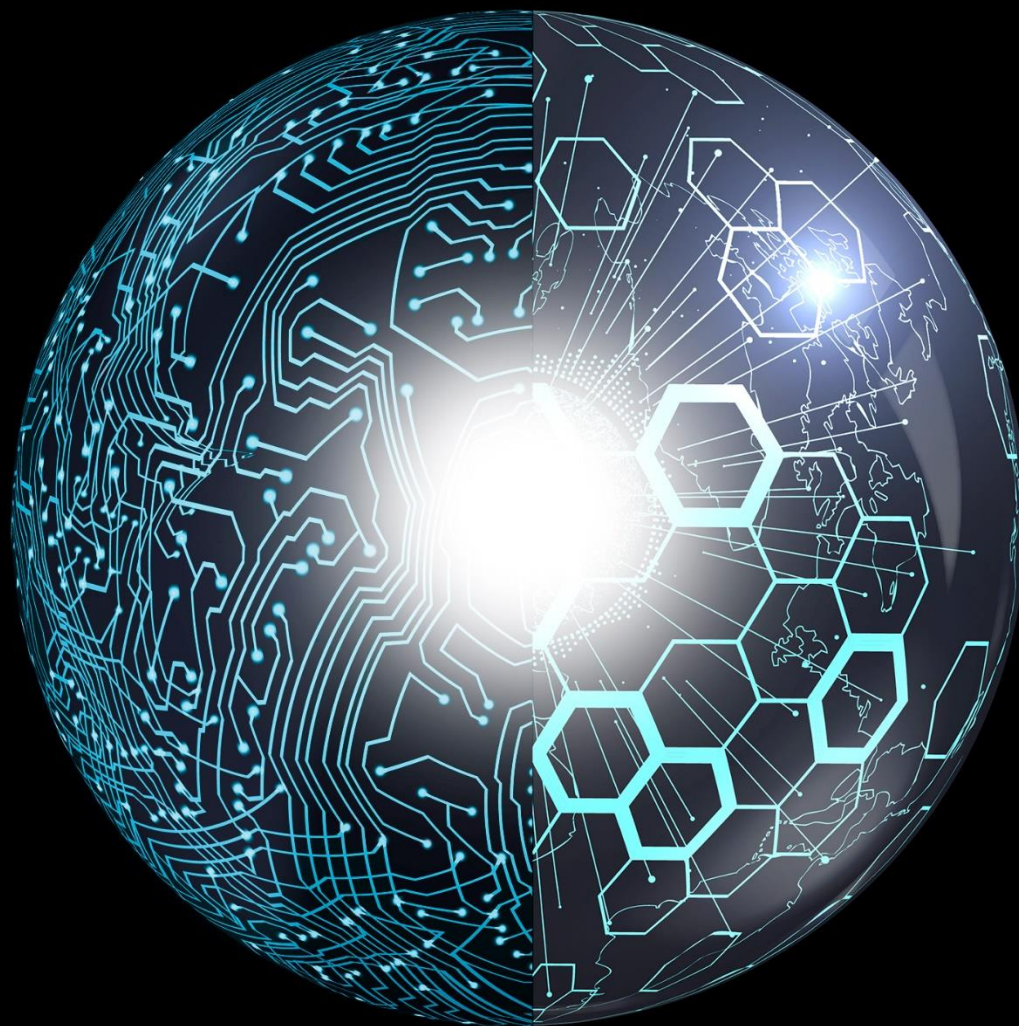


# Deloitte.



## **Building resilience in internal audit**

Guiding principles for thriving in a time of remote internal auditing and beyond

With COVID-19 impacting every aspect of the work environment, Internal Audit (IA) should reassess the manner in which it delivers services to the organisation. During this time of unparalleled change, IA may continue to provide assurance over the most consequential risks, while simultaneously increasing its role in advising management and the board on the shifting risk and control landscape, including anticipating new emerging risks. Now, more than ever before, IA should consider deploying enabling digital technologies, beyond analytics and automation, with the objective of becoming more resilient, cost-conscious, and smarter about providing services that make an impact.

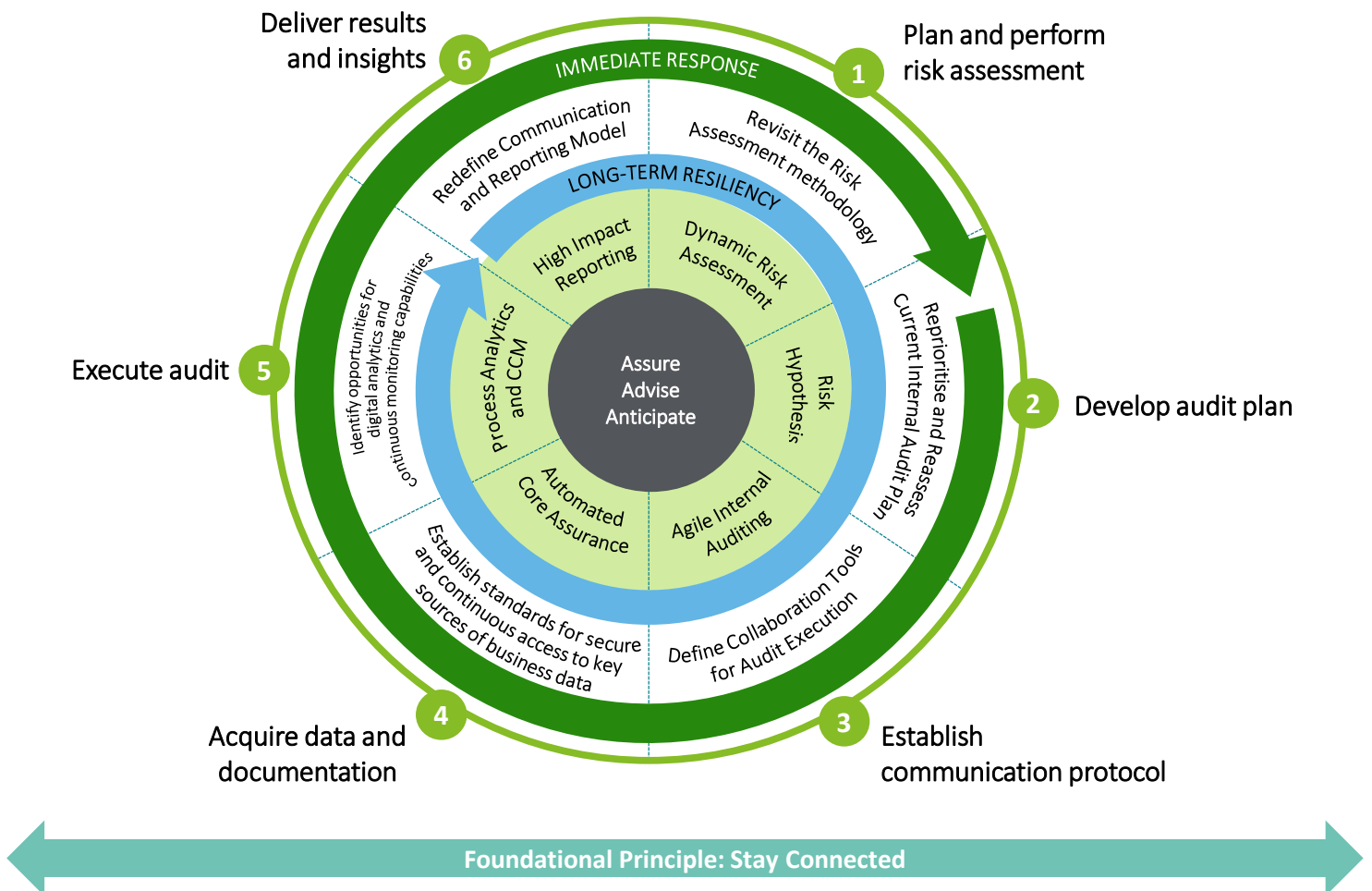
But how can IA become an adaptive team player and high-value contributor when every aspect of service delivery is disrupted?

