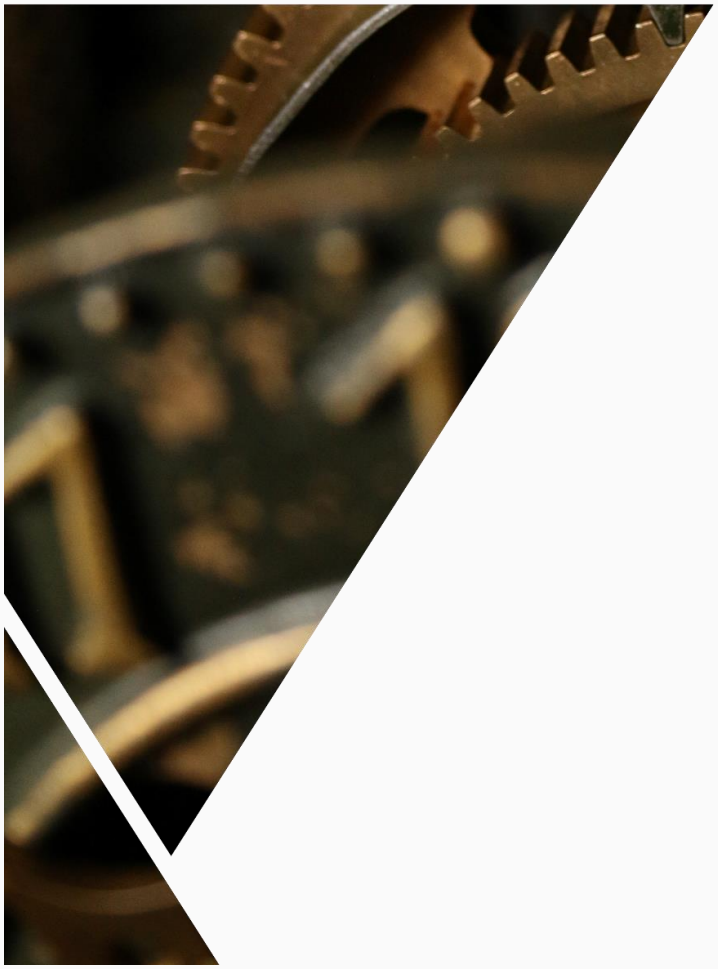
July 2021 Edition 4

Risk Update

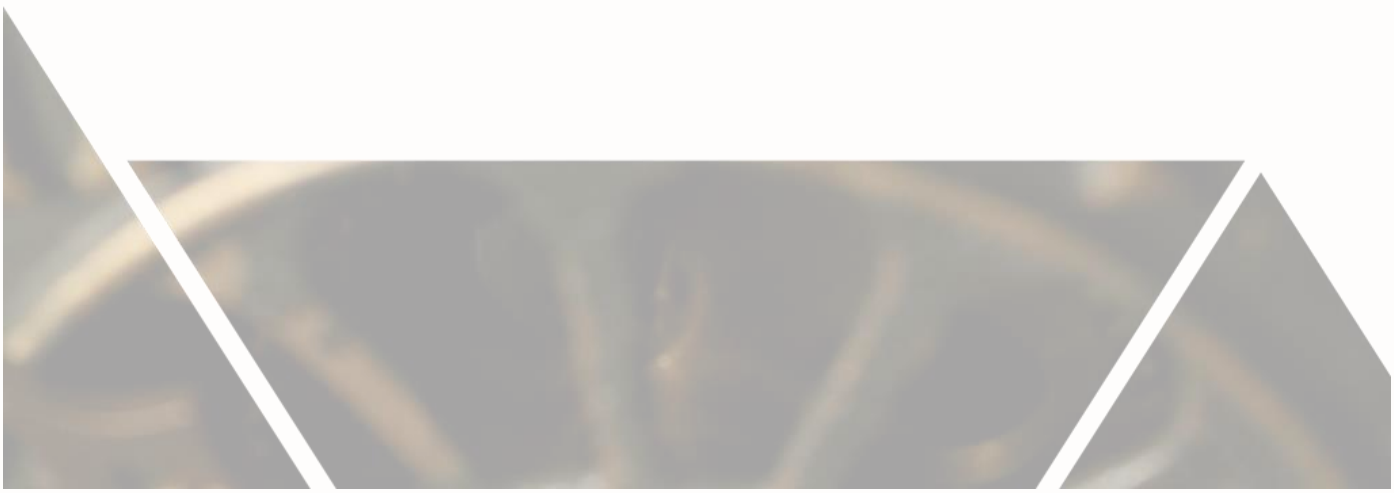


Controls and Automation

Assure, repeat, assure.

