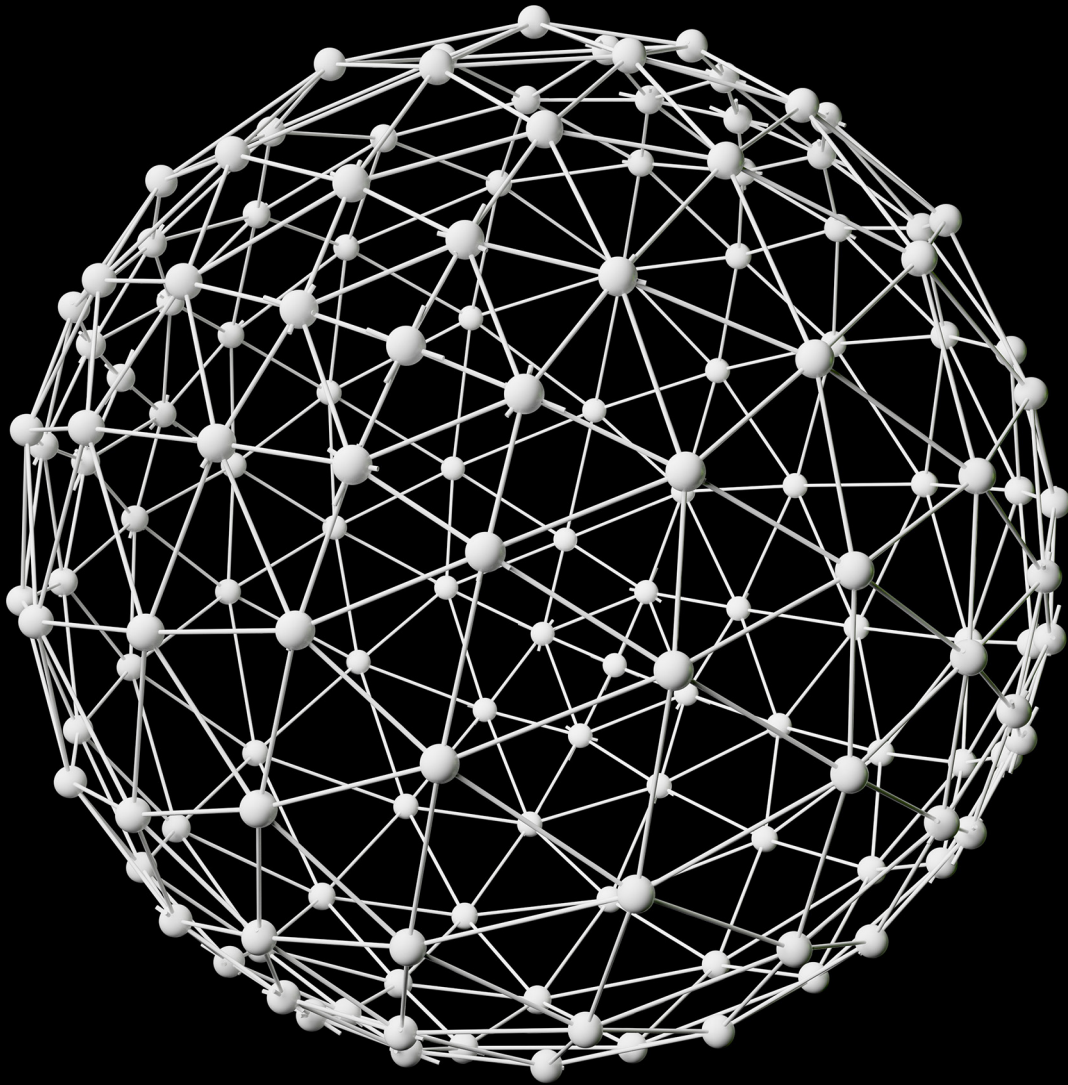


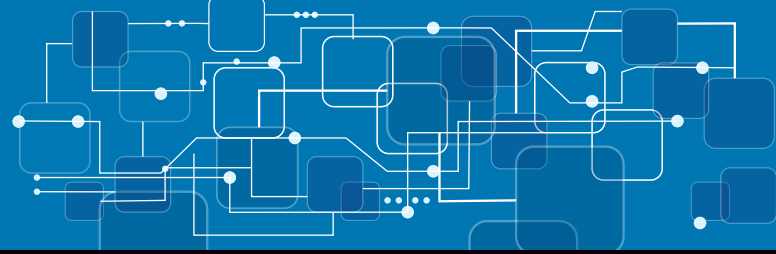
Deloitte.



RISK EXCELLENCE

Connect. Modernize. Digitize.

Take Command of Risk



Take command of risk

Something fundamentally important is happening. Organizations are on the brink of a new age of capabilities; the acceleration of digital technologies is radically changing organizations in ways that will challenge the basic assumptions and operating models of entire industries.

