

June 18, 2024

**TO:** Each Trustee,  
Audit Committee

**SUBJECT:** Audit Committee Meeting on June 20, 2024 – Agenda item VIII

---

Following you will find supplemental information regarding the below-mentioned item.

**Item VIII. Audit Consultant Comments**

(Memo dated June 17, 2024)



June 17, 2024

Member of the LACERA Audit Committee

RE: June 2024 Agenda

While all audit committee meetings are important, this meeting on June 20, 2024, will be a milestone in the evolving role of the audit committee at LACERA. The audit committee plays an important role in assisting LACERA boards in fulfilling their fiduciary oversight duties, which remain the same. However, the role of oversight continues to evolve from traditional financial reporting, controls and audit activities to also include ethics, compliance, and risk management. To recognize the evolving role of the audit committee, staff propose changing the name of the committee to the Audit, Compliance, Risk, Ethics (ACRE) Committee and updating the committee charter.

Alignment of the ACRE Committee Charter to the new *Global Internal Audit Standards* is necessary to ensure effective oversight, organizational independence, and to conduct internal audit activities in conformance with the Standards. The Institute of Internal Auditors (IIA) released the new IIA Standards on January 9, 2024, with an effective date of January 25, 2025. The IIA encourages early adoption of the Standards and continues to release resources to assist internal audit functions to adopt and implement the new Standards. For instance, the IIA released a Model Internal Audit Charter Tool and User's Guide. The new ACRE Committee Charter is consistent with the IIA Standards. (Item VI, A – ACRE Committee Charter)

The *Global Internal Audit Standards* require the use of an internal audit charter. The IIA also issued a Model Internal Audit Charter for Public Sector Use. The new audit charter redefines the purpose of the internal audit function, commits to conformance with the Standards, establishes the mandate and authority, outlines organizational position and reporting relationships to establish independence of the internal audit function. The charter also describes the roles and responsibilities of the chief audit executive including managing the internal audit function, communications, quality assurance and improvement, along with the scope and types of internal audit services. The proposed internal audit charter is consistent with the IIA model charter and best practices. (Item VI, B – Updated Internal Audit Charter)

The compliance charter delineates the purpose, scope, and responsibilities of LACERA's compliance function. The charter outlines the roles and authority of the chief ethics and compliance officer, specifying their independence to avoid conflicts of interest and ensure unbiased oversight. It also details functions for monitoring compliance activities, managing compliance risks, and reporting to senior leaders, the ACRE committee, and boards. The proposed Ethics and Compliance Program Charter is consistent with best practices for an effective compliance program. (Item VI, C – Ethics and Compliance Program Charter)

Over the past few months, I have reviewed the ACRE Charter, Internal Audit Charter, and the Ethics and Compliance Charter, and met with staff to discuss my comments and edits to these documents. Additionally, I received 12 hours of continuing professional education to learn about the new IIA Standards.



There may be interest in a compliance program survey conducted by Funston Advisory Services (FAS). I participated on the survey team as a Compliance Leader for FAS. This benchmarking survey shows the prevailing practices among twenty-seven large pension systems implementing ethics and compliance programs. While most of the systems are making good progress, there were some common themes for continuous improvement and lessons learned that may benefit LACERA. The National Association of State Retirement Administrators published the survey. Here is a link to it, if you're interested. [Integrated Enterprise Compliance Survey Results.](#)

As I reviewed the material for the June 2024 meeting, there are a few suggested questions the audit committee may consider asking to exercise oversight responsibilities:

Agenda Item	Question	Expected Response(s)
Item VI, A – ACRE Committee Charter	1. How do the new IIA Standards enhance the audit committee's ability to exercise its oversight responsibilities?	<ul style="list-style-type: none"><li>• Additional reporting requirements to the committee</li><li>• Greater emphasis on collaboration among CAE, Audit committee, senior management</li><li>• Introduction of "essential conditions"</li></ul>
	2. The ACRE charter includes oversight of Enterprise Risk Management. Will Enterprise Risk Management program have a charter like the internal audit program and the ethics and compliance program?	<ul style="list-style-type: none"><li>• Best practices suggest an Enterprise Risk Management should have a separate charter and a risk policy for the ACRE to review and approve.</li></ul>
Item VI, B – Updated Internal Audit Charter	3. With the release of the new IIA Standards, what is the internal audit doing to prepare to implement the new Standards?	<ul style="list-style-type: none"><li>• Training, gap analysis of old to new Standards, updating charters, developing plans for strategic planning, building relationships and internal audit performance measures, reviewing guidance from the IIA, preparing a Conformance Readiness Assessment</li></ul>
	4. Do the new IIA Standards change the independence or scope of services performed by internal audit?	<ul style="list-style-type: none"><li>• No change on the importance of organizational independence</li><li>• Scope of services essentially remain the same except the new IIA Standards do not use the term "consulting services". Internal audit provides assurance, advisory, and other value added (non-audit) services.</li></ul>



Item VI, C – Ethics and Compliance Program Charter	5. The charter is very comprehensive and includes several program activities. When do you anticipate hiring the Chief Ethics and Compliance Officer?	<ul style="list-style-type: none"><li>• ASAP?</li></ul>
	6. When will the ACRE committee review an annual workplan for implementing the compliance program?	<ul style="list-style-type: none"><li>• After hiring the Chief Ethics and Compliance Officer.</li><li>• Annual plan in March or June of 2025?</li></ul>
Item VI, D – Approval Fiscal Year 2024-25 Internal Audit Plan	7. Will the independence of internal audits be compromised by developing the ERM charter, framework, or structure of the program?	<ul style="list-style-type: none"><li>• Not if appropriate safeguards are implemented, such as not assuming the role of management, developing risk mitigation strategies, or approving policies.</li><li>• An ERM program assessment within 12 months of internal audit involvement must be performed by an external assessor.</li></ul>
	8. Does the audit plan assume filling the three currently vacant positions? If so, what projects in the plan would be deferred or not completed if the positions were not filled timely?	<ul style="list-style-type: none"><li>• Yes, IA is in the process of hiring</li><li>• IA may defer certain projects, or a service provider may perform the audit project.</li></ul>
	9. Are there any significant risk not included in the audit plan due to resource limitations?	<ul style="list-style-type: none"><li>• IA conducts a risk assessment and may or may not have resources to include significant risks in the audit plan.</li></ul>

I look forward to the June meeting. Please let me know if you have any questions or would like to discuss these comments.

Sincerely,

Larry Jensen

LACERA Audit Committee Consultant



# Integrated Enterprise Compliance Survey Results

National Survey of Largest U.S. Public Retirement Systems



February 2024

## Table of Contents

Introduction .....	2
Integrated Enterprise Compliance .....	2
The Four Lines Model.....	3
Summary of Findings and Conclusions .....	4
Enterprise Compliance Operating Model.....	5
Enterprise Compliance Program Design .....	12
Enterprise Compliance Program Delivery .....	20
Program Effectiveness and Improvement .....	25
Appendix A – List of Participating Systems .....	29

The Integrated Enterprise Compliance Survey and this report were prepared by Michael Gold, Larry Jensen, Randy Miller, and Rick Funston.

In 2015, Michael Gold retired from TIAA-CREF, an industry leader in the defined contribution marketplace, after 22 years of service. He held many senior management positions within asset management at TIAA-CREF. He joined the Funston Advisory Services Network in 2019 and has participated in numerous reviews and led compliance improvement programs.

Larry Jensen is known for his public pension fund expertise in audit, risk, and compliance. He brings over 25 years of practical experience working with two of the nation's largest public pension funds (CalPERS and CalSTRS) as Chief Risk Officer, Chief Audit Executive and Chief Compliance Officer. Larry now leads our Compliance service offering.

Randy Miller has been Chief Operating Officer of Funston Advisory Services LLC (FAS) since its founding in 2010. He is a leader of our fiduciary and operations reviews and is an expert in public retirement system governance. He leads FAS InGov® peer benchmarking for public retirement systems. He has co-authored a number of white papers on the topics of public pension fund governance, operations, and risk. He has extensive experience in planning and conducting complex reviews and improvement programs in large organizations.

Rick Funston is the Chief Executive Officer of Funston Advisory Services LLC (FAS). FAS is recognized as one of the nation's preeminent advisors to public retirement systems in the areas of governance, operations, and risk intelligence. He is also the CEO of Board Smart LLC, a Governance eLearning Resource for pension trustees and executives. In 2001, he created the concept of risk intelligence and is the principal author of numerous articles and several authoritative books on governance and risk.

## Introduction

Using our proprietary Integrated Compliance Framework shown below, a peer benchmarking survey was conducted in November-December 2023 by Funston Advisory Services LLC. The survey was sent to more than 100 of the largest U.S. public retirement systems (more than \$5 billion in AUM). We received 27 responses. The results are based on self-reports and were not independently verified. For a list of respondents see Appendix A.

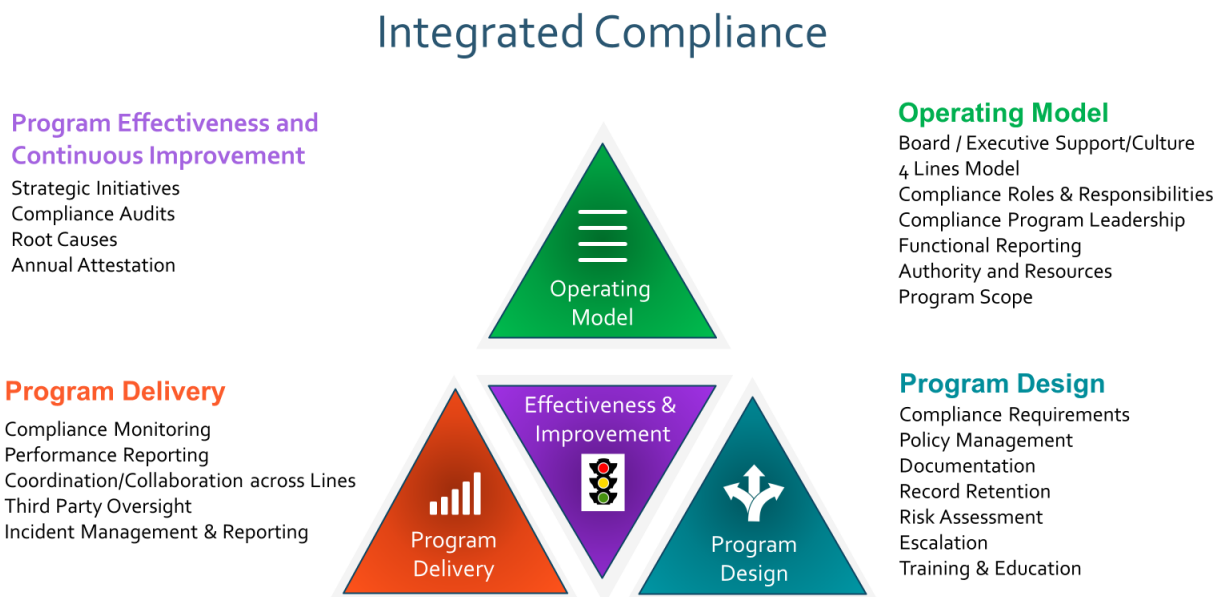
Participants included 19 state integrated systems (investment and benefits), 4 state investment boards, 1 state benefits administration system, and 2 county and 1 municipal integrated system. Fifty percent had assets under management between \$5-30 billion and fifty percent with assets greater than \$30 billion. About 45% had no assets managed internally, 10% had 0-5% of assets managed internally, and the remaining 45% had 25% or more assets internally managed. On average, there are 4.5 Full-Time Equivalent (FTE) staff resources with compliance responsibilities.

