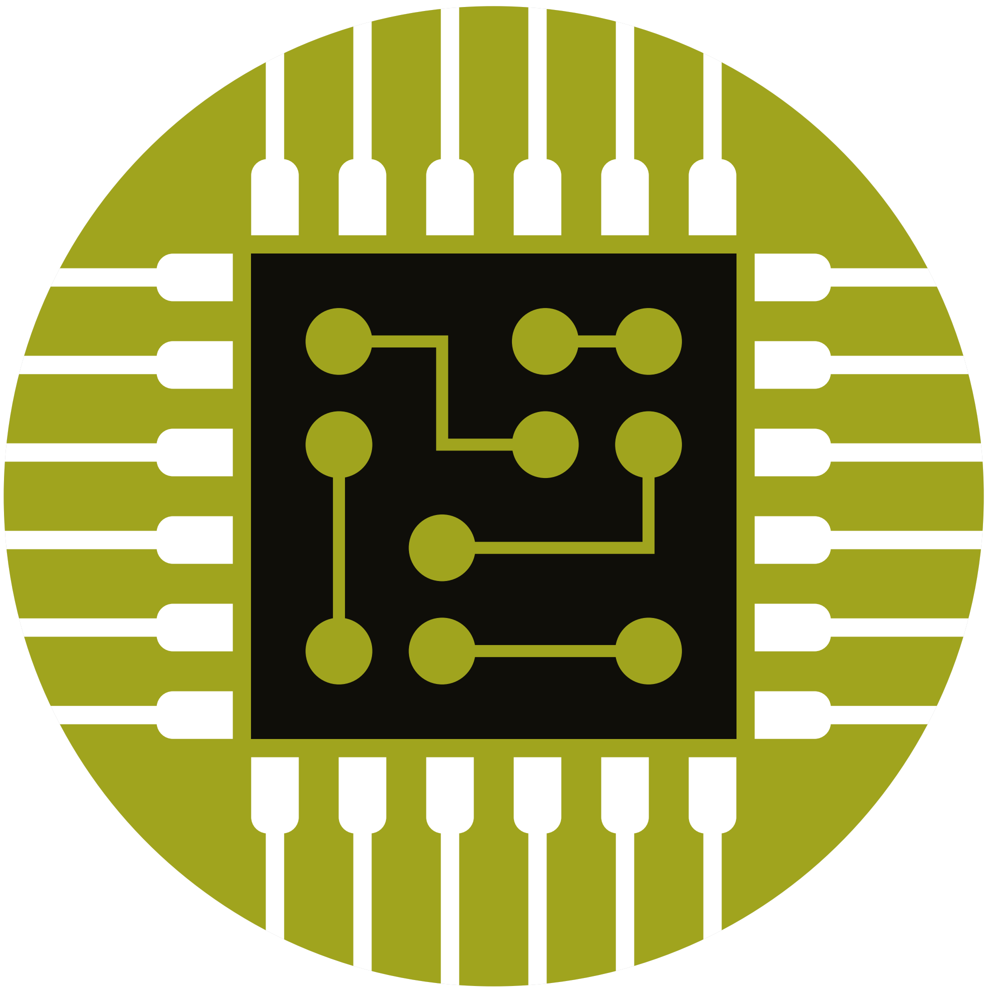
Deloitte.