To this end, Deloitte has compiled a set of **guiding principles** across a standard IA lifecycle as an **immediate response**, enabling internal auditors to adjust to the “next normal” of remote internal auditing. We have also highlighted **transformational digital technologies and methodologies** that can be utilised to drive change and increase **long-term organisational resilience**.

## Guiding principles

Taking the time to institute a set of guiding principles for remote internal auditing is instrumental in preserving IA’s ability to perform well, be present for stakeholders, and remain sustainable in the long term.

We have grouped the guiding principles to align with a standard audit lifecycle, addressing six areas that can be evaluated as IA shifts to auditing with low-to-no contact.



# 1. Revisit the risk assessment methodology

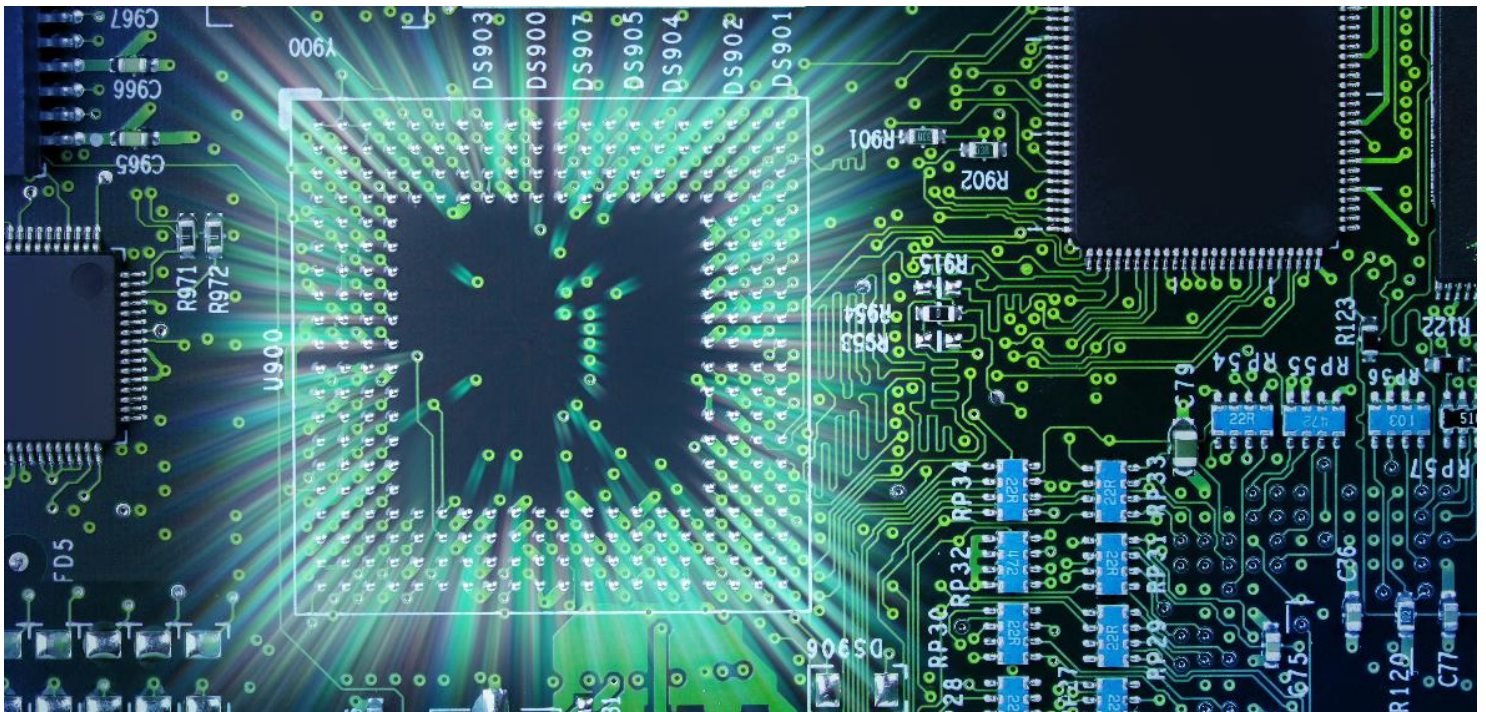
## *Lifecycle phase: Plan and perform risk assessment*



