

Purpose-built: Sarbanes-Oxley (SOX) program operating models

The case for a purpose-built SOX program operating model




Designing an operating model is crucial to the success of your Sarbanes-Oxley (SOX) program. It not only matches the structure to the mission and culture of your organization but also determines the success of the ownership and governance of the SOX program.

Key benefits

- **Governance setting the structure** – SOX Section 404 requires an annual assessment by the CEO and CFO on the effectiveness of the system of internal controls. An intentionally designed operating model serves to provide the structures and processes required to meet the objectives of SOX 404.
- **Resource alignment and accountability** – Assigning resources based on their knowledge, authority, and role within the organization to achieve required outcomes efficiently.
- **Interdependent relationships** – SOX end-to-end program responsibilities flow with strategically designed interdependencies that serve to drive a stronger control environment and understanding of objectives.

SOX roles and responsibilities across the three lines

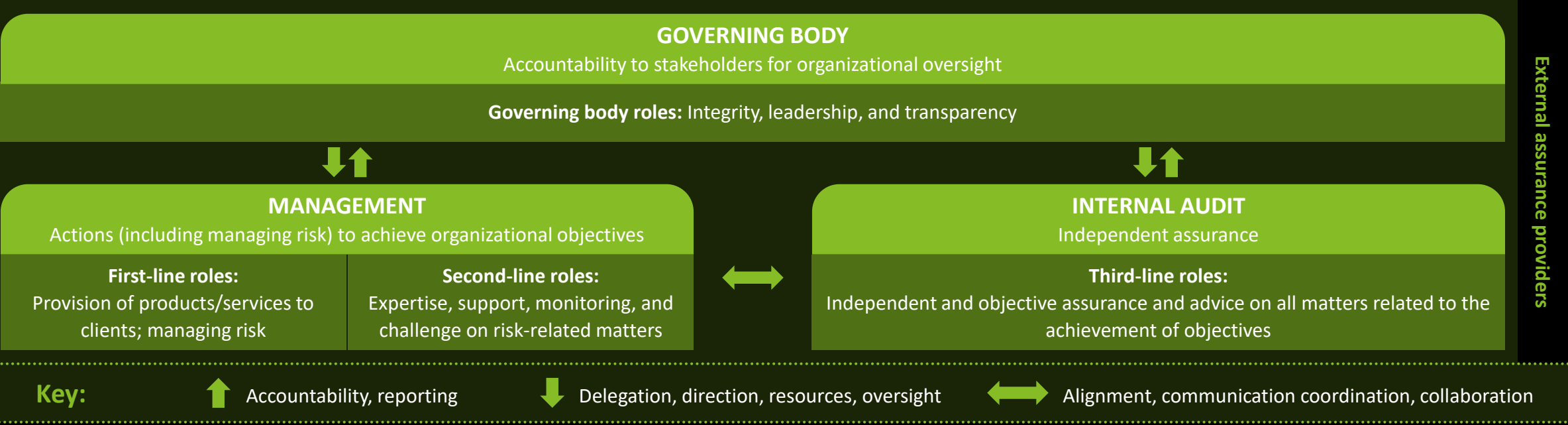
Below are the activities typically seen across the three lines for a SOX program; however, organizations structure SOX programs in different ways.

 First-line activities	 Second-line activities	 Third-line activities
<ul style="list-style-type: none">Identify risks of material misstatement, risks associated with IT, and select/design controls to mitigate risks*Update control documentation to reflect current state (i.e., narratives, flowcharts, written control descriptions, risk control matrices)*	<ul style="list-style-type: none">Perform risk assessment at financial statement level, including fraud risk, outsourced service providers, and IT systemsProvide guidance to first-line for risk identification, control selection/design, control risk ranking, and remediation plans for deficienciesMaintain control documentation*	<ul style="list-style-type: none">Receive scope of annual program from second linePerform control testing of annual programIdentify and report deficiencies and related root causeCoordinate with external audit for third-line roles, such as testing timeline and testing attributes/samples for reliance
<ul style="list-style-type: none">Execute controlsLead walkthroughs with external audit and internal audit for annual audit cycleRetain audit evidence and provide for annual audit cycle*Provide input on deficiency root cause and impactDevelop remediation plans for deficiencies*	<ul style="list-style-type: none">Coordinate with external audit for second-line roles, such as reliance opportunities, risk assessment, and deficiency assessment*Evaluate severity of deficiencies*Monitor/report deficiency remediation* trackingReport results to Audit Committee on risk assessment, deficiency evaluation, remediation plans, and external audit coordination*	<ul style="list-style-type: none">Report results to Audit Committee on second-line rolesMember of SOX Steering Committee
<ul style="list-style-type: none">Monitor performance of outsourced service providers (OSPs) and evaluate annual SOC 1Certify through quarterly 302 sub certification*Identify opportunities for continued improvement	<ul style="list-style-type: none">Establish and deploy SOX training programAssess and report 302 certification results*Member of SOX Steering CommitteeImplement/maintain GRC platform*	

* Technology is an important element of any operating model; this depicts the three-line activities that are optimized through technology enablement.

