Testing and Monitoring Industry Survey 2025

September 16, 2025 (Presented to the Participants 10.28.25)

Background and Introduction

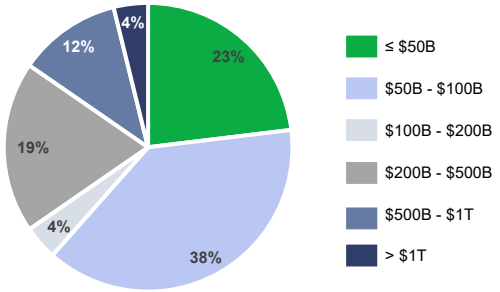
Background, Scope and Key Themes

- Many institutions have been recently focusing on building sustainable testing programs that provide greater risk coverage, satisfy regulatory requirements, drive business value, all at a reduced cost
- This year's Testing and Monitoring (T&M) Survey primarily focused on three areas:
    1. Overall Control Environment Maturity
    2. T&M Activities and Operating Model
    3. T&M Data and Technology
- Multiple themes emerged from the survey results, most notably:
    1. Evolving Controls Environments
    2. Opportunities for further Testing Centralization
    3. Room to improve 1st Line of Defense (1LOD) and 2nd Line of Defense (2LOD) interaction including redundancies and testing gaps
    4. Adoption of Automation and Gen AI remains relatively low

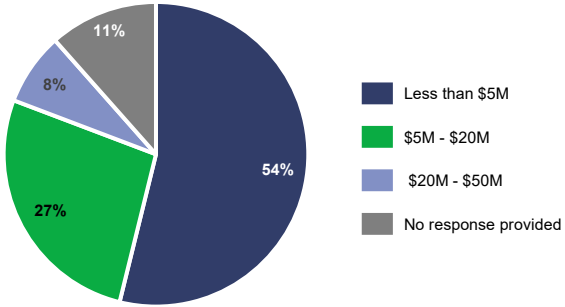
Respondent Demographics

Refer to the visuals below highlighting our respondents (26 total) financial institution size, average testing and monitoring (T&M) costs and correlation between these areas

