Internal audit during and beyond the Covid-19 crisis

A response to the crisis enabling Heads of Internal Audit to assess the key risks, redefine priorities and prepare for the future.

mazars

Dear internal audit community,

We publish this paper in challenging times. The world as we know it has seemingly paused, and we face unprecedented fights on both a health and economic front. Throughout this period, the role of internal audit will be critical.

This document has been drafted to enable internal auditors to provide tailored and relevant services aligned to industry guidance such as that of the Institute of Internal Auditors. The following pages include guidance on areas to assess and practical suggestions on how to engage with your stakeholders.

Since this is a time of global crisis, we have worked together as a global community to bring you this information. We hope that you find it useful and please get in touch if you have any questions or would like to discuss matters further.

As always, be well and stay safe.

Peter Cudlip
Global Head of Governance,
Risk, Compliance and Sustainability
Mazars

April 2020

Contents

The role of internal audit during Covid-19

What is business as usual in these unprecedented times?

The Covid-19 pandemic has had disruptive and unprecedented effects on individuals, businesses, governments and society. As such many organisations have shifted to employees working from home and adopted new operating models to continue business.

These exceptional times require a refreshed approach from internal audit (IA) drawing on the specific set of skills, competences, oversight and knowledge that IA brings. IA can't simply insist on delivering existing audit plans for organisations. Organisations are going through significant disruption and audit plans are unlikely to be fit for purpose now.

How should IA adapt its approach?

IA should fully assess the operational impacts organisations are facing and the new control environments they are operating under (mostly working from home and electronic based) and adjust the audit plan accordingly. This is so that IA can provide targeted and valuable contributions to organisations across their immediate priority areas over the coming months.

Organisations must understand and mitigate the crisis risks they currently face in the context of their own obligations, activities, objectives and values. Changing priorities at organisations should translate to changed priorities for IA. IA should provide relevant insights and assurance for the management of emerging risks due to the crisis.

IA should also be proactive and continue to play an important role in helping organisations understand the impact of Covid-19 on their control environment. This includes helping organisations build and shape their control environments in the context of home working arrangements and to provide insight and assurance on how effectively those controls are operating. IA has a role to provide consulting advice and front-line support under Global Internal Auditing Standards.

How should IA continue to deliver its ongoing assurance and advisory activities?

IA should undertake the following key actions:

- Understand and assess the full range of immediate risks:
  - Governance, communications and reporting
  - Risk and issue management
  - Controls environment
  - Operational risks
  - Human capital – health and safety and wellbeing
- Assess crisis management and business continuity plans, including IT arrangements.
- Advise on future risks and thinking beyond immediate risks.
- Adapt to remote working, still delivering effective services.
- Continue to monitor and update the organisation's needs and audit plan.

IA should provide direct support to management including being part of senior discussions. This is in order that IA provide valuable and timely inputs during these unprecedented times, rather than providing audit and assurance 'after the event' through performing 'post-mortem' reviews at some point in the future.

This is a time when IA can add real value and support organisations and stakeholders through difficult and challenging times.

Understanding and assessing the full range of immediate risks

Boards and Audit Committees want assurance that organisations have been able to adapt to the disruptions brought on by the Covid-19 pandemic. IA should support through the following actions:

- Understand and assess the potential impacts to organisations based on the immediate risks they are faced with. IA may facilitate the risk assessment.
- Consider the immediate challenges i.e. the issues organisations are currently facing, whether mitigation activities are sufficient, as well as considering the risks faced. It's likely the immediate issues are more of a current priority than potential risks.
- Help the board and senior management re-assess risks and whether current issue mitigation activities are sufficient.
- Help refocus the business on what matters most.
- Provide support and advice on key challenges they may be facing including government measures that they could benefit from.

There are a number of immediate risk areas that organisations should already be assessing and mitigating, they include:

- Governance, communications and reporting.
- Risk and issue management.
- Controls environment.
- Operational risks.
- Health and safety, and wellbeing.

The following pages look through each of these areas in further detail.

Practical guidance for auditors

- In the short term, auditors should disregard the corporate risk register (as it is probably outdated) and directly engage with stakeholders to understand the challenges they are facing. Pick up the phone and check on your key stakeholders.
- Think big picture. It's likely that some organisations face existential threats and IA should consider the current wider landscape and constraints organisations are operating under.
- Re-prioritise the audit plan. What is at the top of your audit plan is probably no longer related to the top risks the organisation faces. A fast but thorough reassessment of the top risks should be conducted, and the audit plan should be revised accordingly.
- Pushing to deliver the existing audit plan is not the best approach. There are a number of ways to support organisations including advisory/project work to attending management meetings and providing direct support and guidance.
- Audits should focus on just the key exam questions when planning audits. Audits should not progress per business as usual. Auditors need to ask tough questions about which scope areas are really essential to be covered and focus only on these. Its unlikely that organisations will have the appetite to review 'nice to have' or low priority areas for the next three to six months.
- Auditors should reduce the amount of stakeholder input required and produce short, sharp reports or advisory pieces.
- Audit reports should recommend only the most critical issues are remediated; anything else will likely be challenged.
- IA should consider adopting agile approaches. For example, short term prioritisation of audit areas with regular review and updates to the audit plan, aligned to organisational needs.
- IA can accelerate the use of analytics to deliver IA work remotely and to increase coverage.
- IA should talk about using the IA budget in a different way, for example direct support for key activities such as risk management, new systems and processes.