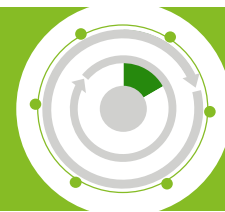
As the organisation adjusts its operations to cope with the impact of COVID-19, IA should reprioritise and reassess its audit plans and revisit its risk assessment methodology to respond to the changing landscape. This includes discussing and collaborating with key stakeholders to identify emerging, shifting or net-new risks and determining how to work with the business most effectively in planning mitigation strategies. Examples of net-new risk areas or those that may be significantly altered include:

- Cybersecurity
- Revenue assurance
- Cost recovery
- Crisis management
- Forecasting and planning
- Capital allocation and spend effectiveness
- Human capital and benefits
- Supply chain assurance
- Liquidity modelling
- Organisational resilience

Given the unknown social impact and global economic fallout from the pandemic, IA should remain agile in its focus and dynamic in its risk-assessment capabilities. (See *Spotlight Opportunity: Benefits of dynamic risk assessments during unexpected events.*) IA should also assist the organisation in assuring data protection and resilience as much of the workforce shifts to a remote model. Assessing the cyber security posture is especially prudent as social-engineering schemes and attacks on home security networks become prevalent.



# Spotlight opportunity: Benefits of dynamic risk assessments during unexpected events



Unexpected events like COVID-19 create a confluence of effects that can disrupt or slow business activity. Historically, many IA functions rely upon simple formulae for their annual risk assessments, working within the same parameters and repeating the same interviews year after year. This staid approach can hamper internal auditors from anticipating emerging risks spawned by a crisis. Using data and analytics to drive the risk assessment can help internal auditors to be more proactive. Rather than relying on an annual risk assessment, these tools enable IA to constantly engage with the business to understand the changing risk landscape.



## FAQs



### What is Dynamic Risk Assessment (DRA)?

DRA refers to the continuous monitoring of business operations, functions and processes enabled by automation. It is also known as Continuous Business Monitoring or Risk Sensing. Done well, DRA generates new insights to inform risk professionals as well as new alternatives on how to respond. DRA eliminates audit approaches that are manual, fragmented, often unrepeatable, or largely based upon gut instinct and replaces them with repeatable, standardised tools and methods. Overall, it transforms the audit-planning process and annual risk assessment by enabling continuous risk monitoring and adjustment to audit plan. To be clear, DRA is more than just technology. Leading with technology is a sure-fire way to fail. Effective enablement of DRA requires vision, people, process, and technology.

### Are there different approaches to DRA?

There are two primary models for implementing DRA: quantitative and qualitative. A hybrid of the two is also valid depending on the nature of the audit landscape.

- **Qualitative:** Utilises unstructured data such as interviewee notes, risk scans, and external data sources, such as media news outlets and social media, to provide structured insights into organisational risk trends.
- **Quantitative:** Compares performance against a baseline of factors—such as those relating to a comparable entity's factory, location, business unit, or geography—to identify negative trends, outliers, and anomalies to inform audit planning.

### How can Potential Risk Indicators (PRI) enhance DRA?

As part of a modernised risk assessment, PRIs can be used to measure performance against an established baseline of factors related to a comparable entity's facility, location, business unit, or geography. These comparisons can be helpful in revealing negative trends, outliers, and anomalies to inform internal audit planning. In addition, field results gathered over time from PRI-driven assessments can provide organisations with more accurate predictors. This process is often a precursor to developing real-time assurance.

### How can I leverage external data within my risk assessment?

Company information pulled from various systems (e.g., financial, operational, internal audit, and human resources) can be enriched with external information, such as credit ratings and economic and risk indices. For example, when considering PRIs related to facilities or locations, it may be useful to factor in Corruption Perception Index ratings, which rank countries based on corruption risk.

### I have already conducted my stakeholder interviews prior to the unexpected event. How can I engage them again with minimal disruption?

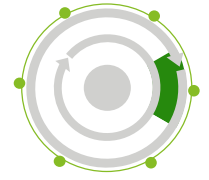
Surveys can be used to gauge a changing risk landscape with minimal disruption. By designing templates with clear questions and risk areas, IA can use the qualitative DRA model to determine what the emerging risks are and how to embed them into the audit plan.

### Where can I find more resources on DRA?

[Internal audit insights: High impact areas of focus - 2020](#)

## 2. Refresh and reassess current internal audit plans

### *Lifecycle phase: Develop audit plan*



The pandemic has likely rendered the current internal audit plan obsolete. Accordingly, IA should reprioritise the audit plan as soon as possible to provide assurance over the most consequential risks while being cognisant of the impact on operations. This includes determining which audits can be performed remotely versus those that absolutely require an in-person presence. From an assurance perspective, internal auditors should also consider how operational changes will affect the audit timeline. For instance, process owners may need to move their controls to a virtual environment, which takes time. Importantly, IA should be actively engaged in advising the business around such changes and update its testing plans accordingly. Other suggestions for refreshing and reassessing current internal audit plans include:

**Reprioritise the audit plan** to be relevant in the current environment. IA may add more value during this time by providing readiness assessments on new processes or regulations related to COVID-19.

**Redeploy resources** to advise the business on COVID-19 response projects such as crisis management, business continuity planning, cybersecurity assessments, and other areas that will likely be significantly impacted in the short- to middle-term. In addition, IA should also consider how it can help reduce the assurance burden on mission-critical areas by collaborating across the lines of defence as well as with external auditors to prevent duplicative or disruptive efforts.

**Enhance the use of digital tools** to assess the impact on the organisation's internal controls environment. For example, IA can glean important information about changes in personnel, environments, and systems from quarterly SOX assessments. IA should also consider how it can most effectively communicate the impact of the changes and the readiness of new processes.

**Increase use of analytics and monitoring** to evaluate the impact of the changing risk landscape on the three lines of defence as well as how it could affect the control environment more broadly. IA can use this time to brainstorm ideas for digital enablers that could offer useful information to the business, such as potential efficiencies or root causes of repetitive issues.