Amstelveen

Contents



Preface

Welcome to the fourth edition of our Risk periodical, the Amstelveen Risk Update. In this edition, our team has provided a series of perspectives on the themes of Controls and Control Automation.

Effective assurance starts with well informed planning, and emerging technology trends and their adoption within an organisation should inform controls testing plans. **Andrew Millward** discusses five current technology trends and five related control areas to consider in assurance planning.

Control automation continues to have strong benefits for internal controls functions. **Katherina Sau** covers the impact of automating processes and controls on efficiency and processing error rates, as well as three pitfalls to watch out for when automating.

Finally, **Benjamin Zhang** discusses five considerations for applying automation to control testing, and how this can be done without compromising the independence of assurance.

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

The 5 trends and 5 themes to consider in your IT control assurance planning

As we enter a new financial year, it is a good time to take stock of the key technology trends relevant for many organisations and aligning your IT control assurance plans around these trends.

BY **ANDREW MILLWARD**

Setting context: 5 current technology trends

1 IT services are being delivered and secured remotely

Looking ahead to a post-COVID world, remote working in one form or another is likely to be a permanent fixture. In order to rapidly adapt in 2020, many organisations had to fast track remote technology arrangements including rolling out new teleconferencing software, changing VPN configurations, implementing processes to remotely provision and support devices and more. It was not uncommon to hear "what would normally take us 6 months got done in 4 weeks."

Given the speed these changes were implemented, it would be prudent to retrospectively check that the appropriate governance and security controls are in place for these arrangements.

2 The cloud may be taking over, but there are shared responsibilities

Cloud transformation is at the core of almost every organisation's IT strategy and has been for some time. It has been nearly 6 years since APRA published their initial information paper for regulated entities outlining their expectations for adopting the use of cloud computing services. As such, by now most financial institutions have put in place repeatable processes for upfront and ongoing due diligence over the these arrangements. However, as more and more critical services are being migrated to the cloud, it is vital that there is continued clarity on the shared responsibility model and investment in supporting infrastructure, such as identity and access management services and integration of security logging and monitoring.

3 COVID-19 has accelerated the already rapid digitisation of products and services

The business models for many organisations were completely transformed in 2020. A global survey of executives by McKinsey found that in the first 6 months of the pandemic, across all continents and industries, the average share of products and/or services that are digitised increased by 60%, which would usually take over 7 years to achieve. Now more than ever, the greatest risks to a company's assets are no longer physical - they are digital. Intangible assets represent an increasing portion of balance sheets and make up over 90% of the S&P 500 market value[2]. To a large extent this is a combination of both software and data.

---

[1] https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#

[2] https://www.oceantomo.com/intangible-asset-market-value-study/

4 Cyber attacks are increasingly targeted for the purpose of financial and political gain

The perception of a typical hacker has historically been a bored teenager in the back room of their parent's house using known tactics and exploits (a so called "script kiddie"), largely for entertainment or bragging rights. However, there has been a significant shift in recent years towards targeted attacks orchestrated by organised crime groups seeking financial gain as well as state-based actors for the purpose of political gain through espionage, retaliation, intimidation and destabilisation.

Ransomware is a common and high impact attack carried out for financial gain. It is also increasingly coupled with exfiltrating sensitive data and the threat of public disclosure. Another common threat is financial fraud, for example where an attacker changes staff or supplier bank details to redirect payments. This is often achieved through business email compromise and/or social engineering.

State based attacks have become incredibly sophisticated, often targeting the control or disruption of critical infrastructure or organisations such banks, universities, utilities, hospitals etc. Sometimes these attacks are covert, for example to gain access to valuable intellectual property. Other times they aim to disrupt, for example by gaining access to industrial control systems.

5 Heightened regulatory and compliance focus on security risk management

Across government, industries and supply chains there is a focus on strengthening the requirements and expectations of robust security risk management practices. The Australian Cyber Security Strategy 2020 charts a roadmap for regulatory reform that aims to clarify the cyber security obligations of both the public and private sector. As such, it appears likely there will be further significant change to the regulatory requirements across a wide range of industries over the coming years .