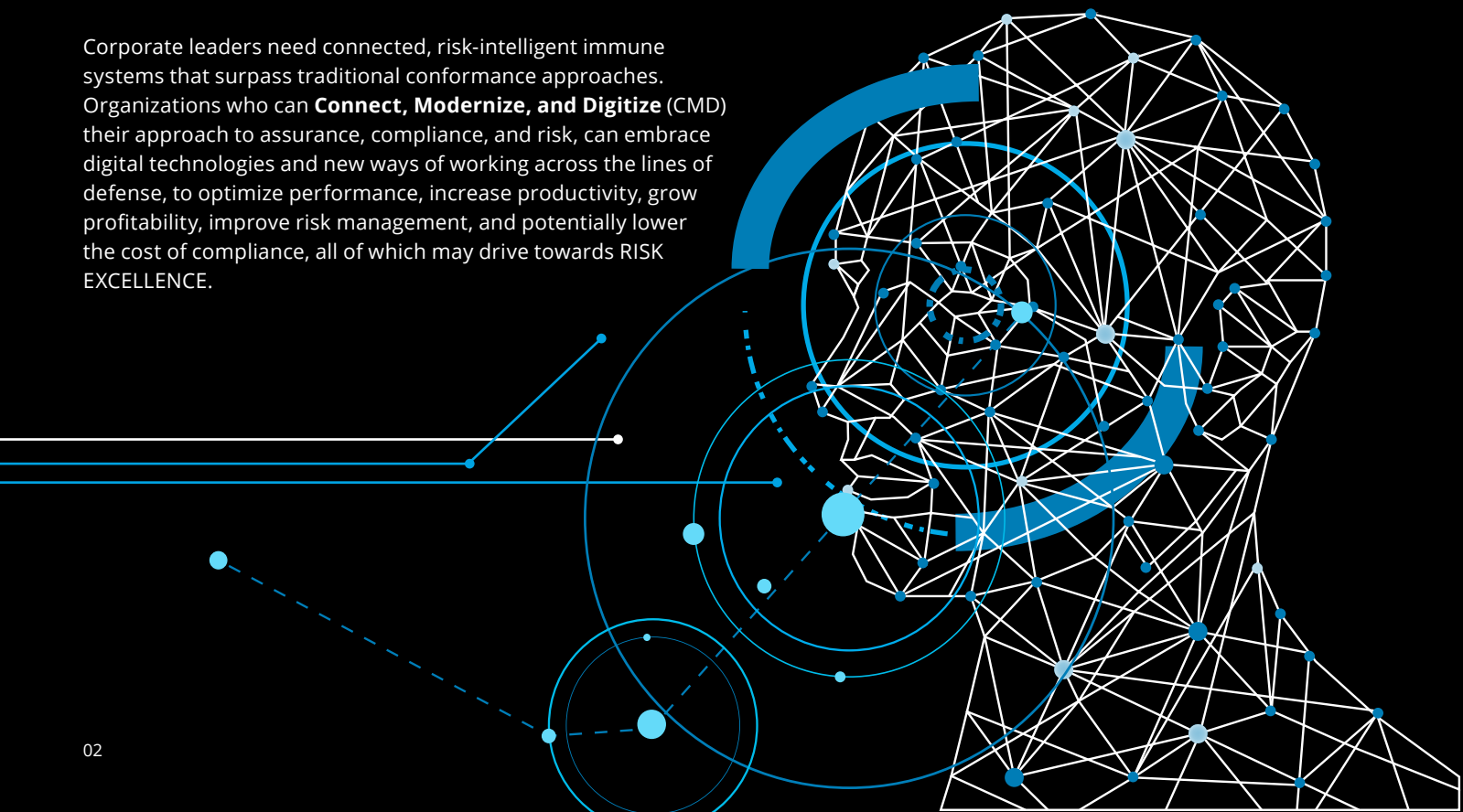
For companies to stay relevant, competitive, and ensure their survival, they must both harness these new capabilities, and also navigate the risks of disruption. Just as a chameleon changes its colours to adapt to its surroundings, the mechanisms that protect and support the organization must also adapt. However, in a rapidly changing digital world, many of the existing organizational defense mechanisms are no longer sufficient, thus limiting organizations' ability to predict, manage, and respond to risk.

With a traditional three lines of defense model, there are persistent challenges posed to organizations, including burdensome compliance programs and misaligned assurance activities, which limit the ability of organizations to optimize efforts. Issues can be compounded by disconnected site-specific tools and siloed solutions resulting in lapses and errors, and, often times, very public management failures. Together, these conditions perpetuate the image of traditional three line of defense functions as intrusive and of limited value.

Corporate leaders need connected, risk-intelligent immune systems that surpass traditional conformance approaches. Organizations who can **Connect, Modernize, and Digitize** (CMD) their approach to assurance, compliance, and risk, can embrace digital technologies and new ways of working across the lines of defense, to optimize performance, increase productivity, grow profitability, improve risk management, and potentially lower the cost of compliance, all of which may drive towards RISK EXCELLENCE.

The ongoing digitalization of business processes, transactions, and relationships, along with the decreasing cost and increasing accessibility of digital technologies, holds tremendous potential for assurance, compliance, and risk management functions. Yet in many cases most of that potential has gone untapped—until now.

The cost and accessibility of cognitive, analytical, and automation technologies are no longer the limiting factors they were even a few years ago. By incorporating assurance by design into business processes, leveraging automation for control functions, and innovating assurance activities, organizations are able to generate greater visibility into risk and faster response to remediation. Those organizations who achieve the CMD paradigm shift in assurance, compliance, and risk and are realizing benefits.



