenges for implementing risk management analysis and controls.

WHAT IS RISK MANAGEMENT?

At its most basic, risk management is the process of identifying, assessing, controlling and reviewing risks.

Governance, Risk and Compliance are not new concepts to organisations. Companies have been managing these for years, particularly in highly regulated industries such as Pharma and Financial Services.

GRC concepts can be applied to IT applications and systems in all organisations. Assigning incorrect access rights to a job-critical application or system can either hinder an employee from completing their work or create a situation where someone has too much access. In the case of the latter, it can lead to a possible single point of failure, a conflict of interest or exposure to error and fraudulent activity. No organisations are immune to threats of this nature.



RISK OF NO RISK MANAGEMENT

Without any risk management processes, organisations leave themselves open to compromise and vulnerabilities.

IT access right assignment failures may initially seem to be limited to the individual level but without the proper oversight, control, and remediation (or mitigation), the repercussions could have a much wider impact.

The consequences could be far-reaching, such as:

- **Fines and Penalties**
- **Reputational or brand damage**
- **Redundancies or closure**

DO RISKY ASSIGNMENTS EVER BENEFIT AN ORGANISATION?

The short answer is **no**.

Risks describe potential weaknesses within the organisation. They highlight vulnerabilities. The also suggest failings such as:

- **Areas within an organisation or department where checks and balances are not being carried out appropriately.**
- **Work practices that could be in contravention with existing compliance regulations.**
- **Incompatible or inefficient organisation structure or reporting lines.**

It captures where positive change is needed, where loopholes can be closed and where pressure points can be eased. It can help share the burden, assign responsibility and accountability proportionately and possibly relieve stress from resources. Having the means to identify and act on risks and breaches is beneficial if the risks are properly mitigated or remediated.

CHALLENGES

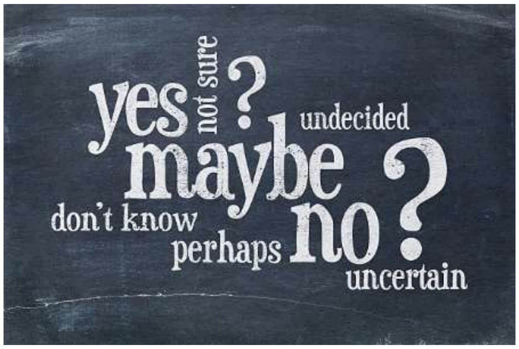
Identification

Access to IT services has historically been based on Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). Roles can be further broken down into access groups, permissions, and attribute settings. Regardless of the terminology used, they all amount to what can be grouped as entitlements.

Auditors, compliance officers, and risk managers are not going to have knowledge of how these entitlements are being used across the organisation (and should not be expected to). Given the sheer volume of data that can be associated with entitlement, the task of categorising them and defining risks associated with them can become quite complex.

Those that identify and manage risk need to be presented with data that is coherent, easy to understand and can be used to form risk definitions that make business sense.

Assessment and Control



While the risks may be identified, who is best placed to assess, manage, and mitigate them? The audit and compliance departments may have identified and categorised the risk, but the application owners and business line managers must be involved in any remediation or mitigation process.

They are the ones who will need to decide if the end users require the access, have the correct access or if access should be revoked.

The Ecosystem

As more and more organisations transition from on-premises managed IT systems to cloud based services, the ability to control and manage access and administration function becomes more complex. This in turn increases the risk of violations as more end-users are onboarded or request access to these systems. Added to this is the multitude of ways where end-users interface with corporate systems:

- **Where** (home, office or in transit)
- **What** (work or personal Laptop, hand-held devices)
- **How** (username and password, multi-factor authentication, federation, biometric – physical or behavioural, etc).

The Known Unknowns

A proliferation of access rights, privileges and permissions can evolve naturally over the course of time. New applications, Merger & Acquisition activity, system migrations and the promotion of personnel can lead to *entitlement drag* and a growth in entitlement data which may be viewed as unmanageable. It can seem chaotic and unstructured and may need to be "mined" regularly to capture new candidate roles and restore order to the madness. In turn, these new roles will need to be risk assessed – a time-consuming activity.