Refer to Mazars' Covid-19 Hub which includes guidance on hot topics and government measures:

www.mazars.co.uk/Home/Services/Covid-19-Your-Business

Governance, communications and reporting

Organisations that have quickly adapted their approach to governance, communications and reporting should be better placed to understand and mitigate operational impacts. IA should support through the following actions:

- Assess whether clear responsibilities between the board, audit and risk committees, and the management team are in place.
- Assess whether timely and relevant information is being received by the board.
- Help management develop centralised, timely messaging from leaders disseminated to employees to instil confidence and calm, and counter against fear and misinformation.

Risk and issue management

Boards and audit committees want insight and assurance that organisations have been able to quickly adapt their operational approach and that it is working effectively.

IA should consider how to best contribute to risk management processes. For example, feeding into risk management groups/meetings and facilitating the risk assessment process.

This is particularly important for risk and issue management processes which IA should support through the following actions:

- Review the operational risk management capabilities, such as crisis management, business continuity, third-party risk and insurance.
- Verify that all key members of the team have been identified and fully understand their duties and are confident in their ability to carry out the responsibilities.

Practical guidance for auditors

- Assess whether management has adequate resources internally or externally to help in assessing and mitigating risk. Determine whether management are planning for longer time horizons; this should be a minimum of 6 months with current government measures in place.
- Assess whether governance and reporting processes have adapted to home working. This includes whether what is being reported and escalated upwards is appropriate and focused on the high risk or high priority areas, i.e. the operational areas most impacted.
- Offer support to organisations that is not just limited to IA. It might be that organisations have insufficient staff for a number of reasons (including staff on sick leave) and require 'boots on the ground'. Therefore, they might require risk, controls and compliance specialists to bolster in-house teams across the business.

Practical guidance for auditors

- Understand risk and issue management processes including reporting and escalation. Does the organisation place value in risk management, how has it changed since home working has started?
- To what extent is Covid-19 impacting on the existing risk management framework and corresponding risk registers? Is the organisation pro-actively working to identify possible risks, impact and mitigating responses?
- If the operational risk management capabilities do not exist or are insufficient, offer to involve risk management and IA professionals to assist in the development and roll-out of a risk management framework.

Understanding and assessing the full range of immediate risks

Control environment

Boards and Audit Committees will want assurances that organisations have been able to quickly and effectively adapt their operational approach and control environment to the new ways of working brought on in response to Covid-19.

This is especially important for the maintenance of the control environment which IA should support through the following actions:

- Understanding how organisations have implemented and embedded a new control environment under these challenging circumstances.
- Ensuring that (adjusted) key controls are in place, such as minimum level of segregation of duties, evidencing of management reviews and approvals etc.
- Consideration of training, support and additional management oversight, checks and reporting should be given.

Practical guidance for auditors

- Auditors should not rely on last year's file or a bank of expected controls when assessing new control environments.
- Auditors should go back to a blank page, document and assess processes in order to capture controls before assessing whether they mitigate current risks.
- Some questions that auditors should consider are:
  - Are key controls covered and effectively designed in the primary processes?
  - Should additional controls be considered regarding the organisation's exposure to internal and external influences?
  - How can management supervision of employees be maintained when staff works from home?
  - Have additional management checks been considered and designed, such as risk and compliance?
  - Have new management reports been designed and implemented?

Operational Risks

Stakeholders within organisations will want assurance that business units and teams understand their key operational risks and have put effective measures in place to mitigate those risks. That could be over, but not limited to, the following areas:

- **Customer behaviours.** These are likely to reduce demand and sales, resulting in lower revenues and cashflow impacts. This could result in an existential threat to organisations.
- **Supply chains.** There could be interruptions in supply chains resulting in risks to production. Organisations should:
  - Determine which business partners and vendors may be most severely impacted and if alternative vendors can provide a solution to meet business needs.
  - Assess if suppliers have documented plans for business unit continuity and information technology disaster recovery, including for critical business.
  - Change the production mix and plan for new delivery methods to reach customers.
- **Capital and liquidity.** IA should understand working capital requirements against scenario planning assumptions and forecast cashflows. This includes assessing whether organisations have made use of government schemes.
- **Contract compliance.** There is a risk that contractual obligations may be impacted. Organisations should:
  - Consult their legal advisors and review their contracts to determine the impact and the rights they have.
  - Take reasonable steps to mitigate the impact of Covid-19. They may need to quantify the amount of financial damage and the impact on their long-term business relationships.
  - Review their existing insurance policies to find out whether any losses they incur relating to Covid-19 can be covered under existing terms.

