Government
Internal Audit
Agency

Nathan Paget

COVID-19 Considerations

OFFICIAL-SENSITIVE
This paper suggests areas for consideration in the current phase of the response.

Internal Audit – Work Impacts / Mitigation

1. **Embedded Assurance** – embedding IA in teams and conducting short focused reviews in critical areas.
2. **Secondment out of IA** – Where the business demand for skills that we have is needed and a priority.
3. **Remote Auditing** – Carrying on with activities where they can be reviewed remotely.
4. **IA Plans** – Plans are being agreed on a quarterly basis as any annual plan would be nugatory.

Other considerations

Actions taken on remaining work 2019 – 2020

- All audits started and the majority of fieldwork completed to be concluded, as they can be worked remotely.
- HIA – Year end opinion to cover the timetable for year and activities (subject to changes).
- Governance Statement will need to cover the COVID-19 response.

Planned work 2020-21

- Draft plan 2020-21 – Not presented and replaced by quarterly plans.
- Prioritization – Depending on impacts we will assess the Q1 audits to explore the possibility of remote review.
- We will keep the monthly liaison meetings on how DEFRA teams are coping, and support as required.

Tackling the COVID-19 challenges (1)

Crisis management / Response:

- Establish a crisis response structure with established workstreams, clear responsibilities and accountabilities.
- Develop likely and reasonable worst case scenarios and their potential impact, to support crisis and response planning.

Workforce:

- Assess potential impact and develop options to identify and move labor with the key skills to support the critical work – BC plans are a good reference point.
- Proactively manage where, when and how disruption will impact the availability and effective utilization of skills in the business.
- Health & Safety – in a COVID-19 sense and wider business sense.

Operation & Supply Chain:

- Develop a rapid communications plan and approach to build and maintain trust and reputation during the crisis for key stakeholders.
- Tailor best practice templates and communications materials such as emails, FAQs and intranet.

Tackling the COVID-19 challenges (2)

Focus on Data:

- Identify data needs and develop protocols for data extraction, preparation and analysis.
- Model the impact of scenarios on the sector and stress test finances against downside economic scenarios.

Customers:

- Prioritize actions to protect customer relationships and interests.
- Model customer behavioral change.

Corporate Support:

- Legal, IT, Commercial and Insurance: review existing insurance coverage, IT infrastructure and resilience, force majeure, contract clauses.
- Finance, financing, restructuring and year end arrangements.

Further Considerations

Operations, policy and functional representatives within your organisations should be proactively engaged to consider the specific challenges faced, consider suitable options, assess risks and decide how best to manage these.

Attempting to define a single approach or attempting to be comprehensive in coverage would be misguided because each organisation has its own context, but **some categories of risk may be more common** for consideration as each organisation seeks to respond quickly, proportionately and cooperatively.

People

The health and well-being of employees during the outbreak is a key risk, as well as a necessity in the continuing management of other areas of risk faced.

- Risk assessments: conducted and regularly reviewed to ensure a safe place of work for employees and contractors, including good hygiene practice and Personal Protective Equipment.
- Organizations should ensure that they know about people that are at higher risk due to pre-existing health conditions and take action.
- Make and implement plans to reduce travel and facilitate working from home where possible. The use of technology to enable work to continue without physical proximity will be essential. Give employees clear guidance on when they should attend work and when they should stay away. Review this advice on a regular basis, based on the changing situation and good management information.

Operations

Organizations will have deployed aspects of their business continuity plans, and these will form the basis of their response. Not all arrangements though may have foreseen a situation as widespread, complex and potentially prolonged as the challenges being faced. Nor do plans always prove deliverable when faced with real life situations.

- Be agile and re-prioritise ruthlessly. Review key objectives and priorities in the light of current information. Balance ‘business as usual’ against new demands and changing priorities. Undertake risk assessments in respect of the impact on your key objectives and prepare and implement response plans, including near-term actions.
- Form multi-disciplinary teams that span across operations and functions to evaluate the challenges and options holistically. Model, stress test and understand the implications of various scenarios. Empower designated staff to make decisions quickly.

Commercial

Suppliers will also have deployed aspects of their business continuity plans.