Financial Institution Asset Size

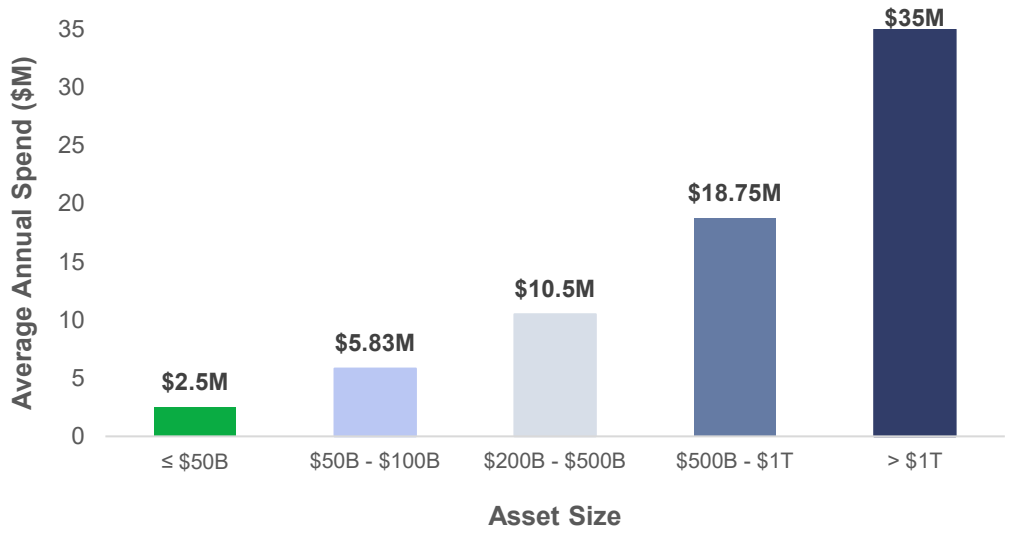


Average Annual T&M Costs*



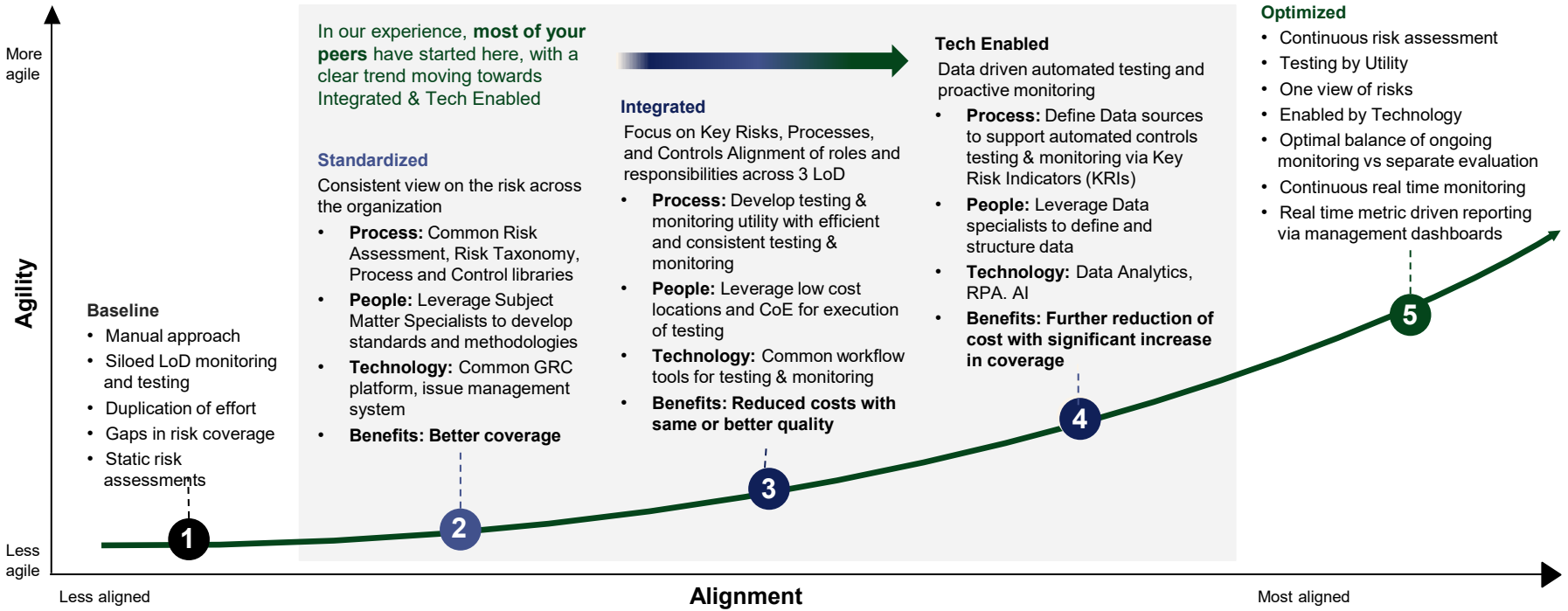
*Costs include all T&M related activities, include costs associated with resourcing and investments within tooling

Average T&M Spending Based on Financial Institution Asset Size



Note: No data available for Financial Institutions of $100B - $200B Asset Size

Controls Monitoring & Testing Transformation is a Journey



In Your Own Words …

How do you best describe your Testing and Monitoring programs including its overall maturity?

- *“While I feel like our control methodology is fairly mature and has certainly evolved substantially in the past five years, we have some opportunities to improve. Most notably,* ***increasing the percentage of controls that are automated and leveraging GenAI to facilitate testing****, especially of script-based controls."*

- *“We are undertaking an overhaul of our 3 lines of defense, and* ***1LOD does NOT have a testing protocol currently****..."*

- *“While the 1LOD testing program is mature, there continues to be opportunities for* ***automation and efficiency*** *as our process is very manual. Furthermore, we've tested the same scope for years so there is a feeling by our BU leaders to test differently or reduce the scope if we continue with our current approach.* ***There are likely opportunities to reduce testing if we enhance monitoring in 1LOD.****”*

- *"At present,* ***the majority of control validation is performed by the Second Line of Defense (2LOD)****…" and "By standing up a dedicated testing framework, we aim to strengthen the 1LOD’s ownership of control performance and introduce more robust, ongoing validation mechanisms."*