Key recent and emerging regulatory highlights:

- Security Legislation Amendments (Critical Infrastructure) Bill. Likely to be legislated in 2021 and will impact a broad range of industries.
- The Corporations Act contains broad obligations for risk management particularly for financial services. ASIC launched a landmark case in 2020 related to cyber risk failings at a licensee.
- APRA CPS 234 (Information Security) applies to financial institutions. Tripartite independent security reviews are currently underway.
- CORIE framework which sets the Council of Financial Regulator's requirements for industry-wide cyber resilience exercises. It is currently under pilot.
- SWIFT Customer Security Program for financial institutions recently updated control requirements for 2021. Failure to comply may be publicly disclosable.

Building the plan: 5 control areas for focus

Whether planning controls to uplift as part of your cyber security or technology risk roadmap, or control areas to assess as part of your IT Audit Plan or Control Assurance Plan, the following areas, shaped by current technology trends, are worth considering.

Data Protection and Privacy

The immense volume of data being stored and processed means ***identifying*** and ***classifying*** it is an important first step to effectively ***governing*** and ***protecting*** it, regardless of whether it is hosted on premise or in the cloud.

Indicative controls:

- Information classification and inventory
- Data governance framework
- Privacy framework
- Data loss prevention
- Encryption
- Identity and access management
- Background screening
- Staff training

Cyber Resiliency

It is inevitable that IT systems will be compromised. Being able to ***detect*** and ***respond*** in a timely manner is critical to minimising the damage and meeting regulatory obligations. The ability to ***recover*** is the last line of defence, particularly in the case of ransomware.

Indicative controls:

- Vulnerability management
- Logging and monitoring systems (i.e. SIEM)
- Threat intelligence
- Security incident, breach and crisis response planning and testing
- Backups and IT disaster recovery

Cloud Governance and Security

Implementing cloud solutions requires careful ***planning*** and ***due diligence*** to ensure they are fit for purpose. Ongoing ***monitoring*** provides continued assurance they remain fit for purpose and that unmanaged solutions aren't introduced.

Indicative controls:

- IT architecture, planning, and procurement processes for cloud solutions
- Project governance and delivery controls over major cloud programs
- Third party risk management and assurance processes, with sample testing for key cloud arrangements
- Technical controls for preventing, detecting and securing unsanctioned cloud use, such as use of a cloud access security broker
- Processes for managing use of unsanctioned cloud solutions

Corporate technology and endpoint management

Remote working has changed how endpoints and corporate technology are ***secured*** and ***serviced***. It is important that there is a balance between convenience and security given corporate technology is a central part of the overall employee experience and the gateway to the organisation's digital assets regardless of where they are hosted.

Indicative controls:

- Secure configuration of devices
- E-mail and browser hardening
- Benchmarking of endpoint configuration against control frameworks (e.g. Essential 8, CIS)
- Technical controls in place over remote access methods (e.g. Citrix, VPN)
- Mobile Device Management controls
- Endpoint detection and response
- IT request and incident management
- Device imaging and build processes

Software development, including DevOps

The ability to rapidly ***develop, test and deploy*** software that is robust and secure is essential to delivering digital products and services that meet customer and community expectations.

Indicative controls:

- Definition of requirements
- Software engineering practices, such as code management, peer reviews, and secure code scanning
- Functional and non-functional testing
- Agile processes and practices
- Change and release management

Other takeaways and reminders

Don't forget the other key building blocks to factor into your IT assurance planning:

- The current IT risk profile
- Technology and Cyber Security strategies and roadmaps
- Major IT transformation programs underway
- Related assurance and compliance activities.

The shift from manual to automated controls

Organisations are up against constant changes in technology, compliance and regulation, and yet internal control functions remain static. Implementing automation into internal control functions can assist in improving efficiency, reducing costs, and result in development of more robust controls.

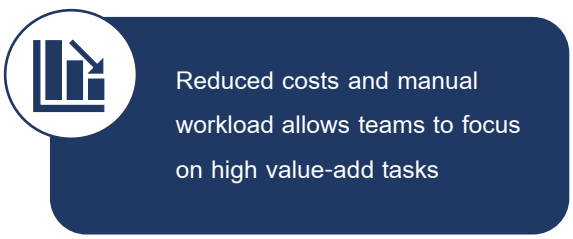
BY **KATHERINA SAU**

In a world where organisations are faced with changes in technology, compliance and regulation, it is alarming that internal control functions tend to remain static. As it stands, many organisations still rely on manual controls because they fear automation will relinquish their control have over existing activities in key business processes.

