



Risk Update

Edition 3, July 2020

Contents

03 | Preface

05 | Business Continuity Management during COVID

08 | Six remedies to curb your GRC implementation fears

11 | Key considerations when implementing periodic User Access Reviews

Preface

Welcome to the third edition of our Risk periodical, the 'Risk Update'. In this edition, our team has provided a perspective on three specific risk areas.

Over the past year, global, political, economic and environmental events have caused significant disruption to organisations and their day to day operations. With organisations slowly returning to 'normal' operations, **Romana Bizjak** discusses considerations for business operating in this context, and the mindset, organisational, and strategic changes which may arise.

Although their implementation can be challenging, Risk and Compliance software solutions enhance an organisation's risk management capabilities and practices. **Jack Armsworth** discusses six strategies to enable the implementation process to be as smooth as possible.

Finally, User Access Reviews are a key technology control area, and often a recurring source of findings. **Abishek Rathour** explains how to effectively design a user access review process to mitigate the risk of inappropriate access to an organisation's data.

I hope that you find this publication both useful and interesting. To provide feedback or input on content, please contact info@amstelveen.com.



David van Gogh
Director





Business Continuity Management during COVID



Romana Bizjak

Business Continuity Management assumes that an organisation will resume to a known state of operations within a set period of time. COVID-19 has challenged how we respond to disruptions.

The importance of business continuity planning has been demonstrated over the last year within Australia and globally. Global political, economical and environmental events have caused significant disruptions to organisations and their day to day operations. Events such as Brexit, natural disasters like seasonal floods or Australia's largest bushfires and the global COVID-19 health crisis have caused long-term changes to the global economy.

Traditional business continuity planning assumes that a business will resume to a known state of operations. This logic has been challenged by COVID-19, with a large number of organisations being forced to develop new business and operating models, without necessarily having time for proper due-diligence and analysis. Few organisations have faced situations like these before, and so few know what the new normal may look like once business resumes. Under typical

business continuity scenarios, corporations would have expected to return to their normal business operations within a matter of days or weeks. In many cases, this choice was removed when businesses responded to the global pandemic and government restrictions were imposed. Organisations are now entering into a situation where the positive learnings can be harnessed into creating a major shift of mindset and working models as we know them.

“By now, organisations should have started to think about what the ‘new normal’ will look like for them.”

Below are a few questions that every organisation should consider during the Business Continuity planning process, given these recent developments.

1

Is the organisation's strategy still relevant?

With the future still ambiguous, it is advisable for organisations to re-visit their business strategies and assess the impacts of recent events against it. This should take into consideration internal and external factors that might have changed and their associated risks, such as the loss of offshore suppliers or closures of borders impacting trade arrangements. Others may find new opportunities in the current environment, such as the continued investment and improvement in networks and telecommunications.

Not only is it important to revise the strategy but also to assess the operating model against it, to ensure that an organisation has the right capabilities and capacity to execute against it.

Key Considerations:

- ▶ Understand the impacts that COVID-19 has had on the industry and re-evaluate organisational strategy against these changes.
- ▶ Assess the current operating model and determine whether a tactical shift in business operations is required.
- ▶ Evaluate capacity and capability requirements against the revised business strategy and operational model.

2

Are key risks post COVID-19 understood?

Organisations should assess their business continuity plans against this new strategy. Where changes are expected, organisations should confirm key processes and prioritise critical activities and resources to run these processes.

It is important to keep a close eye on the market, and allow for flexibility with responding to re-strategising offshore processes. This includes vendor or sourcing requirements, as well as re-assessing political or regional risks where satellite

offices, data centres and other offshore distribution or development centres are located. Organisations should establish governance mechanisms and processes to manage COVID-19 related risks with forward looking Key Risk Indicators for monitoring purposes. When linking back to the organisation's strategy and business objectives, an organisation should identify and assess the key risks that could impact the business during the transition and into the future.

Key Considerations:

- ▶ As global supply chain challenges accelerate, prepare for further disruptions by re-thinking how to manage short term supply chain risks and how to develop long term supply chain resilience.
- ▶ Identify the main sources of disruption impacting your business, then review and update the business impact assessment.
- ▶ Ensure that the organisations risk management system supports visibility of risks both during and post COVID-19.

3

Can the organisation support flexible working arrangements?

Having a significant proportion of the workforce working from home five days a week has set a precedent for workforce preferences of the future. Employees have demonstrated that they can collaborate virtually and deliver outcomes, all from the comfort of their homes. It is up to employers to develop strategies and plans that facilitate flexible working arrangements in the future, allowing employees to have greater autonomy over how they choose to calibrate their work-life balance. Organisations should consider these factors and plan for scenarios involving employees working from the office or remotely. This may involve considering owned and leased office spaces and associated expenses, and determining whether there are more effective ways to operate, such as through re-investment of these savings into technologies that

enable virtual collaboration. Continued work from home capabilities could reduce the need for larger office spaces and reduce operating costs.