Practical guidance for auditors

- A should assess how organisations are reacting to changes, including the associated governance processes and controls including over:
  - Capital and liquidity
  - Cash collections
  - Supplier payments
  - Production
  - Supplier and vendor management.
- IA should assess how effectively change management processes are being undertaken.
- IA should assess whether organisations have asked themselves the difficult questions to truly understand the operational impacts of Covid-19. This includes putting in place short, medium and long term actions.
- IA should advise on liquidity and financial management and, in particular, focus on contract risk.

Refer to Mazars' Covid-19 hub which includes guidance on cashflow management:

www.mazars.co.uk/Home/Services/Covid-19-Your-Business/Covid-19-Cash-Flow-Management

Understanding and assessing the full range of immediate risks

Human capital – Health, safety and wellbeing

Employers have the same health and safety responsibilities for home workers as for any other workers. With the government's social distancing and self isolation measures there are now greater risks to the mental and physical wellbeing of individuals.

Organisations have rapidly made home working arrangements for the large majority of the workforce in order to follow government guidelines and ensure that operations can carry on. As a consequence, the typical health and safety checks might not have been fully undertaken. It's expected that the current government lockdown will remain in force for a prolonged period of time and to a lesser extent beyond the summer period.

Therefore, organisations will want assurance from IA that they are providing appropriate support for their employees to enable them to work in a safe environment. This includes putting in measures to support employees' mental wellbeing, in addition to their physical wellbeing.

Practical guidance for auditors

When someone is working from home, permanently or temporarily, IA can support organisations to consider:

- How will they keep in touch with home workers?
- What work activities will they and can they be doing (and for how long)?
- Can this activity be done safely?
- Should control measures be put in place to protect them?

Auditors should assess whether 'workarounds' used during the lockdown period are normalised and appropriately controlled.

Auditors should assess whether the impact to new ways of working have been considered by HR and performance management processes, such as annual performance assessments, and the approach to training and coaching.

Refer to Mazars' Covid-19 Hub which includes guidance on people in your business:

www.mazars.co.uk/Home/Services/Covid-19-Your-Business/Covid-19-People-In-Your-Business

Assessing organisational resilience

IA should consider what impact Covid-19 is having on an organisation's resilience including existing crisis management and business continuity plans. This is in order to assess whether there are any gaps in those plans. IA could also provide assurance on effectiveness of selected crisis actions.

IA should consider when they last reviewed these arrangements and whether any further advice, support or assurance could be provided. This could include assessing lessons learnt of how those plans worked in practice.

IA could also consider what arrangements organisations are putting in place for the 'recovery' phase and how they will meet demands as restrictions are lifted etc.

Organisations should have implemented existing crisis management and business continuity plans by now. For many organisations, having to operate with the majority of the workforce working from home, is not something that was planned for. This brings a number of IT challenges which IA should assess, for example:

IA should assess the changed risks related to the stronger dependency and use of IT as core enabler in the crisis, which may include the following areas:

- Whether security settings for remote connections and secured individual access mechanisms are in place and operating effectively.
- Determine sufficiency of network capabilities for a large number of employees working remotely for an extended period.

Due to greater flexible working and remote arrangements, individuals require greater access to systems, including covering when people are off work. Therefore, critical user access controls should be maintained. IA should consider the monitoring controls in place, whether there is appropriate segregation of duties and audit trails for changes to access.

Practical guidance for auditor

As noted previously, many organisations will have implemented and embedded new control environments. These have been supported with IT Auditors and should assess the following:

- Whether there is sufficient IT capacity to deliver the services required.
- Whether appropriate security measures are in place.
- That controls have been designed and implemented adequately.

There is still value in reviewing crisis management and business continuity plans for any gaps and to determine the best way to ensure stakeholders are informed of the organisation's activities. This includes educating staff on the protocols to follow should a local outbreak occur or further measures introduced by the government.

Refer to Mazars' Covid-19 Hub which includes guidance on business continuity measures:

www.mazars.co.uk/Home/Services/Covid-19-Your-Business/Covid-19-Business-Continuity-Measures

Advising on future risks and thinking beyond immediate risks

Whilst organisations are often focused on their immediate risks and challenges IA should support organisations in thinking beyond their immediate challenges. This could be to the wider risks that organisations could face
as they adjust to the 'new normal'.

These risks could include cyber, fraud, culture and human capital, supply chain, health and safety and reputational threats. Given the quick change for many organisations to home working, organisations should initially consider fraud risk:

- The change of controls, whether intentional or unintentional, may also trigger the circumvention of controls, softening of segregation of duties principles or overriding usual approval procedures.
- Deviations from the business-as-usual mode and the potential rationalisation of resources often results in a lower level of control. This together with increased operational pressures, could create opportunistic behaviours by individuals.

IA should assess and help organisations interpret regulatory changes such as banking requirements for increased portfolio stress tests or continuity documentation.