Section I: Control Environment Maturity

Summary of Responses: Control Environment Maturity

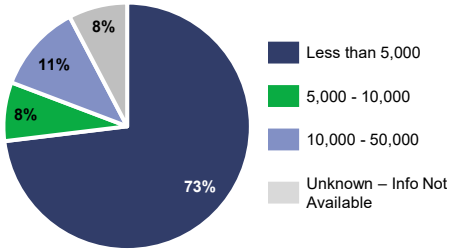
Purpose of Survey Questions: To understand the design and landscape of supporting control environments, including total volume, level of automation and standardization of controls. The maturity of the greater control environment is critical to the success of testing and monitoring initiatives promoting greater efficiency and sustainability of these programs

Main Takeaways

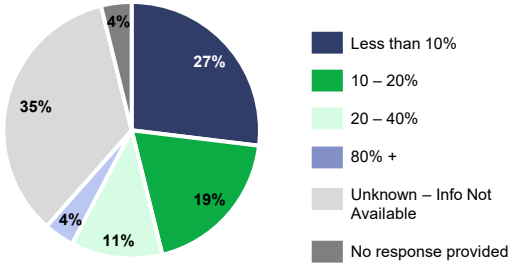
- **Controls identification likely still a work in progress** for most institutions, 73% reporting less than 5,000 controls including larger financial institutions
- **Internal Control structures continue to mature**: 69% of institutions reported that they have less than 20% automated controls and 46% of institutions reported less than 20% standardized/common controls
- **Limited transparency of key control environment indicators** (i.e., "Unknown/Information is Not Readily Available") including:
  - Common Controls (35%)
  - Automated Controls (27%)
  - Controls Associated with Issues (35%)

Key Results

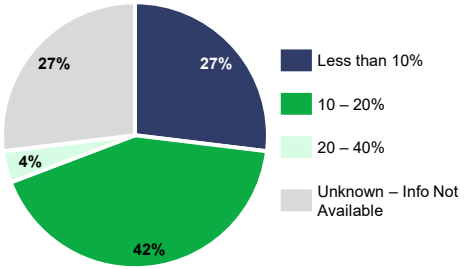
How many total controls are currently in your control library? *(Q.9)*



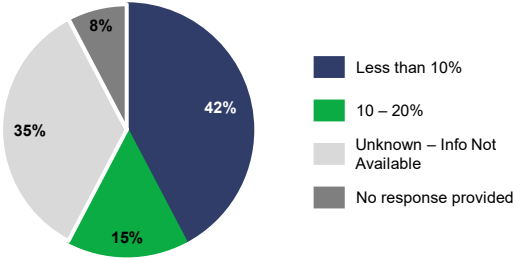
Within your control library, what percentage of your controls can be classified as "common" controls, including those deemed as "shared" or "enterprise-wide"? *(Q.10)*



