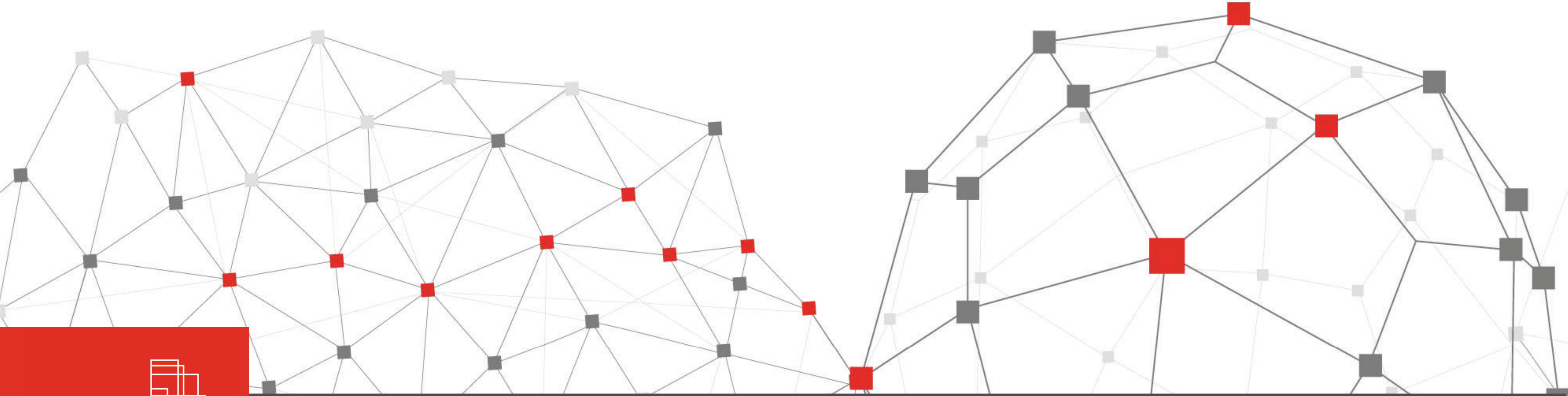
COVID-19

Navigating business as UNusual
IA's response to the COVID-19 crisis



March 2020

Overview

Background

The ongoing COVID-19 situation presents a substantial challenge for business, Governments and the community. We are likely to see an impact over many months on many business stakeholders including employees, customers, suppliers and other stakeholders such as regulators. With COVID-19, Internal Audit executives may — understandably — feel in uncharted territory. Their companies face multiple major new challenges, all at once. These challenges often compete with each other, and they all demand a rapid response. New risks are still arising and current ones evolve by the hour.

What does this mean for internal audit?

In these challenging times, Internal Audit executives have an obligation and an opportunity: to help their companies manage the most critical risks that COVID-19 has either created or magnified and help ensure that organizations can maintain a strong system of internal control during this period of change and uncertainty. While business leaders juggle the dual imperative of crisis response and operational continuity, Internal Audit executives can help them weigh risks and opportunities to make essential business decisions.

Immediate actions

Ensure the continued safety and care of your team (including regular communication)

Redirect your risk expertise to COVID-19 priorities

Identify new delivery models and ways to add value and mobilize accordingly

Proactively communicate with both management and audit committee stakeholders

Redirect any excess capacity to activities that will strategically help the business and the department

COVID-19: Companies need to respond to the crisis and build resilience over time

Waves

Respond (days)

Crisis management
- Health + safety
- Business continuity
- Workforce / Mobility
- Vendor management

Stabilize (weeks)

Operational response
- Reporting + Monitoring
- Resource management
- Cyber security
- Fraud waste and abuse

Evolve (months)

Scenario planning
- Business resiliency
- Operational transformation
- IT transformation

8 areas of focus for the business

Pain points, approach, and solutions will shift by Wave

- Crisis Response
- Supply Chain
- Operationalize Changes
- Finance & Liquidity
- Workforce & Workplace
- Regulatory & Tax
- Strategy & Brand
- Vendor Management

How can Internal Audit respond and partner with business?