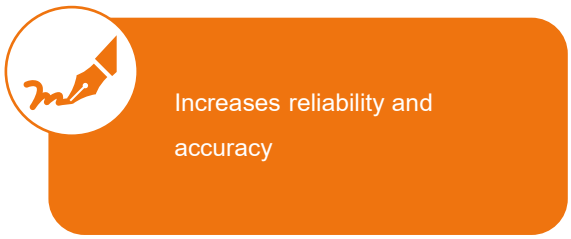
However, industry insights reveal that this perception is not realistic. Automation is commonly attributed to numerous efficiencies and cost advantages, including more efficient use of personnel, increased productivity and a reduction in errors. Ultimately, automating internal control functions will lead to more robust controls.

Benefits of automated controls

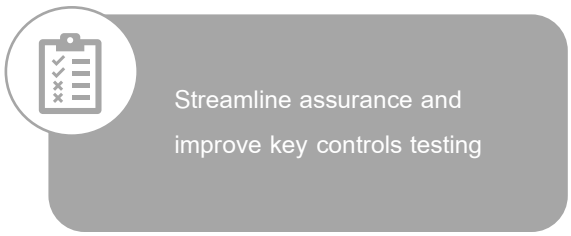
Automating and properly implementing internal controls will result in the following benefits for line one risk teams:



Reduced costs and manual workload on key business processes and compliance activities enables teams to focus on timely issue/exception resolution and gives the team an opportunity to complete deep dive analysis when required. As a result, the team can complete root cause analysis rather than addressing secondary issues with temporary fixes.



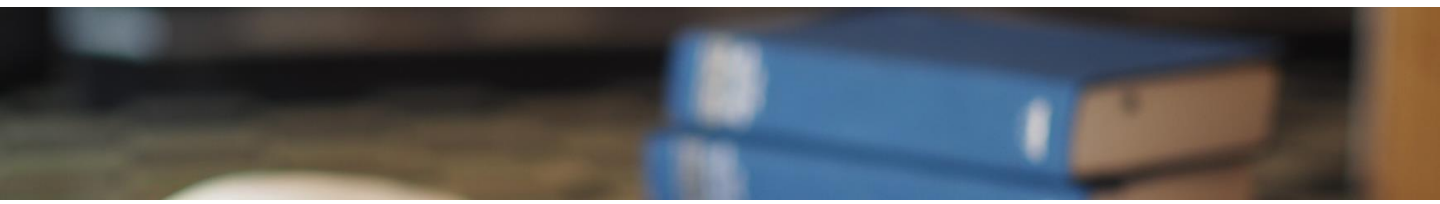
If designed well, automated controls are **more reliable and accurate**, reducing the likelihood of intentional errors that manual reviews and checks are susceptible to.



Automation of entity level controls will **streamline assurance and improve key controls testing** across the organisation. A single control which addresses multiple regulatory requirements can be shared across the organisations divisions/business units.

In addition, second line and third line teams can have greater confidence in automated controls. The impact is twofold:

1. A reduction in administrative burden in testing controls; and
2. Improved effectiveness, time and quality of compliance control activities.



Case study

A retail company has been operating for over five years and has a newly appointed CRO. The CRO has requested that Line 1 teams across the business review their internal controls to consider whether associated overhead costs can be reduced. The company has previously encountered issues with repeated human error and possible cases of fraud. The CRO has asked Line 1 teams to come back with proposed options for manual controls that can be automated. Below are examples of recommendations that were made to the CRO:

Unauthorised vendor payment processing

A review is performed to check that vendor payment processing has been approved by two separate authorised delegates. A member from Finance checks that the vendor batch processing payment has been signed off by a separate preparer and reviewer and ensures that the grades are appropriate.

The company could automate this by granting access and enabling workflows for approvals and enforced delegations of authority in the system.

Incorrect discount applied

A review to check customers are applying the right discount/claim code to a corresponding promotion. A member from Finance checks claims from their retailers to ensure each line item has the correct discount, amount and claim is within the promotional threshold.

The company could automate this using rules-based logic, whereby the system will make sure that the claims and details match before applying the discount.

These automated controls will not only improve efficiency and reduce costs but are significantly more robust.