The responsibilities of IIA’s Three Lines Model¹

While the Three Lines Model should complement each other to achieve a unified goal of providing effective risk management and governance, each plays its own different role. It is critical to have the right people in place to manage risks (first line), monitor risks (second line), and provide independent assurance (third line).

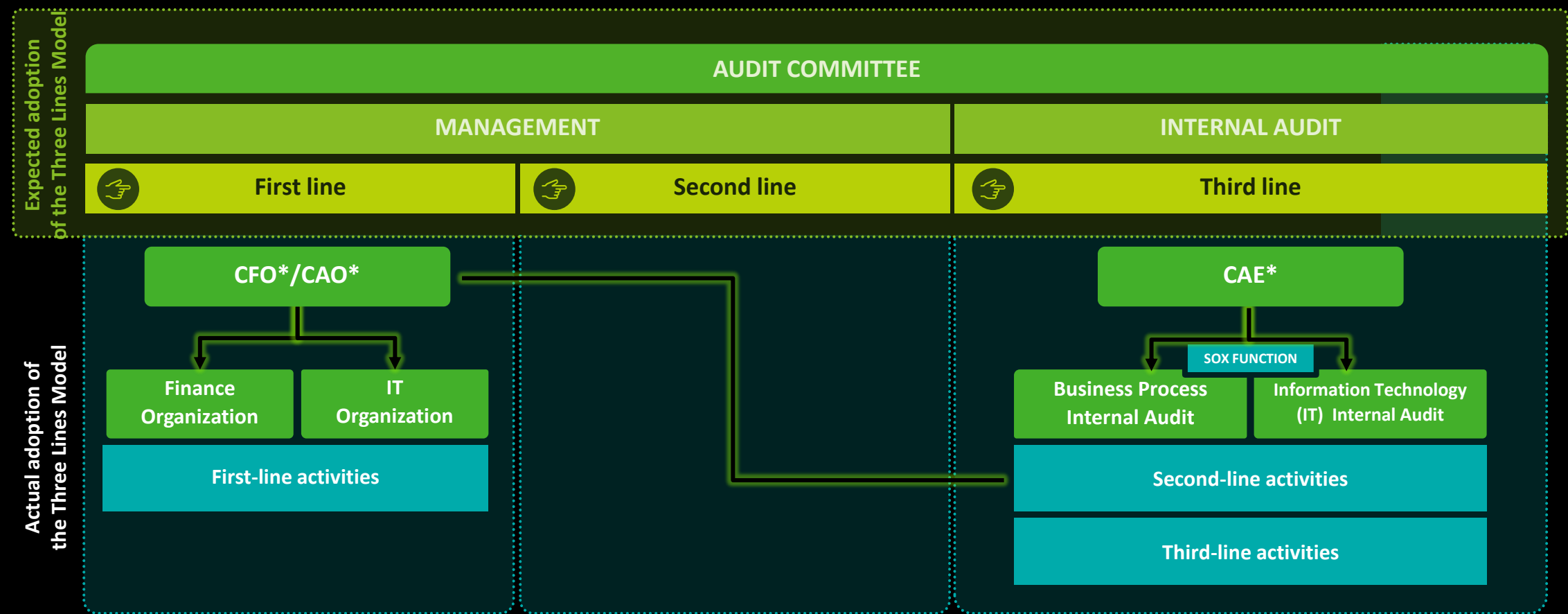


The Three Lines Model helps organizations achieve their broader objectives alongside strong governance and risk management processes. Organizations aligned to the framework will observe the below characteristics of an optimized model.