1 Redirect your risk expertise to COVID-19 priorities

2 Identify new delivery models and ways to add value and mobilize accordingly

3 Proactively communicate with management and audit committee stakeholders

4 Redirect any excess capacity to activities that will strategically help the business and your department

1. Redirect your risk expertise to COVID-19 priorities

Internal audit, risk management and compliance functions have an opportunity and obligation, to collaborate, step forward, and to help the company through diverse challenges resulting from COVID-19.

IA Consideration	
Directly connect into the company's COVID-19 Response Team and review the response plan	● Provide assistance to stress test IT, operational risks and vulnerabilities and offer real-time insights and advice to help mitigate risks being encountered during response activities ● Provide assurance to the Response Team as they are rolling out and executing activities (e.g., making real-time policy, process and control changes) to effectively address risk

Tactical Examples

- Real-time review of the business continuity plan (BCP) and response.
- Support effective scenario planning.
- Attendance at the COVID-19 Steering Committee to provide input on risk mitigation.
- Deployment of resources to support response activities.

Sample BCP Considerations for the Business - Engage a BCP SMS for support

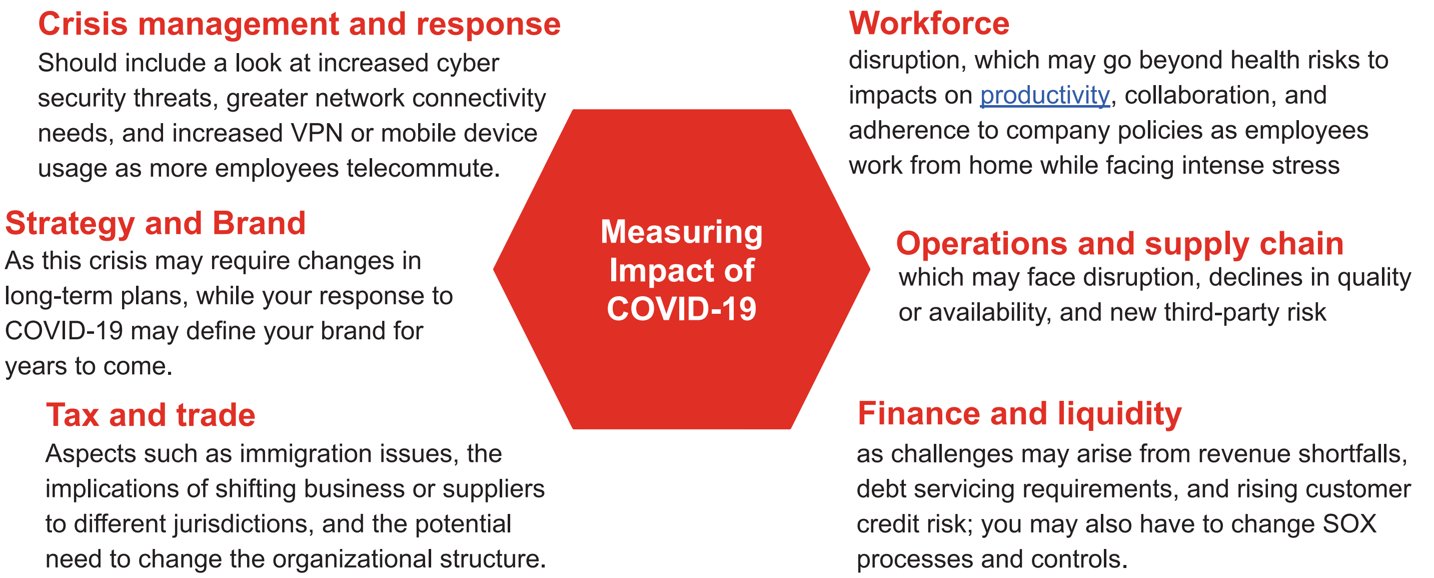
✓ Identify the critical work that delivers your P&L, the workforce that does that work and the capacity of the organization to move labor to sustain those critical activities.
✓ Consult with key third parties to ensure they will be able to continue to deliver desired service levels during the emerging COVID-19 situation.
✓ Monitor exposure trends and restrictions against the supply chain.
✓ Create an internal and external stakeholder map for key communications (considering staff, customers, suppliers,regulators, etc.).
✓ Implement a clear crisis communications strategy to protect your reputation and maintain the trust of your stakeholders.
✓ Monitor the changing laws and regulations affecting your workforce.
✓ Provide accessibility of data insights to support vital decisions.
✓ Review and update sales-and-demand planning strategies, including assessed changes in customer behavior.
✓ Assess restructuring needs, either financially or operationally, to reduce risk and protect value.
✓ Update working capital plans and forecasts in light of the changed circumstances resulting from COVID-19.
✓ Assess IT infrastructure support amidst heavy use of remote access.
✓ Secure and maintain IT systems and data.
✓ Assess whether changes in the IT environment could increase vulnerability to a cyber attack.