Key Considerations:

- ▶ Evaluate the changes to the workforce model against the new operating model and plan for scenarios to support a flexible work arrangement.
- ▶ Plan to enable a connected culture in a remote work environment supporting organisational values and overall business strategy

4

Is the work environment safe enough to create trust?

As a consequence of ongoing health risks associated with COVID-19 and a shift in mindset towards more flexible working arrangements, Workplace Health and Safety (WHS) has become more complex for organisations to manage. The health and safety of employees, contractors suppliers and visitors is paramount as organisations start to go back to their office or work site, requiring organisations to assess the related risks and logistical control challenges.

Organisations should develop and implement appropriate WHS measures, programs and guidance for employees to create awareness and ensure WHS requirements are understood and maintained. This includes updating WHS policies and procedures, and ensuring that they are still relevant and reflective of the current environment and WHS requirements.

Supporting the mental wellbeing of people is more important than ever. Organisations should therefore also seek to implement mental wellbeing and support programs for employees during and after the transition, including equipping managers with appropriate training and tools to help employees during these times.

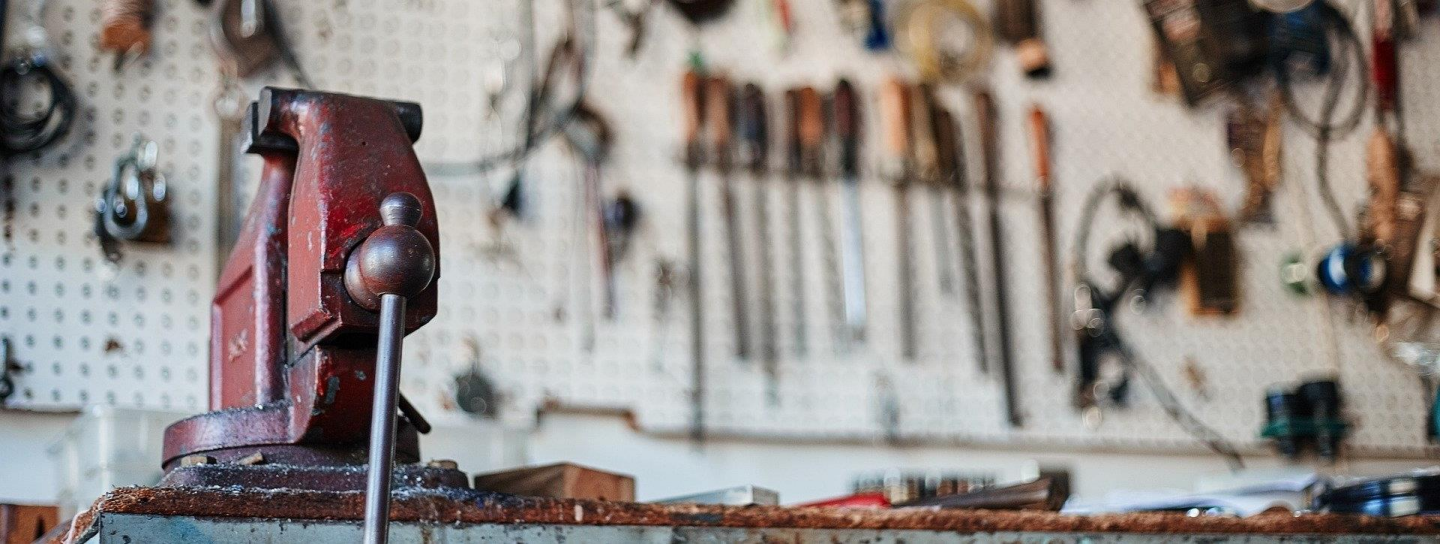
In times of ambiguity, it is especially important that mechanisms and channels are in place to enable timely, accurate and insightful information. Planning of communication to management, employees and other impacted stakeholders is indispensable, as well as allowing for opportunities for stakeholders to ask questions. A popular way to obtain feedback is through conducting regular pulse surveys offering an anonymous channel where individuals may feel more comfortable to speak up about their experience during the transition.

Key Considerations:

- ▶ Ensure WHS policies and procedures are updated, relevant and reflective of the current environment. Refer to Safe Work Australia for additional guidance:
<https://www.safeworkaustralia.gov.au/>
- ▶ Develop communications structures that enable frequent and empathetic communication.
- ▶ Evaluate employee mental and physical wellbeing programs to support flexible and remote work arrangements.