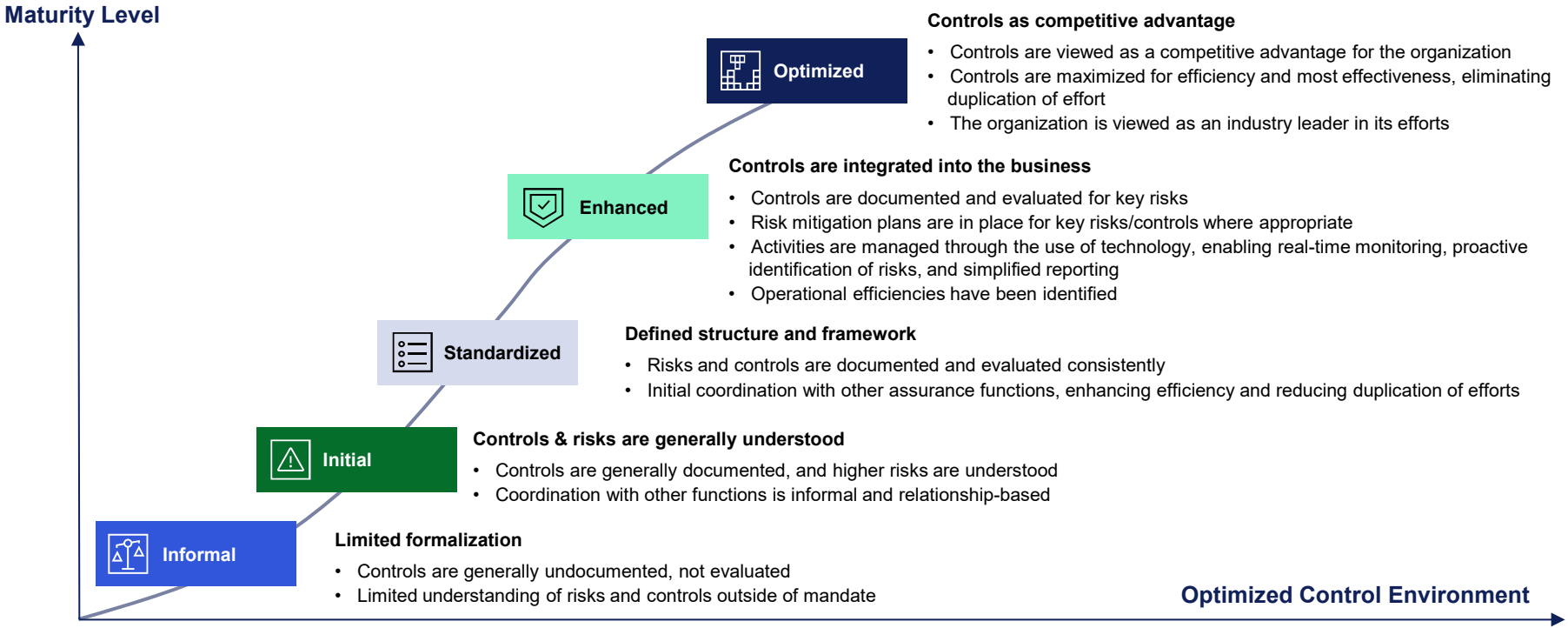
Approximately what percentage of your controls are automated? *(Q.11)*



Approximately what percentage of your controls are associated with self-identified issues, issues raised by 1LOD or 2LOD, audit issues, and/or regulatory findings? *(Q.13)*



Control Environment Maturity Model



Section II: Testing & Monitoring Activities and Operating Model

Summary of Responses: T&M Activities and Operating Model

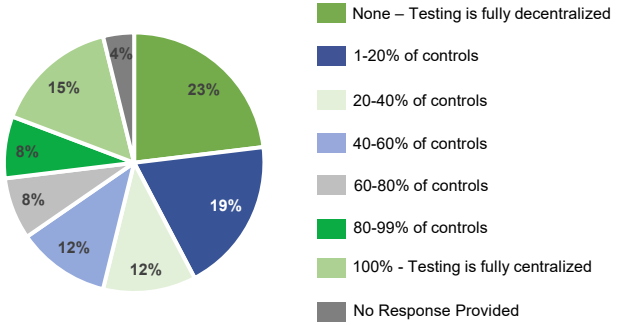
Purpose of Survey Questions: To assess how institutions design, structure, and execute their testing and monitoring activities, with a focus on centralization, the interaction between the first and second lines of defense, and standardizing key activities. Maturity in these areas is critical to improving consistency, reducing cost, and strengthening the overall effectiveness of testing and monitoring programs

Main Takeaways

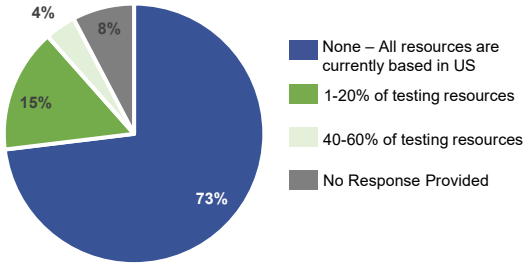
- While **most institutions have a centralized testing unit** (73%), the extent of centralization differs considerably
- Overwhelming **majority of respondents do not utilize offshore support teams** (73%)
- Majority of institutions have some level of **monitoring in place (85%)**, however, 54% of those respondents did not utilize metric-driven indicators
- Half of the respondents reported either **minimal interaction between 1LOD and 2LOD or notable gaps/duplication of testing** (50%)