What is CMD?

CMD is a strategic and adaptive way of building resilient organizations by connecting, modernizing, and digitizing assurance, compliance, and risk management activities across an organization.

CMD aims to help not only to digitize but also to connect, and when appropriate, to transform the ways in which the enterprise delivers assurance, compliance, and risk management, to the benefit of the larger organization. CMD has been specifically designed to help assurance, compliance, and risk functions in their effort to address the challenges they face in adopting technology. How? By focusing on goals, risks, processes, roles, and responsibilities rather than taking the siloed, tools-focused approach that actually compounds the challenges.

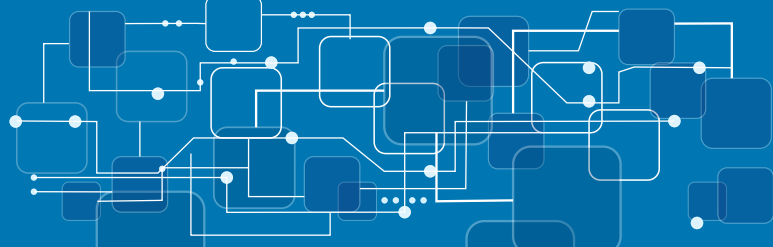
CMD is designed to generate higher-quality assurance at a lower cost, greater impact and value across the governance model, and provides actionable insights for the business. The core components of CMD include:

Connecting and aligning assurance, compliance, and risk management efforts creates the operating and governance models necessary to align activities across the three lines of defense, and aligns them to where they can be done most efficiently and effectively. It starts with understanding requirements (including skill sets); optimizing the layers of assurance; aligning tools and methods; and creating a line of sight for reporting risk signals, conformance indicators, and performance outcomes.

Modernizing the three lines of defense enables organizations to take a holistic approach to identify, monitor, manage, and assure risk in a rapidly changing world, where evolving business models and disruptive technologies are the norm. Modernizing elevates compliance, risk, and assurance to new levels of agility, predictive accuracy, real-time assurance, and informed risk taking to support operational excellence and achievement of strategic goals.

Digitizing reduces repetitive lower-value compliance monitoring and testing activities to allow resources to focus on higher-value activities and meaningful work. Automation of operational discipline across the three lines of defense drives faster identification and response times to risk, builds assurance mechanisms into the day-to-day processes by design, and instills confidence through complete coverage of data sets. It also enables assurance providers to embrace an agile mind-set; experimenting with new methods across the risk spectrum and using real-time information to identify and prioritize on the areas of highest risk.





A CMD initiative is not just a technology solution but a combination of a new mind-set, skill-set, and tool-set for organizations. A CMD initiative:



Assesses people, processes, and technologies, and automates and connects those that can, if automated and connected, benefit users and the organization; in contrast, purely technology-focused efforts overlook such considerations.



Goes beyond automation to foster connection and efforts of the three lines of defense as appropriate to stakeholder needs, organizational culture, and regulatory mandates.



Transforms and reinforces a sound operating model of risk management, such that risk owners are informed and empowered, and assurance providers, such as Internal Audit, focus on the areas of greatest risk.

Post-transformation assurance may appear different, in various ways.



Assurance by design underpins processes, which evolve to continuous or real-time modes. Exception handling routines, transparent reporting, and governance over remediation reduce the need for sample-based testing. Assurance activities shift to assessment of automated business rules, monitoring of Key Risk and Performance Indicators (KRIs/KPIs), and analysis of unresolved exceptions.



Core assurance activities, especially those that are more routine and transactional focused become automated, relying on analytics and process automation to replace less efficient manual activities. Reports become shorter and more impactful with stakeholders conducting rapid analysis of visual dashboards.



Assurance migrates, as appropriate, to the second and first lines, which can develop protocols in consultation with Internal Audit and Compliance and, going forward, enabling Internal Audit to provide assurance on the integrity and effectiveness of the processes and controls.

Of course, organizations have different needs, perspectives, regulatory expectations, and appetites for change. Some are willing to revisit the traditional three lines of defense model, while others are not.

Therefore, organizational cultures, stakeholder needs, and regulatory requirements can all be accommodated within CMD. Yet, given the range of possibilities, formulating a vision for CMD and understanding the possibilities can help you decide how far you want to go.



Why CMD?

There are many reasons to connect, modernize, and digitize assurance, compliance, and risk management, including:

From a first line, business unit perspective, risk management can seem ancillary rather than integral to their roles. Risk data often arrives after the fact, enabling the business to only react to risk rather than to capitalize on it. We have then seen businesses experiencing assurance fatigue, one notable example of this was a company with more than 50 distinct global assurance processes. CMD builds assurance mechanisms into the design of business processes to achieve both conformance and desired performance outcomes.

