Internal Audit during COVID-19

As organisations are navigating a new reality – confronting interruptions and disruptions – it is more vital than ever that organisations ensure good risk mitigation practices remain in place to manage rapidly evolving risks and minimise impacts.

Adding value during times of crisis

The recent events that have unfolded as a result of the COVID-19 pandemic are an important reminder that neither internal audit (IA) plans nor the ways of accomplishing these plans are static. Redefining the IA plan to reprioritise audits based on evolving organisational risks, ongoing regulatory requirements and the practicalities in executing each audit can help support management in addressing the most crucial risks while also reinforcing the IA team's relevance and purpose.

The COVID-19 pandemic presents an opportunity for organisations to embrace new ways of working and the technological enhancements that will continue to enable them even after a return to business as usual. For internal auditors, the pandemic also presents an opportunity to reaffirm the importance of the function by actively and flexibly responding to evolving risks in a changing environment.

To assist in this process, Grant Thornton has identified the **Essential 8 internal audits** that we consider as the most relevant for organisations to consider for IA plans in the current environment. Keeping with good practice, the plan should be continuously reviewed as risks and priorities change.

Essential 8 Internal Audits

The uncertain timeframe of COVID-19 means remote working practices are quickly becoming business as usual and management should push forward with an internal audit plan to actively manage risks during the pandemic.

The **Essential 8** audits cover a range of topical risks that may have increased due during the pandemic – including assessing third-party exposure, monitoring of cyber threats, protecting employees' heath and ensuring continuity of business operations.

Below we have outlined the **Essential 8** along with further explanations on why these are important to consider including in your internal audit plan during the pandemic.

- Business Continuity Management
- Cyber Security
- Payroll Compliance
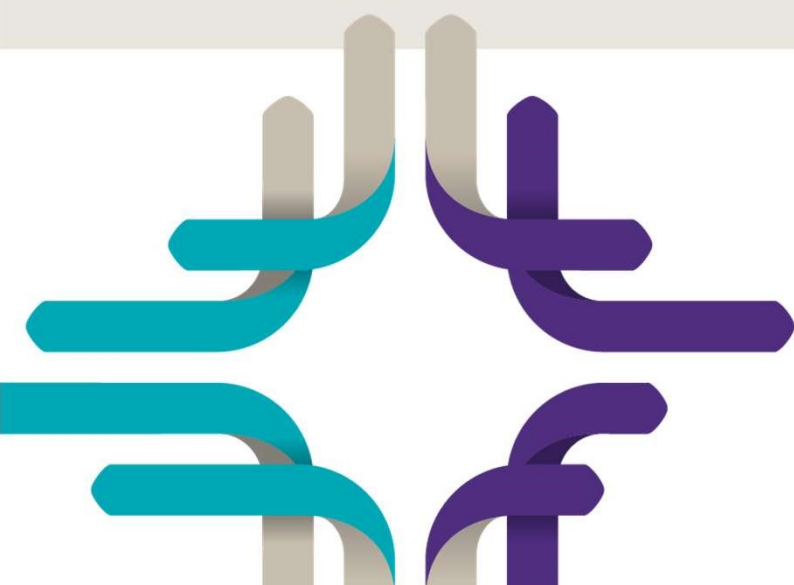- Procure to Pay
- Remote Working
- Modern Slavery
- Program Management
- Vendor / Outsourcing

Business Continuity Management – Real-time review

- Unique opportunity to identify real-time lessons learned from the pandemic as stakeholders have enacted the Plans recently so issues / insights / lessons learnt are top of mind
- A good time to refresh key risks and dependencies including suppliers and vendors.
- Important to remember that additional disruptions are possible during the pandemic.

Cyber Security

- Rise in scam and phishing activities where attackers use COVID-19 as bait to impersonate authorities and brands (misleading employees and customers into giving up confidential information).
- Higher demands on remote access technologies creates pressure on security that may result in external frauds, especially when employees use unsecure personal devices to perform official duties.
- Challenging to enforce, detect and respond to security issues in a remote working environment.
- Rapid changes in systems and access levels places greater emphasis on strict controls around remote security management.

Payroll Compliance

- A hot topic before the pandemic outbreak and may be even more difficult to assess and manage in the current environment.
- In addition, many organisations are making large volumes of changes and agreeing non-standard working arrangements during the pandemic.
- Added difficultly to oversee/control dispersed workforce
- Increased pressure may also result in internal frauds.

Procure to Pay

- A key risk for organisations pre-COVID-19 with the process facilitating significant expenditure. With remote work practice key controls such as segregation can be difficult in this time. It is more important than ever to have strong oversight including both preventative and reactive controls in place to mitigate risk of human error or fraudulent transactions
- Emergency procurement and payments in response to the pandemic exposes the organisation to internal and external fraud where limited controls exists.
- Mismanagement of contract variations occurring as organisations re-negotiate terms of businesses (including variation approvals and reporting).

Remote Working

- The need to move the majority of the workforce to operate remotely has occurred rapidly. As outlined above, increased cyber risks are associated with this, however, there is also significant risk to your organisation's number one asset – your people.
- It is more important than ever for Management and Boards to have oversight and understanding of how the organisation is mitigating the key risk of the remote workforce which includes (but not limited to):
  — Poor workspaces impacting productivity or potential WHS issues
  — Isolation / lack of human interaction impacting mental wellbeing
  — Disengaged team members resulting in decreased productivity / loss of key talent
  — Systems and hardware failure / outages impacting ability to operate as BAU
  — Lack of oversight of teams increases risk of fraudulent activities

Modern Slavery

- Another hot topic before the pandemic outbreak which may have increased risks in the current environment. COVID-19 should not take away the importance of this matter.
- Many organisations will be required to report on their modern slavery program as soon as 31 December 2020.
- Increased job insecurity in the pandemic environment can result in the vulnerable population being taken advantage of and coerced into forced labour and related practices.

Program Management

- Perceived benefits of business case may have changed in light of COVID-19 impacts, as well as viability of effective project execution.
- Organisations may look to revise expenditures and focus on projects with lower cash outlays or stronger potential for near term returns.

Vendor / Outsourcing Management

- Operational and revenue impacts from potential disruptions to key suppliers and vendors require ongoing monitoring.
- Business case and risk profiles for suppliers may have shifted due to changing business priorities.

Our Services

As an established global professional services firm, Grant Thornton understands internal audit plans and the need to have independent oversight. An objective audit program is necessary to ensure the information collected is reliable and trustworthy, an aim we will be fully committed to fulfil. With the extensive experience in internal auditing held by our team, you can have confidence in our ability in designing, delivering and reviewing audit plans.

Contact us for your Internal Audit enquiries:

George Sutton
National Head, Business Risk Services
Sydney
+61 2 8297 2451
George.Sutton@au.gt.com

Matthew Green
Partner, Technology Risk
Melbourne
+61 3 8663 6168
Matthew.Green@au.gt.com

Jarrod Lean
Partner, Business Risk Services
Sydney
+61 2 9286 5451
Jarrod.Lean@au.gt.com

Katherine Shamai
Partner, Business Risk Services
Melbourne
+61 3 8663 6123
Katherine.Shamai@au.gt.com

Stuart McDowall
Partner, Grant Thornton Consulting
Brisbane
+61 7 3222 0282
stuart.mcdowall@au.gt.com

Daniel Farthing
Director, Technology Risk
Sydney
+61 2 8297 2650
daniel.farthing@au.gt.com

Jane Stanton
Director, Financial Services
Sydney
+61 2 8297 2620
jane.stanton@au.gt.com