IA should also provide advice regarding communication and revised audit practices. There might be a need to assist organisations communication with stakeholders and adopt emerging guidance regarding virtual audit evidence.

Furthermore, there will be a need to assist organisations to evaluate whether control transformations have been embedded adequately. IA can assess whether controls continue to operate as intended and whether documentation is adequate. This may include remote working policies, transaction authorisation and reconciliation and physical security, among other topics.

Practical guidance for auditors

- Internal auditors should use knowledge of similar organisations (through peer relationships or co-source partner) to advise on how other organisations are facing similar challenges.
- Internal auditors should pass on best practise between organisations including over the future risks they are expecting.
- Regarding the potential risk of fraud and accordingly, IA should consider the following questions:
  - Is there an existing Fraud Risk Assessment in the organisation? Has it been updated to reflect threats and risks for Covid-19?
  - Has the organisation considered which processes have a higher risk of fraud?
  - Are key controls covered and effectively designed in processes?
  - How can employees be controlled or checked upon if they work from home?
  - Is there sufficient awareness of areas where fraud is possible, such as invoicing and payments?
  - Has the organisation considered implementing low friction counter measures to prevent fraud risk? These can include electronic checks to identify and verify the applicant/business/ beneficiary account, or using upfront fraud prevention clauses in application forms and processes.

Continuing to monitor and update the organisation's needs and audit plan

IA should work closely with management to continually monitor what is happening within and outside of organisations.

IA should support organisations to start looking past the current crisis and to consider resumption planning. There may a realisation by many organisations that their resumption plans are inadequate. Additionally, it is highly likely that changes in business models will require new resumption strategies and tactical plans.

Going forward it is likely that organisations will look at their processes to ensure they can be delivered in an agile, remote way. This will include further digitalisation and automation. There will likely be a need for organisations to re-evaluate manual processes and plan for more automation to not only improve efficiencies and cost performance but also reduce risk of reliance upon on-site resources. Robotics Process Automation (RPA) may include the design and implementation for operational areas as well as IA. There may be areas that IA should assess over the governance, risk and controls around these transformed processes.

IA needs to be agile and to adjust plans accordingly and where possible work with other functions within the organisation such as risk and compliance.

IA can help organisations build an integrated approach to providing insight, assurance for the board and audit committee.

Practical guidance for auditors

- Auditors should engage in a continuous and frequent dialogue with stakeholders to monitor and understand the challenges they are facing.
- Auditors should increase the number of progress meetings, regularly call and check on their key stakeholders.
- Auditors should continue to focus on the big picture and not be bound by IA plans. These should be adjusted and amended as organisations face different challenges.
- In additional to standard IA services IA could offer to provide advisory services or resources to take on business roles if required.

How we can help

There are many ways in which organisations should prepare for the 'new normal' and operating after the pandemic recedes. These could be driven by:

- Changes in strategy
- Changes in operating model
- Changes in IT strategy and architecture including automation of processes
- Changes in customer and supplier relationships and interactions
- Changes in the working environment

There are many drivers for change within organisations. We have the capabilities and capacity to support organisations in many ways – through internal audit engagements, advisory or consulting arrangements.

The following pages include some of our core services offerings which organisations could find useful to help navigate through these challenging and unprecedented times.

Organisational resilience

Organisations operate in a constantly changing environment with the need to prepare and plan for a wide range of strategic and operational risks, and respond quickly to crises. Building resilience is an imperative for all organisations and requires an effective combination of risk management and continuous improvement. Every organisation, irrespective of size or shape, requires an organisational resilience framework that addresses the following areas. We can support organisations to document a framework or provide assurance over existing frameworks.

Governance

Providing oversight, decision making and strategic direction in crisis and change.

Risk and issue management

Identifying, assessing and mitigating risks to reduce the probability of impact of those risks,

Change management

Moving to new ways of working to seize opportunities, respond to risks or crisis, and continuously improve.

Disaster recovery

Recovering infrastructure, systems, applications and data following a crisis.

Crisis management

Responding to a crisis through effective control, communication and management.

Business continuity management

Enabling an effective response to crisis so that important services can continue to be delivered.

IT resilience

Appropriate IT resilience can prevent or delay the need to invoke your IT Disaster Recovery Plan in the first place. IT resilience should focus on:

- **Technology**. Component and device resilience, removing unacceptable single points of failure and scalability.
- **IT people**. Key person risk, staff and third-party capability.
- **IT processes**. Alignment to IT standards including incident response and capacity and availability management.

Traditional IT Disaster Recovery (ITDR) assumes loss of a key application or a total IT outage (a data centre fail, for example) and details the processes IT would follow to recover these in line with the agreed timescales. The ITDR Plan is unlikely to detail how to manage a fundamental, almost overnight, change in how users and customers consume IT.

Traditional Business Continuity Plans (BCPs) assume the loss of a single office building rather than an entire shutdown of all office buildings at once, or government legislating a national economic shutdown for an undefined period of time.