Internal Audit Insights

High impact areas of focus

2016-2017

Contents

High impact areas of focus 2016-2017

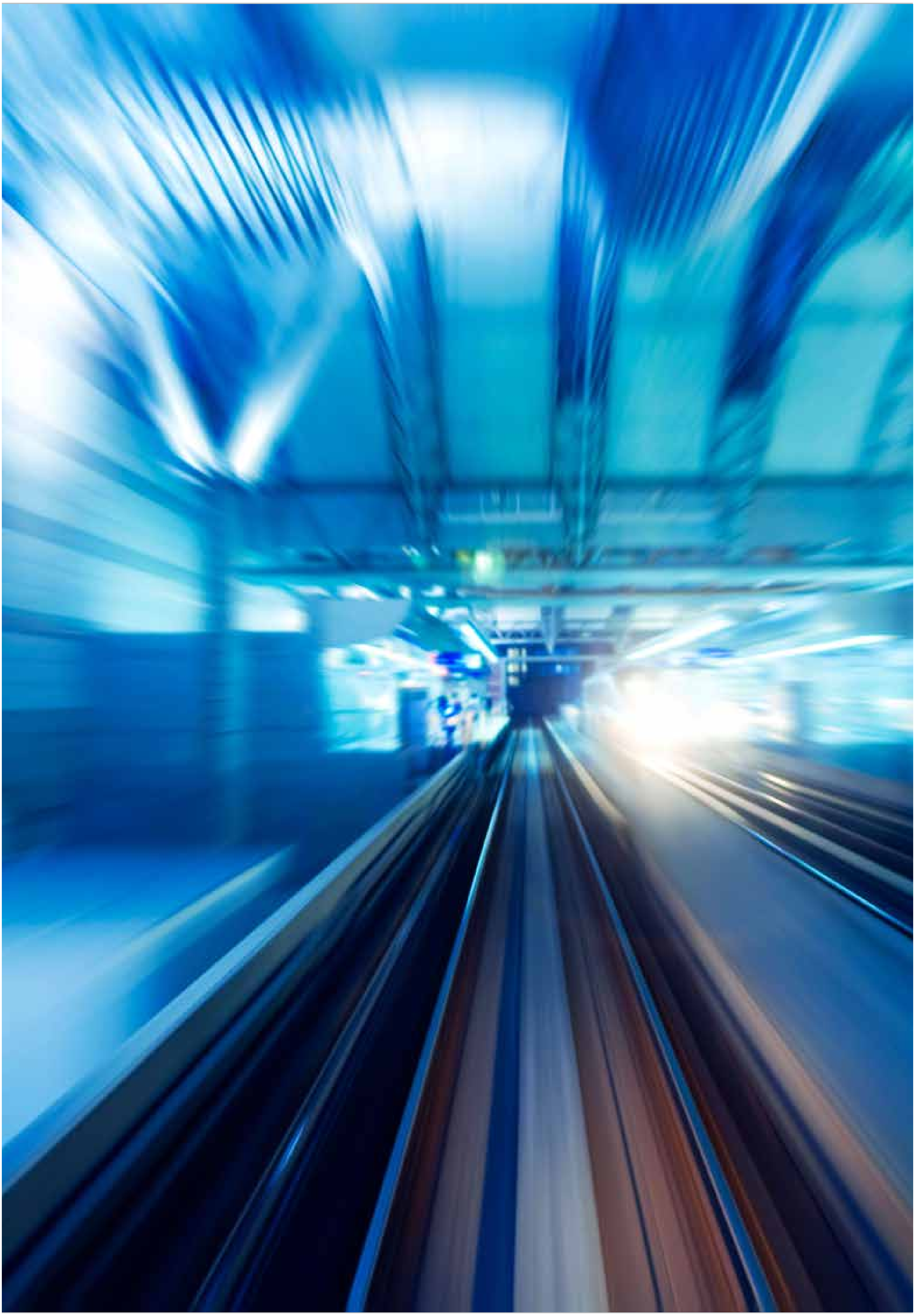
In many organizations a growing audience of stakeholders is expecting more from internal audit. They expect internal audit to align with business strategies, chart a course forward, and launch efforts that will fulfil existing and emerging needs.

Stakeholders want internal audit to assure, advice and to anticipate. They want assurance that controls are working properly, to advice on enhancements and operational issues, and to anticipate and provide insights on risks to the organization.

Boards and senior executive teams now want internal audit to go beyond "table-stakes" audits. Table-stakes audits allocate too many resources to low-impact areas and too few to high-impact areas of the business.

But, generally, low-impact areas involve well-established systems and controls, and well-known risks and issues. These areas must be addressed, but they should not divert resources from high-impact areas. Given the current risk environment, disruption across industries, and mounting pressures on organizations, this much is clear: Internal audit is headed for a leading role on a bigger stage in a brighter spotlight than ever before.

In this paper Deloitte has flagged 10 areas along with potential steps for you to consider in upcoming audit plans to ensure you are looking good in that spotlight.



Cyber security

Impact area

Too many IT audits are done on a point-specific basis – for security, data access, or the firewall – with the results presented as a "cyber security audit." While this approach does provide some assurance, it may not truly represent the organization's full exposure with respect to cyber security risk.

The definition of cyber security should be comprehensive and based on standards and frameworks, such as ISO, COSO and ITIL.

Cyber security should cover all digital assets and the processes and systems that produce, store, analyse, and transmit data. It also extends to email, social media, big data, and the Web.

And while being secure is more important than ever, internal audit should also assess their organization's ability to be constantly vigilant and resilient in the face of shifting cyber threats.