- Principles-based approach and adaptation to align with organizational objectives and circumstances
- Risk management focused to achieve objectives and create and protect value
- Understand roles, responsibilities, and their relationships and interdependencies
- Ensure alignment of activities and objectives to stakeholder priorities

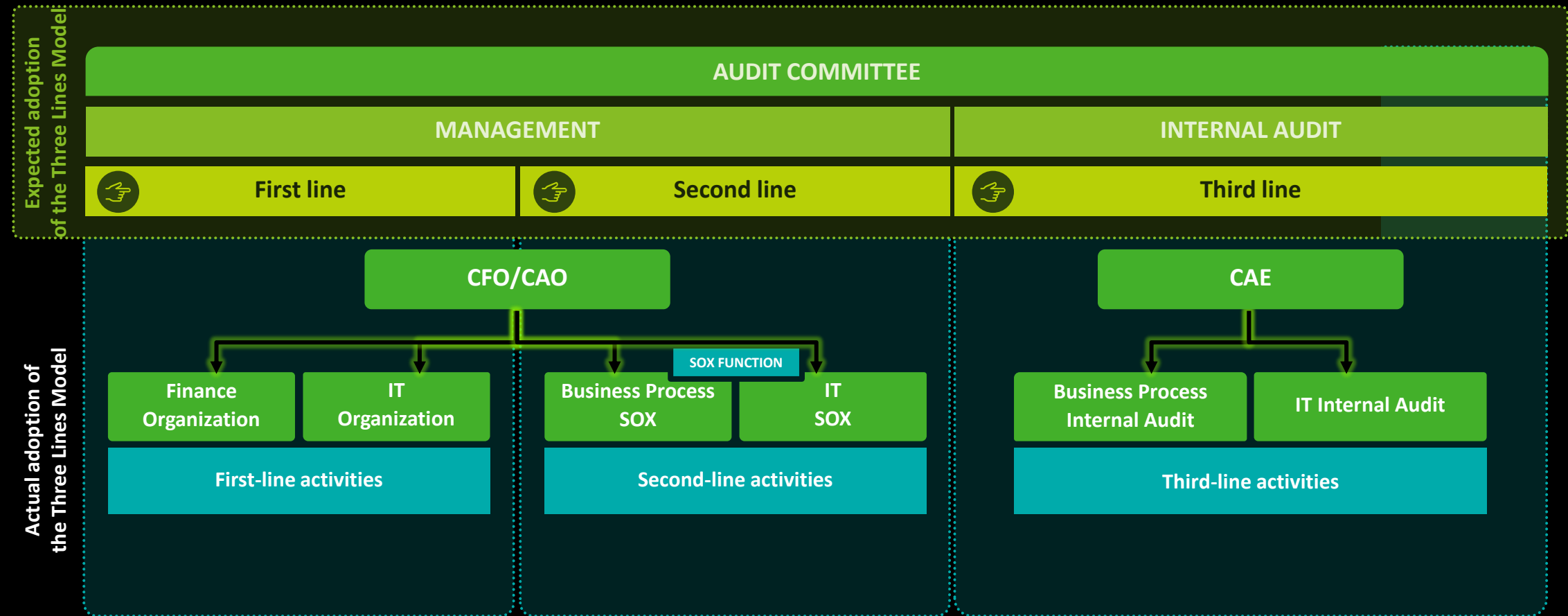
¹Source: Institute of Internal Auditors (IIA), "The IIA's Three Lines Model: An update of the Three Lines of Defense," July 2020. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense?utm_source=google&utm_medium=cpc&utm_campaign=20253036447&utm_content=&utm_term=&gad_source=1&gclid=Cj0KCQjwgl-3BhDnARIsAL6KZ6_EVW7Skd9z0kHI2_SoeWGbTHTZ7NRjd8_J7tDITQxEW0KGAXIFc2EaAojfEALw_wcB
Copyright © 2024 Deloitte Development LLC. All rights reserved. Purpose-built: Sarbanes-Oxley program operating models 4