## Integrated Enterprise Compliance

An integrated enterprise compliance program is a coordinated approach that spans multiple business functions, organizational units, and locations to ensure compliance with applicable rules, regulations, and policies. There are four major elements:

1. The Operating Model
2. Program Design
3. Program Delivery
4. Program Monitoring and Continuous Improvement

Figure 1. Integrated Compliance



The components of each element are shown above, and we provide further explanation and summary responses on the following pages. A separate report will be prepared for each respondent organization that compares its responses to peers.



## The Four Lines Model

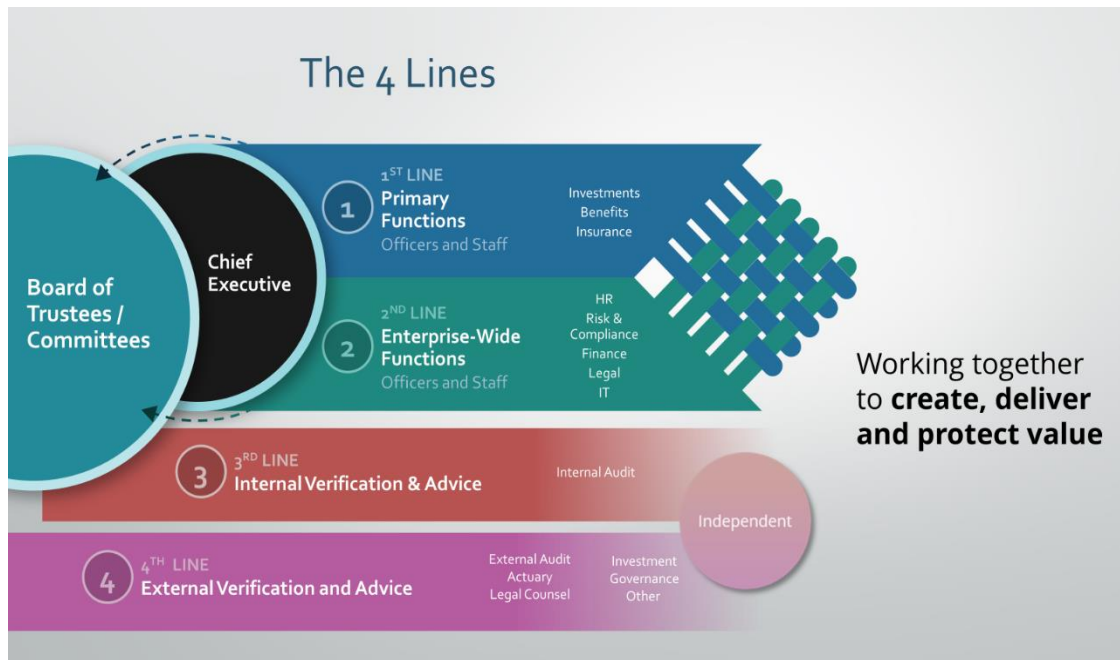
### Evolution from the Three Lines to Four Lines Model

The Institute of Internal Auditors (IIA) first issued its Three Lines of Defense Model in 2013. The IIA model was updated in 2020 to reflect value creation roles as well as value defense by referring to it simply as the Three Lines Model.<sup>1</sup>

By including both value creation and value defense, it may be helpful to see the 1<sup>st</sup> Line as the primary business functions, e.g., investment, insurance and benefits, and the 2<sup>nd</sup> Line as enterprise-wide functions that exist to support the 1<sup>st</sup> Line such as Legal, HR, IT, Compliance and Risk, etc. The 1<sup>st</sup> and 2<sup>nd</sup> Lines have frequent communication with the board and its respective committees as shown by the dotted lines, but these functions are part of the executive chain of command and are not independent of management. The 2<sup>nd</sup> Line is also primarily responsible for compliance within its own functions. The 3<sup>rd</sup> Line is Internal Audit which typically reports through the Audit Committee to the Board of Trustees. It is independent of management.

In addition, there is a 4<sup>th</sup> Line comprised of External Auditors and Advisors and, in some cases, regulators or other oversight bodies.<sup>2,3</sup> The 4<sup>th</sup> Line is also independent of management. While regulators and oversight bodies may conceptually be part of the 4<sup>th</sup> Line, they do not report to the Board and are not included as a Line. Figure 2 below shows the Four Lines and their relationships.

**Figure 2. The Four Lines Model**



<sup>1</sup> <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf>

<sup>2</sup> <https://www.bis.org/fsi/fsipapers11.pdf>

<sup>3</sup> <https://www.icaew.com/technical/audit-and-assurance/assurance/what-is-assurance/assurance-glossary/four-lines-of-defence>



## Summary of Findings and Conclusions

**Although all systems have compliance requirements and generally comply with those requirements, the structure and clarity of the compliance program varies significantly among this peer group:**

- About 45% have a dedicated Chief Compliance Officer (CCO) and 45% have an executive with other duties who is also responsible for compliance. The largest systems with internally managed assets typically have a dedicated compliance officer, while the smallest have assigned this role to executives with other responsibilities, typically the general counsel, or they do not have a designated compliance executive.
- The reporting relationship of the compliance officers varies significantly (Board, Board committee, Chief Executive, General Counsel, Chief Financial Officer, Deputy CIO), but most often the CCO reports directly to the Chief Executive.
- Compliance programs primarily focus on investments but extend to benefits and administration.
- Given the inconsistencies in the results, some systems may be overconfident in the effectiveness of their current compliance programs.
- Some systems are just beginning the process of developing a structured compliance program.

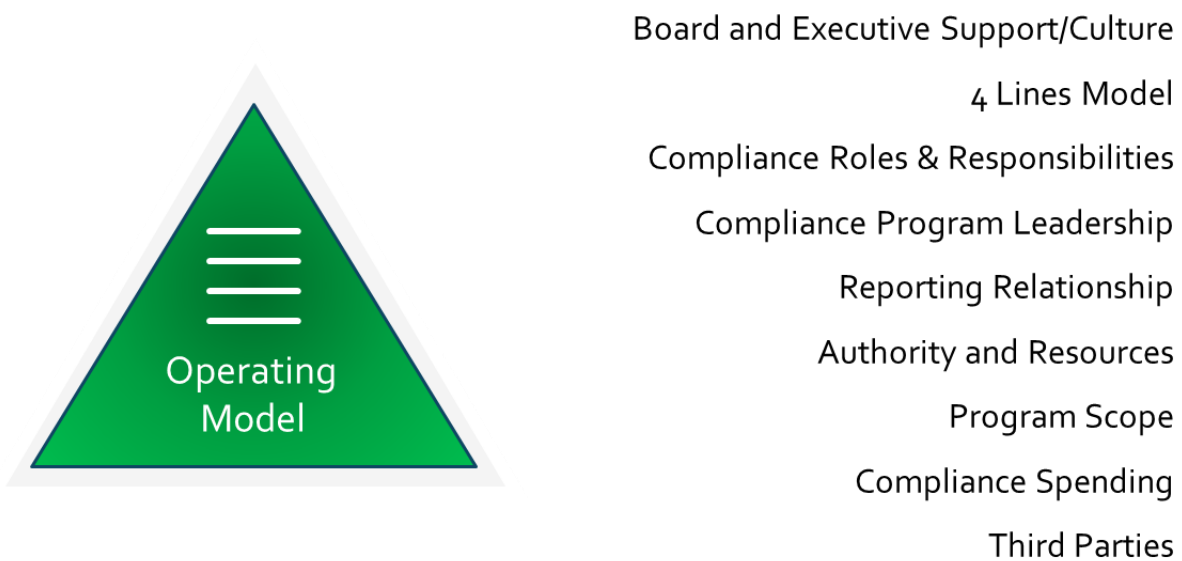
**The IIA's Three Lines model does not appear to be well understood or reflected in practice. For example:**

- Over 60% of respondents reported that the Compliance function is primarily responsible for establishing compliance requirements and testing controls, whereas in our opinion, Compliance should have a support role with primary responsibility for compliance residing with the 1<sup>st</sup> line functions. Compliance should assist both 1<sup>st</sup> and 2<sup>nd</sup> line functions with compliance responsibilities.
- At about one quarter of systems, compliance roles and relationships appear to be unclear between the Lines.

**Major opportunities for compliance improvement among the peer group are:**

- Clarifying compliance roles and responsibilities, including:
  - Ensuring the 1<sup>st</sup> Line business functions, e.g., investment, benefits, insurance, and 2<sup>nd</sup> Line enterprise-wide functions, e.g., Legal, HR, Risk, Finance and IT, are leading development of compliance requirements and testing controls, with the assistance of the Compliance function.
  - Reinforcing the independence of the 3<sup>rd</sup> Line (Internal Audit)
- Using risk to prioritize critical and necessary compliance requirements, as well as controls and resources.
- Establishing on-going compliance monitoring and auditing processes and making better use of exception reporting to highlight potential non-compliance.
- Improving third-party risk management and oversight.
- Adding compliance performance in the annual goals of leadership for both 1<sup>st</sup> and 2<sup>nd</sup> Lines.
- Requiring annual compliance attestations of both internal and third-party rules and requirements.
- Improving and tailoring compliance training for all employees.