**Use analytics to establish dynamic testing procedures** when assessing audit evidence. In a remote environment, there may be circumstances that prevent process owners from completing their normal procedures. While IA should be understanding of these hurdles, they should increase their scrutiny of whether the adjusted processes adequately address the associated risks.

This may include performing extra steps such as corroborating evidence with preparers and reviewers separately, directly accessing underlying data from the system, and leveraging analytical capabilities to independently develop an expectation or threshold level.

#### Quick tips

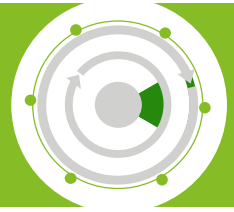
Reprioritise and reassess current internal audit plans

**Assess the risk ratings** throughout the controls framework. Particularly, controls that are new, require a high level of judgement, or have historical issues should be evaluated to determine whether the original risk rating is relevant.

Determine whether the current risk assessment model lends itself toward a **dynamic environment**. If not, it should be worth the effort to revamp the model, since it can enhance the advisory value IA can deliver.

**Be flexible!** Uncertain times can be jarring for people throughout the organisation. Keep this in mind while planning—it is okay to delay certain audits if they are superseded by other priorities and can be done later in the year.

# Spotlight opportunity: Risk hypothesis—The importance of asking the right questions



Developing a risk hypothesis within the planning phase and revisiting it throughout the audit lifecycle can enable the audit team to stay focused throughout the audit. When seeking insights from data, it is important to ask the right questions and to remain skeptical about the value of any particular finding, always inquiring, “So what?” Linking questions to key testing hypotheses—or statements of what might go wrong—can help drive the analytics approach. By embedding analytics in every phase of the audit process, which is also known as “insights-driven auditing,” IA can help the business navigate a world that has become vastly more volatile, uncertain, and complex.

## FAQs



### Why is it important to construct a risk hypothesis?

The short answer is “focus.” It’s easy to get lost in the data without a clear objective for why you’re collecting and analysing it. A risk hypothesis essentially provides that objective, or point of focus, by stating what the audit might find if the controls weren’t effective. A well-stated risk hypothesis also encourages the IA team to draw upon non-traditional data sources, as well as established ones, to deepen their insights.

### When should I build risk hypothesis?

In order to deliver the greatest benefit, the risk hypothesis should be developed in the planning phase prior to scoping the audit. Bolting analytics onto the audit, such as during fieldwork, without the guidance of a risk hypothesis limits the benefits.

### How do I effectively build my hypothesis?

Through exploratory data examination and discussions with business leaders, internal auditors can usually find the clues they need to build an effective risk hypothesis. For instance, if a cursory examination of purchase orders raises flags and the CIO suspects that the business might not be effectively controlling its technology spend, the corresponding risk hypothesis could be that employees are going outside of regular procurement channels to purchase technology.

### What are some benefits of insights-driven auditing?

- **Perform the same audit faster.** For example, insights-driven auditing can improve data access and reveal key insights before fieldwork commences. Also,

making connections and comparing performance and key benchmarks between products, processes, and business units means auditors can focus on what is of utmost importance and avoid merely confirming the obvious. It also enables auditors to assess transaction risks in real time.

- **Perform the same audit cheaper.** For example, connecting the auditor directly to the process, through exploratory analytics and data visualisation, drives a more focused audit, while still testing 100 percent of the population. Moving to automated routines over manual ones usually saves time and money.
- **Perform better audits.** For example, combining data from inside and outside the organisation adds new richness and granularity to insights and understanding of risk. Benchmarks, comparative analysis, and trending enhance on-the-job learning and development while delivering a more impactful result to business stakeholders.
- **Make innovation a centerpiece.** For example, data science disciplines combined with next-gen technologies enhance, automate, and continuously improve not only the audit process but also reporting and service delivery.

### Where can I find more resources on risk hypothesis and insights driven auditing?

[Internal audit analytics: The journey to 2020 Insights-driven auditing](#)

### 3. Define collaboration tools for audit execution

#### *Lifecycle phase: Establish communication protocol*



By utilising tools that enable collaboration and establishing mutually agreed upon protocols, IA can efficiently work with process owners to gather and review requested documentation in a remote environment.

**Select a collaboration tool** for documentation gathering based on essential capabilities, such as making and distributing request lists, uploading documentation, and tracking status. Process owners can be trained on the system via video demonstrations or conference-call sessions

**Establish a turnaround protocol** to align expectations between IA and process owners. A mutually-agreed-upon turnaround time of two weeks from the date of request usually gives process owners adequate time to gather documentation and to follow up with their team members as necessary. An established turnaround protocol can also help internal auditors anticipate how long it will take to execute the audit plan

**Leverage screen-sharing and screen recording** to assess processes, such as configuration or code testing, which would typically be reviewed in-person with the process owner. Instead of requesting static screenshots, a live review conducted online can be more effective since it gives internal auditors the ability to ask questions in real time and drill down into modules that they otherwise wouldn't be able to access directly

#### Quick tips

##### Collaboration tools

Consider obtaining **audit trails** to ensure the integrity of the evidence provided.

**Request documentation in advance** to give process owners extra time to gather data that may not be as readily available in a remote work environment.

Capture **full screenshots** to ensure the image or screen recording has not been modified.



# Spotlight opportunity: Agile Internal Audit—Communication and collaboration are key to delivering value



Flexibility in response to changing business needs has gone from a nice-to-have to a have-to-have in this environment. The traditional top-down model of organising and managing an internal audit function does not adapt well to disruption, and for most IA departments, going to a 100 percent remote model is not something they planned for. Agile IA is a way of working that has a built-in ability to pivot to whatever the circumstances call for. Strong communication and collaboration protocols are established within the team as well as with leadership and key stakeholders.

## FAQs



### What is Agile IA?

Agile IA is a way of approaching internal audits based on **iterative development** where requirements and solutions evolve through **collaboration** between **self-organising, cross-functional teams**, all focused on delivering the most important **business value** and **continually improving**.