Covid-19 is unusual because it fundamentally changed the way an organisation would use IT without causing any actual or direct IT related IT disasters or failures. Instead we see:

- Capacity pressures on remote working solutions and networks.
- Increased traffic to websites.
- Increased IT demands on IT service desks (including cultural shifts/help).

Covid-19 will be a likely catalyst to permanently shift working patterns including -

- Less travel / consumerism = reduced emissions and pollution.
- Businesses are forced or learn to embrace remote working more regularly.
- Businesses may find that their employees don't want to fully return to office-based working once the closures are lifted.

Remote working and future cost/revenue pressures could also result in other business changes such as –

- Business Strategy
- Restructuring
- Accommodation Strategy - (rationalisation of commercial buildings)
- All these changes could fundamentally alter an organisation's IT needs requiring a reassessment of:

1. IT resilience / ITDR & BCP alignment
    - Covid-19 IT lessons learned. What went well and what not so well? Did IT third parties support you as expected?
    - IT resilience. Is your IT resilience appropriate for your business?
    - IT disaster recovery. What ITDR arrangements are in place and are these appropriate for the future direction of the business?
    - Business Continuity Plan (BCP) alignment. Are your ITDR arrangements aligned to your BCP?
2. IT architecture.
    - Is the IT architecture correct for the future direction of the business?
3. IT strategy.
    - Will Covid-19 prompt a change in business and digital strategies that need to be reflected across your entire IT function?

If the business strategy will change as a result of Covid-19, consider completing the above in reverse order. IT resilience should still be reviewed in the short term also with a specific focus on IT stability.

Change and programme assurance

All organisations have undertaken change as a result of Covid-19 with many viewing this as a challenge, but it's also an opportunity to redesign process so that they are more efficient. This is something which can be undertaken remotely and to remove points of failure. Organisations will implement change initiatives and programmes to deliver the 'new normal' and post pandemic operational environment.

Therefore, having effective change and programme assurance is essential to assess whether key change risks are being effectively managed. Our change and programme assurance methodology considers these three key areas:

- Programme management. Is the programme or project appropriately defined, planned, resourced, budgeted, managed, governed and aligned with strategies and other change initiatives?
- Change management. Is the change management effort appropriate with reference to expected leading practice approaches?
- Business as usual. Is any potential disruption to business as usual activities caused by the programme or project being effectively managed and mitigated?

Health check approach

Programme closure

- Is there plan for programme closure?
- Has a lessons learned exercise been planned?

Planning and preparation

- Is the business case clear?
- Are objectives clear and measurable?
- Is there a high-level programme plan that is up to date?

Key deliverables

- Are key deliverables in place?
- Are they of appropriate quality?

Governance and structure

- Is there an appropriate programme board in place?
- Is this board informed and effective?

Implementation

- Are there detailed implementation plans?
- Is a testing strategy defined?

Controls and quality

- Has the business case been updated throughout the programme?
- Are change controls in place?

Reporting and communication

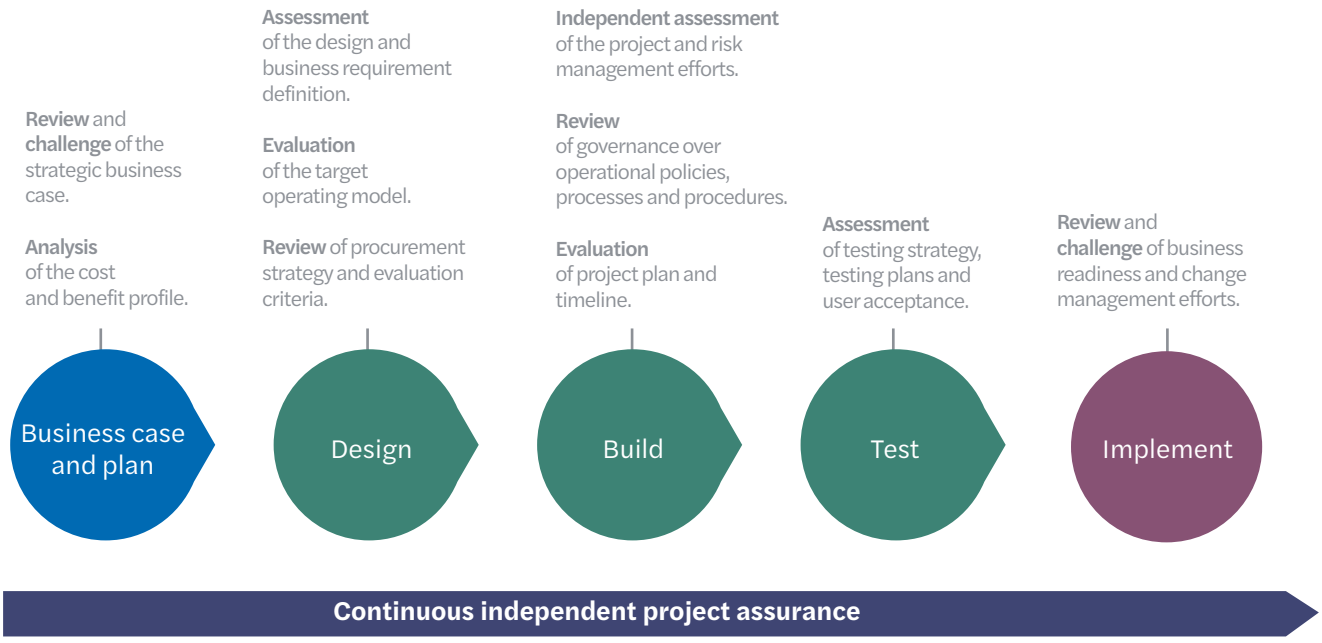
- Is there effective regular reporting?
- Has a communications strategy been defined and implemented appropriately?