## Enterprise Compliance Operating Model



### Expectations

A strong culture of compliance and “tone at the top” begins with board and executive support and is then reflected in the tone at the middle and front-lines of the organization. A system’s commitment to sustain a strong culture of compliance is evidenced by ensuring that compliance performance is included in the annual goals and evaluations of leadership across all Lines. The culture of compliance extends beyond the internal operating environment to include critical counterparties that support the business and support functions of the enterprise.

There should be clear roles and responsibilities between management (1<sup>st</sup> and 2<sup>nd</sup> Lines) and independent verification and advice provided by the 3<sup>rd</sup> and 4<sup>th</sup> Lines. The primary responsibility for identifying and managing performance and risk resides with the 1st Line. This includes all aspects of performance risk including strategic, investment, operational, financial, compliance, and reputation.

The 1<sup>st</sup> Line is responsible for providing reasonable (but not absolute assurance) that performance and risk are within policy and for ensuring the effectiveness and efficiency of controls. These responsibilities extend to the identification of all compliance rules and requirements, the prioritization of risk, identification of causes, and design of controls, measures of control strength and monitoring and reporting results. Most 2<sup>nd</sup> Line functions, such as Legal, IT, Finance, and Human Resources, also have responsibility for complying with requirements within their areas.

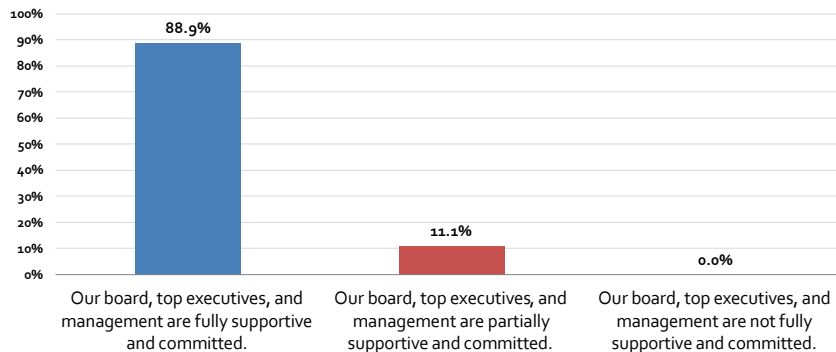
As a 2<sup>nd</sup> Line function, compliance plays a supportive role in the development of requirements and a key role in reasonably assuring that the 1st Line is effectively fulfilling its responsibilities as described above. Compliance support responsibilities should be clearly defined. There should be transparency and timeliness in reporting to the executive and the board and escalating incidents of non-compliance as appropriate. There should be appropriate authority and resources to fulfill these responsibilities. The program scope should include all applicable compliance requirements.

### Board and Executive Support

Support from the board and executive is reported to be strong by almost 90% of the participants. Tone from the top is critical to sustaining an effective compliance program.

### Board / Executive Support

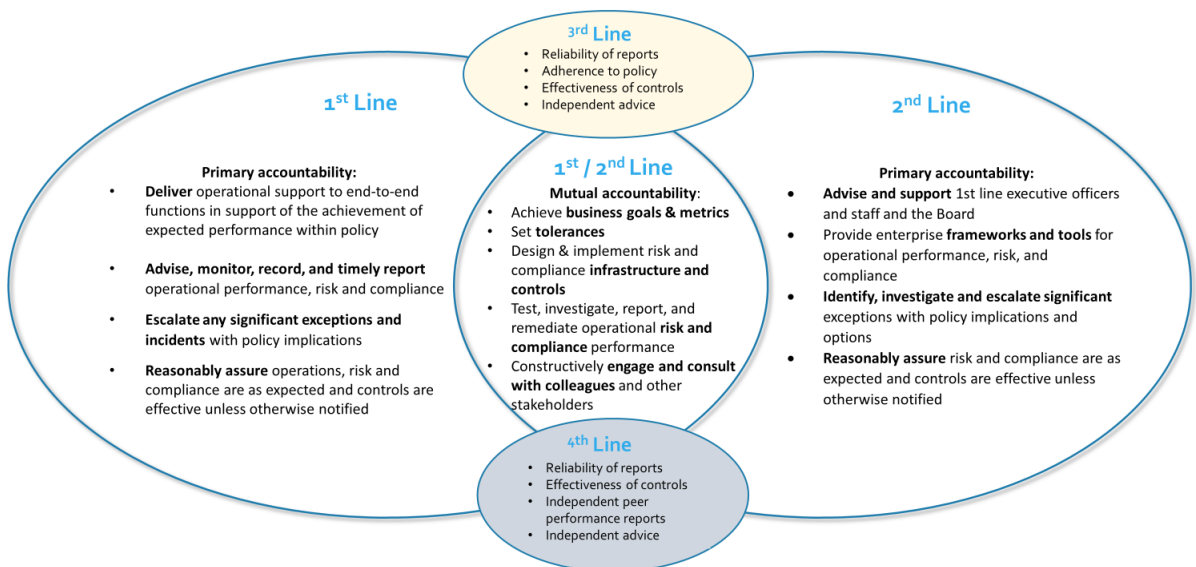
Which of the following statements best reflect how your board, top executives, and management support and engage the organization's compliance efforts and maintain a culture of compliance?



### Four Lines Model

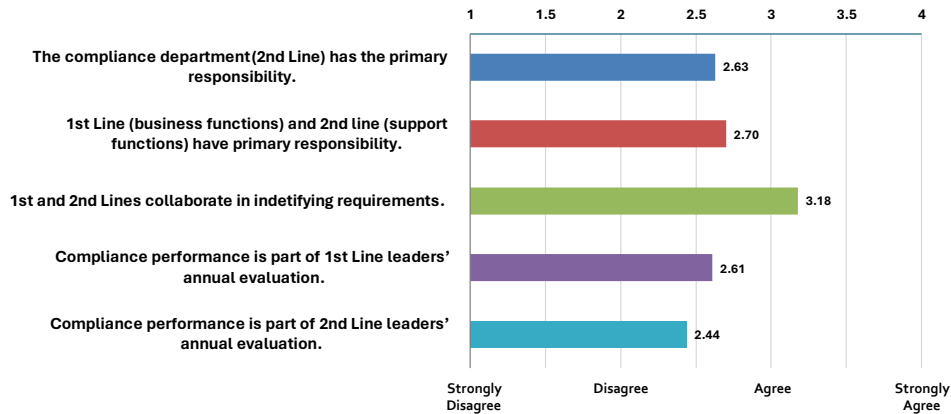
As noted earlier, the IIA's Three Lines Model does not appear to be well understood or widely deployed. The Four Lines Model shown below is intended to clarify the roles and accountabilities of each Line. The primary responsibility for identifying and managing risk should reside with the 1st Line. This includes all aspects of risk including investment, strategic, operational, financial, reputational and compliance.

### 4 Lines Accountabilities



## Primary Responsibilities

Responsibilities to maintain and enforce our agency's compliance rules and requirements are based on the following operating model.



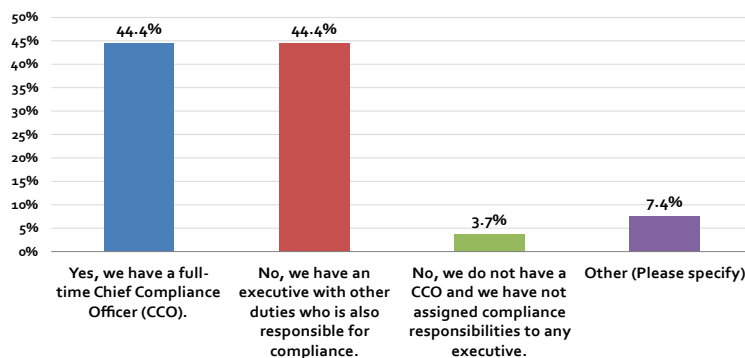
For the 1st Line, compliance responsibilities include the identification of all rules and requirements, prioritization of risk, identification of sources, design and documentation of controls, assessing control strength and monitoring and reporting results. A system's 2<sup>nd</sup> Line and compliance function should play a supportive role in the development of requirements and a primary role in assuring that the 1<sup>st</sup> Line is effectively fulfilling its responsibilities as described above. The 2<sup>nd</sup> Line is part of management's chain of command and is, therefore, not independent.

## Program Leadership

The peer group is evenly split at about 45% between those with a designated Chief Compliance Officer (CCO) and those with an executive that also performs other functions. The largest systems have dedicated CCOs. The smallest have an executive with multiple responsibilities or have not assigned an executive with compliance responsibilities.

## Chief Compliance Officer

Does your organization have a dedicated Chief Compliance Officer (CCO)?



"Other" responses:

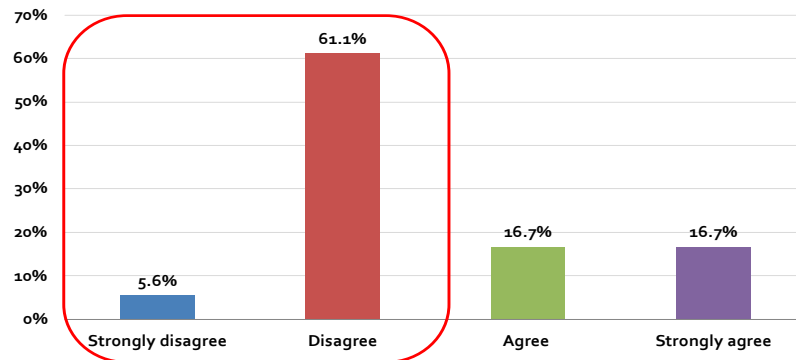
- We will have a Compliance Officer in the near future.
- Internal audit.