### Why Agile IA now?

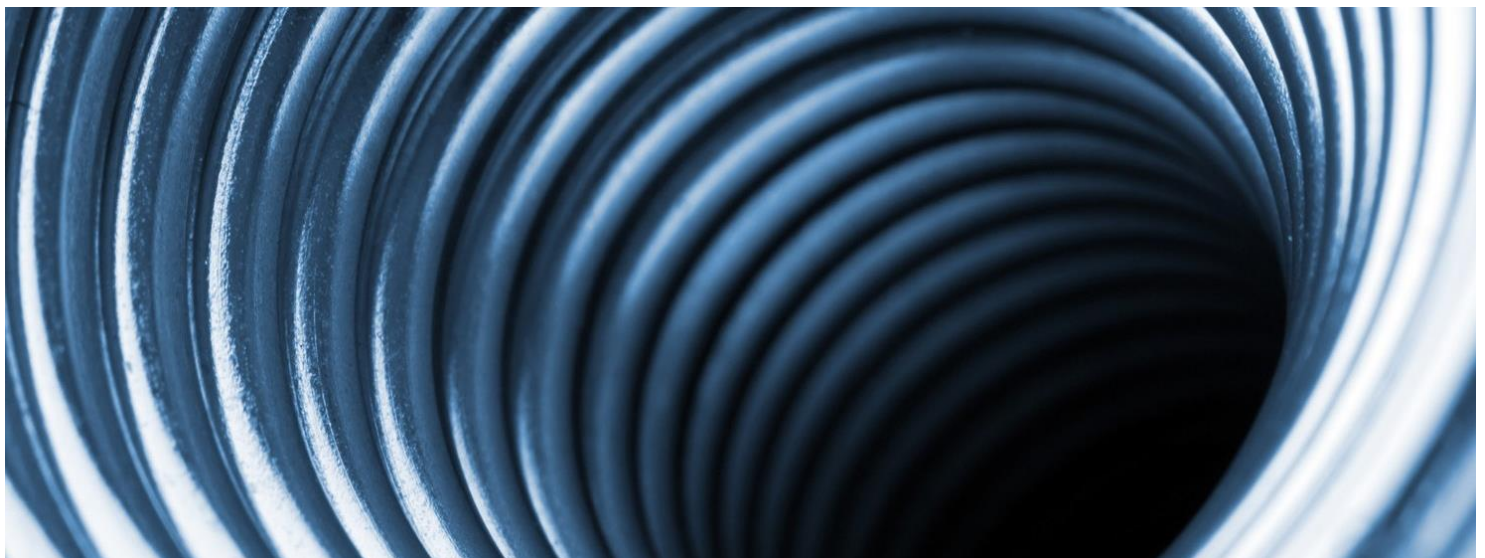
Agile values, principles, and practices enable IA functions to quickly pivot to focus on emerging risks and to navigate the current remote working environment. Organisations that have implemented or are implementing Agile IA have reported:

- Small, self-organising teams are more connected and feel more accountable to each other. They are used to working without being managed and function well in ambiguity.

- Agile IA teams are used to reprioritising work based on new and emerging risks, both within an individual audit and with respect to which audit comes next.
- Agile IA teams have adopted the discipline of frequent, targeted communication (i.e., Agile events) both within their teams and with stakeholders. In particular, the daily stand-up event has proven to be very useful. It entails connecting for 15 minutes to answer three questions: what was accomplished yesterday, what will be accomplished today and what is needed to make progress?
- Given improved collaboration with stakeholders, teams that use Agile principles have reported better responsiveness even during times of crisis.

### Where can I find more resources on Agile IA?

[Becoming agile: Elevate internal audit performance and value](#)





## 4. Establish standards for secure and continuous access to key sources of business data



### *Lifecycle phase: Acquire data and documentation*

Obtaining testing data and documentation can be difficult during remote internal auditing, especially if key stakeholders are not used to providing IA complete read-only access in the first place. Given the business focus on operational continuity amidst the global pandemic, relying on stakeholders during this period to obtain testing data can further jeopardise timely delivery. This is an opportunity for IA to establish continuous access to key sources of business data, and move away from the conventional model of internal auditing.

With higher risk of non-approved devices accessing the network in a remote environment, IA may likely need to put new standards in place for data-access and information sharing. Change may not be immediate, but these standards will pave the way for future audits that are driven by analytics and automation.

**Access to data** is essential for remote internal auditing. Accordingly, IA's ability to continue to provide assurance largely hinges upon standardising protocols across the organisation for accessing and sharing data.

Often, IA has to spend many hours obtaining access to source systems and business data, which takes time away from analysis. While auditors can continue to execute their audit plans through virtual walkthroughs and meetings, IA can use this unique situation as an opportunity to build the data pipelines—in other words, to collaborate with the business and IT to gain persistent, scaled access to data sources. This is more feasible today than in the past, since enterprise data warehouses, data lakes, and cloud computing now offer real-time access to vast quantities of enterprise data. Better data access not only benefits IA, but also the business and IT, by allowing everyone to spend considerably less time on data acquisition, to access higher quality data, and to be more flexible in responding to plan changes.

**Data compliance.** Maintaining compliance with data privacy regulations can be difficult when working remotely, given that the technology environment is more distributed. IA should collaborate closely with IT to ensure security, confidentiality, and privacy in accordance with applicable regulations and internal policies. IA should also avoid creating shadow business intelligence environments to support its needs. Obtaining data extracts from desktops, moving data files via email, and using non-conforming enterprise solutions can expose the company to considerable risk. While enterprise data platforms can resolve many of these security concerns, some internal auditors may still be concerned about loss of objectivity when they can't independently source the data. Data validation techniques can be incorporated into the process to alleviate this concern, since the rewards of using enterprise data solutions generally far outweigh the risks.