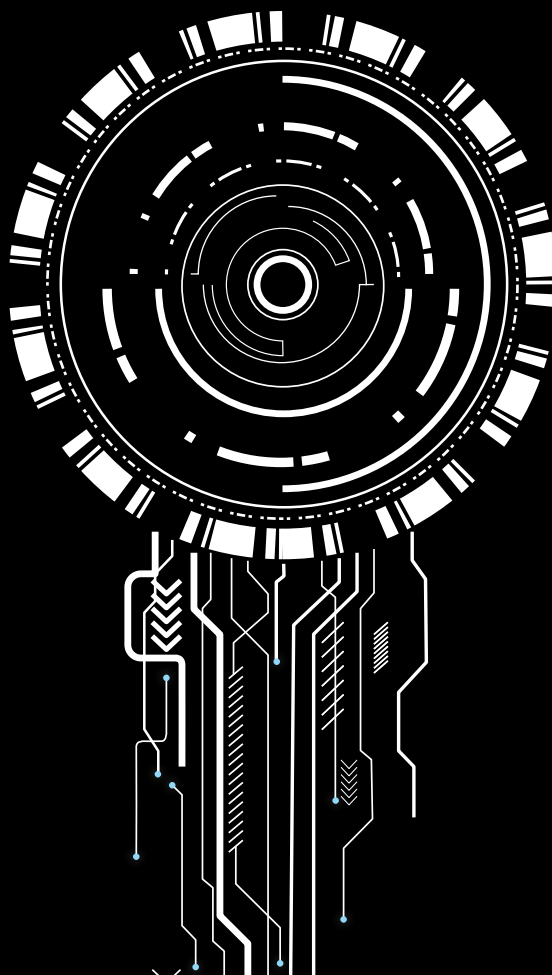
From a second line risk management perspective, evolving risks and regulations create continual pressure to do more, increasing the cost of assurance and compliance. Automating operational discipline and assurance by design can reduce the burden of expensive compliance monitoring programs and perceived duplication between second and third line assurance providers. These functions also want to deliver as much value to the business as possible, and to focus on the most important risks. CMD helps create capacity for second line functions to spend more time helping management navigate the truly greatest risks.

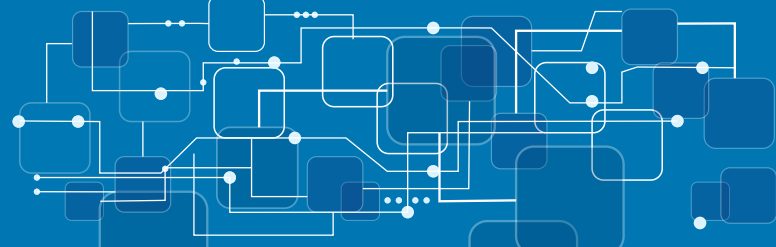
From a third line Internal Audit perspective, stakeholders are demanding more assurance on an expanding range of risks, more forward-looking advisory services, and more penetrating insight, as well as foresight. The exponential growth in data volumes and technologies means assurance providers are struggling to keep pace with assurance needs.

Organizations need a more intelligent way to meet growing demands, but also increase the speed of assurance and insight. CMD can help Internal Audit functions meet these expectations, and through helping the organization achieve CMD, enhance its organizational impact and influence.

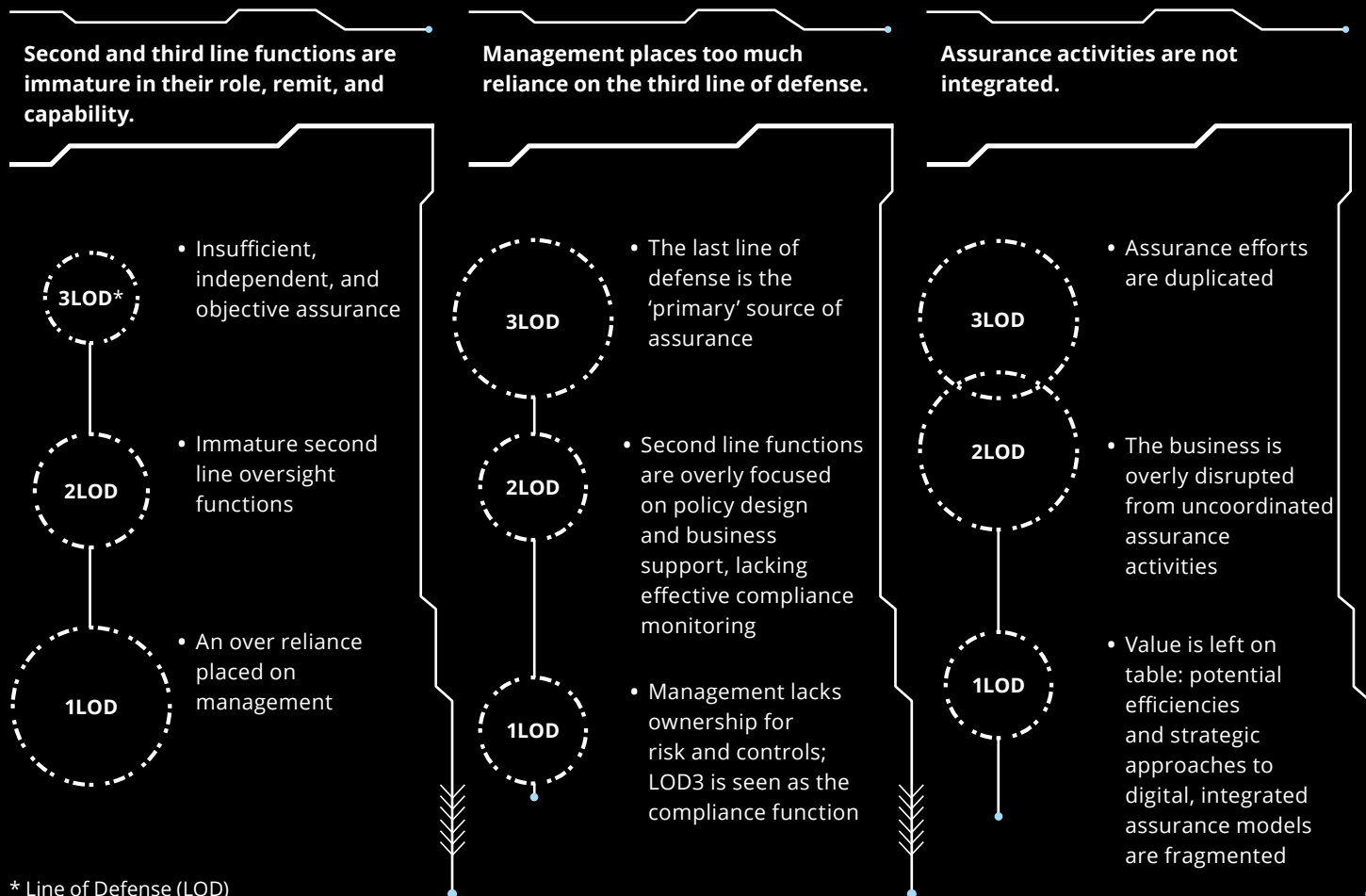
Failure to address these issues can lead to common problems:

- First line functions in the business can lack ownership for risk and believe it is being managed in the second line and third lines.
- Duplicative compliance and assurance efforts in the second line disrupt the business, generate excessive costs, and provide fragmented perspectives on risks, and how they are being addressed.
- Internal Audit—the “last line” of defense—is often seen as the primary source of assurance or, in some cases, as a policing function, which undermines its brand, stakeholders’ trust, and, potentially, the organization’s risk management behaviors.





These problems can lead to suboptimal operating models for risk and assurance management. Three models that are typically found in organizations are outlined below.



If left unchecked, an organization's assurance model may result in unhelpful consequences. For example, where too much reliance is placed on the third line, Internal Audit functions can:

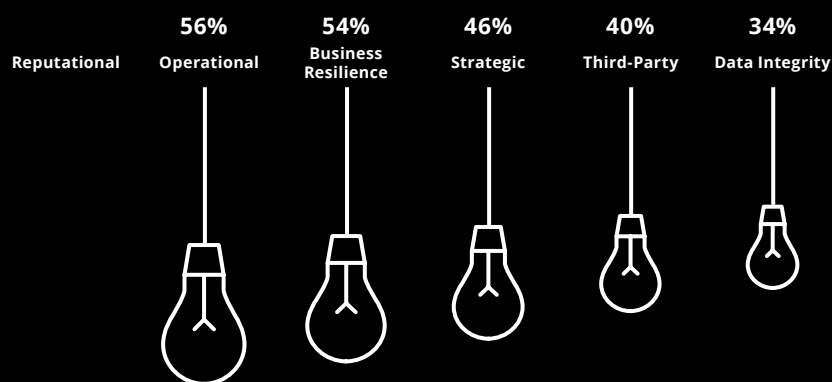
- Spend a disproportionate amount of time on compliance, detracting from the truly greatest risks;
- Erode trust with management; Internal Audit is perceived as a 'policing function';
- End up reporting low-level compliance exceptions, failing to create impact or drive change; and
- Create an industry of management actions and follow-up, often distract the business from managing greater risks.

CMD can help address these issues as well as another long-standing challenge: many organizations still struggle to harness technology to enhance assurance, compliance, and risk management. Many have launched pilot projects and one-off efforts that, while often useful, have lacked impact. Failure to scale and to link projects to a strategic vision limits their potential, leaving them siloed and sequestered. Such efforts strike management as "technology projects" or, at best, as faster ways of doing the same thing.

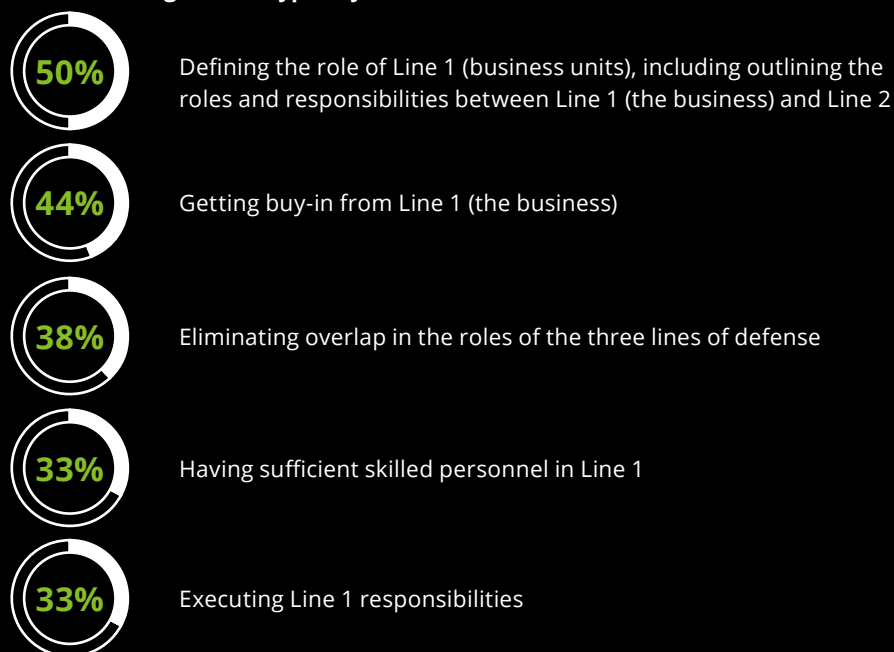
Deloitte's 11th Global Risk Management Survey¹ outlines the continued challenges facing organizations in achieving connected, modern, and digital immune systems.