- Confirm these with key suppliers and their supply chain. Take this further and look across your wider extended enterprise. Critical processes need to be studied in detail, getting more information from suppliers as required to assess potential risks resulting from non-performance or the stoppage of services.
- Understand how your contracts work. Ensure that you maintain safety and maintain transparency if alternative suppliers are used.
- Ensure you have appropriate legal advice.
- Further guidance and advice should be obtained from your Commercial function as necessary.

Financial

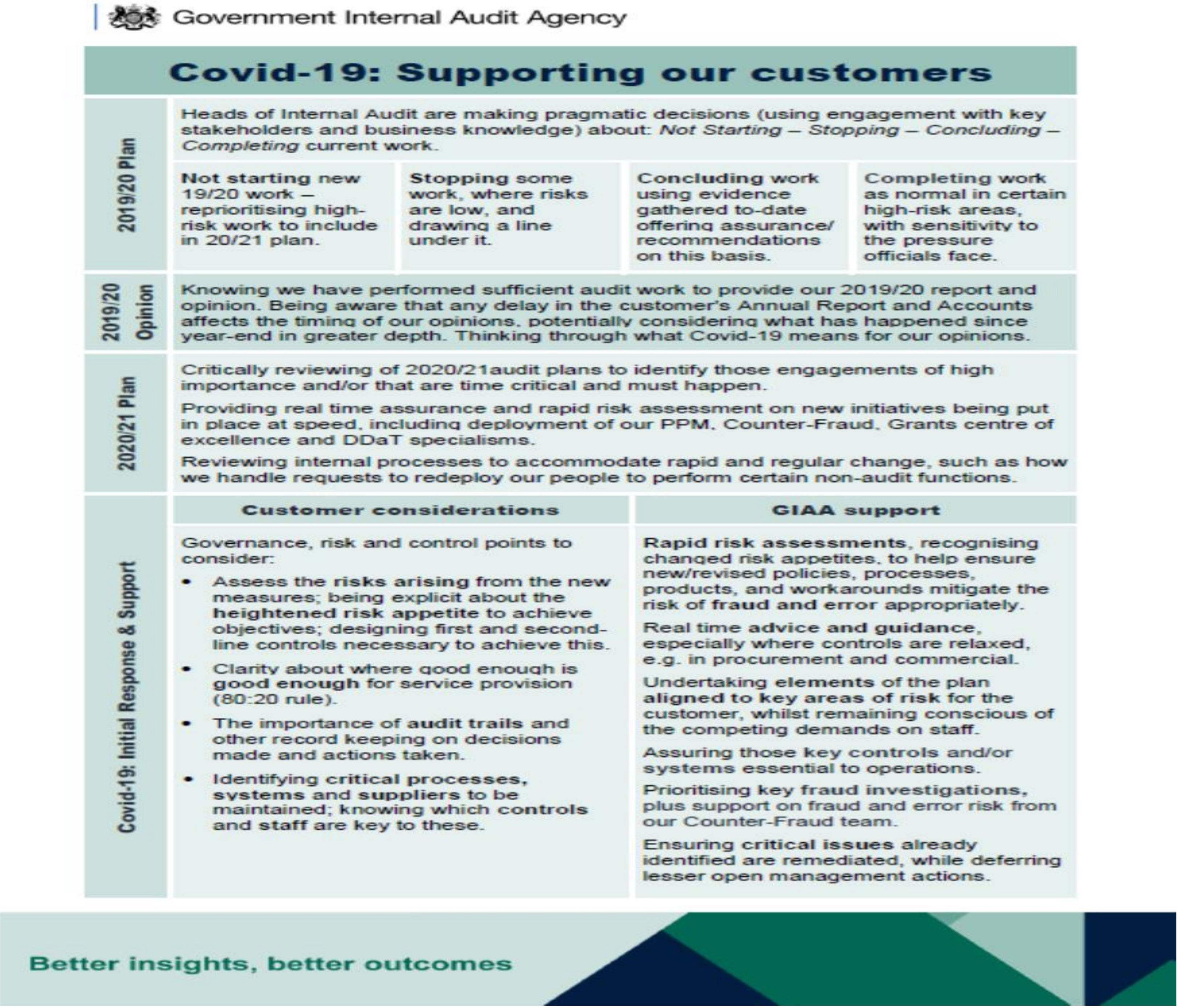
Maintaining effective financial management in accordance with requirements and obtaining value for money from the resources deployed remains essential, as does maintaining trust and transparency through reporting.