What to look out for when automating

As organisations' risk and control environments mature overtime, senior management should prioritise the automation of controls. While there are many benefits, it is even more important to understand the pitfalls to automation. Without a structured roadmap for integrating and implementing automation, increased costs and wasted resources can undermine any potential efficiency and control effectiveness that automation can bring.

Investment in software, resources and training

You can expect large upfront costs before the benefits outweigh existing manual processes. Integration of automated controls requires modern software, additional resource capability and capacity, and may be difficult and expensive to implement.

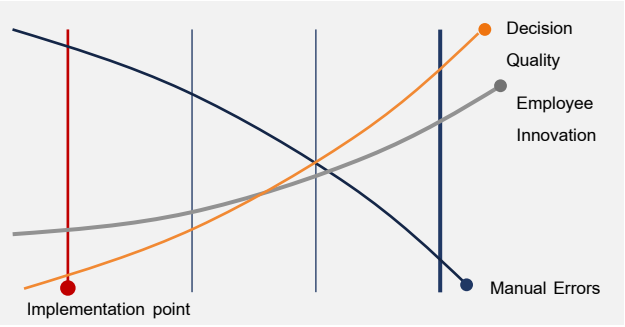


Figure 1: Benefits of automated controls over time

Automation needs to be configured correctly for controls to be robust. It is recommended that periodic reviews over rulesets and coding be undertaken to ensure configurations continue to meet business requirements and minimise costs.

Key Considerations:

- Planning! Define the organisations control automation strategy and blueprint, and evaluate potential options for software / platforms.

Trying to automate all manual controls

Since automated controls are performed entirely by a system or application and do not require human intervention, it is important to consider what type of controls to automate. Repetitive, routine, resource draining and simple controls should be automated. Customer facing activities that are best performed with personal interaction should not be interfered with.

Key Considerations:

- Review existing internal controls framework to identify areas for control automation.
- Identify top manual controls to be automated by looking at previous years efforts or estimating the most time-consuming control tests for the current year.
    - Manual controls: for circumstances where judgement, discretion and scrutiny are required
    - Automated controls: for high volumes of repetitive tasks.

Adapting to change

People tend to fear automation because they are concerned that they will be replaced by robots. However, not everything can or should be executed by a machine. There will always be a level of human interaction and human intelligence required. Importantly, automation can lead to an increase in skillset as resources can be used for stimulating tasks.

Key Considerations:

- Overcoming inertia – getting the right people on the right page.
- Nominate a Champion – this person champions the cause, influences people to adopt control automation and educates them to look for more opportunities to apply automation.

Can you automate controls testing and still provide independent assurance?

Developments in artificial intelligence, machine learning and robotics have demonstrated that many activities thought to be too complex to be automated, can now be outsourced to a ‘digital’ workforce.

BY **BENJAMIN ZHANG**

What is Controls Testing?

Controls are activities and processes that organisations put in place to help manage and reduce the inherent risks. Controls testing involves assessing the adequacy and existence of controls that is relied upon by organisations to mitigate risks.

Controls testing can be an arduous task for auditors and depending on the complexity of the controls environment, often involves a considerable investment of time and resources. Therefore, a key question that is often asked by management is how can we reduce the cost and time spent on compliance activities?

Manual vs Automated Testing

There are a number of benefits when it comes to using automation, with one of the primary reasons being to reduce the cost and time spent on compliance activities. As most of these activities are heavily reliant on cognitive abilities, the predominant approach has been to rely on people to perform these tasks.

Before we explore the role of automation, we should first understand what the typical activities are within a controls test. In any audit review, the following activities will need to be performed by the Internal Audit function:

- IT Risk Assessment and Scoping
- Gather Audit Evidence
- Perform Testing Procedures
- Issue Report with Recommendations

Five considerations to make before adopting automation

1 Can the control testing be automated?

Automation of controls testing is dependent on the complexity of the control and the level of judgement required by the Internal Auditor when evaluating if a control is meeting its control objectives. For example, controls such as terminations testing can be automated as these have defined variables that can be configured in a supporting tool. This could include performing an assessment to determine whether the employee's termination date in the organization's network (e.g. Active Directory) is greater than the end date in the central HR system. This could be an indicator that removal of terminated user roles are not being performed in a timely manner.