1. Redirect your risk expertise to COVID-19 priorities

IA Consideration	
Evaluate emerging risks of new operating models and business practices and redirect attention to time-sensitive risks	● Emerging risks due to COVID-19 responses ● Policies and controls related to any stimulus funds (CARES Act) or other non-traditional funding ● Other disruption (liquidity, workforce, changing processes) ● Succession planning and workforce management
Support mandated compliance activities to meet regulatory requirements	● Coordinate with key stakeholders responsible for mandated compliance requirements ● Execute mandatory projects required to meet regulatory requirements and identify any that may be able to be deferred

Tactical Examples

- Assess the effect of COVID-19 on risk areas (including the fraud risk assessment) through collaboration with risk functions.
- Understand activities being undertaken to monitor emerging risks.
- Determine the need for framework or controls over any stimulus funds or non-traditional funding being sought.
- Refocus immediate IA resources to highest risk areas (e.g.,IT resiliency and capacity, supply chain, finance, cyber and privacy).
  - Which projects can we halt or postpone?
  - Which projects should we add or accelerate to address new risks?
- Communicate any changes to the AC



Measuring Impact of COVID-19

Crisis management and response
Should include a look at increased cyber security threats, greater network connectivity needs, and increased VPN or mobile device usage as more employees telecommute.

Strategy and Brand
As this crisis may require changes in long-term plans, while your response to COVID-19 may define your brand for years to come.

Tax and trade
Aspects such as immigration issues, the implications of shifting business or suppliers to different jurisdictions, and the potential need to change the organizational structure.

Workforce
disruption, which may go beyond health risks to impacts on productivity, collaboration, and adherence to company policies as employees work from home while facing intense stress

Operations and supply chain
which may face disruption, declines in quality or availability, and new third-party risk

Finance and liquidity
as challenges may arise from revenue shortfalls, debt servicing requirements, and rising customer credit risk; you may also have to change SOX processes and controls.

1. Redirect your risk expertise to COVID-19 priorities

COVID-19 Emerging Risks

Risk	Internal Audit response
Activation of BCP arrangements Management and governance structures	• **Review of BCP arrangements:** Critical analysis of BCP plans for weaknesses and unidentified impacts specific to COVID-19 (supply chain, staff availability, customer demand). This could include simulation of various contingency scenarios to 'stress test' continuity plans and assess impact on associated process and controls.
New or elevated workplace health and safety IR risks associated with increased use of remote working	• **WHS remote worker readiness assessment:** Assess the clarity of policies, procedures and effectiveness of communications relating to employee wellbeing and safe working arrangements from an employee perspective. Review the implementation of remote worker and mobility into BCP. • **Employer obligations for remote working:** Assess processes and controls to manage impact of increased remote working arrangements and compliance with employment obligations.
Transparency & Employee management Protect employees during uncertainty	• **Honouring employees' entitlements:** Underpayment of staff remains a hot topic across a number of industries. As organisations make choices about their workforce in the time of crisis, it is critical that employees have access to entitlements and are treated with fairness. Internal Audit should focus on reviewing organisations' governance frameworks and processes related to employee entitlement policies in changing times (e.g. additional/special leave management, accuracy of wages, robustness of underlying systems that support one-off choices implemented by organisations, etc).
Risk Culture Consider impact on risk culture across the organisation	• **Behavioural impacts of COVID-19:** Employees will be facing challenges with their day-to-day tasks and decision making due to personal stress; pressure on increased demand or downturn; implications of rapid implementation of a remote workforce; potential acceptance of mistakes and oversight in the current environment; and prioritisation of 'critical activities' impacting compliance, control requirements, customer and/or regulatory obligations. This may have a direct impact on compliance with internal policies and practices, which heightens the risk faced by organisations in key areas as highlighted in this document.
Fraud Lapse of key fraud controls and management attention	• **Core processes impacted, the potential for fraud and the indicators to look for:** Consider how data analytics (some of the tools in use by Internal Audit or Risk) can be used to look for these indicators and investigate real time. Additionally, as long term staff are forced to work from home and change their normal routine, this may uncover long running fraud practices. Therefore an increased need for urgent investigation and remediation will be required.