- Ensure that you can continue to make essential payments, support businesses and pay employees and suppliers. Use scenario analysis to examine and stress test liquidity and prepare response plans to ensure sufficient cash is available.
- Ensure that the design and implementation of extended or new payment mechanisms, including the use of grants and loans, are supported through robust risk management processes, including managing the risks of fraud.
- As operational challenges are faced and decisions are made, forecasts will need to be revised, but these will often be more inherently uncertain and potentially short-term, based on varying scenarios. Ensure that there is transparency over assumptions, scenarios and the basis of latest forecasts and estimates.
- Further guidance and advice should be obtained from your Finance function as necessary.

Technology/Security

The response to COVID-19 will trigger a significant and default “work-from-home” mobilization to limit the spread of the virus.
Organizations will experience an unprecedent amount of traffic accessing the network remotely. Recurring or prolonged interruptions in technology services will be amplified.

- Ensure that networks are load-tested to ensure that the increased traffic can be handled.
- Ensure that systems critical to operational priorities are understood, prioritized and maintained where possible.
- Ensure home working arrangements maintain standards of data protection and security.
- Ensure security updates and patches are applied routinely.
- Ensure employees are aware of the need for vigilance and the dangers of opening attachments and links from untrusted sources.
- Ensure monitoring for attacker activities deriving from work-from-home users.
- Further guidance and advice should be obtained from your Digital, Data and Technology function as necessary.



Government Internal Audit Agency

Covid-19: Supporting our customers

2019/20 Plan

Heads of Internal Audit are making pragmatic decisions (using engagement with key stakeholders and business knowledge) about: *Not Starting – Stopping – Concluding – Completing* current work.

Not starting new 19/20 work – reprioritising high-risk work to include in 20/21 plan.	**Stopping some** work, where risks are low, and drawing a line under it.	**Concluding work** using evidence gathered to-date offering assurance/ recommendations on this basis.	**Completing work** as normal in certain high-risk areas, with sensitivity to the pressure officials face.

2019/20 Opinion

Knowing we have performed sufficient audit work to provide our 2019/20 report and opinion. Being aware that any delay in the customer's Annual Report and Accounts affects the timing of our opinions, potentially considering what has happened since year-end in greater depth. Thinking through what Covid-19 means for our opinions.

2020/21 Plan

Critically reviewing of 2020/21audit plans to identify those engagements of high importance and/or that are time critical and must happen.

Providing real time assurance and rapid risk assessment on new initiatives being put in place at speed, including deployment of our PPM, Counter-Fraud, Grants centre of excellence and DDaT specialisms.

Reviewing internal processes to accommodate rapid and regular change, such as how we handle requests to redeploy our people to perform certain non-audit functions.

Covid-19: Initial Response & Support

Customer considerations

Governance, risk and control points to consider:

- Assess the **risks arising** from the new measures; being explicit about the **heightened risk appetite** to achieve objectives; designing first and second-line controls necessary to achieve this.
- Clarity about where good enough is **good enough** for service provision (80:20 rule).
- The importance of **audit trails** and other record keeping on decisions made and actions taken.
- **Identifying critical processes, systems and suppliers** to be maintained; knowing which **controls and staff** are key to these.

GIAA support

Rapid risk assessments, recognising changed risk appetites, to help ensure new/revised policies, processes, products, and workarounds mitigate the risk of **fraud and error** appropriately.

Real time advice and guidance, especially where controls are relaxed, e.g. in procurement and commercial.

Undertaking elements of the plan **aligned to key areas of risk** for the customer, whilst remaining conscious of the competing demands on staff.

Assuring those key controls and/or systems essential to operations.

Prioritising key fraud investigations, plus support on fraud and error risk from our Counter-Fraud team.

Ensuring critical issues already identified are remediated, while deferring lesser open management actions.

Better insights, better outcomes