Key Results

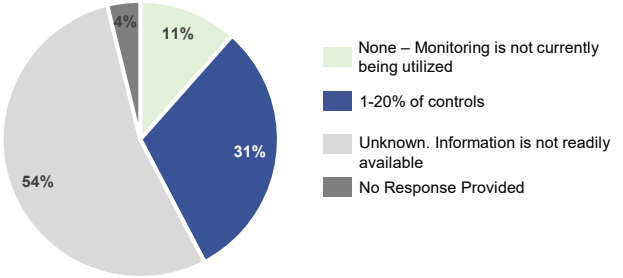
Approximately what percentage of controls are currently being tested within a centralized unit? *(Q. 31)*



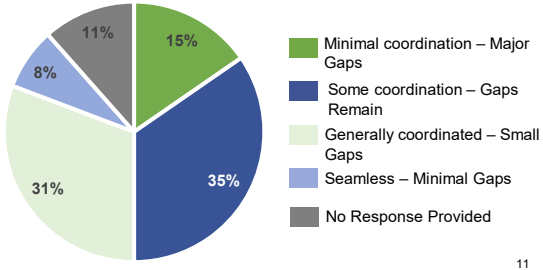
Approximately what percentage of testing resources are offshore? *(Q. 36)*



What percentage of controls are monitored through the usage of key risk indicators, key performance indicators and key control indicators? *(Q. 21)*



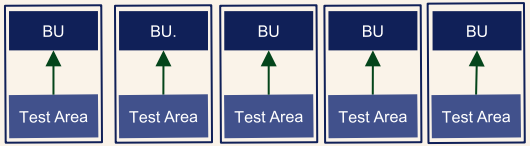
How would you best describe the coordination and efficiency between the lines of defense? *(Q. 42)*



Operating Model Options for Testing

Below are three common types of operating models for testing organizations. Most institutions initially target a **Hub & Spoke Model (Hybrid)** and continue to centralize where possible.

FEDERATED MODEL



A decentralized approach where business units deploy their own testing standards, frameworks and tools, and execute testing specific to their business area(s).

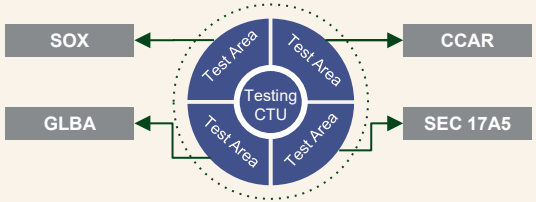
Pros:

- Increased accountability and ownership of business unit testing activities

Cons:

- Potential for business to act in silos resulting in difficulty managing testing across segments/risk types, and limited ability to identify challenges or best practices across BUs
- Less opportunity for optimization and alternative delivery models

HUB & SPOKE MODEL (Hybrid)

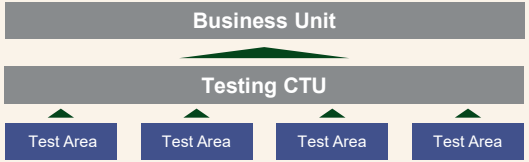


A joint service approach where standards, frameworks, tools and technology are owned centrally and leveraged by all testing groups. Testing is executed using a hybrid model, where some is executed centrally and some is executed by the business units.

- Clear accountability and ownership of business unit testing activities
- Leveraging the Center Testing Utility concept to promote efficiency, quality and workload sharing
- Allows for a hybrid model for executing testing activities

- Potential for decreased business unit ownership of testing depending on the amount of centralization

CENTRALIZED MODEL



A centralized approach where standards, frameworks, tools and technology are owned centrally, with a single testing function that performs testing across business segments, with no dedicated segment alignment.

- Clear accountability and ownership of testing at the enterprise level
- Creation of a “Central Testing Utility” thereby increasing quality, workload sharing, cost effectiveness, and standardization.

- Perceived lack of specialization for specific testing needs
- Perceived abdication of control over testing activities at the business unit level

First Line of Defense (1LOD) and Second Line of Defense (2LOD) Responsibilities

One of the primary critical success factors for 1LOD and 2LOD Testing Programs includes a clear understanding of the different roles and responsibilities embedded within each of these lines of defense