# Spotlight opportunity: Automated core assurance



“We have more risks than we have time to cover them” is a constant refrain for internal auditors, and this constraint is likely to tighten. Increasingly, stakeholders expect coverage of strategic, operational, and emerging risk areas, but these new demands come in addition to IA’s ongoing role in providing core assurance, such as assuring that the finance and operational accounting areas are working properly (e.g., procurement, payables, payroll, and health and safety) and that the organisation’s most-challenging risks are being managed appropriately (e.g., cyber, digitalisation, and change management). Automating core assurance by harnessing analytics, robotic process automation (RPA), and artificial intelligence (AI) allows IA to monitor controls and flag nonconformance in real-time. Through automated reporting, these findings can be rapidly communicated to the business for immediate remediation.

## FAQs



### What are some benefits of automated core assurance?

Mainly, it helps reduce the tradeoff between core process assurance and strategic risk coverage, allowing IA to deliver both. It also facilitates better resource allocation so that IA can focus on identifying the greatest risks, analysing why issues occur (including the behaviours that contribute to non-compliance), and devising remediation strategies. Overall, automated core assurance shifts IA’s role from an identifier of issues to a partner in developing solutions. With it, audits begin with known issues, which enables IA to add value by helping the business to improve processes and controls.

### How do I know which audits to automate?

The general approach is to look for audits that repeat on an annual basis, share data across several other tests, and have minimal variability over time. IA should keep its risk profile, scale and audit plan in mind when creating the selection methodology, and engage auditors from the bottom up in identifying the right automation opportunities. For additional guidance,

Deloitte has developed a methodology for identifying audits that are good candidates for automation, meaning those that could yield substantial risk reduction, provide great assurance, and offer a compelling return on investment.

### How do I work with the first and second lines of defence to reduce automation overlap?

IA can assist management in identifying opportunities to enhance first- or second-line capabilities for providing assurance on processes or controls. During planning of new systems or changes to existing ones, IA should discuss each line’s assurance needs and potential mechanisms for meeting them. Likely processes include those subject to regulatory reporting in which a bot can pull 100 percent of transactions or accounts, prepare the data, conduct the initial analysis, identify the exceptions, and route them to the appropriate second-line people. This enables IA to review the processes, tools, and results.

### Where can I find more resources on automated assurance?

[Digital testing and controls automation: A transformative approach to automating your control environment](#)

## 5. Identify opportunities for digital analytics and continuous monitoring capabilities



### *Lifecycle phase: Execute audit*

As audit teams find themselves working remotely, the value of exception-based monitoring and analytics-driven process analysis is becoming readily apparent. IA departments possessing these capabilities are generally demonstrating greater resiliency and flexibility in these challenging times, and they provide inspiration for others to continue on their digital journeys.

**Target analytics and automation** toward audit areas that require standardised and repeatable tests, such as those required for meeting SOX or other regulatory reporting standards. Rather than having to deploy new technologies, this can often be done by using existing automation, analytics, and data visualisation technologies that are readily available within the company's portfolio. These tools are frequently enough to start building a book of automated controls that can be assessed through exception review.

**Reflect on the current use of digital tools** and assess the potential for reducing risk management costs, without impairing effectiveness. Take Continuous Controls Monitoring (CCM) for example. CCM would enable the first line of defence to take ownership of its risk profile and the second and third lines of defence to become strategic advisors. (See Spotlight Opportunity: Value-based investigation with Continuous Controls Monitoring.)

**Determine if testing workarounds will be needed** in instances where evidence is not readily available in digital form. This may be the case for organisations that utilise manual documentation or have restricted access to systems. IA can overcome these hurdles by communicating the importance of monitoring risks in real time and asking the business and IT for direct access to the required systems.

#### Quick tips Collaboration tools

Evaluate **manual testing procedures** to determine where analytics can be utilised and what value it can offer.


Be understanding of **operational changes** due to the remote work environment and brainstorm with the business on how to address associated risks.

Practice an increased level of **professional skepticism**, especially for processes that have been altered due to the remote environment.

Requesting **direct access to systems** is an important step in making the audit more efficient and effective.

# Spotlight opportunity: Utilising process analytics to offer insights to the business



 In the wake of an unexpected event, companies often want to identify operational areas that can be optimised or streamlined. This can be challenging because business processes are complex. Even with large-scale ERP investments intended to automate and standardise business processes, root causes of problems can be difficult to detect. IA can leverage process analytics within the testing environment to detect complications and provide insights into fundamental deviations from established processes and controls.

## FAQs



### How does process analytics add insight to the business?

Process analytics takes transactional data from business financial and ERP systems and uses it to reconstruct what actually happened within the end-to-end process (e.g., order to cash or purchase to pay) based on 100 percent of the data. It changes the conversation from finding out what happened, where and by whom; to understanding why things happened the way they did. It does this by:

- Showing what really happened: Process analytics helps IA to discover the actual flow of transactions and highlight any deviations from the expected process flow, such as bypassing a control, or duplicating steps and workarounds.
- Providing context: An insight only becomes actionable if it has context. For instance, it may be good to know if invoices are paid after their due date, but this information only adds value if the back story is known, such as what are the execution patterns and which categories of vendors are involved. Process analytics can help IA shine as a business advisor by adding context to its findings, which can ultimately be used to develop and refine the remediation plan.
- Enabling self-service: Process analytics can empower people to do it themselves. Process analytics makes it possible to explore business issues faster and execute root-cause analyses without help from third parties or data scientists.

### Where in the audit lifecycle can process analytics be used?

Process analytics can benefit IA throughout the audit lifecycle. For example, it can be used in an exploratory sense to pinpoint the root cause of failed transactions and ineffective controls and processes. This insight, in turn, can help the team formulate more effective audit test procedures. It can also be used to execute audits and communicate a stronger, well-supported message to stakeholders by:

- Revealing an end-to-end process view
- Drilling into and quantifying the issues at the activity and user levels
- Establishing a single version of the truth to improve decision making.

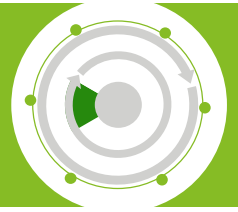
### What is the difference between process analytics and process mapping?