1. Redirect your risk expertise to COVID-19 priorities

Operational & Financial Risks

Risk	Internal Audit response
Supply Chain Visibility and efficiency of the supply chain	• **The robustness of the supply chain is key:** From the sourcing of raw material to distributing product to clients in local markets. A deep understanding of the supply chain and the risks presented by your third parties will help respond today and improve them for tomorrow. • **Understand and prepare:** Accessing critical supply chain data across all tiers to properly assess the potential risk and opportunities to enable the business to take advantage. Where applicable, prepare to set up a temporary inventory recovery and evaluation process and pursue alternative sourcing strategies.
Cash & Funding Resilience Consider short, medium and long term funding	• **Cash and liquidity should be front of mind:** Short, medium and long term funding requirements can be impacted. It is important to support management through the re-prioritisation of spending and financial obligations, as well as consider what opportunities are there to accelerate cash collection/generation. The skills of Internal Audit professionals can support the business in this area, while the business deals with continuity • **CARES Act and other Stimulus Funding:** Assess and provide real-time advice as your organization implements policies and controls related to any stimulus funds or other non-traditional funding in response to COVID-19 federal and state programs and/or legislation
Third Party Continuity of supply from third party service providers	• **Review arrangements with third party service providers:** Assess risks associated with outsourced arrangements and the robustness of third party controls (e.g. third party business continuity, integrity of reporting, service delivery KPIs, etc). Where organisations are significantly dependent on third parties to deliver core services, consider a 'fit-for-purpose' assurance program over key risks and controls associated with the delivery of services by a third party. • **Project health checks:** Review of projects to assess the impact of COVID-19, checking contingency arrangements on the critical path for project delivery and assessing the ability of third parties to deliver as per their contract. Internal Audit could also assist in project prioritisation linked to strategy and value creation.
Market Opportunities & Vulnerabilities Volatility in stock prices	• **Check-point audits throughout the M&A lifecycle:** Assess process & procedures at a point in time and provide recommendations for improvement in areas such as controls integration, effectiveness of key acquisition activities against leading practice including scenario analysis, due diligence, integration and transaction recording / consolidation processes.
Tax & Regulatory Potential Impacts	• **Favorable tax implications:** Support business through process & controls implemented in order to meet criteria of any provisions including, among other things; delay of payment of employer payroll taxes, (NOL) changes; postponement of estimate tax payments due; delay of estimated tax payments for corporations; partial above-the-line" deduction for charitable contributions and modification of limitation on charitable contributions •

1. Redirect your risk expertise to COVID-19 priorities

IT Risks

Risk	Internal Audit response
Remote administration & IT Support Capacity Increased use of remote working arrangements	• **Remote worker readiness assessment:** Review organisational readiness for staff and other workers to continue operations from locations outside of office sites. Consider clarity and consistency of technology protocols and communications to staff. • **Access and communication readiness:** Consider suitable capacity of remote technology, IT support and self-service arrangements, secure remote access via VPN, communications and capacity.
New or elevated cyber security risks Potential exposure due to new tools and increased use	• **Cyber hygiene assessment:** Review organisation's general cyber hygiene such as vulnerability management, patching, security awareness, anti-phishing and DLP • **Incident monitoring and response:** Support ongoing governance arrangements remain in place (security monitoring) with appropriate investigation and action performed as issues are identified.
Privacy & Data Protection Potential exposure of customer personal information	• **Revisiting data breach policy and practices:** Restricting teams (incl third parties) with remote access to personal information on an 'as needs' basis and reiterating privacy obligations for employees, especially during business continuity invocation.
Managing rapid infrastructure change Pressure to implement major infrastructure changes in a short period.	• **Revisiting policies impacts by Crisis Management:** Internal Audit should consider the interplay between accelerated change processes while ensuring system integrity and security. Auditors will need to determine the acceptability and effectiveness of any temporary or emergency changes to approvals.