	Risk owners (1LOD)	**Risk programs** (2LOD)
Objective	Identification, ownership and assessment of risk and controls across the organization.	Oversight and monitoring of risk and control programs.
Roles and Responsibilities	• Assign procedural and operational responsibilities • Convert strategy into operating objectives • Understand and manage established risk limits (appetite, tolerance, etc.) • Day-to-day identification and evaluation of risks and controls related to objectives • Identify needed changes to control procedures and program frameworks • Control design and performance development and ownership • Control evidence to address requirements • Evaluate control failures • Design and implement corrective actions to address process and control deficiencies	• Provide and maintain policies, standards, tools, methodologies and programs • Clear understanding of strategy, business architecture and risk profile of the business • Establish/implement risk limits (appetite, etc.) • Establish and maintain program and frameworks based upon changes and developments in the business • Collaboration with other risk programs and lines of defense to maintain collective oversight of key risk areas • Educate management on risk and control concepts, requirements and responsibilities • Risk and control monitoring and testing (i.e. effective review and challenge) • Aggregation and a portfolio view of risks
Common Pitfalls (from a Testing Perspective)	• Lack of an enterprise-wide testing program and approach across compliance and operational risk areas • Absence of granular methodologies, procedures and tools that provide the ability to execute controls testing in a high quality and consistent manner • Lack of clear reporting and communication process of assessment results to 1LOD governance and other lines of defense • Issues management challenges specifically as it pertains to ownership, mitigation plan development, monitoring/tracking, and remediation testing	• Lack of understanding and coordination with 1LOD as it pertains to risk and control assessment coverage • An ineffective or ill-defined “effective 1LOD review and challenge” process that fails to detail what is reviewed (i.e. what, how it is reviewed (e.g. level of reperformance required), and how identified testing gaps are remediated • Supplemental testing being performed directly by 2LOD without additional oversight

Section III: Testing & Monitoring Data and Technology

Summary of Responses: T&M Data and Technology

Purpose of Survey Questions: To evaluate how institutions are leveraging automation, GenAI, and reporting tools to support testing and monitoring activities. Broader adoption of these capabilities signals stronger programs that can deliver higher quality results through more efficient and standardized T&M activities.

Main Takeaways

Opportunity for Further Automation Adoption:

- **Over 73% of respondents report no automation usage** across testing and monitoring lifecycle

Gen AI is still experimental for most institutions:

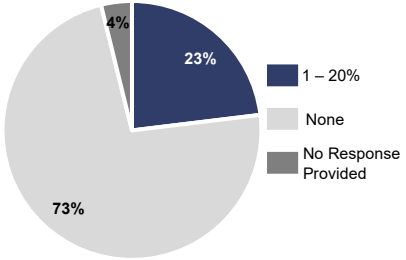
- **Only 8% of respondents reported any use of Gen AI** in testing activities
- Most common activities include sample selection, test script generation, and narrative drafting

Reporting still relies on traditional approaches and datapoints:

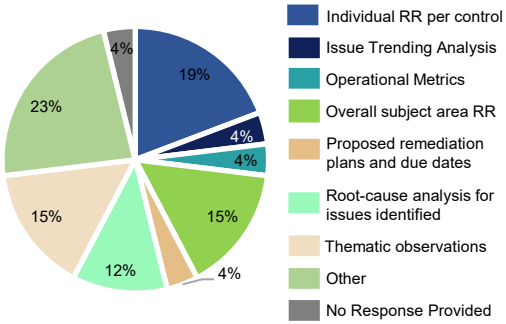
- **17% of respondents reported using data visualization tools** and around **35% continue to rely upon manual reporting methods** for both testing and monitoring.
- **Most common reporting elements are those that are foundational** (e.g., individual risk ratings), but more advanced components like operational metrics (4%), trend analysis (4%) and thematic observations (4%) are less pertinent

Key Results

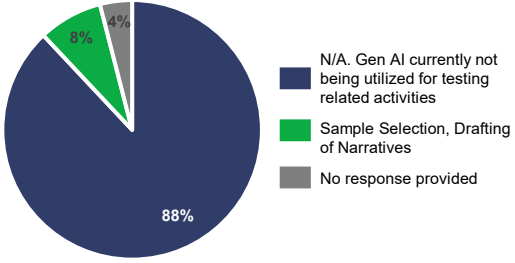
What percentage of controls are currently being tested utilizing automation, including Gen AI? (Q. 15)