## Leadership Compliance Performance Evaluation

Less than 40% of systems agree their compliance performance is included in the annual goals of business and support function leadership. This can potentially undermine a culture of compliance

## Leadership Compliance Performance

Compliance performance requirements are documented in support leadership's annual goals and are a component of their annual evaluation

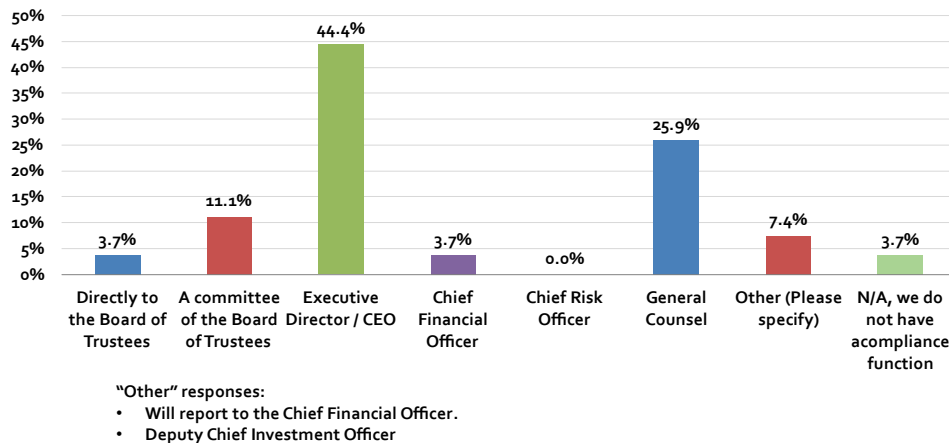


## Reporting Relationship

The reporting relationship, i.e., to whom the Chief Compliance Officer reports, varies greatly. Nearly half report to the Executive Director, one quarter to the General Counsel, and 15% to the board or one of its committees. It was unclear from the survey responses whether those with Compliance functions reporting to the board are direct reports or just have regular communication.

## Reporting Relationship

To whom does the Chief Compliance Officer(or whoever is responsible for compliance) functionally report?

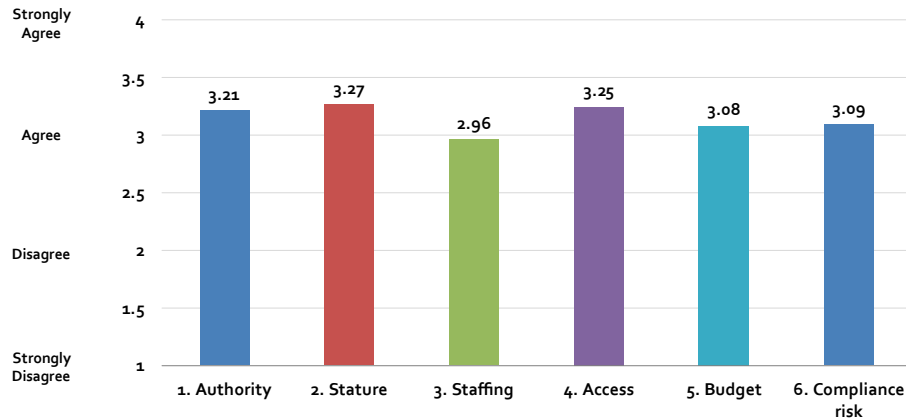


## Authority and Resources

Most systems report having adequate authority, stature and access. However, the adequacy of staffing is rated lower than all other aspects. See Risk Assessment for improving resource utilization based on criticality.

## Authority and Resources

Our organization's compliance program is structured effectively with respect to each of the following. Please indicate whether you agree or disagree with the statement.

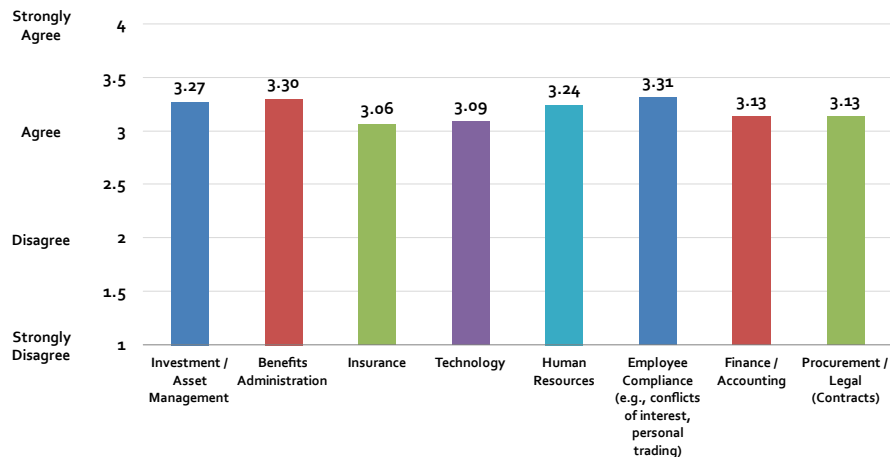


## Compliance Requirements

There is general agreement on the inventory of compliance rules and requirements.

## Compliance Rules and Requirements

Our organization maintains an inventory of compliance rules and requirements for the following business and support functions .

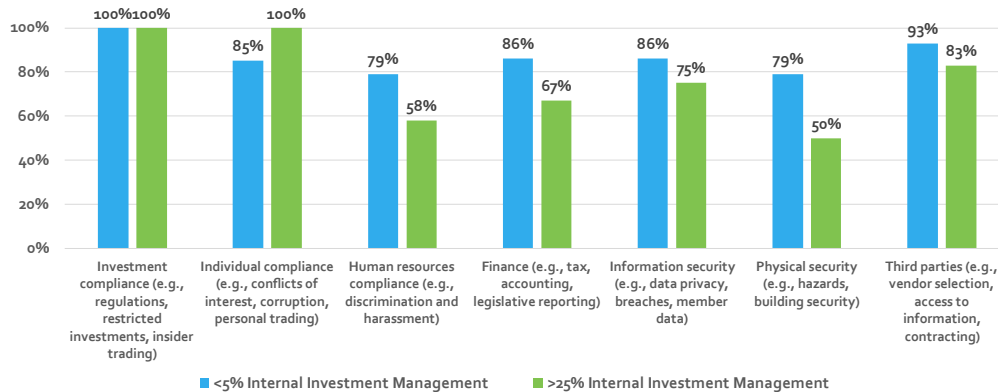


## Program Scope

Nearly all the compliance programs cover all major functions, e.g., investments, benefits, health insurance (if offered), administration, and third parties. Investment and individual (employee) compliance are the most common. Compliance programs appear to be less likely in the 1<sup>st</sup> Line functions of benefits administration and health and in the 2<sup>nd</sup> Line, i.e., HR, Finance, and cyber and physical security.

## Program Scope

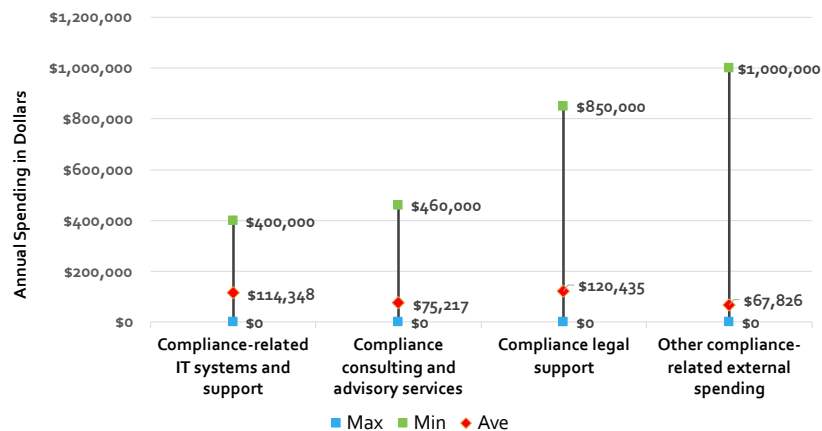
Which of the following elements are included in your organization's compliance program ?



## Compliance External Spending

## Compliance Spending

What is the approximate average annual external spending on compliance over the past three years?



Although some systems utilize external resources, in most systems compliance is handled by internal staff. Small and medium-sized systems are more likely to utilize outside resources. About 90% report external spending on compliance for IT systems, consulting, or legal support. Spending varies from system to system but averages over \$350,000 annually with the greatest amount for legal support, then IT systems and support.

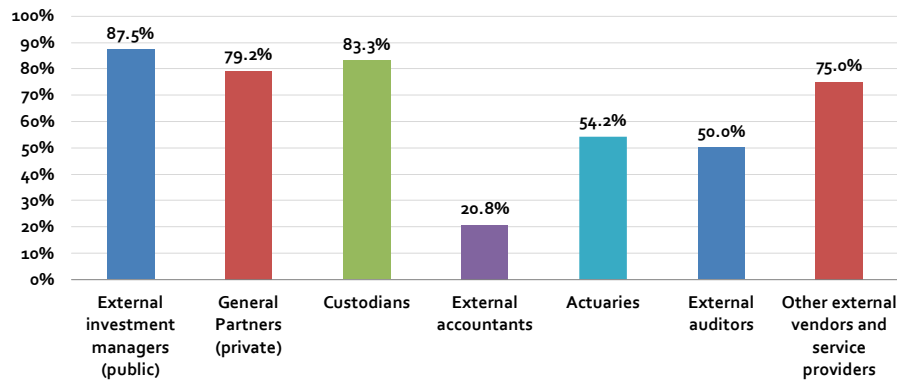


## Third Parties

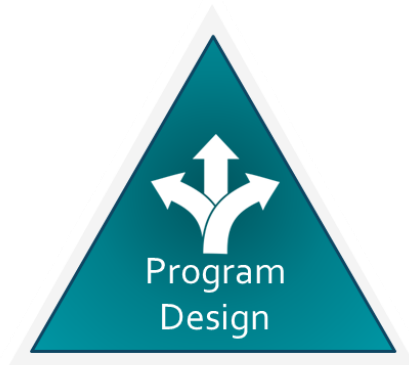
The highest level of third parties subject to compliance requirements exists within investment management at approximately 80% of respondent systems for external asset managers, general partners, and custodians. Other service providers, such as actuaries and auditors, are reported by approximately 50% of respondents.

## Third Parties

Identify all external parties subject to compliance requirements at your system .



## Enterprise Compliance Program Design



### Compliance Requirements

Policy Management

Documentation

Record Retention

Risk Assessment

Escalation

Training & Education

### Expectations

There should be an inventory of all compliance rules and requirements. The repository should be regularly reviewed and updated for completeness. There should be an effective policy management process that includes clearly assigned ownership, periodic review and update of policies, and mandatory staff certification of compliance with critical compliance and ethics policies.