Closing Thoughts

Recent events have been testimonies of the criticality of an organisation's business continuity planning and preparations. Continued health threats and ongoing economic uncertainty highlight the importance of continuing to respond to the ongoing ambiguity. This requires organisations to look for opportunities in the current environment and challenge current business strategies in face of expected risks and logistical challenges, without compromising the safety of their most important assets, their people.



Six remedies to curb your GRC implementation fears



Jack Armsworth

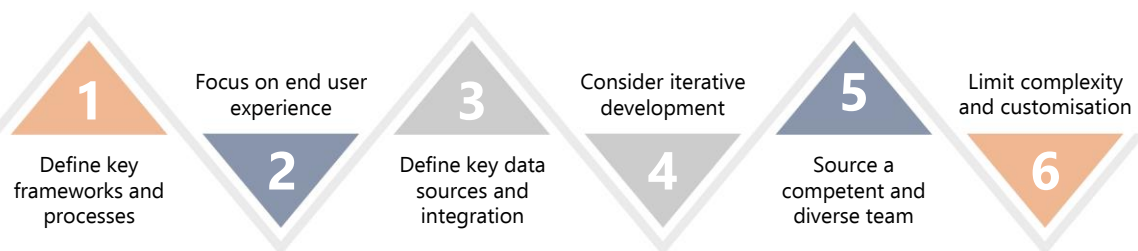
GRC solutions can enhance and even automate some of an organisation's risk management capabilities and practices, but their implementation often appears challenging. However, with the right planning, team, access to data and a focus on the end-user, a great outcome is achievable.

What is GRC Software?

Governance, Risk and Compliance (GRC) solutions assist organisations to consistently implement and maintain risk and compliance frameworks, processes, and procedures through the centralised management of related data stemming from risk activities. GRC tools provide a platform to manage and understand risk exposure across organisations. Choosing and implementing the right GRC tool can be difficult, as the organisation's needs and circumstances must be considered, as well as the tool's capabilities in meeting these.

Why can it be difficult to implement?

Traditionally, these solutions involve complex, long running implementations that cut across multiple business functions. Aligning delivery priorities and requirements across differing core business units as well as group/corporate functions like Finance, Security, Technology, Legal, Compliance and Audit is challenging enough, before consideration of the consolidation of multiple pre-existing toolsets, data-migration and the integration of different systems.



1

Define key Risk Management frameworks and processes in advance

It is important to understand the business context before defining your list of functional requirements or user stories. Agreeing the frameworks, processes, and ways-of-working that your GRC solution will need to support will enable you to assess options and scope features with confidence. Taking a solution out-of-the-box is preferable for ease of maintenance and support, but may not meet your functional Minimum Viable Product (MVP). Defining your key Risk Processes, reporting requirements and having a prepared risk and control taxonomy in advance will help you clearly articulate MVP, support your market evaluation, and enrich conversations with key vendors. If possible, ask vendors for a Sandbox, and test out how your key processes and risk and control libraries will be uploaded and executed out of the box, and what customisations may be required.

Focus on the end user and their experience

A great GRC solution will support risk management and compliance across all three lines of defence. However, these tools are often highly bespoke and not intuitive for users that are unfamiliar with GRC concepts. Define your end user personas, starting from risk and non-risk users. This will help build out user journeys, support your functional requirements and even form the basis for your security and access permissions. Focus on what your users will need from the GRC solution and what the easiest way will be for them to meet these needs. There is often an over-reliance on risk teams to maintain GRC data, so enable your business stakeholders to take accountability with a well-designed user experience. Practically, this means involving your end-users during the build by demonstrating the solution within a Sandbox, and their participation in showcases and User Acceptance Testing.

2

Consider key data sources and leverage integration

If you want more than a glorified spreadsheet, consider how you can use data to drive informed risk decision making. This may include leveraging risk and control libraries or internal asset inventories (such as Configuration Management Databases) and Service Management tooling (such as those used to track IT change, incident, and problem management). Some GRC tools offer low/no code integrations or alternatively may natively integrate with systems your organisation uses to manage key controls. Centralisation of incident data can be achieved through integration with disparate systems containing non-IT incidents (e.g. fraud and WHS/HR), and workflow systems which track remediation activity. Understanding key data requirements and selecting a tool that allows you to access these will help when defining risk profiles, automating controls assurance and monitoring compliance.