1. Redirect your risk expertise to COVID-19 priorities

Compliance Risks

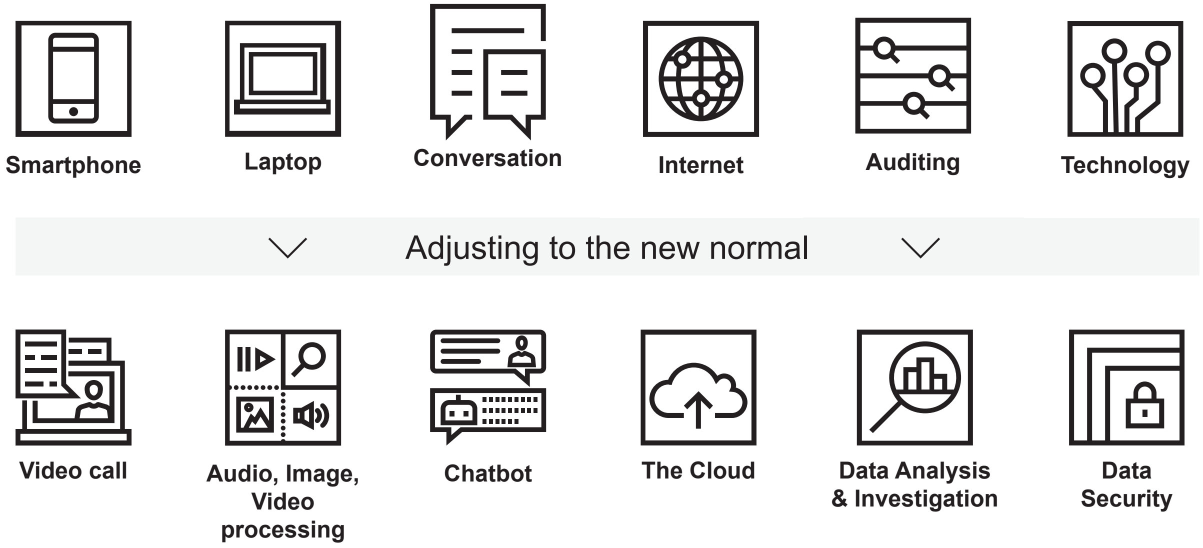
Risk	Internal Audit response
Regulatory/ government enforced changes due to COVID-19 Maintain compliance and plan for potential interim changes	• **Interpretation and implementation of regulation:** Continue open lines of communication with relevant regulators and ensure that where changes are required. Internal Audit could play a role by providing its resources and skills to the business or are involved in a consultative manner during the implementation. • **Compliance with deadlines:** Assess process and controls to manage compliance with legislative and contractual timeframes and/or client service KPIs for regulatory reporting, and legislated customer service obligations.
Changes to the control environment Management and governance structures	• **Process and control mapping of business critical functions:** Map key processes and controls of affected areas and understand the impact of potential changes to these controls under various contingency scenarios. For example, this could consider: impact of changes to management roles and structures on delegations of authority; changes to system access and change controls to enable flexible work arrangements. • **Continue to meet compliance/regulatory requirements:** Ensure the business is meeting regulatory obligations. Regulatory and/ or compliance-related reviews should continue to be prioritised within the plan where applicable, unless clear direction is provided by regulatory bodies.
Financial Reporting Resiliency over finance & accounting processes to provide shareholder information	• **Ability to meet regulatory and related requirement filings:** Ensure company has prepared a comprehensive summary of its required regulatory and related requirements, including annual and quarterly tax filings and payments, respective payroll, statutory audit requirements globally, and debt compliance required filings. • **Evaluate audit impact with external auditor**: Liaise with external auditor to determine if the completion of audit or review procedures has been impacted by the COVID-19 outbreak. • **Significant and unusual transactions:** Support business through risk assessments and process & controls implemented related to any significant and unusual transactions. • **Disclosure requirements:** As events continue to unfold, should support the business through decisions regarding required disclosures in areas such as, risk factors, and management's discussion and analysis of results, liquidity, and capital resources.
Internal Controls over Financial Reporting (Sarbanes Oxley -SOX)	• **Assess materiality impacts:** Changes to businesses models and functions within the organization may change planned materiality thresholds and the underlying controls. • **Evidence retention**: Re-evaluate current controls to ensure they address risks; consider impacts to how the evidence of control performance is created and maintained, especially if controls were manually performed.