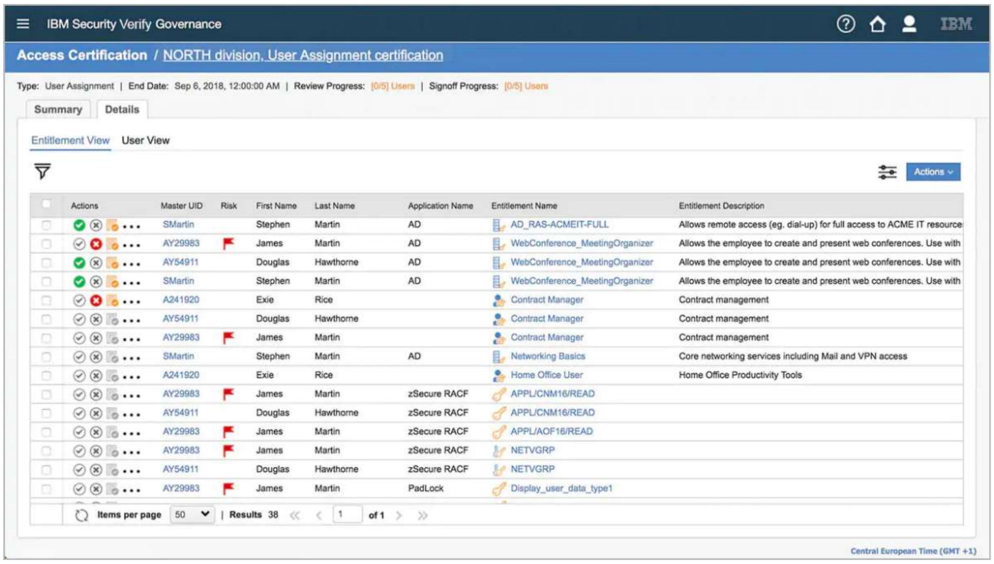
Consequently, the main stumbling blocks to having an effective IT Risk Management process is the ability to define risks, identify risk violations and act on them quickly. But even when risk violations have been identified, there is the need to present this information in a format that is understood. Plus, there are the competing interests of ensuring that access to business-critical applications is provisioned effectively while continuing to ensure that risk management analysis protects your business.

SUMMARY

Risk Management should not be an inhibitor to doing business. Instead, it should be supportive of business needs. **IBM Security Verify Governance** (**ISVG**) can aid auditors and risk managers to drive improvements in GRC processes to meet regulatory requirements. It uses the concept of 'Business Activities' rather than roles and entitlements to identify key business processes and functions. These business activities offer the following benefits:

- Written in terms that are easy to understand. (Role and entitlement names are often meaningless or open to interpretation).
- Can be pre-loaded into ISVG based on the type of organisation.
- Risk modelling is more intuitive as it is based on what an individual can do with the entitlements they have been assigned.

Determining what an individual can do and validating that against risk definitions can result in *risky* individuals being highlighted in a more meaningful way. In effect, a red flag can be raised (almost literally).



Access Certification / NORTH division, User Assignment certification

Type: User Assignment | End Date: Sep 6, 2018, 12:00:00 AM | Review Progress: [0/5] Users | Signoff Progress: [0/5] Users

□	Actions	Master UID	Risk	First Name	Last Name	Application Name	Entitlement Name	Entitlement Description
□	✓ ✗ ...	SMartin		Stephen	Martin	AD	AD_RAS-ACMEIT-FULL	Allows remote access (eg. dial-up) for full access to ACME IT resource
□	✓ ✗ ...	AY29983	⚑	James	Martin	AD	WebConference_MeetingOrganizer	Allows the employee to create and present web conferences. Use with
□	✓ ✗ ...	AY54911		Douglas	Hawthorne	AD	WebConference_MeetingOrganizer	Allows the employee to create and present web conferences. Use with
□	✓ ✗ ...	SMartin		Stephen	Martin	AD	WebConference_MeetingOrganizer	Allows the employee to create and present web conferences. Use with
□	✓ ✗ ...	A241920		Exie	Rice		Contract Manager	Contract management
□	✓ ✗ ...	AY54911		Douglas	Hawthorne		Contract Manager	Contract management
□	✓ ✗ ...	AY29983	⚑	James	Martin		Contract Manager	Contract management
□	✓ ✗ ...	SMartin		Stephen	Martin	AD	Networking Basics	Core networking services including Mail and VPN access
□	✓ ✗ ...	A241920		Exie	Rice		Home Office User	Home Office Productivity Tools
□	✓ ✗ ...	AY29983	⚑	James	Martin	zSecure RACF	APPL/CNM16/READ	
□	✓ ✗ ...	AY54911		Douglas	Hawthorne	zSecure RACF	APPL/CNM16/READ	
□	✓ ✗ ...	AY29983	⚑	James	Martin	zSecure RACF	APPL/AOF16/READ	
□	✓ ✗ ...	AY29983	⚑	James	Martin	zSecure RACF	NETVGRP	
□	✓ ✗ ...	AY54911		Douglas	Hawthorne	zSecure RACF	NETVGRP	
□	✓ ✗ ...	AY29983	⚑	James	Martin	PadLock	Display_user_data_type1	

Items per page 50 | Results 38 « ‹ 1 of 1 › »

Central European Time (GMT +1)

ISVG offers a platform for provisioning, managing and certification of access to various endpoints, be they on premise or cloud based, while also ensuring that compliance with regulations is met and risks are managed.

Employing **ISVG's** Identity Analytics capability and integrating it with modules such as IBM Security Verify (**ISV)** Analytics Bridge and **QRadar**'s User Behaviour Analytics, will augment an organisation's ability to reduce identity and access risk while also identifying internal threats based on a user's activity and risk scoring.

LEARN MORE

To learn more about how to identify, assess, manage, review your access risks based on business activities, and how this can be achieved in an IBM Security Verify Governance solution, visit **www.madigansolutions.com**

ABOUT MADIGAN SOLUTIONS

Madigan Solutions UK Limited is a leading provider of IBM Security Verify solutions. Whether your needs are access management, identity management & governance or privileged access control & monitoring, Madigan Solutions can help you satisfy those needs.