Process mapping usually derives information from conversations and manual examination of supporting documentation. In contrast, process analytics solely relies on the ERP system's data to provide transaction-level mapping. Because the mapping is purely fact-based and it does not require manual data collection, it can provide unbiased insights into the specific issues.

### Where can I find more resources on process analytics?

[Process Analytics | Deloitte Process X-ray™](#)

# Spotlight opportunity: Value-based investigation with Continuous Controls Monitoring



Many organisations are seeking strategies for maintaining a highly effective risk management program during tough economic times. Continuous Controls Monitoring (CCM) may be one such strategy. It can allow companies to reduce risk management costs, without impairing effectiveness. Much of its power lies in enabling the first line of defence to take ownership of their risk profiles and empowering the second and third lines of defence to become strategic advisors.

## FAQs



### What is CCM?

CCM is a technology-based solution for continuously monitoring processes and helping second and third lines of defence to transition from traditional, sample-based testing models to economical monitoring of full populations. As a platform offered as a managed service, CCM empowers and enables the first line to own and run their operational processes, while retaining transparency and creating an audit trail. This trail, in turn, allows the second and third lines of defence to monitor first-line activities, thus eliminating redundancies in testing and associated costs. Through these shifts, it allows IA to redeploy resources from rote testing to value-based investigations.

### How does CCM work?

CCM is a cloud-based, digital, managed-service solution that delivers transformative automation and actionable control monitoring. Using an open architecture, it is source-agnostic and able to process any application or contextual data. The service provider can pull data from client source applications or the client can push data to the solution themselves in a fully automated way.

### Who could benefit the most from implementing CCM?

CCM can help companies with heterogeneous IT landscapes and disparate processes that are struggling to make sense of their data and provide adequate levels of assurance; those looking for new ways to simplify risk performance or to rationalise controls; and those seeking to emphasise risk and control accountability within the first line of defence in order to embed controls into management processes.

It can also benefit IA teams engaged in digital transformation at the enterprise level, but that are still using traditional approaches to risk management, as well as those who are grappling with manual processes that are no longer sustainable as the organisation becomes increasingly digitised.

### Where can I find more resources on CCM?

[Continuous controls monitoring: Empowering business with actionable risk insights](#)

## 6. Redefine reporting and communication model

### *Lifecycle phase: Deliver results and insights*



As the IA organisation shifts toward a virtual operating model, it is imperative that its communication strategies shift as well. This often implies modifying the frequency and means of communicating with stakeholders.

**Compile a list of all stakeholders** who should stay informed, mapping each audience group to the method and cadence of communication that would be most effective. Factors to consider include:

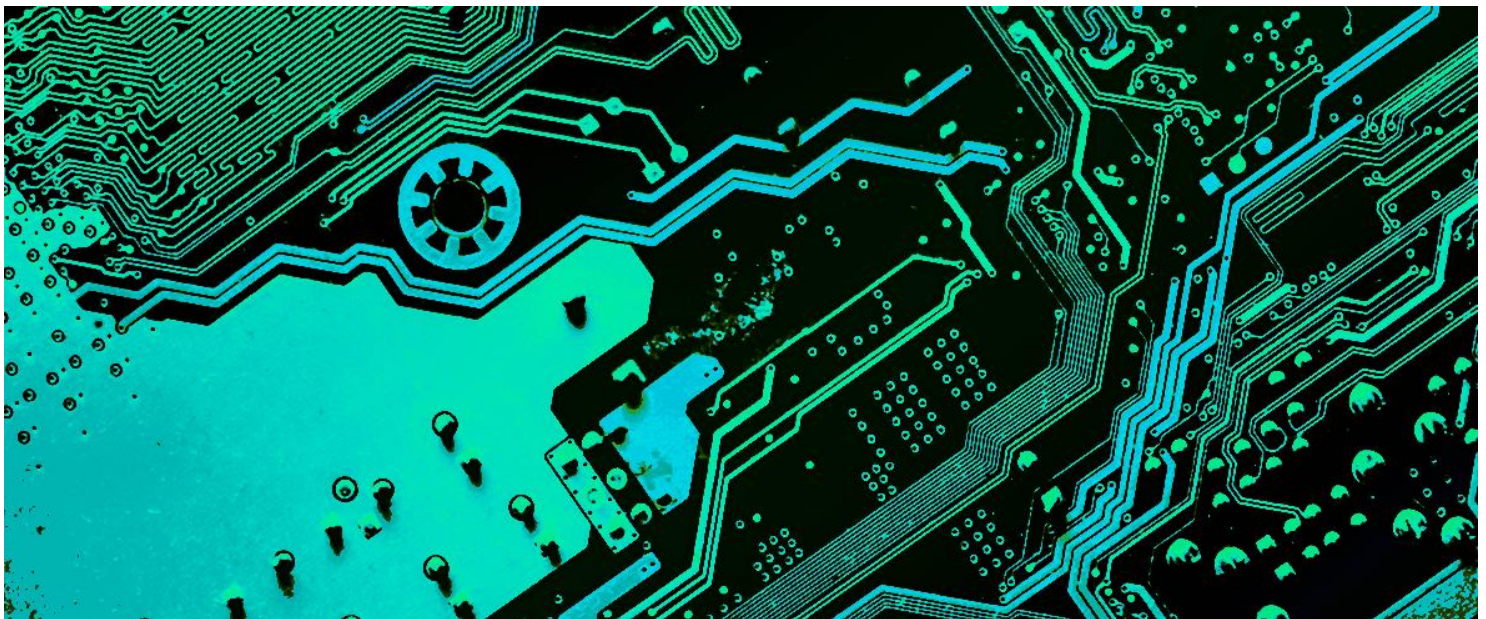
- How much or how little information does the audience need in order to stay informed?
- Would the audience like to see more details through a monthly newsletter or some other vehicle?
- Would the audience prefer an analytics dashboard where they can see the status of projects or testing?
- Who is responsible for tracking the status and any action items as audits progress?

---

**Consider increasing the frequency of communication** with each of the key stakeholders, including the Audit Committee. Also, don't underestimate how valuable informal interactions in the office once were. Try to mimic those interactions in a virtual setting.