Risk management

- Are risks identified and assessed?
- Are actions regularly reviewed and reported?

Our approach includes programme or project 'health checks' and 'deep dives' around key areas for concern. A health check can be undertaken at any time either as a one-off point in time assurance, or can be updated iteratively to provide continuous assurance through the project life cycle. Deep dives can also be undertaken at any point and would be limited scope with a full depth focus on a specific identified risk area.

Deep dive approach



Ethical hacking

Are you aware of all the vulnerabilities which your organisation could fall victim to?

IA should consider what impact Covid-19 is having on organisation's IT security and to assess whether there are any gaps. We have been seeing Covid-19 being used in cyber attacks, including spear-phishing, business email compromise, malware, ransomware and malicious domains. Coronavirus themed domains are on an increase and criminal threat actors are targeting more businesses for financial information, or requests to transfer money.

Penetration tests are simulated attacks carried out by our penetration testing team who employ the same techniques that attackers do.

These tests reveal if your systems or applications will withstand hostile attacks and whether discovered vulnerabilities can lead to further intrusion and exploitation.

By having staff to work from home, the Covid-19 outbreak has brought cyber security risks related to remote working to the forefront. Without the perimeter defences and the layers of controls from the internal networks, user computers are directly exposed to new attacks and the user security awareness has become even more relevant.

In the meantime, while the IT teams are adapting their toolsets to manage remote computers, the internet exposed infrastructure of the company is still relentlessly probed and attacked. Thus, businesses are at risk of being compromised, losing or disclosing sensitive data and breaching data protection and regulations as well as potentially damaging reputation. Therefore, this represents an important area of senior management focus.

How can we help?

Mazars has developed a unique approach towards our high quality services, deploying them in a range of complex environments and scenarios.

Using our extensive skills in penetration testing, we are able to replicate the tactics, techniques and procedures of sophisticated attackers to identify vulnerabilities before they can be exploited. This provides the protection and detection capabilities an organisation requires to repel the next generation of vulnerabilities.

Our specialised testing team provides a holistic approach towards threat activity management of an organisation.

Our services go beyond penetration testing to explore the response and recovery aspects to test your security as a whole by replicating the latest attack Tactics, Techniques and Procedures (TTPs).

As the pandemic intensifies, cyber criminals continue to take advantage of opportunities and phishing attacks and ransomware are set to rise.

Our security services help support business uncover vulnerabilities and assess risk, including:

- Remote working security hardening, including end user computers, remote access solution and mobile devices.
- Web application penetration testing.
- External infrastructure penetration testing.
- Phishing exercises mirroring real life campaigns

Robotics Process Automation (RPA) – Your digital workforce

The measures undertaken in every country to prevent the spread of coronavirus are having a major impact on organisations across sectors. In usual circumstances, they would be expected to provide their products and services without disruption and in line with government guidance – but, as we know, there are a number of challenges to achieving that in the current crisis.

Organisations we've spoken to foresee an enormous peak or decline in the demand for their services and are exploring ways to undertake the work required to serve their customers profitably, whilst balancing that with the likelihood of limited staff capacity. There is, however, an opportunity to optimise their operations, reduce costs and increase efficiency of their customer engagement services, and one of the key considerations to this is the deployment of their digital employee or workforce.

What is a digital workforce?

A digital workforce is a set of software robots, usually referred to as robotic process automation or RPA. RPA is already used in many organisations to execute monotonous and repetitive activities – for example, within support processes. A software robot executes these activities instead of your employees without requiring large and impactful changes to your IT environment. This development can be done in a relatively short period of time (often in weeks). And once in place, the big advantage is that a software robot can be productive 24/7 without errors – providing services without disruption. Furthermore, RPA can work on top of existing legacy applications, thereby saving you costs on any new system upgrades or implementation projects.

How can the digital workforce help?

The digital workforce can perform many of your core and support activities including, but not limited to, the following.