2. Identify new delivery models and ways to add value and mobilize accordingly

IA consideration	
Prioritize relevance, speed and flexibility—virtually	● Traditional auditing is likely on hold - focus on advisory projects related to crisis ● Evaluate how can IA deliver value with reduced resources and / or capacity in virtual environment ● Evaluate impact of virtually connected operating model embraced by the business
Encourage innovation through new ways of working that are as flexible as your business can support	● Leverage analytics to drive insights and assurance with less business disruption ● Applying analytics and virtual collaboration tools to conduct end-to-end projects. ● Relying on self-service for access to data and records.

Tactical Examples

- Identify the impact to current audit plan and postpone, cancel audits as necessary and pivot focus to add real-time value through proactive advisory / consulting support. Consider updating communication and reporting mechanisms.
- Assess the most efficient and effective ways to deliver audits using various communication technologies, file-sharing tools, and remote-access mechanisms.
- Use data analytics capabilities throughout the audit to focus on higher risks and provide valuable insights to the business
- Evaluate the impact of the virtually connected operating model embraced by the business.



Smartphone

Laptop

Conversation

Internet

Auditing

Technology

Adjusting to the new normal

Video call

Audio, Image, Video processing

Chatbot

The Cloud

Data Analysis & Investigation

Data Security

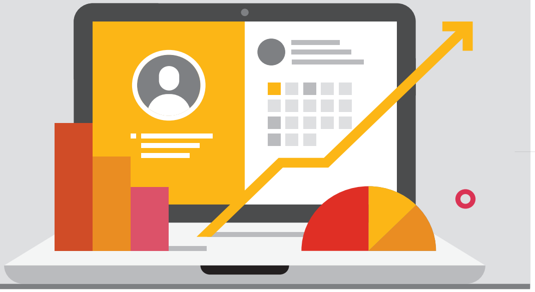
3. Proactively communicate with management and audit committee stakeholders

IA Considerations	
Revisit IA communication to stakeholders - communicate value, be transparent and stay close to business **Reduce blind spots during a time of dynamic change**	● Be transparent and articulate the impact and limitations due to COVID-19 on the business, risk assessment and audit response. ● Communicate emerging risks, company mitigation strategies and/or instances where management has intentionally accepted the risk. Share how IA is providing assurance over emerging risks. ● Challenge the department to do more to adapt, find innovative ways to operate or help in new areas. ● Communicate the value associated with new projects or activities (e.g., real-time feedback to enable stronger management responses, mitigating potential for misconduct, identifying fraud, enabling regulatory compliance. ● Regularly engage with auditees and stakeholders to get feedback on risk and IA's response.

Tactical Examples

- Establish communication and reporting protocols to align on timing and mechanisms for reporting and communication
- Update leadership and the Audit Committee with emerging risks, mitigation activities and Internal Audit value reporting
- Leverage company approved virtual technology to connect and share updates with key stakeholders and Audit Committee members
- Engage role-based touch points with stakeholders to keep up to date on developments

Leverage video technology, visualization dashboards and collaboration tools to share valuable insights.



Communication checklist

✓ Have communication and reporting protocols been established or refreshed with executive leaders and the Audit Committee as needed?

✓ Do Internal Audit communication or reporting templates need to be updated to address new advisory / consulting support?

✓ What is the escalation process for reporting heighted emerging risks to senior leadership?

✓ What innovative ways can reporting and communication be enhanced (e.g., leveraging visualization, access to real-time status)?