3

4

Define a legitimate MVP and iterate

Like any system implementation, the modular nature of GRC solutions make them great candidates for iterative development. Even if you are implementing functionality over time, you can get value from your solution immediately. For organisations without an existing GRC solution, define the MVP to get your team up and running. For those moving off an incumbent, you may want to focus on ensuring that existing functionality is workable and introduce new features progressively to avoid complexity. Aside from this functional approach, the MVP can also be structured according to departments and depth. In the case of a departmental approach, some choose to roll out their GRC solution to certain teams (e.g. IT) first, before the rest of the organisation. Slicing the implementation according to depth means deploying your risk processes (e.g. risk profiling) one organisational level at a time.

Get the right mix of skills in your implementation team

We have found that it takes dedicated and experience resources to support a GRC implementation. If you are planning on using an external delivery partner, your risk teams should be supported by Business Analysts and Product Managers who understand risk management, and if possible, have experience with the chosen solution to challenge and validate design decisions. This will allow you to define detailed functional requirements and get the most value out of your delivery partner, all while your business as usual Risk Management team can get on with supporting the business.

5

6

Limit complex workflows

The configurable nature of GRC solutions gives organisations the ability to build out highly complex workflows. It is tempting to customise business rules, approval requirements and security controls to manage how records are created, assessed, reviewed, and endorsed. In our experience, defining repeatable, flexible MVP workflow requirements for key objects will greatly decrease delivery complexity, improve the user experience, and assist operations teams in defect troubleshooting. As well as these, fewer customisations will often make upgrade pathways easier and quicker to implement. When vendors release patches and major platform upgrades, builds which are closer to out-of-the-box are easier to digest and typically have fewer functionality clashes and demand lower effort for verification testing.



Key considerations when implementing periodic User Access Reviews



Abishek Rathour

An effectively designed user access review (UAR) process mitigates the risk of inappropriate access to an organisation's data, which in turn reduces the risk of either erroneous data entries being made, or confidential data being leaked.

Introduction

User access reviews are a key review area from internal risk management teams and external auditors, and often a recurring source of findings. In this article, we look at some key considerations for user access reviews, which should be considered when implementing a user access review across a business unit, application or organisation.

Tooling

Identity access management tools are becoming increasingly popular for large and complex organisations. These tools help automate the 'hire to retire' process including periodic UARs. By automating some or most of the process, the risk of human error is reduced, which is a common area of control breakdown. It is important to consider the cost and the complexity of the IT environment and user base before implementing such a tool.

Policy and Procedure

Policy and procedural documentation are integral for a well-functioning UAR process. A well-defined

policy clearly identifies the requirements for the user access review such as frequency, timeliness and accountability of control owner(s). A control owner leaving an organisation is a common reason for the UAR process breaking down. However, a well-documented policy and procedure ensures that in the event of changes to control owners, the UAR process is not impacted.

Frequency

The frequency of the review is dependent on a range of factors, which includes size of user base, turnover within the organisation and number of third-party users with access. The user access review should be performed more than annually for critical applications. A more frequent review should be performed for privileged users as the risk of inappropriate activity is higher due to the elevated access.

A targeted UAR for an individual user could also be performed by their line manager upon a position or team change. This helps determine what access should be retained in the new position or team.

Scope of review

The user groups to be included in the review should be noted in the policy or procedural documentation. Key considerations include whether access is more than read-only (i.e. – write access) and whether it includes contractors and/or suppliers.

The scope should also consider whether users with access to the supporting infrastructure to the application should be included. This is dependent on what activities a user with access to the database and/or operating system can perform. Privileged access to the database should be included in scope if it allows users to make direct data changes. Similarly, if privileged access at operating system level allows users to change critical application functionality and/or create new users, then it should also be included in the UAR.

Completeness of user listings

This is a key area of breakdown for user access reviews. Organisations should retain sufficient evidence to validate that the user listings used as part of the UAR are complete. This includes retaining screenshots of the parameters applied to generate the listing. Where possible, screenshots showing row count should also be retained to validate that the raw user listing was not modified after generation.

Where user listings are generated automatically, the respective teams should perform procedures to validate that the underlying script or query is generating a complete and accurate user list. The script or query used to generate the listing should be retained. This is to validate that the script or query has not been modified since initial testing performed, to validate that it generates a complete and accurate user listing.

Precision of review



Role descriptions: In some instances, the role name does not provide a clear description of what it allows a user to do. The review sheet should include a description of what a role allows a user to do so the reviewer can evaluate whether the role is required by the user as part of their day to day activities.



Segregation of permissions: The review should also be performed to determine that permissions assigned to roles or entitlements do not create a segregation of duties violation. For example – a segregation of duties violation would occur if a role allows a user to both create and approve purchase orders.