Steps to consider

If one hasn't already been done, internal audit should conduct a cyber risk assessment based on a robust framework that considers security, vigilance and resilience to develop a risk-based audit plan.

Internal audit should consider the threat profile (who might attack, why they might attack and what they might go after) when developing the plan.

Depending on the organization, high-risk areas might include data protection, vendor management, cyber incident management, and resiliency, among others. This is an iterative, multi-year endeavour calling for a programmatic, prioritized approach.

Cyber security audits demand ongoing improvement of internal audit talent and skills and close engagement with IT and security staff, business units, and risk management.

Internal audit analytics

Impact area

Audits based solely on sample-based testing will not satisfy stakeholder needs in areas such as emerging risks, strategic alignment, and performance improvement; hence, the need for analytics.

Fortunately, today's analytical tools do not demand deep technical expertise to facilitate analysis of entire populations of transactions. For example, analysing all orders, invoices, and payments in a unit will detect more irregularities, control breakdowns, and fraud than sampling hundreds of transactions, and enables auditors to drill down.

Analytics can apply risk indicators to large datasets to detect risks that would otherwise remain hidden. Yet internal audit groups lag in this area because they often underestimate the benefits and overestimate the complexity. Meanwhile, those that have adopted analytics have seen enhanced focus, efficiency, effectiveness, and value.

Steps to consider

If one hasn't already been done, internal audit should conduct a cyber risk assessment based on a robust framework that considers security, vigilance and resilience to develop a risk-based audit plan.

Internal audit should consider the threat profile (who might attack, why they might attack and what they might go after) when developing the plan.

Depending on the organization, high-risk areas might include data protection, vendor management, cyber incident management, and resiliency, among others. This is an iterative, multi-year endeavour calling for a programmatic, prioritized approach.

Cyber security audits demand ongoing improvement of internal audit talent and skills and close engagement with IT and security staff, business units, and risk management.


Analytics
Audience
Country
City
Status
Sex
Age
Interests
Collaboration
Behavior
Technology
Mobile
Custom 1
Custom 2
Custom 3
Income
Daily Unique Sales by Country
Home
Dashboard
Repoting
Customization
Help
Daily Product Sales by Country

Crisis management planning

Impact area

Globalization and the virtualization of business mean that any crisis can have widespread impact, while social media ratchets reputational risks to new heights.

Still, when many internal auditors think “crisis preparedness,” they think business continuity, emergency response, and disaster recovery.

Today, crisis management planning must integrate those elements across silos into a broad response plan. That plan must also incorporate internal and external communications and, when necessary, global coordination to keep management in front of any crisis.