- **Revenue management**.
- **Customer engagement**.
- **Contract management**.
- **HR functions** such as payroll, benefits management, education and training records management, recruitment and new joiner processes.
- IT functions such as infrastructure/application monitoring, folder and file management, user/directory and release management, network monitoring and desktop support.
- **Finance functions** such as reconciliations, claims processing, expense payments, returns management and inventory processing.

How can Mazars help?

Mazars have extensive experience across sectors and can leverage our RPA capabilities and robot libraries to develop and deploy your digital workforce. We have partnerships with all of the leading RPA software providers while also remaining independent, so you know that we are working with the best software for your particular needs.

We can deliver the engagement remotely, using our remote working arrangements such as MS Teams, Huddle, and remote RPA development and deployment using our development centres in Slovakia and India. The use of robot libraries and remote development shortens the development time considerably and also reduces the overall cost of development. Our maintenance services can support you whenever necessary, even after deployment of robots in your environment.

Our services

Continuous monitoring

As the pandemic evolves, organisations are reconsidering their conventional ways of operating business to create a new normal for the future. Equally, internal audit and compliance functions have to innovate and evolve fast, for being relevant in the current crisis and new normal. To meet expectations of the business, internal audit and compliance functions are exploring ways to provide insights in a timely manner, reduce overall costs of control testing and identify opportunities for improvements across the business. A key consideration is to automate controls testing using data analytics and use visualisation for engaging their stakeholders, and this need is filled by Mazars Curious, our continuous monitoring tool.

What is Curious?

Curious is our proprietary business process analytics tool that combines the power of the following into one.

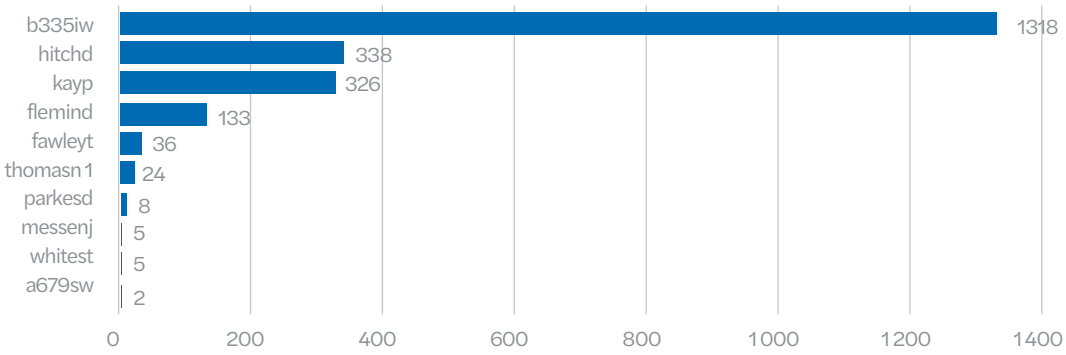
- Controls monitoring
- Process performance
- Fraud detection

Curious test suite has more than 100 tests and relevant dashboards, covering several standard process areas and sub processes, but not limited to the following.

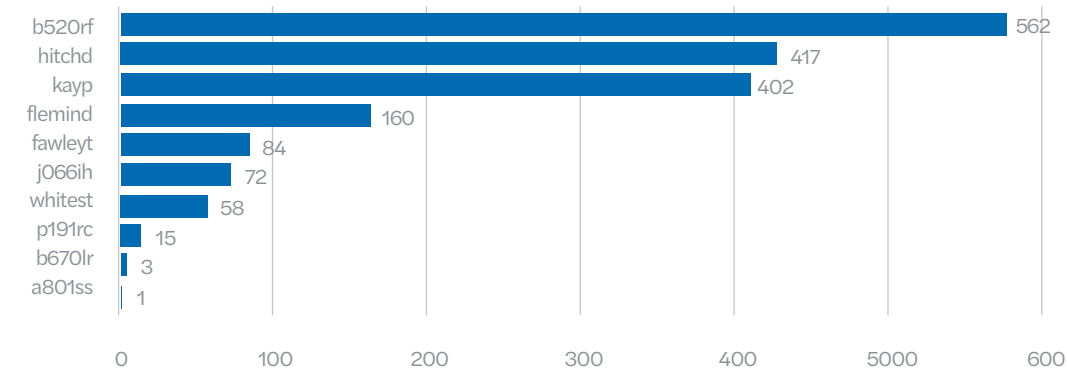
- Sales
- Purchase
- Accounts payable
- Accounts receivables
- Expense analytics
- Spend analytics
- Payroll
- Journals