Almost all respondents considered their organizations to be effective in managing traditional financial risks, such as market, credit, and liquidity. In contrast, little over half of the respondents felt they were effective at managing non-financial risks, such as reputation, operational, business resilience, strategic, third-party, and data integrity risks.

Percentage of organizations effectively managing non-financial risk:



Virtually all respondents (97%) reported employing the three lines of defense risk governance model, but said they face significant challenges. The challenges most often cited as significant typically include:



These challenges are consistent with our experience, as many have been, or are in the process of, clarifying the roles of the first and second lines of defense and working to improve the efficiency and effectiveness within the three lines of defense model.

¹ Global risk management survey, 11th edition: Reimagining risk management to mitigate looming economic dangers and nonfinancial risks <https://www2.deloitte.com/content/dam/insights/us/articles/4222_Global-risk-management-survey/DI_global-risk-management-survey.pdf>

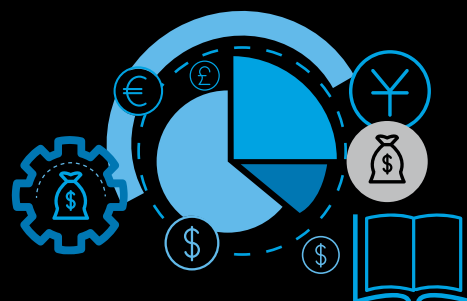
The undeniable truths of today's approach to controls and compliance

Traditional controls are expensive and time intensive. They are providing organizations with a false sense of security and are not keeping pace with digitization and regulatory change. For example, many SOX compliance programs have become too big and too costly. Companies invest too much for too little return. As a result, organizations are testing things in the most expensive way.

Kills performance

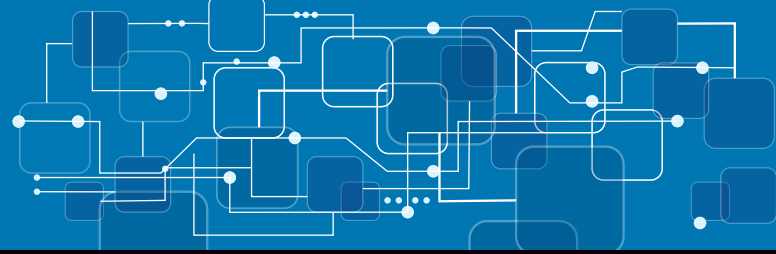


Too expensive



False sense of control





Benefits of CMD

Among other benefits, CMD enables the organization to:

- Align key activities across the lines of defense to reduce overlap, close gaps, and enhance control.
- Provide transparency into process and control performance to help people identify, monitor, and mitigate risk events earlier and more effectively.
- Automate activities to provide assurance in real time or close to real-time.
- Initiate a time/value shift to move talent from manual activities to advising stakeholders and addressing threats and opportunities.
- Provide people with risk-related responsibilities, data-driven insights, and a digital workspace, which they embrace as they exercise higher levels of observation, analysis, and expertise.

Advanced digital technologies transform work by performing repetitive tasks that require lower intellectual horsepower. Teams can focus on work which requires interpretation and insight. We have found no shortage of opportunities to exploit this dynamic in assurance, compliance, and risk management.

Here, we shed light on why, what, and how these developments can be leveraged to deliver these benefits.

About “the who”

As we present the why, what, and how of CMD, you might consider the who. We have seen CMD initiatives initiated and driven by:

- Control owners in the first line of defense—the business—who are accountable for managing risk, and executives and managers, who benefit from better risk data, more informed risk taking, and far less intrusive assurance.
- Second line risk functions like compliance, operational risk, and information technology security, who benefit from more effective (and efficient) compliance and a shift to higher-value activities.
- Internal Audit who, as the third line of defense, traditionally provide the most assurance, benefit through improved execution of risk-related responsibilities across all three lines of defense.