All system-wide policies, processes, procedures and controls relating to the compliance program should be well documented and maintained by 1st Line owners. There should be a record of historical compliance performance. There should be mechanisms to effectively log, track, and report action plans resulting from changes to rules and requirements. The system should proactively monitor legislative, regulatory, statutory and policy-based changes to compliance rules and requirements.

All compliance rules and requirements should be risk ranked according to type (i.e., investment, operational, reputational) and impact (i.e., critical, important, necessary) of risks. A “critical” requirement is one that represents a potential “killer” risk such as loss of tax-exempt status or criminal liability. Risks to “necessary” requirements could result in, for example, civil, regulatory, or contractual liability as well as the potential for meaningful financial loss, reduced investment performance impact, or negative headlines. “Important” requirements are not critical or necessary but important to a well-controlled organization. The strength of controls, from both a design and operating effectiveness perspective, is regularly assessed.

The structure, practices and culture of a system's compliance program should be based on transparent and safe practices for employee reporting and escalation of incidents. There should be standard processes for all levels of compliance reporting up to and including executive management and board level including incident management and resolution.

Compliance training should be available for both orientation and ongoing training for all affected 1st, 2nd, and 3rd Line resources. Such programs should be tailored to the specific needs of the organization and employees’ roles and responsibilities, regularly updated to reflect changes in laws and regulations, and designed to engage employees in a way that promotes understanding and adherence to compliance requirements. All affected employees and external counterparties should periodically attest to their completion of training and understanding of the system’s compliance policies and rules.

## Integrated Enterprise Compliance Survey Results

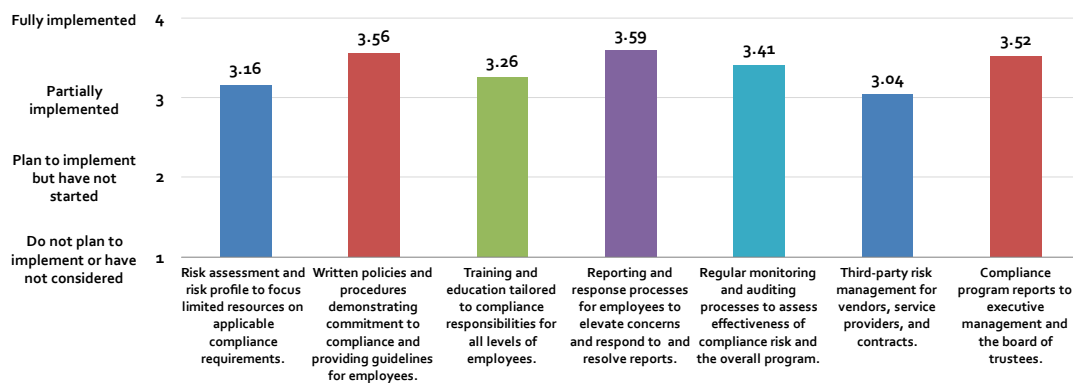
A leading practice is to have a technology platform that enables ready access to all requirements, policies, processes, supporting materials, and related controls.

### Program Design

Overall, written policies and procedures, whistleblower processes and reporting to the executive and board were reported furthest along in implementation. There was less implementation of risk assessment, training and third-party risk management.

## Program Design

Our organization compliance program includes the following elements:

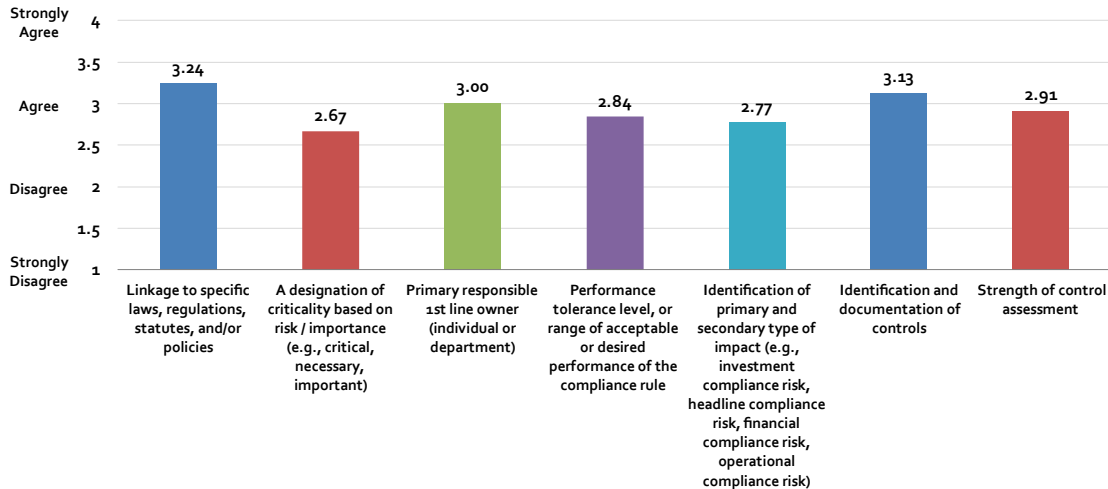


### Compliance requirements

Compliance requirements were most likely to be linked to sources, primary assignment of responsibility within the 1<sup>st</sup> Line and the identification and documentation of controls. There was less agreement that critical compliance issues, tolerances or primary and secondary impacts were identified. This could result in an underestimation of the severity of impacts of non-compliance.

## Repository of Requirements

Our organization maintains documentation of compliance requirements for the following.



## Requirements Management

Our system logs, tracks and reports action plans resulting from changes to rules and requirements to senior management and the board as required.



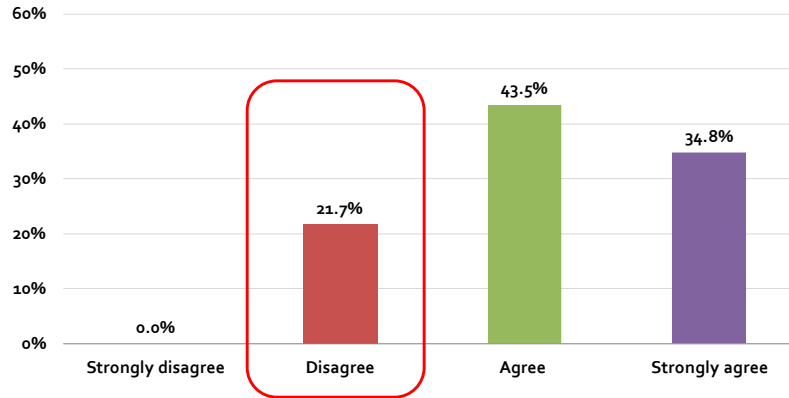
About 44% do not believe they effectively log, track, and report action plans resulting from changes to rules and requirements. This could result in out-of-date requirements.

### Policy Management

About 80% reported their system had an effective policy management process that includes assigned ownership, periodic review and update of policies, and mandatory staff certification of compliance with critical compliance and ethics policies. Ineffective policy management could lead to lack of clarity in ownership, out-of-date policies and incomplete certifications.

## Policy Management

Our system has an effective policy management process that includes assigned ownership, periodic review and update of policies, and mandatory staff certification of compliance with critical compliance and ethics policies.

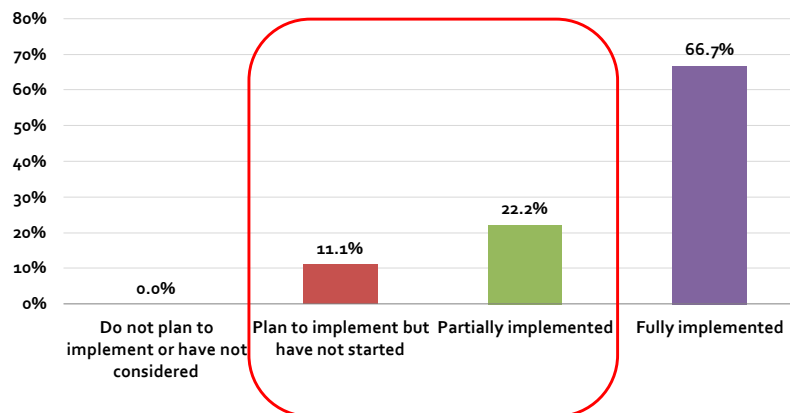


## Documentation

Just 66% indicate they have fully implemented written compliance policies and procedures. Most have identified the linkages to sources of compliance requirements. The absence of written policies and procedures can lead to lack of clarity and consistency; increased risk of non-compliance; difficulty in training and onboarding; challenges in accountability and enforcement; impaired risk management; negative impact on the compliance culture; hindered growth and scalability; and compromised trust and relationships.

## Documentation

Written policies and procedures demonstrating commitment to compliance and providing guidelines for employees.

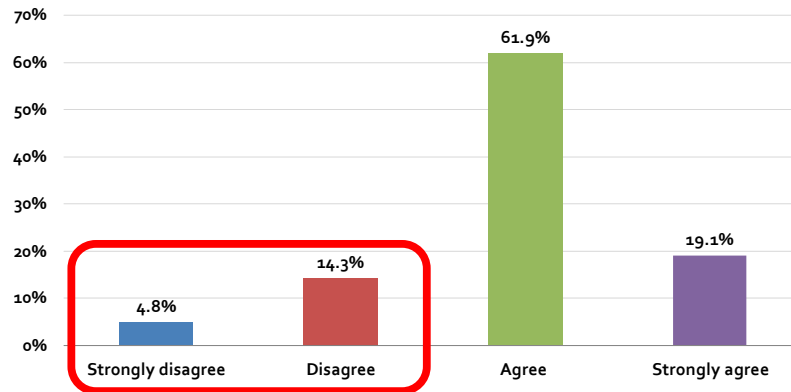


## Record Retention

Over 80% of respondents report they maintain historical compliance results.

## Record Retention

Our system maintains historical compliance results in accordance with our record retention policies.