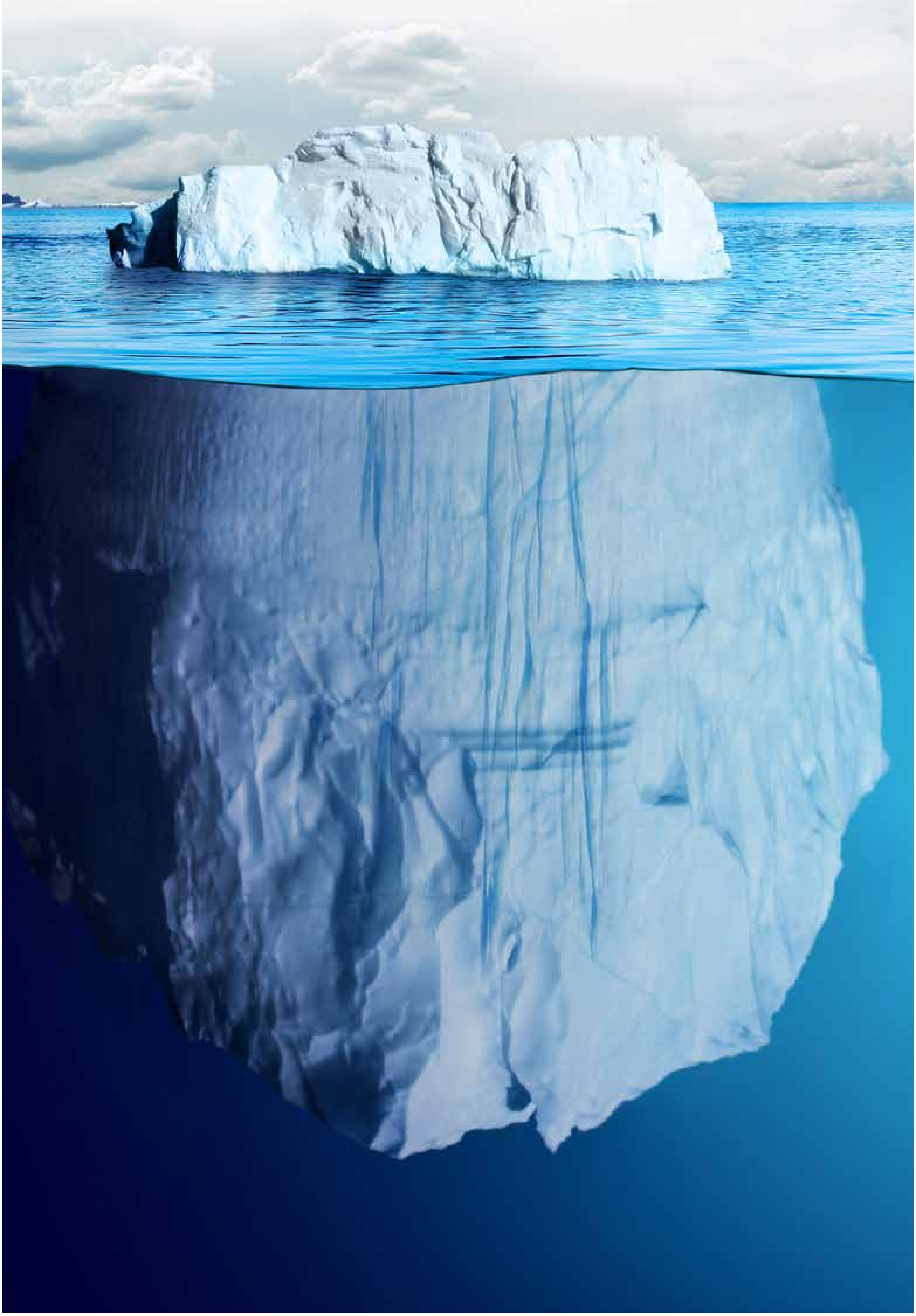
Steps to consider

Audit planning can ascertain whether management has identified the full range of potential crises and their likely impacts.

Impacts of a crisis—natural or manmade, physical or virtual, and local or remote—may compromise operations, employees, supply chains, plant and equipment, and IT and data.

Audit plans should ensure that management has developed integrated plans based on sound assessment of all impacts.

Each audit cycle can then focus on two or three areas and assess the depth, responsiveness, and integration of plans. In organizations with less mature approaches to crisis management, audit’s role may focus more on advisory than assurance, given the need for basic guidance.



Vendor governance

Impact area

While third-party relationships provide many benefits, they also present risks, and management cannot outsource accountability for risk. Meanwhile, management of third-party risk is often spread across various units and functions, obscuring the view of the contract structure and generating a reactive and reparative, rather than proactive and preventive, approach to compliance.

A more complete picture can be developed by reviewing contracts and KPIs of vendors with the aim of realizing the full value of third-party relationships.

Most contracts have right-to-audit clauses but they vary, and those doing the "audit" may lack the skills required to assess specialized business models and complex contract provisions. While vendors may provide specific controls and service reports, they tend to be generic and can fall short of contract requirements.

Steps to consider

The sooner internal audit is involved, the better. For example, internal audit can validate a relationship's workings after a single quarter rather than wait for an annual review. Clarity at the front-end smooths the relationship on both sides, with many vendors appreciating early notice of errors and contract interpretation issues rather than lengthy back-end recovery proceedings.

Data analytics can facilitate review of all transactions to identify anomalies requiring investigation. A hands-on approach to a few critical relationships can prove the worth of internal audit involvement.

In general, organizations miss many opportunities by tolerating less than full transparency in this area. Finding these opportunities is the right of all parties to a contract, and an area where internal audit can add measurable value.

Corporate governance

Impact area

Internal audit can assist organizations in enhancing corporate governance effectiveness.

Three guiding principles for corporate governance internal audits are proportionality, objectivity, and specificity.

Proportionality prompts internal auditors to consider the size, scope, and complexity of the organization as well as its maturity, industry, and regulatory environment.

Objectivity guides internal auditors to consider using external frameworks, such as Deloitte's Corporate Governance Framework, and to consult regulatory guidelines.