The value of a Connected, Modern, and Digital organization



Optimal controls to support better business performance

A strong culture that enables sound risk taking

Smarter controls, maximizing automation

Real-time, simple monitoring and reporting

A fit for purpose control framework

Case study

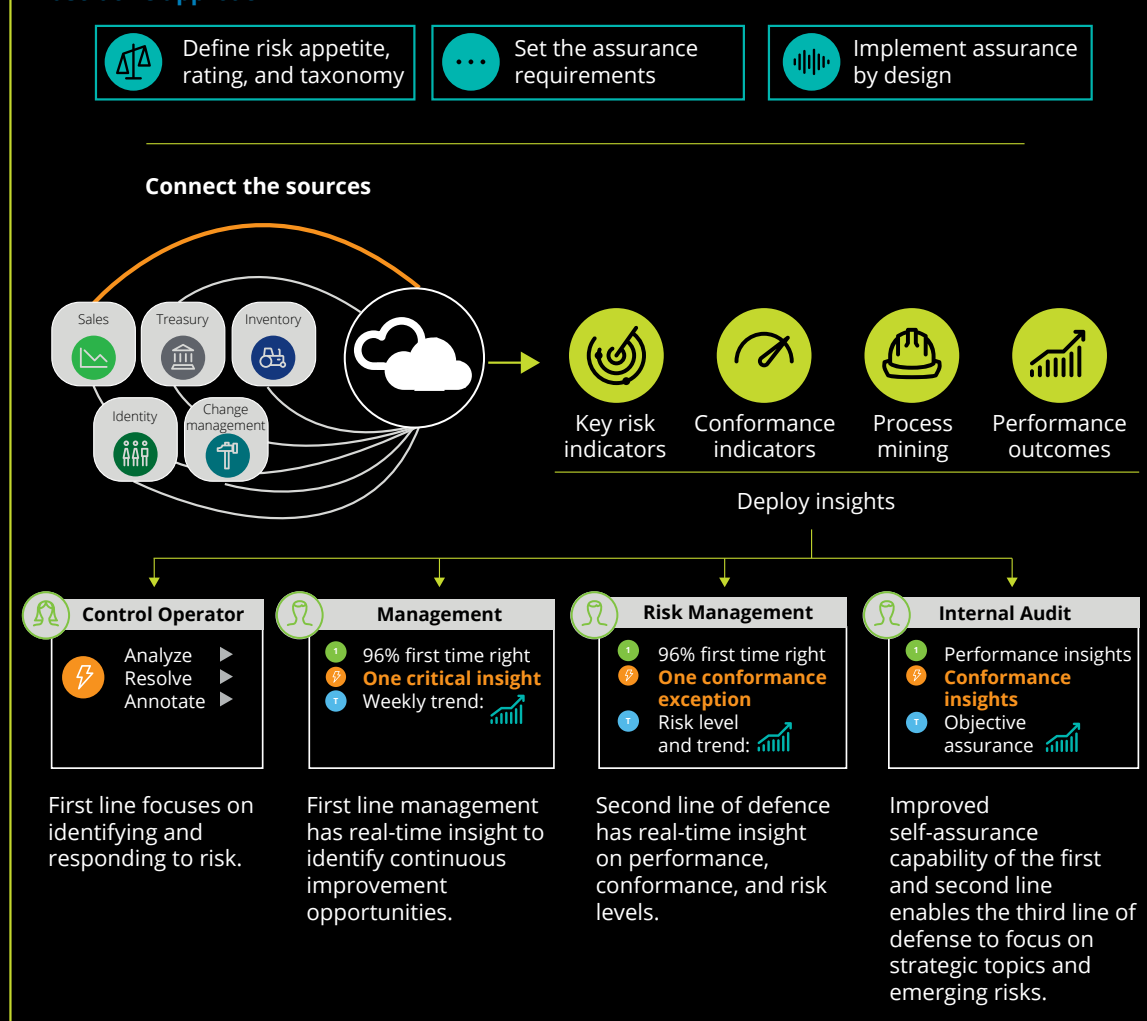
Before embracing a CMD initiative, one organization faced a range of common challenges, including an insufficient control framework, unclear ownership of risk, and duplication of assurance and compliance activities. Using a technology-based solution to continuously monitor risk and assurance, this organization transitioned from using traditional, sample-based testing models across its second and third line, to real-time non-compliance detection. Modernizing its controls, and connecting sources of information through the Governance Risk and Compliance platform, the organization was able to deploy deep insights across all lines of defense. In turn, this enabled management to focus on continuous process improvement, monitor risk levels against risk appetite, and receive positive assurance over conformance requirements and performance outcomes. Ownership of risk management was embedded into the first and second line, enabling Internal Audit to transform from primary to objective assurance provider.

Through its CMD initiative, the organization empowered and enabled the first line to own and operate its operational processes, while retaining transparency and an effective audit trail. This trail, in turn, allowed the second and third lines of defense to monitor first line activities, thus eliminating redundancies in testing, associated costs, and providing a single, real-time, line of sight across risk and assurance activities.