Assigning the reviewer: It is important to assign responsibility for the UAR to someone who has good knowledge of users' day to day functions. This can be either a user's line manager, product manager, application owner or someone else. An option should also exist for the reviewer to delegate the review to someone else where they do not have sufficient knowledge.



Evidence of review: The review documentation should provide sufficient evidence that all users and their corresponding roles have been reviewed. This can be done by commenting next to each line item for the user or 'tick marking'. A signature at bottom of review sheet may not be enough in some instances to satisfy the requirement of Audit and Assurance that each role has been reviewed. Where possible, the reviewees should have a predefined list of options to choose from (i.e. retain, remove or modify).

Follow up actions

The user access review process is only valuable if follow-up actions are executed. Hence, it is important that any modifications and deletions identified are actioned in a timely manner. Accountability should be clearly defined for the team responsible for ensuring that follow-up actions have been actioned.

A high number of follow ups is an indicator that preventative controls (provisioning, modifications and terminations) are potentially not operating effectively. The respective teams should work with internal risk practitioners to investigate.

Evidence that deletions and modifications have been actioned should be retained. This is ideally evident through automation within an Identity and Access Management tool.

This can be also be done through creation of tickets through a ticketing system (e.g. in ServiceNow) including screenshots showing access has been modified or deleted. Alternatively, a new user listing should be generated again and retained to validate that follow-up actions were effectively actioned.

Self-review

There should be procedures in place to ensure that there are no instances where a user reviews their own access. This is a segregation of duties violation.

Timeliness

The review process from initiation to closure should be monitored. Timeliness is an important aspect since a user's access may change from the date of user list generation to when it is reviewed. Ideally, the review should be completed within 30 to 60 days from initiation depending on the user base and complexity of review.

Accountability should be assigned to a team (e.g. an internal governance function) to manage the overall process and ensure that responses are received from reviewees in a timely manner. Another consideration is escalating the review to the 2-up manager, if a response is not provided by the respondent. If a response is not provided by the 2-up manager, the user's access should be revoked.

Retrospective reviews

A retrospective review should be performed for users marked to have their access removed or modified. The retrospective review should identify whether any inappropriate transactions were made by users during the period they were inappropriate.

Checking application logs can be a complicated process as it requires identifying the date the user was deemed inappropriate from and reviewing the changes made within the application by the user. This may not be possible depending on application functionality and whether event monitoring exists.

This can be done by checking the last login dates for terminated users. For modifications, this can be done by checking application logs (if feasible) to check that transactions made by the user were appropriate.

Closing Thoughts

The User Access Review is a key control as part of the general access management controls within an organisation. Organisations should consider and implement the key considerations identified in this article. The level of documentation for user access reviews should be retained at a sufficient level to permit a risk practitioner or external auditor to re-perform the steps and reach the same conclusion.







Managing risk starts with a strong risk culture.

Start measuring your risk culture now with Amstelveen iQ.

▶ What is Amstelveen iQ?

Amstelveen iQ is our proprietary self-assessment platform designed to provide insights to business leaders about their organisational risk culture and provide recommendations for areas of improvement.

▶ What does Amstelveen iQ do?

Amstelveen iQ offers a curated set of questions to understand an organisation's culture and identify trends in organisational behaviour. This helps organisations understand how teams perceive the behaviours and interactions of their colleagues and leaders in the organisation. Responses are used to generate actionable insights and produce a report tailored to the organisation.

▶ Who is Amstelveen iQ for?

Amstelveen iQ is designed for use by Risk Leaders within an organisation. Amstelveen iQ is intended to serve organisations of all sizes, from small start-ups to established enterprises. The platform is most effective when used with teams of 10 or more people.

What are the key benefits of Amstelveen iQ?



Simple and intuitive

The platform makes it easy for staff to respond to risk culture assessment, with a user friendly and mobile compatible interface.



Actionable Reporting

Push button reporting that generates a professional and personalised report that outlines the results of your risk culture assessment.



Proven Framework

Our risk culture platform is based on our proven risk culture framework.



Safe and Secure

Your staff can feel confident that their assessment responses are anonymous and that data is securely stored and transmitted to our cloud platform.

To find out more about Amstelveen iQ or Amstelveen's professional services, please contact info@amstelveen.com or visit our website amstelveen.com/iq.

Amstelveen

Amstelveen's team of professionals work on major technology and business change projects, and enhance capability in risk management, internal audit and corporate governance functions. We provide specialist support to the largest public and private organisations in Australia and New Zealand.

This publication contains general information only. We accept no duty of care nor liability for reliance on the information within it. To obtain information specific to your circumstances, please contact us at info@amstelveen.com.