Option 1: SOX is overseen solely by the third line

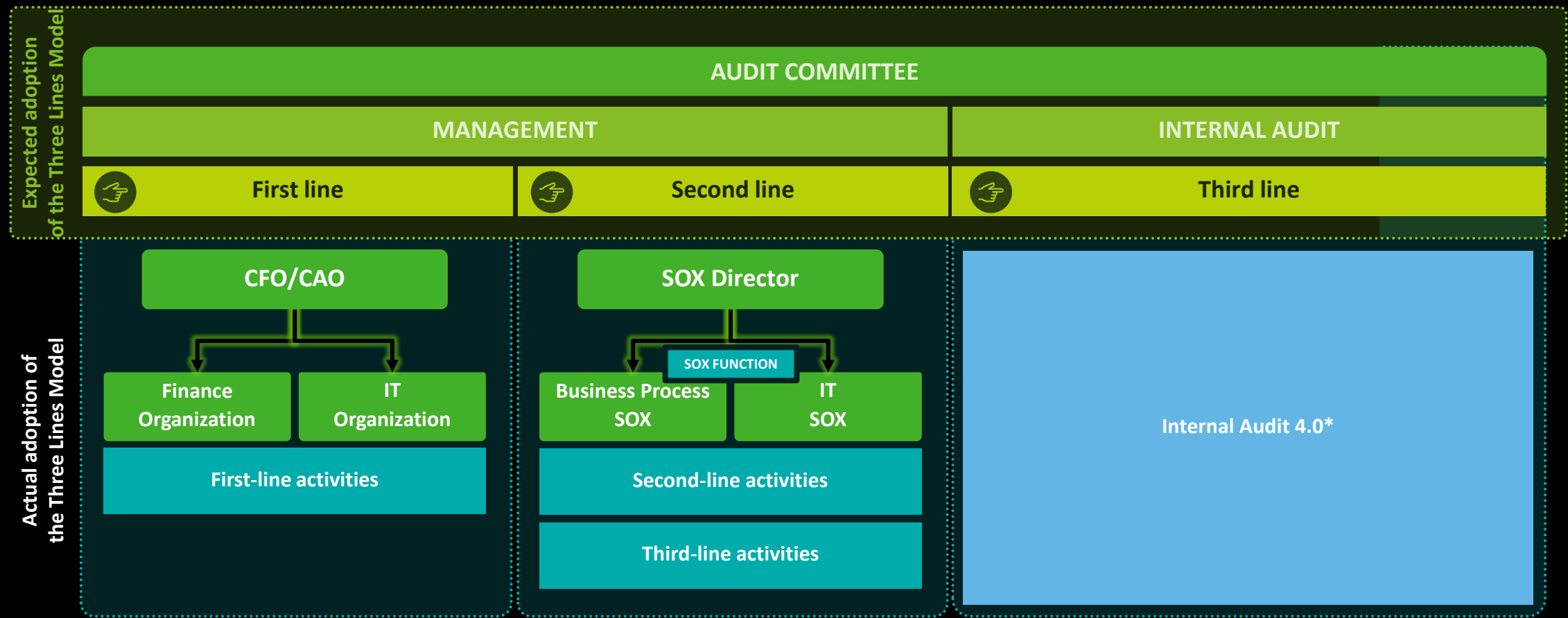


*CFO – chief financial officer, CAO – chief accounting officer, CAE – chief audit executive

Option 2: Assurance in the third line and a ‘SOX function’ in the second line



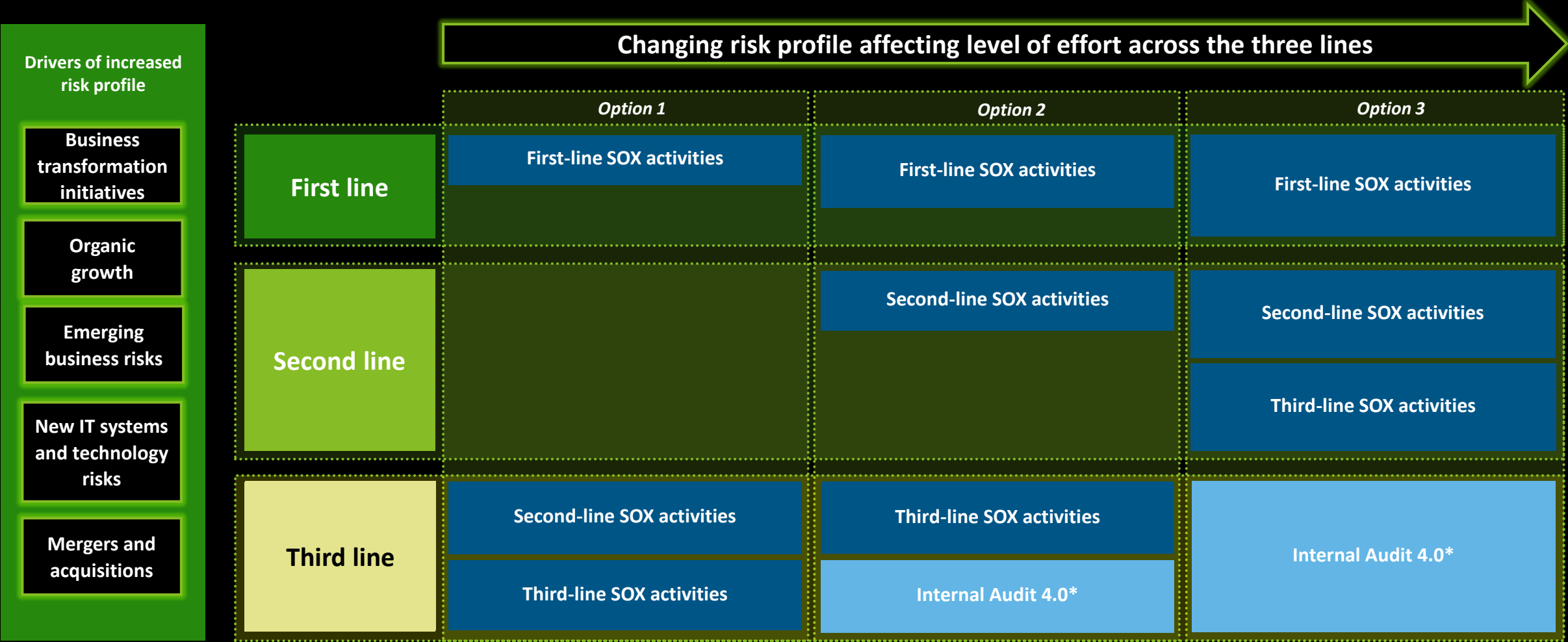
Option 3: SOX function 'owns' SOX, sitting in the second line