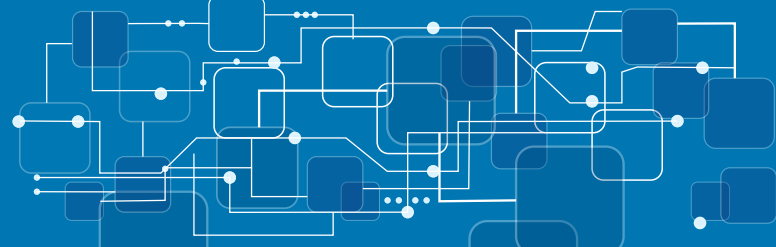
Key benefits:*

- Optimized the assurance, compliance, and risk management activities
- Provided an integrated line of sight across the lines of defense
- Embedded accountability and responsibility for risk
- Created synergies and cost savings
- 35-40% reduction in duplicate assurance activities
- 55-60% increase in effective mitigation of risk across all business

Illustrative approach



*Individual benefits may vary with each organization's unique circumstances



Key considerations

A CMD initiative can begin in any of the three lines of defense. We have seen investments from the business, from second line functions, and from Internal Audit to fund initial efforts. We have also found sponsorship to be critical, with the most frequent champions being the controllership, CAE, CFO, CRO, or CCO—often in some combination.

A CMD initiative can also support or drive other initiatives, such as business process outsourcing, and new ways of working, such as workplace digitalization. Placing such an initiative in the context of CMD — or vice versa — can generate unprecedented momentum and value.

A CMD initiative is generally of the magnitude of larger strategic projects and it can be productive to place it in the context of a series of smaller bite-sized projects or to use it to accelerate progress towards smaller goals:



- **Understanding the assurance landscape:** CMD requires a clear understanding of the total assurance landscape and plan. Who is doing what? What are the capabilities of assurance providers? A comparison of assurance activity, performance outcomes, and resource allocation can also help identify excessive costs and areas of over/under assurance. The resulting understanding of assurance sets the stage for CMD.



- **Education and training:** CMD does not only require organization changes to the assurance target operating model, but a mind-set shift in how organizations think about risk and assurance. It is important to build momentum for change through education and training of both the assurance functions and the business.



- **Understand what is driving the demand:** Understand what is driving the assurance demand and who is “setting the volume dial.” For example, compliance and regulatory obligations, management system requirements, or strategic risk.



- **Optimize the assurance layers:** Who is supplying assurance resources and is there an opportunity to de-layer through alignment, coordination, and agreement over the assurance strategy?



- **Modernizing controls:** Years of neglect, lack of objective challenge, reactivity to regulatory demands, and sheer expediency have created the unwieldy, time-consuming, costly control frameworks now burdening most organizations. Controls modernization updates controls using cognitive and analytical technologies to reduce the number of controls, right-size the controls, and gear assurance to risks that matter.



- **Automating core assurance:** A key part to the assurance strategy is automating assurance over core processes and controls that can enable the second and third lines to dramatically increase the efficiency of their assurance efforts. This frees up resources for both lines to focus more intensely on the most important risks. The definition of “core” will vary by industry and organization and may include essential business processes or specific regulations, such as General Data Protection Regulation (GDPR).



- **Leveraging digital assets to drive insight:** Deloitte surveys of Internal Audit² have found that organizations are committed to digitalizing their business models and processes, thereby creating huge volumes of potentially valuable data. These two facts—digitalization and the potentially valuable data being produced—present transformative opportunities to move assurance to the second and first lines and to revolutionize audit work.



- **Developing your internal brand strategy:** A CMD initiative can spearhead efforts to raise the profile of the organization's assurance, compliance, and risk management functions. CMD can enhance the impact and influence of those functions at a time when both are sorely needed, given the evolving risk landscape. By the same token, because CMD will affect key stakeholders' roles and responsibilities, leaders of the initiative must develop change management strategies and communication mechanisms to drive understanding, acceptance, and ownership of the revised assurance model.

² **The innovation imperative** – Forging Internal Audit's path to greater impact and influence, Deloitte's 2018 Global Chief Audit Executive research survey
<<https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/at-deloitte-global-chief-audit-executive-survey-2018.pdf>>

Take command now!

Digital technologies are revolutionizing assurance, compliance, and risk management, just as they are the business itself. They are freeing people from repetitive tasks while equipping them with powerful tools and insights. They are changing the roles and responsibilities of risk managers and internal auditors. They are enabling broader, deeper, more forward-looking views of risks and ways to not only address, but also to exploit them.

Leaders who see the opportunities and harness these technologies—and reallocate their talent accordingly—are generating results far greater to those of legacy compliance and assurance methods and delivering on the promise of intelligent assurance. In addition to efficiency gains, productive collaboration, and real-time insights, they are helping risk-related functions to keep pace with the larger organization's digitalization initiatives. They are also helping those functions to position the organization to better understand and address the risks of digitalization.

To explore the potential of CMD in your organization, contact your Deloitte professional today.

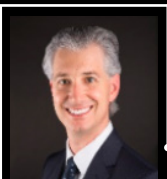
Contacts



Neil White
Deloitte & Touche LLP
nwhite@deloitte.com



Sandy Pundmann
Deloitte & Touche LLP
spundmann@deloitte.com



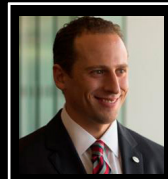
Stuart Rubin
Deloitte & Touche LLP
stuartrubin@deloitte.com



Adam Berman
Deloitte & Touche LLP
aberman@deloitte.com



David Tiernan
Deloitte LLP
datiernan@deloitte.co.uk



Geoffrey Kovesdy
Deloitte & Touche LLP
gkovesdy@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.