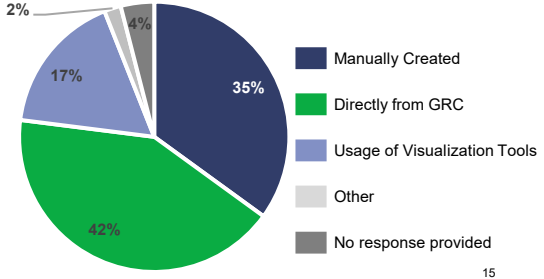
Specify the contents required within testing and monitoring reporting. (Q. 30)



Please select all options for how Gen AI is being utilized within testing related activities (Q. 18)



For testing and monitoring related activities, please specify how reporting is created. (Q. 26 & 27)



Identifying and operationalizing automation throughout the testing lifecycle is a critical success factor for efficient target state operating models

End-to-End Tech-Enablement

This end-to-end testing workflow — utilizing a suite of technology solutions and AI models — drives transformation across the control testing life cycle. Users can detect obligations (e.g., within regulation, policy, and contract); auto-generate risks, controls, and/or test scripts; execute low-cost, high-coverage testing; and analyze and report insightful results that inform decision-making.

Trigger

Technology can power effective risk management across the organization's risk profile and is especially powerful in facilitating change management (e.g., new/updated obligations, new product/process).

- Reg requirement/ Guidance
- Policy/ Procedure requirement
- Contractual obligation

Potential Automation and AI capabilities

Obligation identification & plain text summary

User can bring a single citation or group of citations into the text box to generate obligations, or start with an obligation (e.g., policy, contract), and generate summaries.

Risk statement

Control objective & description

Control design diagnostic

AI models reference the obligations and/or summaries to generate drafts of the related risk statements, control objectives, and control descriptions. User can use AI models to diagnose the design of existing control descriptions for essential components (5 Ws).

Outcomes-based test scripts

Control test scripts

Operational procedures

AI models generate test scripts directly from obligations, and/or from control descriptions.

Automated rules-based testing

Testing is conducted via customized, rules-based data analysis/query, or a licensed software-as-a-service (SaaS) solution.

Data analytics, visualization & reporting

Results of testing can be aggregated and analyzed utilizing GenAI and/or software solutions to summarize themes, identify emerging risks, and prioritize.

Time Savings (Efficiency)

80–90%	50–60%	50–90%	25–50%

Demonstrated efficiencies that may be realized through tech-enablement across the risk management program & life cycle.

Enabling technology: AI Model SaaS Existing software

Results Capture / Reporting: Tech-enabled metrics and defined KPIs will help you visualize testing outputs for strategic analysis and actioning

Access to pertinent KPIs can lead to quicker identification of process flaws, potential gaps, and overall areas for efficiencies. Examples of key operational KPIs:

1 Control population

KPIs can be filtered by queue, teams, individuals, and triggers:

- Open control volume (in SLA vs. out of SLA)
- Unassigned controls
- Controls assigned by tester
- Trend analysis to enable workforce planning

2 Execution

KPIs can be filtered by queue, teams, individuals, and triggers:

- QC scores
- Quality scores on productivity as well as QC'd controls by tester and team, to enable coaching and training
- Quality trends and complexity analysis

3 Productivity

KPIs can be filtered by queue, teams, individuals, and triggers:

- Completed controls
- Average testing time
- Average review time
- Overdue controls
- Escalated/de-escalated controls
- Escalation rate
- Daily, weekly, monthly trends (e.g., resolved, escalation, and de-escalated)

4 Exception reporting

Notification alert sent:

- Open control volume out of SLA
- No open controls — idle time
- QC results below threshold
- Average testing time below average
- Resource performance outliers
- Issue reoccurrence
- Commonality of root-causes

Comprehensive metrics

Automate metrics reporting and analysis for real time production KPIs and month-over-month trend analysis to quickly discover and remediate observations and monitor adherence to SLAs.

Reporting, ad-hoc analysis, and end-to-end views

Automated daily reporting on alert progress and completion through dashboarding and live connections to the production environment.

Benchmarking and trends analysis

End-to-end review of in scope policies, procedures and metrics. Team leads will recommend industry-wide best practices.

Thank you

Contact Information of PwC Presenters:

- Joe Oporto - joseph.oporto@pwc.com
- Igor Maryams - igor.maryams@pwc.com
- Phillip Gluck – phillip.j.gluck@pwc.com