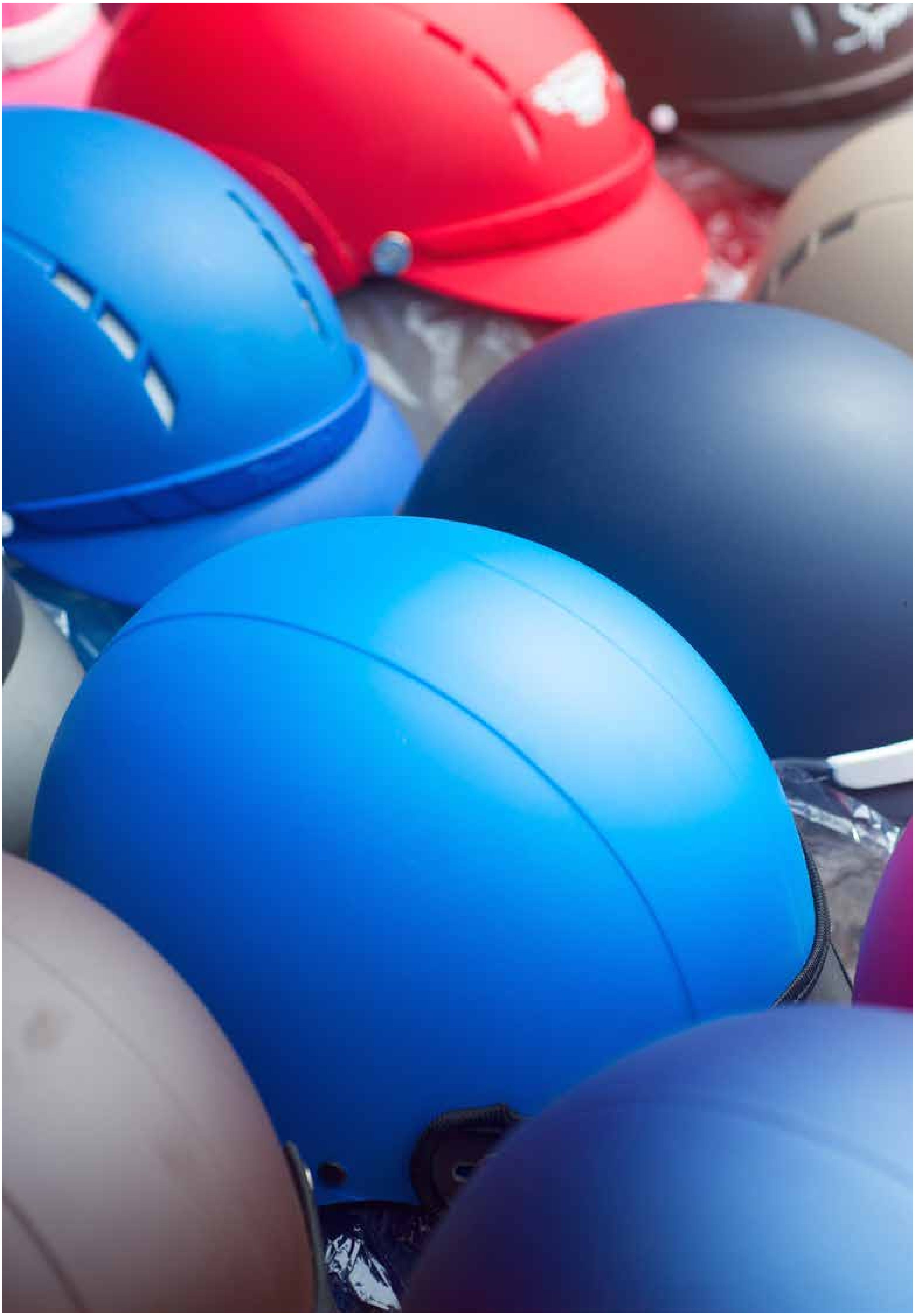
Specificity prompts internal auditors to focus on mechanisms and behaviour.

Steps to consider

Internal audit should review the organization's corporate governance framework and mechanisms, and plan internal audits accordingly.

The audit function can also assess board and senior management practices against leading industry practices and review the board's and management's self-assessment against those practices.

General areas to assess would include governance, strategy, operations, planning, performance, integrity, talent, risk, culture, compliance, and reporting. In examining these areas, internal audit can assure stakeholders of the maturity and effectiveness of board and senior management governance practices and advise the board and management of ways to enhance their governance.



Dynamic internal audit planning

Impact area

Dynamic internal audit planning uses qualitative and quantitative methods on a frequent or continuous basis to identify issues and allocate resources to key risks—a leap forward from static or rotational audit plans.