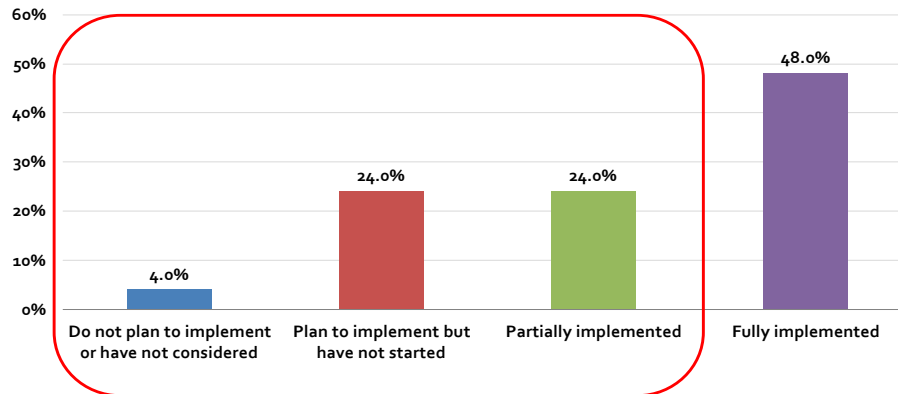


## Risk Assessment

Although most respondents maintain a comprehensive inventory of compliance rules and requirements, 48% say they have fully implemented risk assessments while 24% have only partially implemented it and 24% say they plan to do so. 5% report they aren't yet considering it. More than 30% report that performance tolerances need to be better defined. Better use of risk assessments and clarification of tolerances can help prioritize compliance requirements and resources. Risk assessments should consider the primary and secondary impact, strength of control, and criticality. Almost 30% do not perform strength of control assessments and nearly 50% do not designate criticality of a risk. Effective risk assessments establish priority of compliance requirements to optimize the focus of limited resources.

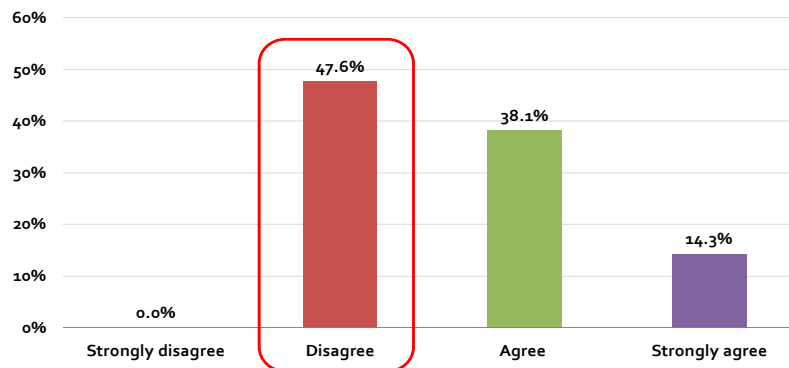
## Risk Assessment

Risk assessment and risk profile to focus limited resources on applicable compliance requirements



## Criticality

We maintain documentation of compliance requirements for a designation of criticality based on risk / importance (e.g., critical, necessary, important)



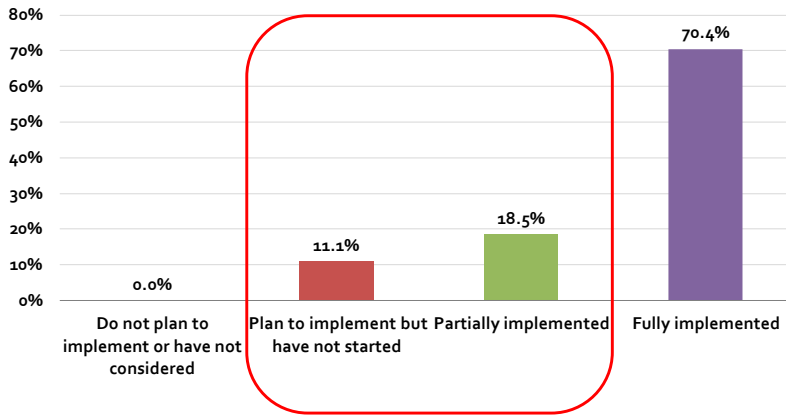
## Escalation

About 70% of respondents have fully implemented compliance policies and procedures, compliance concern escalation processes, and compliance reporting to executive management and the board. Inadequate escalation can result in delayed resolution of issues; increased frustration among employees; inconsistent decision-making; missed learning opportunities; damage to reputation; legal and financial risk; and strategic misalignment.



## Escalation

Reporting and response processes for employees to elevate concerns and respond to and resolve reports.

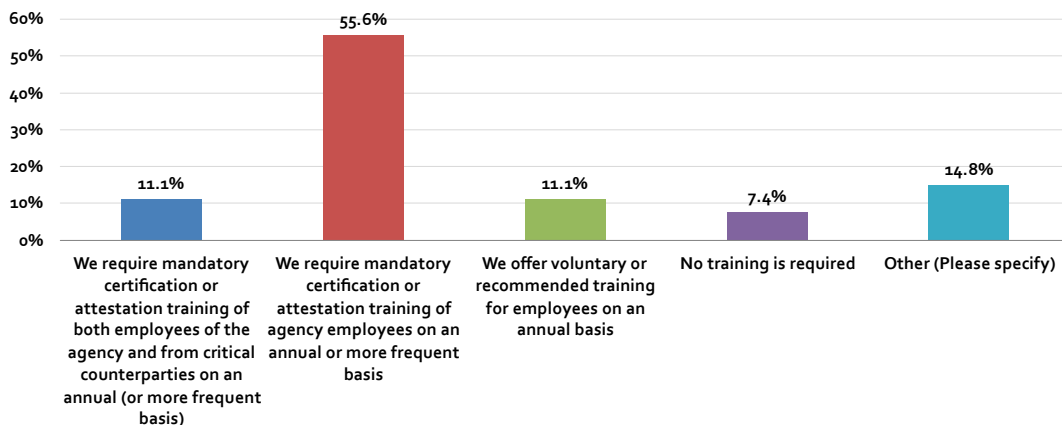


## Training and Education

66% report they require mandatory training. 11% require it of critical counterparties. Only 40% have tailored compliance education and training for all employees. Lack of timely education can lead to increased risk of non-compliance; legal and financial consequences; reputational damage; operational disruptions; decreased employee morale and productivity; and erosion of corporate culture.

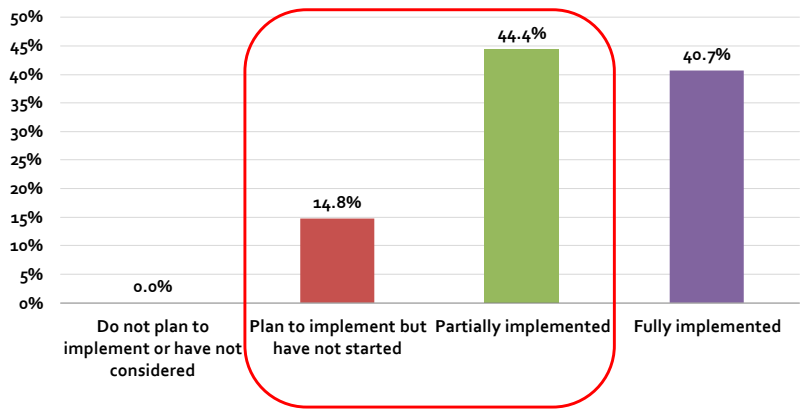
## Annual Training and Education

Which of the following statements most closely reflects the level of compliance training and education that your agency requires?



### Tailored Training

Training and education tailored to compliance responsibilities for all levels of employees.



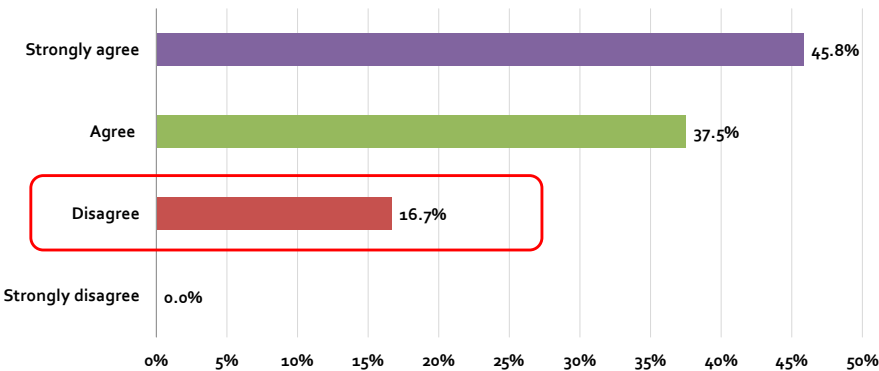
### Overall Design Effectiveness

Although most systems believe their compliance program is structured effectively in most aspects, 25% have concerns about staffing and 20% with budget. These concerns could possibly be addressed through prioritization based on a comprehensive risk assessment.

Despite some shortcomings identified throughout this report, 85% of respondents strongly agree or agree their compliance program has been designed to effectively prevent, detect, and remediate instances of non-compliance. This may reflect some degree of overconfidence in the effectiveness of their compliance programs.

### Overall Design Effectiveness

Our organization's compliance program is designed to effectively prevent, detect, and remediate instances of non-compliance with applicable laws and regulations.



## Enterprise Compliance Program Delivery



Compliance Monitoring

Performance Reporting

Coordination/Collaboration across Lines

Incident Management & Reporting

Third Party Risk Management

### Expectations

There should be a clear understanding of the individual and reciprocal roles and responsibilities of all 4 Lines. They should collaborate and coordinate their activities. Compliance monitoring should be performed periodically to check how well 1<sup>st</sup> and 2<sup>nd</sup> Lines meet their compliance responsibilities. There should be clear and effective processes for monitoring and reporting compliance as well as incident reporting. Compliance performance compared to policy expectations should be clear, transparent, and reported timely to senior management and the board.

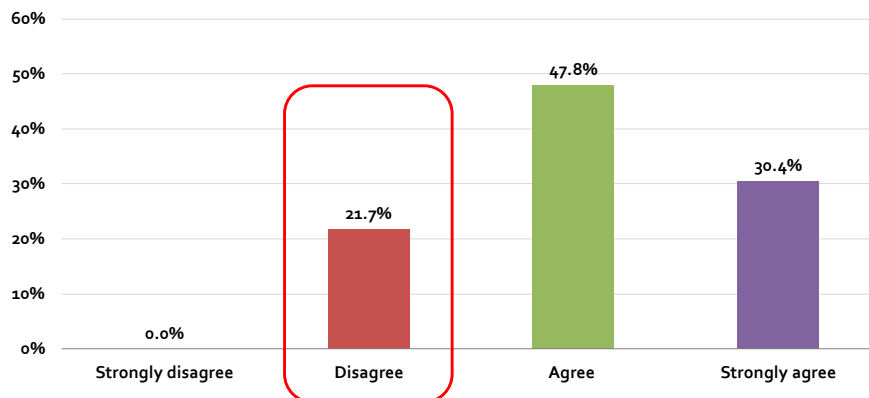
There should be regular joint meetings, shared risk and compliance platforms, and a unified approach to risk management and internal controls, ensuring that all parts of the organization work together seamlessly to identify, assess, manage, and monitor compliance risks. There should be clearly defined compliance performance requirements for 3rd party contracts including Independently Managed Accounts (IMAs), Limited Partnership Agreements (LPAs) and key 3<sup>rd</sup> party contractual Service Level Agreements SLAs.