On the other hand, controls that require the Internal Audit judgement may not be suitable for automation of controls testing. An example of this includes determining that changes are sufficiently tested and approved prior to migration to production. Testing over these type of attributes is reliant on an auditor's judgement, as automation would be insufficient to determine the nature and complexity of the change.

Key Considerations:

- Consider the complexity of the control and level of judgement required.
- Control being automated should have defined variables, which can be configured in a supporting tool (e.g. – terminations testing).
- The automated control should require minimal Internal Auditor judgement (e.g. – testing for changes).

2 Do you have the right tools and expertise?

Automation of control testing is dependent on the available tools and expertise of the personnel to configure them. Examples of tools that can be used to assist with automation include BluePrism, Alteryx and ServiceNow. These tools allow for automation through the process of collation, processing, documenting and output of testing results.

It is important to note that to properly utilize such tools, it requires appropriate personnel who are knowledgeable and experienced in using the tool. Hence, an organisation must consider whether it has the skills and capabilities necessary to create and manage bespoke automated workflows.

The tools should also be able to select samples (where necessary) in line with the organisation's requirements. For example, the tool should be able to randomly select samples from a population, where an organization's policy mandates random sampling.

Key Considerations:

- Determine whether the expertise of key personnel to automate controls testing is available in-house or needs to be sourced
- Determine the supporting tools that can used for automation. A cost benefit analysis should also be performed.

3 Is the source data complete and accurate?

As part of the automation of controls testing, it is important to ensure that the population used for the testing is complete and accurate. This is a key requirement in controls testing to ensure that no data has been accidentally or intentionally excluded.

Within the automation of controls testing, it is important to build in verification procedures to ensure that the data source is validated for ensure that the appropriate parameters are applied to generate it.

In addition, it is also good practice to perform a manual reperformance of the completeness and accuracy of the source data. This is to ensure that the right level of assurance is provided to key stakeholders by ensuring no emission of the population.

Key Considerations:

- Ensure verification procedures for completeness are built in supporting tool.
- Consider implementing manual reperformance of population to validate completeness.

4 Will the level of assurance be sufficient?

The Internal Audit function provides assurance over whether the controls meet their control objectives. This is shared with the Audit and Risk Committee (ARC). In addition, there may be arrangements with the External Auditor of the organisation for a 'Reliance on Internal Audit Approach'.

Hence, it is important to determine if the level of assurance through controls automation is sufficient to meet the requirements of ARC and the external auditors (where applicable). Automation should be thoroughly tested at implementation through manual re-performance to validate the actual outcomes are in line with the expected outcomes. The procedures for how automation of controls testing is done for each control objective should be sufficiently documented.

Key Considerations:

- Determine the level of assurance based on stakeholders (e.g. – reliance by external audit).
- Determine the level of manual re-performance required to validate control conclusions.

5 Is the automation designed to be future proof?

Whilst automation is a great way to streamline the controls testing process, it is important to consider the compatibility with future upgrades. The automation should be designed in a way so that even if there are changes to the underlying data, the program, workflow or script enabling the automation can also be easily adapted.

Where feasible, hard coding should be minimised. This is to ensure that the automation is compatible with future upgrades without requiring considerable re-scripting.

Key Considerations:

- Consider minimising use of hard coding and using dynamic variables to ensure compatibility with future upgrades.

While true end-to-end automation of controls testing may still be out of reach, a semi-automated control testing approach could help bring efficiency to the tests and allow internal auditors to focus their time on performing more value adding activities. Controls testing can be automated, however it's dependent on the complexity of your organisation, the availability of your tools and skillset of the workforce. As with all new technologies, careful consideration over organisational fit and readiness needs to be made before leaping to a wide-scaled adoption.

AUTHORS

Andrew Millward
Director

Andrew is a technology risk and information security professional with over ten years of experience in risk management, internal audit and information security. He has worked in a variety of roles advising and supporting risk management functions, internal audit, project teams, steering committees and project sponsors of large Australian corporations.

Katherina Sau
Manager

Katherina is a risk and assurance professional with five years of experience in operational risk and transformation, risk compliance and assurance, internal audit and project management across Insurance and Financial Services clients. She has experience in enhancing control environments and existing risk-based frameworks based on best practice standards.

Benjamin Zhang
Senior Consultant

Ben has over three years of experience in risk assurance and technology. He has performed GS007, SOX and ITGC audits across a wide range of organisations, including financial services, government and manufacturing. He has experience across external audit, internal audit, project management & data assurance projects.

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.