---

**Use interactive dashboards** to report on audit findings. This can help keep stakeholders and IA aligned on outcomes and recommendations even when people are not physically in the same space.



# Spotlight opportunity: Redefining report and communication model



 For many IA organisations, virtual communication methods are not only unfamiliar but also intimidating. Visualisation techniques, such as dashboards, can help bridge the gap between IA and its stakeholders. Presented properly, graphical representations of data can provide compelling insights and be understood much faster than written text. However, in order to communicate clearly, correctly and efficiently, dashboards must be carefully designed.

## FAQs



### What value can IA deliver through visualisation tools such as dashboards?

Visualisation tools give IA the ability to utilise available data, identify hidden insights, and communicate them throughout the organisation in an easily digestible form. Also, because the images are based on data, they represent quantitative evidence of a hypothesis, which builds trust with the audience and positions IA as an advisor and thought leader. Dashboards are also known to save time in gathering and analysing data, convey insights quicker, and assist IA in creating impactful narratives.

### Who are the stakeholders and how should they be addressed?

Key stakeholders often include: Audit Committees, Chief Compliance Officers, Chief Risk Officers, Chief Audit Executives, CIOs, and CISOs, process owners and their teams, and IA team members. Each group should be addressed according to their needs. For instance, the Audit Committee may prefer summarised, high-level findings with the ability to click-through for more information, while process owners may only want to view information that is pertinent to their department.

### How do we ensure that our message is making a difference?

IA departments may rethink how they convey their findings. The goal should be to produce high-impact reporting, which generally has the following characteristics:

- **Flexible:** Able to communicate ideas in different ways
- **Dynamic:** Can be updated and refreshed easily by various individuals
- **Efficient:** Uses automation to flow data and provide different analytical cuts so IA doesn't have to start every report from scratch
- **Relevant:** Features timely, useful information and emphasises critical points
- **Intuitive:** Uses data visualisation, links, and icons to guide the audience to what they need to know quickly
- **Data-driven:** Insights that are supported and backed by reliable data.

### Where can I find more resources on digital reporting and dashboarding?

[Revolutionising digital reporting in the digital age](#)

# The foundational principle: Stay connected

Underpinning all of the other guiding principles, IA teams should **stay connected** above all else.

As the organisation moves toward virtual operations, IA should communicate often to maintain a positive team culture and to assess the impact of dynamic circumstances on processes, controls, and risks.

**Encourage the use of video capabilities** during meetings to help humanise the audit and keep stakeholders engaged in the conversation. This also makes it easier to practice professional skepticism by reading body language throughout the conversation.

**Set meeting protocols** to clearly communicate the objective and key takeaways. Since people are being asked to participate in more virtual meetings than ever, it is important to set clear expectations. This includes sending agendas prior to the meeting so that attendees can come prepared and be ready to show relevant documentation if needed. Afterward, summarise action items, individual accountabilities, and any documents required to minimise the need for follow-up meetings. Be purposeful in your virtual interactions, more meetings doesn't always mean more is accomplished.

**Catch up with the team daily** to check in on the well-being of your teammates, in addition to receiving status updates. With many conflicting pressures such as children at home and family obligations, it is important to offer support as a colleague, not just as a team leader who needs to get something done. An empathetic approach encourages transparency and offers the opportunity to proactively resolve roadblocks or to redirect and reassign tasks if someone is experiencing difficulties.

**Dedicate time for social interaction.** IA teams inherently seek to build strong relationships throughout the organisation. This doesn't need to stop when working remotely. Take advantage of video capabilities to organise social events, such as virtual happy hours, trivia nights, mid-day yoga breaks, or coffee breaks. Not only can this type of social interaction help further progress on current projects, but it can also shed light on what other teams are prioritising in terms of upcoming projects.

## Quick tips

### Staying connected

**Check your camera and headset** prior to the meeting to minimise technology disruptions.

**Avoid side messaging or multi-tasking** and encourage participants to set their status to "Do not disturb."

Make **eye contact** and limit movement.

Make the conversation as **interactive** as possible by utilising functionalities such as screen sharing, polling, etc.

**Don't be afraid of silence.** Give people time to think and reflect on the conversation.

Allocate a couple minutes **for casual conversation** rather than "jumping right to business."

**Diversify social events** to appeal to different team members. For example, a mid-day yoga session may be easier for people to attend than an after-hours happy hour.



# Conclusion - What might the COVID-19 pandemic mean for IA strategy in the long term?

**Organisational resilience** will likely be the main focus for nearly every company moving forward, making the role of IA ever more pertinent. In the short term, IA can use the guiding principles and tips and tricks in this document to help maintain team productivity and engage stakeholders.

However, in the long term, IA should recognise that a **deeper digital transformation** is likely required. New digital tools and automation technologies are creating a world in which remote internal auditing does not mean compromised quality or plan reductions. Instead, it implies a higher level of functioning. In this new world, IA should embrace continuous risk assessment, exploratory analytics, automated controls testing, and Agile methods as a way of decreasing costs and adding advisory value in any environment—whether physical, virtual or somewhere in between.

## Contacts

### Corporate and Public Sector Internal Audit



**Karl Williams**  
CPS Internal Audit Lead  
[kdwilliams@deloitte.co.uk](mailto:kdwilliams@deloitte.co.uk)



**David Tiernan**  
Associate Director  
[datiernan@deloitte.co.uk](mailto:datiernan@deloitte.co.uk)



**Annemarie Wait**  
Senior Manager  
[await@deloitte.co.uk](mailto:await@deloitte.co.uk)

### Financial Services Internal Audit



**Russell Davis**  
Financial Services Internal Audit Lead  
[rdavis@deloitte.co.uk](mailto:rdavis@deloitte.co.uk)



**Aaron Oxborough**  
Partner  
[aoxborough@deloitte.co.uk](mailto:aoxborough@deloitte.co.uk)



**Owen Jackson**  
Director  
[ojackson@deloitte.co.uk](mailto:ojackson@deloitte.co.uk)



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

© 2020 Deloitte LLP. All rights reserved.