4. Redirect excess capacity to activities that are strategic to the business and dept.

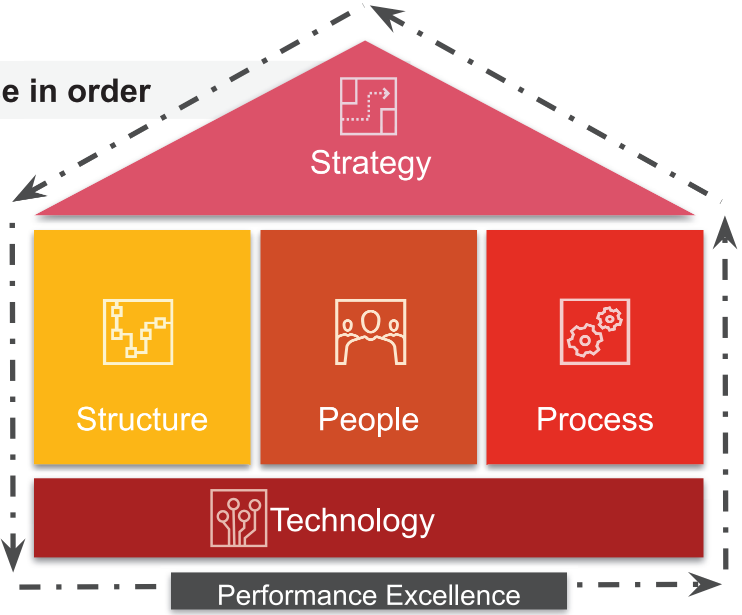
IA consideration	
Redeploy excess capacity to areas within business that require help	● Consider strategic benefits for both business and audit departments to second staff to high priority business areas, similar to a guest auditor program.
Assess current IA Strategy and define any needs or transformation	● Automation / digitization of workstreams ● Digital upskilling and training ● Methodology transformation, using data and technology ● For departments that perform SOX testing, now may be the time to think about strategic transformation.

Tactical Examples

- Revisit or create Internal Audit's Strategic Plan to ensure it aligns with the vision of internal audit's brand and value for the organization.
- Perform talent assessments that evaluate in-house capabilities and design talent profiles and talent portfolios to leverage the right skills at the right place.
- Consider embedding new IA technology or new capabilities by leveraging technology already existing in business.
- Upskill your IA team in emerging risks and new auditing techniques and support them to become tech-savvy using online learning (PwC's Digital Fitness App).

Getting your house in order

Identify opportunities to enhance capabilities and maximize value through each functional area



4. Redirect excess capacity to activities that are strategic to the business and dept.

Redefining your vision for Internal Audit

An IA function is comprised of five functional areas that enable it to accomplish its mission and meet stakeholder expectations: Strategy, Structure, People, Process, and Technology. PwC's IA Transformation framework is applied to each of the internal audit functional areas based on your vision.

Transformation Framework

Strategy

The strategic components of an IA function, including the vision, mission and objectives

- Migration away from control-centric to risk-thematic view
- Proactive engagement with business

Structure

The organization of the IA function and the function's relationships across the organization

- Leverage existing risk management activities
- Teaming structure based on risk themes

People

The expertise and skill sets possessed by IA, as well as training and development opportunities

- Digitally upskilled profile
- Data-driven and issue-focused mindset

Process

Methodology leveraged across the IA lifecycle, as well as higher level processes leveraged to operate the function

- Dynamic risk identification and monitoring
- Agility throughout audit activities

Technology

The incorporation and use of technology across all aspects of the IA function

- Unstructured and structured data sources
- Continuous monitoring of advanced analytics

How PwC can help

COVID-19 response review

We can help you assess whether the response plan and governance is appropriate, sufficient and complete.

Surge sourcing options

Fill gaps in your Internal Audit, IT audit, compliance or SOX resources, with agile, remote, staffing options including local in country, delivery center, and specialist resources.

Crisis risk assessment

We can help you reassess and critically challenge your risks, with an external perspective and experience and prioritize relevant reviews while focusing on fraud and security risks.

Digitization (Analytics & More)

We can quickly set up automations and analytics capabilities leveraging our Digital Lab and can help you identify data analytics procedures to embed in your current audits.

CARES Act Compliance

We can support framework and control considerations to enable compliance with the CARES Act.

Training & Digital Upskilling

We can lead staff training remotely; e.g. on emerging risk areas or data analytics using our suite of training materials.

IT Health Checks

We can exercise IT health checks (e.g., remote access provisioning, Cyber hygiene, remote IT services, mobile computing and device management, security over collaboration tools) to highlight real-time risks and recommended controls.

Fraud risk assessment & monitoring

Leveraging our fraud risk framework and digital capabilities, we can help you identify new fraud schemes and update your risk assessment and monitoring controls.

Thank you

pwc.com