Risks and opportunities arise quickly and must be addressed. Therefore, dynamic planning creates a flexible, adaptable approach in which data analytics and continuous monitoring (via automated data gathering) supplement annual risk-based assessments.

Dynamic internal audit planning can enable the function in its mission to assure, advice, and anticipate. It thus enables internal audit to be highly efficient; it also enables internal auditors to advise management on risks and to provide recommendations and mitigation steps; and it enables audit to anticipate emerging risks and opportunities.

Steps to consider

Recognize that dynamic audit planning requires auditors who are as knowledgeable about strategic, business, operational, and risk issues as they are about financial processes, systems, and controls.

It also requires the flexibility to plan dynamically, to be comfortable with changes to plans, and to respond quickly to new demands. For example, internal audit can assist in an upcoming acquisition by identifying risks and barriers to realizing value, such as issues around addressing regulations and integrating systems and controls.

In addition, artificial intelligence and risk sensing technologies can facilitate dynamic internal auditing.

Data governance and life cycle management

Impact area

Most organizations need some form of data governance. Specifics depend on the organization and its industry, but data governance involves policies and procedures regarding who owns data, who uses it for what purpose, and whether it is reliable and accurate.

Other issues include how data is handled and safeguards to prevent loss or theft and to ensure proper disposal.

Risks typically arise around privacy, regulatory, and reputational issues, with the potential for loss or theft of customer data a common concern.

Internal audit should calibrate its efforts to the organization's need for data governance. For example, financial services, life sciences, consumer goods, and business-to-business companies all use data differently, and need different approaches to data governance.

Steps to consider

Focus first on the most valuable data and higher risk data. Review policies and procedures across the data life cycle, which would include those for gathering, storing, using, and disposing of data and for controlling access and ensuring accuracy and how those policies and procedures are implemented.

Provide advice and insight to units with non-existent or rudimentary policies and procedures.

Avoid judging data quality, but instead focus on the processes and controls needed to produce and protect data of the desired or required quality.

IT internal audit

Impact area

IT issues now include social media, big data, devices, and apps, as well as technology-driven disruption of entire industries. Yet IT internal audit plans often resemble those of five to ten years ago, leading to IT audits that stakeholders often ignore.

While audits on disaster recovery and resiliency must get done, resource constraints should not be allowed to result in IT audits that fail to address key existing and emerging technology risks.

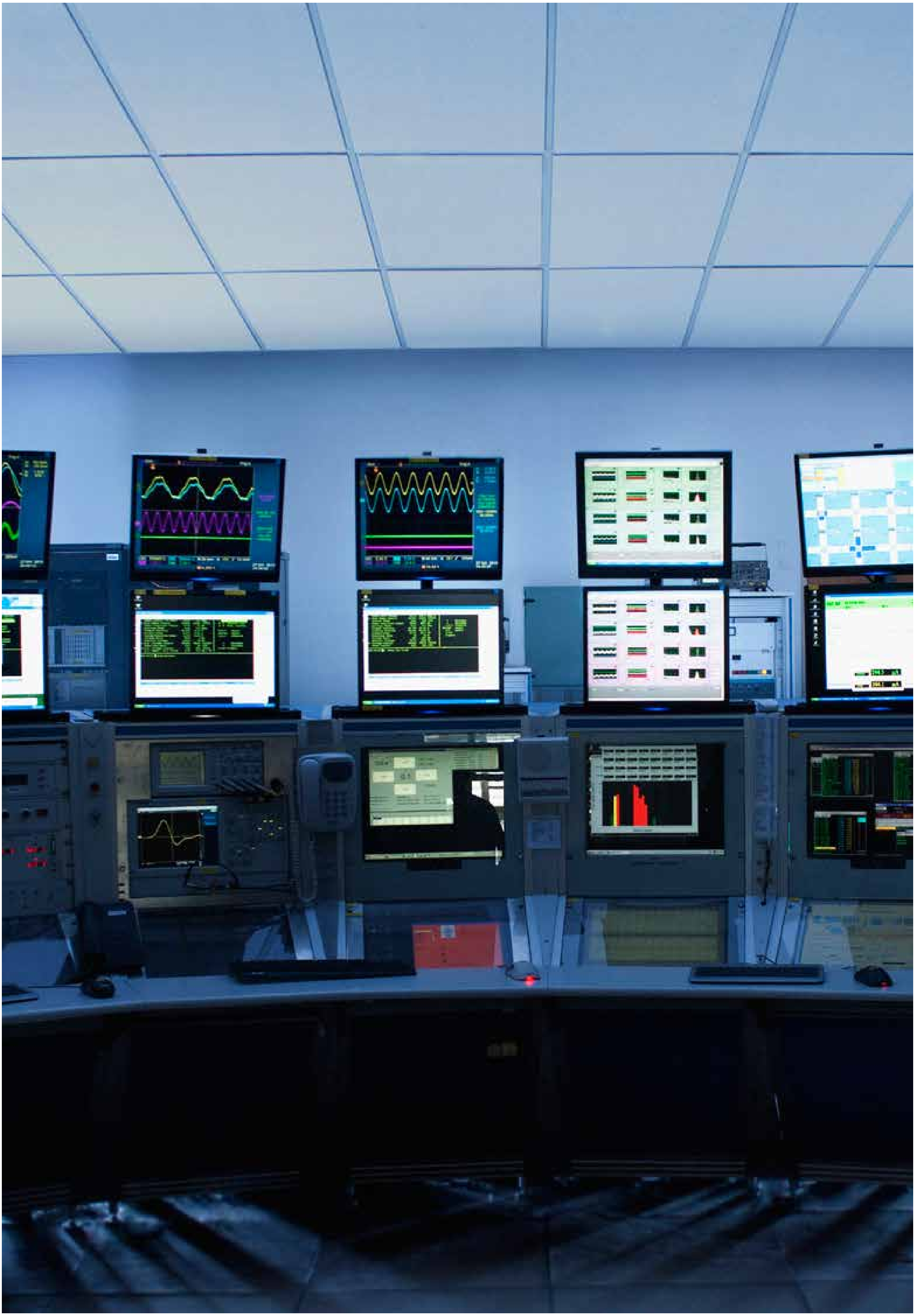
If audit reports generate low value, under-resourcing will persist. Mapping audits against a risk and value chart can show where audit resources are going; too often, 70% to 80% are going to low-risk/low-value areas.