## Compliance Monitoring

Almost 80% reported they perform regular monitoring to assess adherence to compliance requirements for most critical risks and rules. Lack of effective compliance monitoring can lead to, among other financial and legal consequences, undetected non-compliance issues; decreased stakeholder confidence and trust; and decreased employee morale and increased turnover.

## Compliance Monitoring

Our system has a clear, transparent and periodic processes for monitoring compliance performance for most critical rules and risks.

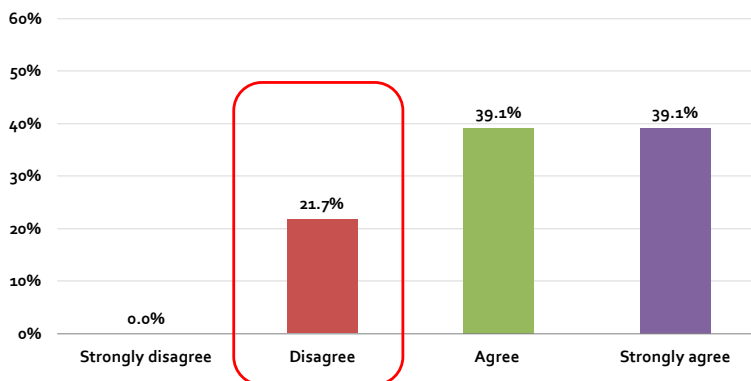


## Performance Reporting

While most agreed their system has a clear and transparent process for reporting compliance performance to senior leadership and the board, more than 20% reported they did not.

## Performance Reporting

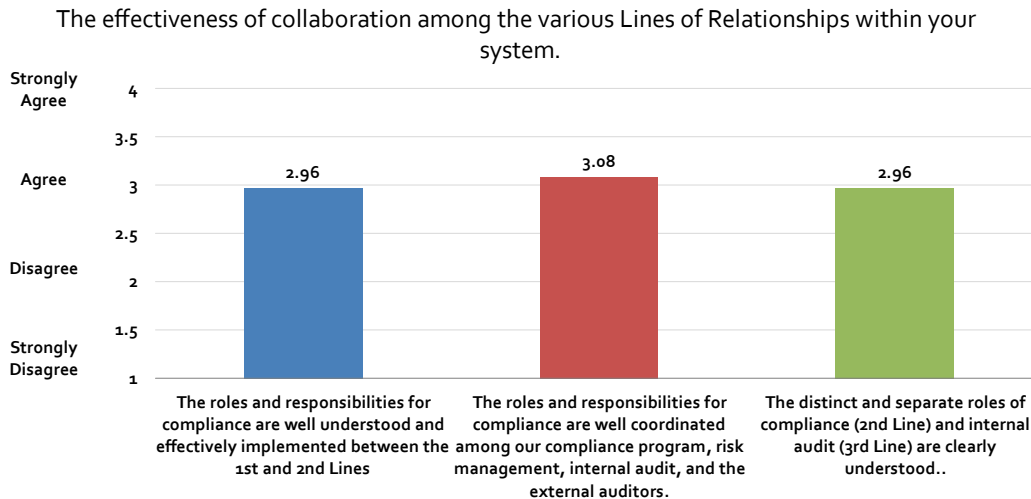
Our system has a clear, transparent and periodic process for reporting compliance performance results to senior leadership for most critical rules and risks



## Coordination / Collaboration across Lines

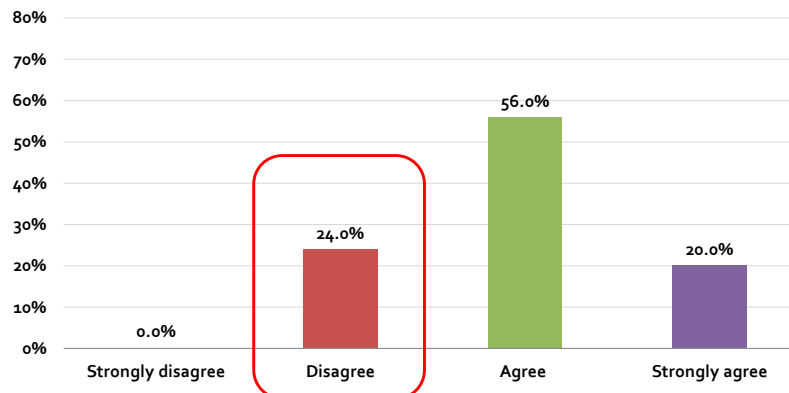
Respondents agreed there is collaboration across Lines. However, opportunities exist to close the gaps in understanding particularly as they relate to the primary roles of the 1<sup>st</sup>, 2<sup>nd</sup> and 3<sup>rd</sup> Lines. Lack of collaboration and coordination across the 4 Lines can lead to increased risk exposure; inefficiencies and duplication; compliance failures; poor decision making; eroded organizational culture; missed opportunities for improvement; and increased negative audit findings.

## Collaboration Across Lines



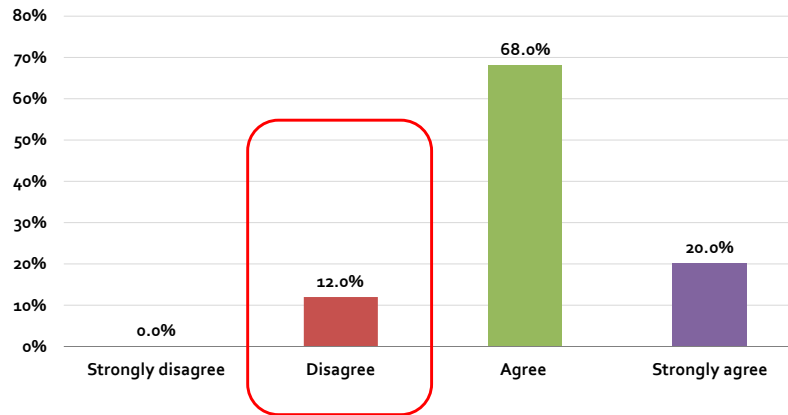
## Collaboration Between 1<sup>st</sup> and 2<sup>nd</sup> Lines

The roles and responsibilities for compliance are well understood and effectively implemented between the 1<sup>st</sup> and 2<sup>nd</sup> Lines



## Coordination Between 2<sup>nd</sup>, 3<sup>rd</sup> and 4<sup>th</sup> Lines

The roles and responsibilities for compliance are well coordinated among our compliance program, risk management, internal audit, and the external auditors.

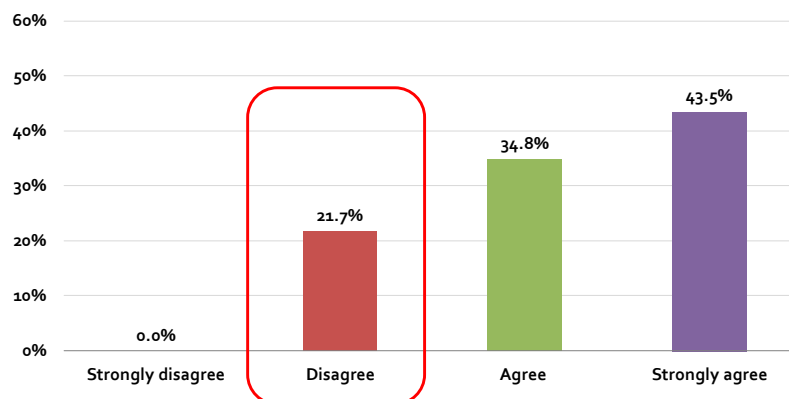


## Incident Management and Reporting

About 80% of respondents believe they have clear and effective processes for anonymous reporting of compliance or ethical concerns that include action plans to prevent recurrence. Lack of effective and timely incident management and reporting can result in delayed resolution of issues; increased vulnerabilities; inconsistent decision-making; missed learning opportunities; damage to reputation; and legal and financial risk.

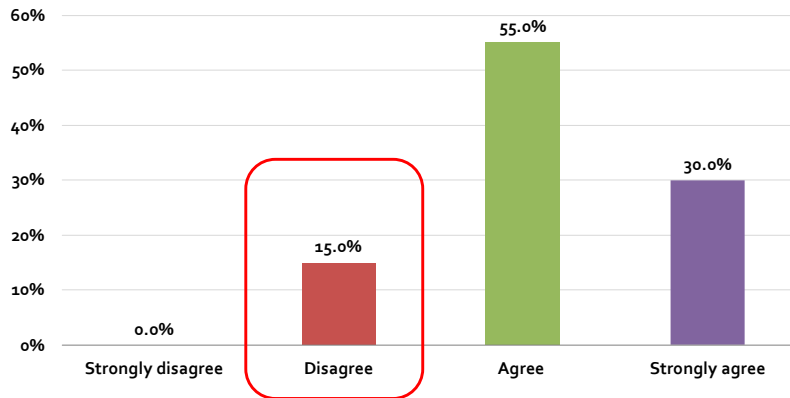
## Incident Management and Reporting

Our system has an effective process for anonymous reporting of a compliance or ethics concerns.



## Incident Management and Reporting

Our system has an incident reporting process that contains an action plan to prevent reoccurrence of compliance violations.