Process control - Approval limits

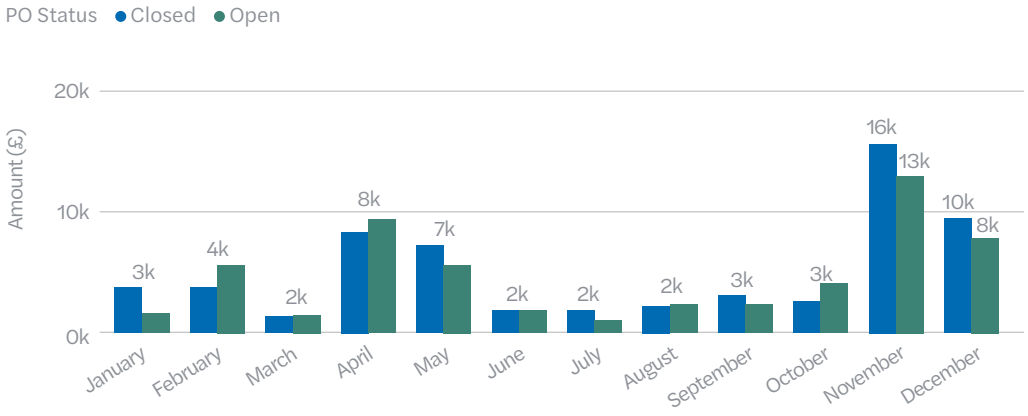
Top 10 approval limit violations by user & transaction count - PO



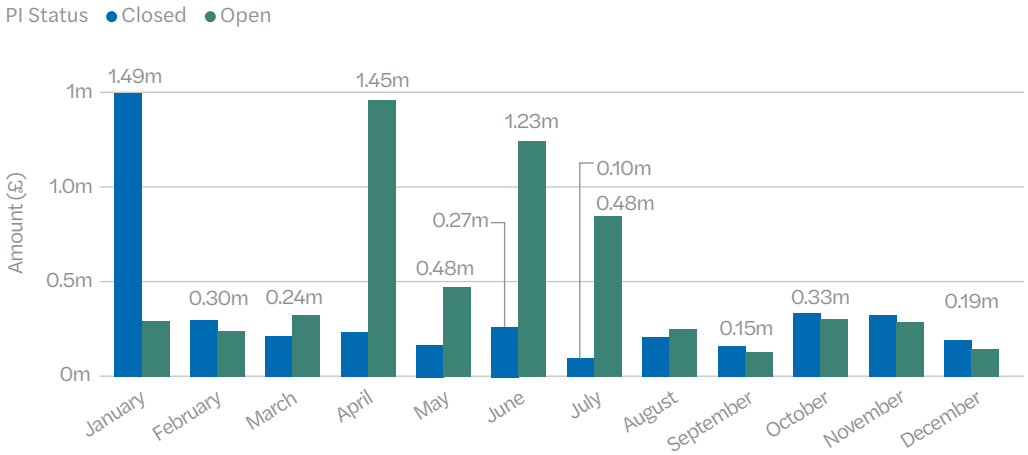
Top 10 approval limit violations by user & transaction count - PI



Violation of approval limits - monthly PO trend (drilldown)



Violation of approval limits - monthly PI trend (drilldown)



Curious can be implemented on premise leveraging your existing investments in IT or provided as a fully managed service.

How can Curious help?

The management or IA function could use Curious to monitor IT systems, process transactions and controls on a frequent or continuous basis, throughout a given period. Curious can drastically reduce the time required to innovate and help accelerate transformation driven by analytics, since it can be easily deployed and customised to meet your needs.

How can Mazars help?

We can quickly implement a proof of concept (PoC) with fixed fees in few weeks, that will demonstrate Curious' value to your organisation. Once the PoC is established, we could help you create a business case and scale-up to cover various process areas in your organisation. We can implement Curious using our remote working arrangements such as MS Teams, Huddle and cloud based environment, with minimal time from your staff. Our pricing also has flexible plans to provide you with different options to meet your needs and be the catalyst for you to embark on transformation journey driven by analytics.

Acknowledgements

With thanks to our global partnership for their contributions

UK

Keith Bonjour
Assistant Manager
Keith.Bonjour@mazars.co.uk

Graeme Clarke
Director
Graeme.Clarke@mazars.co.uk

Matt Dalton
Partner
Matt.Dalton@mazars.co.uk

Christian Fell
Manager
Christian.Fell@mazars.co.uk

Alan Frost
Director
Alan.Frost@mazars.co.uk

Andrew Hoyle
Partner
Andrew.Hoyle@mazars.co.uk

Sam Patel
Partner
Sam.Patel@mazars.co.uk

Syed Shah
Senior Manager
Syed.Shah@mazars.co.uk

Anish Venugopal
Senior Manager
Anish.Venugopal@mazars.co.uk

India

Ravindra Rao
Partner
Ravindra.Rao@mazars.in

Germany

Kai Beckman
Director
Kai.Beckman@mazars.de

Mexico

Enrique Romero
Partner
Enrique.Romero@mazars.com.mx

Netherlands

Michel Kee
Partner
Michel.Kee@mazars.nl

South Africa

Ghitesh Deva
Partner
Ghitesh.Deva@mazars.co.za

USA

Peter Shablik
Director
Peter.Schablik@mazarsusa.com

Contacts

Peter Cudlip
Global Head of Governance, Risk, Compliance and Sustainability, Mazars
peter.cudlip@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws

www.mazars.com/IA

mazars