Steps to consider

Given the pace of technology development and the value of digital assets, audit needs a balanced approach.

Consider grouping IT audit activities into core, advanced, and emerging technology categories. Core activities related to technology have been around for years, with SOX compliance audits being a good example.

Advanced technologies have been around, but haven't been a historical focus for IT internal audits. Emerging issues involve new, potentially disruptive technologies. The IT internal audit plan should be balanced across all three categories.



Data visualization

Impact area

Data visualization transforms analytical output into visual formats, such as bubble charts, heat maps, and interactive graphs, enabling non-analysts to interpret results.

The complexity and prices of these tools, which range from chart libraries to customized dashboards, have dropped sharply.

In scoping an audit, data visualization can pinpoint areas of risk, activity, or concern and assist in resource allocation.

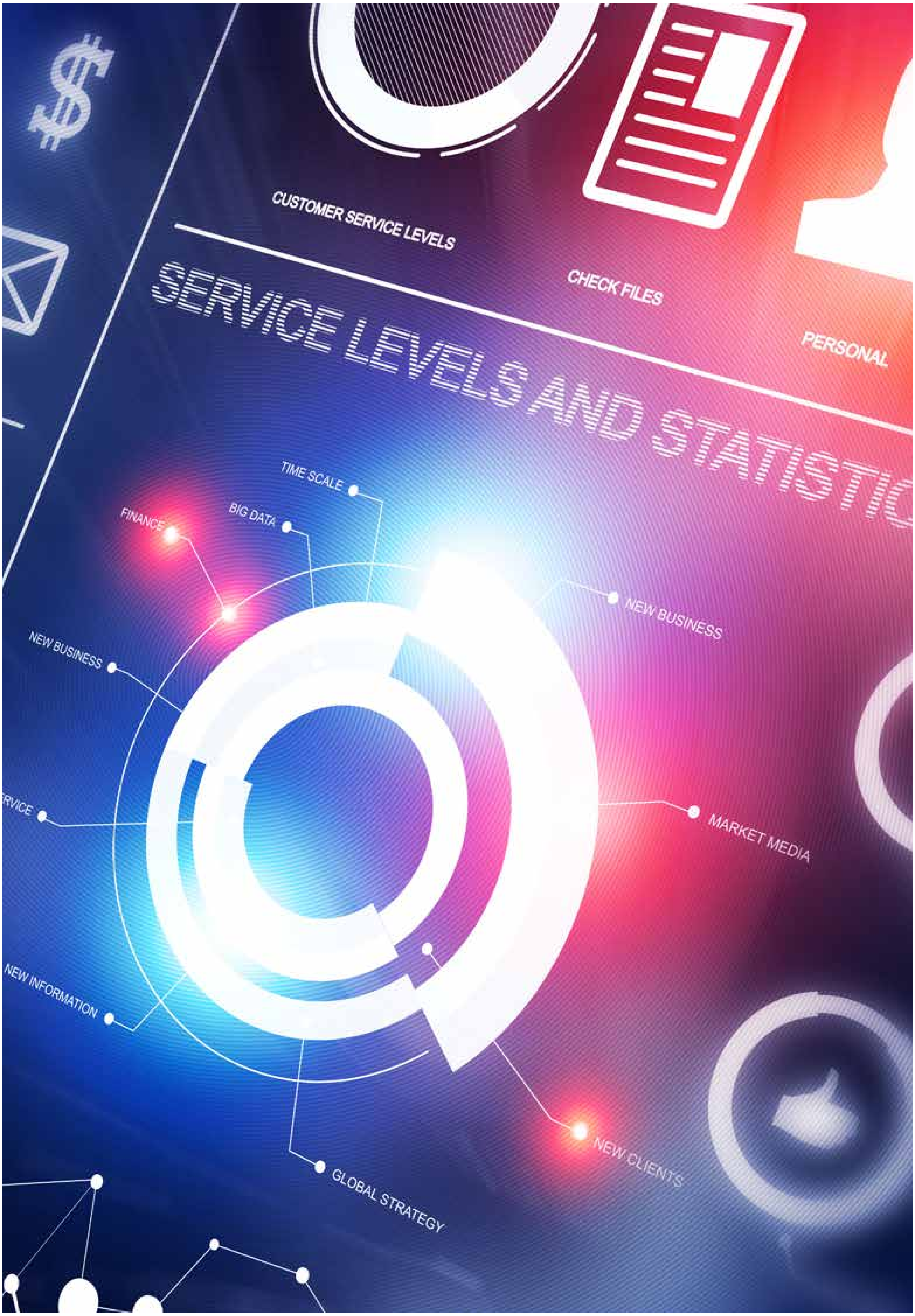
During an audit, visualization can depict trends, patterns, and anomalies that might otherwise be missed, and enable drill down to relevant transactions. In reporting, visualization can better meet stakeholder needs because most people can readily grasp data in visual form.

Steps to consider

Train one or more staff members with the interest and aptitude to use visualization tools.

A desktop license for a good package is relatively inexpensive, and it takes minimal technical expertise to load data into the application.

Then try using data visualization in scoping, execution, and reporting on selected areas of the audit. Data visualization is also meaningful in reports to the Board and Audit Committee.