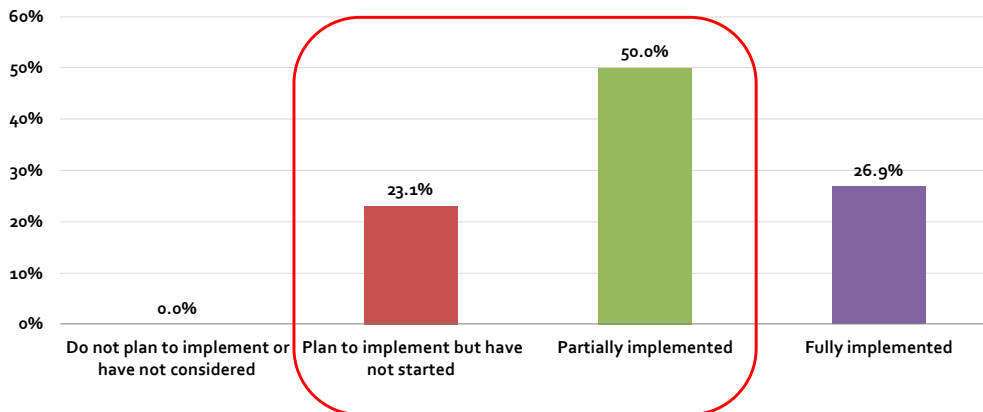
## Third Party Risk Management

Third parties, such as vendors, suppliers, contractors, and service providers, can introduce various risks into an organization, including financial, reputational, operational, and compliance risks. Only about one quarter have a risk management program for third party vendors and service providers.

Managing third-party risk is essential for safeguarding sensitive data, ensuring compliance, maintaining operational resilience, preserving reputation, and supporting financial stability. It is a critical component of an organization's overall risk management strategy.

## Third Parties

Third-party risk management for vendors, service providers, and contracts.





## Program Effectiveness and Improvement



Strategic Initiatives

Compliance Audits

Root Causes

Annual Attestation

### Expectations

The overall effectiveness of the system's compliance program, and key components of it, should be regularly monitored and audited. Strategic initiatives should consider compliance requirements as part of their design and development. Reviews of 1<sup>st</sup> and 2<sup>nd</sup> Line compliance processes and policies of the most critical rules and requirements should be built into audit plans, especially for those performing at levels below desired results. Industry practices suggest periodic self-assessments and an independent audit or review of an organization's compliance program effectiveness and maturity.

Root causes of non-compliance should be routinely investigated, and corrective actions should be developed, implemented and monitored for effectiveness. Strategic initiatives should consider compliance requirements within their project planning and budgeting framework.

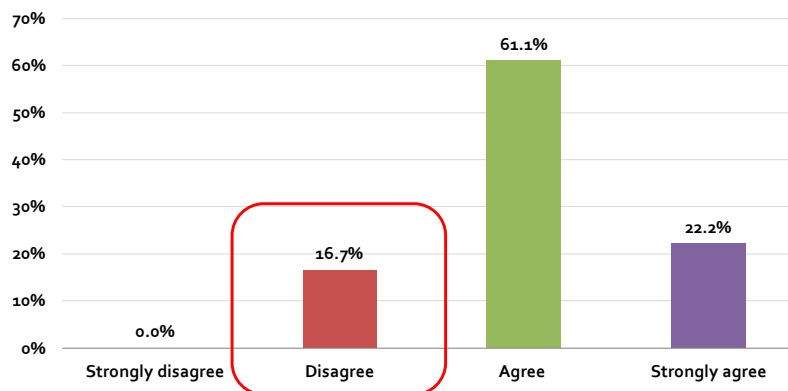
Annual attestation requirements for key staff should be mandatory. All essential counterparties (and their staff) should provide annual attestations (as required).

### Strategic Initiatives

More than 80% said they consider compliance requirements for new initiatives. The consideration of compliance in strategic initiatives can help proactively identify requirements, mitigate the risk of non-compliance and reinforce a culture of compliance.

### Strategic Initiatives

Our system imbeds compliance considerations in the development of strategic and operating plans and in the consideration of new initiatives.

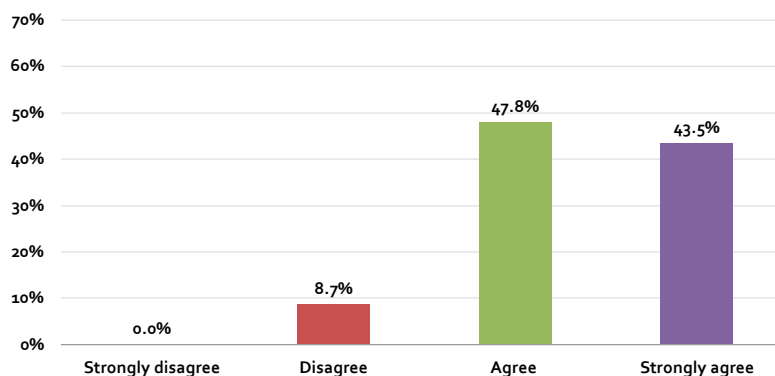


### Compliance Audits

At over 90% of the systems in the survey, compliance performance of the most critical requirements are taken into account in systems' development of audit plans. Approximately the same percentage of systems reports on practices to proactively monitor legislative, regulatory, statutory or policy-based changes to compliance rules and requirements.

### Compliance Audits

Our internal and external audit plans take into account compliance performance of the most critical requirements and/or those that are performing at levels below desired results.

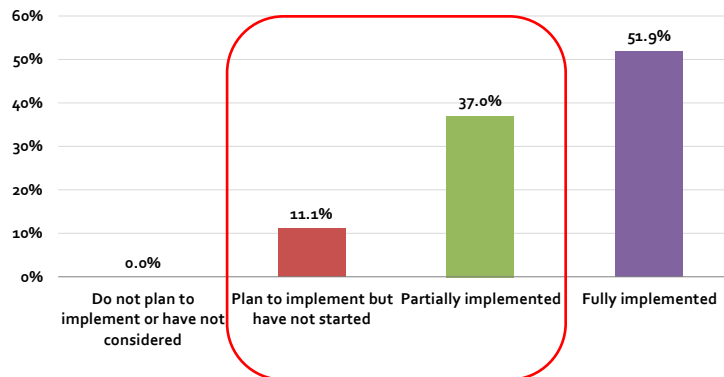


### Monitoring and Auditing

Almost 80% of systems integrate compliance history into records retention capabilities, which can facilitate continuous improvement.

### Monitoring and Auditing

Regular monitoring and auditing processes to assess effectiveness of compliance risk and the overall program.



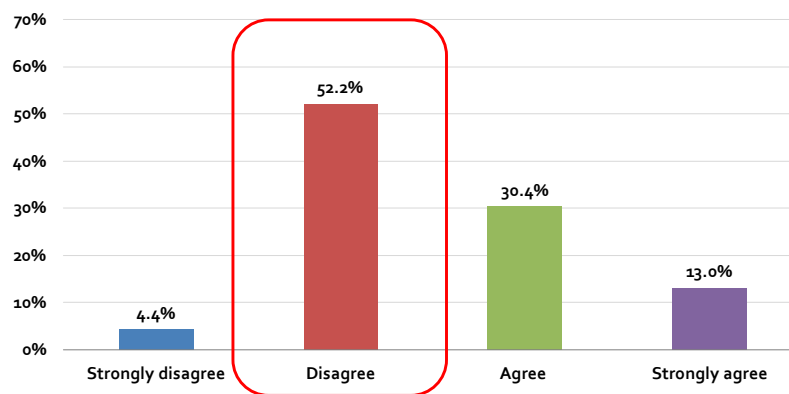
Nearly all respondents believe their internal and external audit plans consider compliance performance and that they proactively monitor changes to compliance rules and requirements.

### Root Causes

Over 55% reported they did not perform root cause analysis of non-compliance events. The lack of robust analysis of root causes, such as people, process, systems or external factors may lead to recurrence of non-compliance.

### Root Causes

Our system utilizes root cause and trend analyses methods to continuously improve performance against compliance risks.

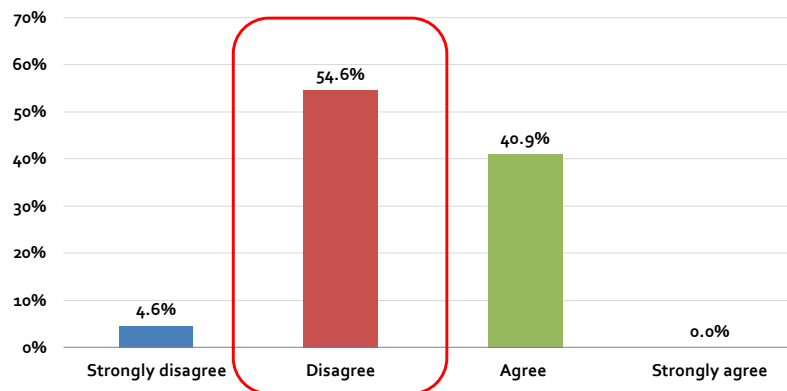


### Annual Attestation

This practice helps ensure that the fundamental elements of a system's compliance program (rules, requirements, controls) remain current. An annual attestation / sign off on the inventory of compliance requirements by 1<sup>st</sup> and 2<sup>nd</sup> Line management is practiced at fewer than 50% of respondent systems. This can result in out-of-date requirements inventories.

### Annual Attestation

Our system has an annual sign off on the inventory of compliance requirements by both first - and second-line management .



**For further Information, please contact:**

#### Larry Jensen

Leader Compliance Services  
Funston Advisory Services LLC  
[ljensen@funstonadv.com](mailto:ljensen@funstonadv.com)

#### Randy Miller

Chief Operating Officer  
Funston Advisory Services LLC  
[rmiller@funstonadv.com](mailto:rmiller@funstonadv.com)

## Appendix A – List of Participating Systems

Twenty-seven public retirement systems, all with Assets Under Management over \$5 billion, participated:

- California Public Employees' Retirement System
- California State Teachers' Retirement System
- Employee Retirement System of Texas
- Employees' Retirement System of the State of Hawaii
- Fairfax County Retirement Systems
- Florida State Board of Administration
- Illinois State Universities Retirement System
- Kentucky Public Pensions Authority
- Michigan Bureau of Investments
- Missouri Local Government Employees Retirement System
- Municipal Employees Retirement System of Michigan
- New Hampshire Retirement System
- New Mexico Public Employees Retirement Association
- New York State Teachers' Retirement System
- Ohio Police & Fire Pension Fund
- Ohio Public Employees' Retirement System
- Ohio School Employees' Retirement System
- Orange County Employees Retirement System
- Oregon Public Employees Retirement System
- Pennsylvania Public School Employees' Retirement System
- Pennsylvania State Employees' Retirement System
- San Diego City Employees' Retirement System
- South Carolina Retirement System Investment Commission
- State of Wisconsin Investment Board
- State Teachers Retirement Systems of Ohio
- Teacher Retirement System of Texas
- Wyoming Retirement System