CUSTOMER SERVICE LEVELS
CHECK FILES
PERSONAL
SERVICE LEVELS AND STATISTIC
TIME SCALE
BIG DATA
FINANCE
NEW BUSINESS
NEW BUSINESS
MARKET MEDIA
NEW INFORMATION
NEW CLIENTS
GLOBAL STRATEGY

Key performance indicators assurance

Impact area

Management uses nonfinancial KPIs to manage customer relationships, product quality, sustainability, and risk, among other things.

Yet processes, systems, and controls for KPIs remain far less developed than those for financial data.

That said, auditing skills and methods are highly applicable to KPIs. Viewing KPIs through an auditing lens can assist in improving related processes, systems, and controls.

KPI assurance is a high-impact area because management teams regularly issue reports and public statements that may be – or may not be – substantiated by KPIs. For example, statements about customer service and product quality, call for accurate, and reliable KPIs. Internal audit is well-positioned to provide assurance.

Steps to consider

Identify where greater attention to KPIs might yield benefits. Consider those invoked in commitments to the marketplace, such as measures of service availability or on-time delivery.

Then apply auditing expertise to the underlying processes and systems. Internal audit can first ascertain whether management is tracking the right KPIs for what is being measured and whether the underlying processes are well-designed and controlled, and then, over time, provide assurance on the data and processes.

Contacts

To discuss any of the topics and approaches in this paper, please get in touch with one of the Deloitte personnel below:

Rob de Leeuw
Partner Risk Advisory
T: +31 88 2882352
M: +31 6 52048367
E: rdeleeuw@deloitte.nl

Olaf Helmond
Director Risk Advisory
T: +31 88 2881734
M: +31 6 55853356
E: ohelmond@deloitte.nl