* See Appendix for more details on Internal Audit 4.0

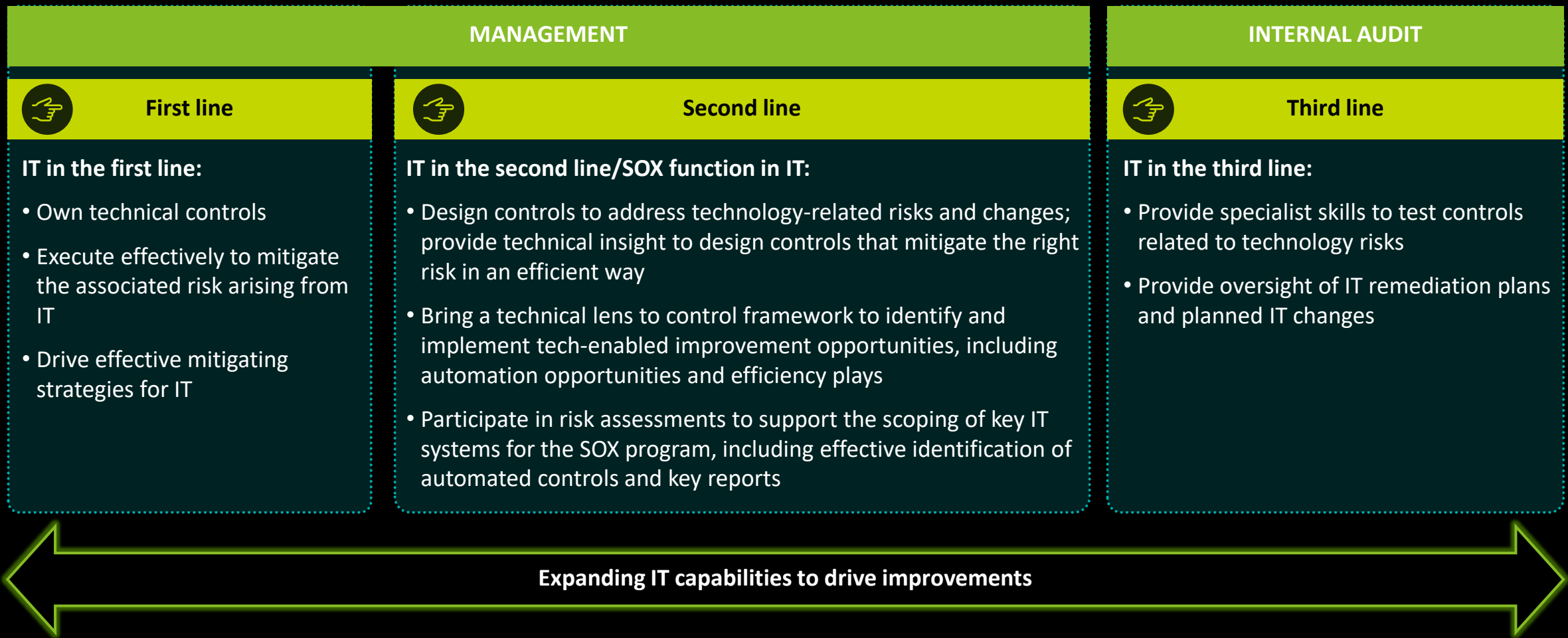
Third line – Internal Audit’s Role in SOX: Changing risk profile considerations

Within the Three Lines Model, it is critical to have the right people in place to manage risks (first line), monitor risks (second line), and provide independent assurance (third line). As organizations experience an increase in their risk profile, this can mean pressure for the third line to explore more strategic initiatives, including operational and compliance audits to drive further value for stakeholders. This change in risk profile can push organizations to change how SOX programs operate across the three lines.



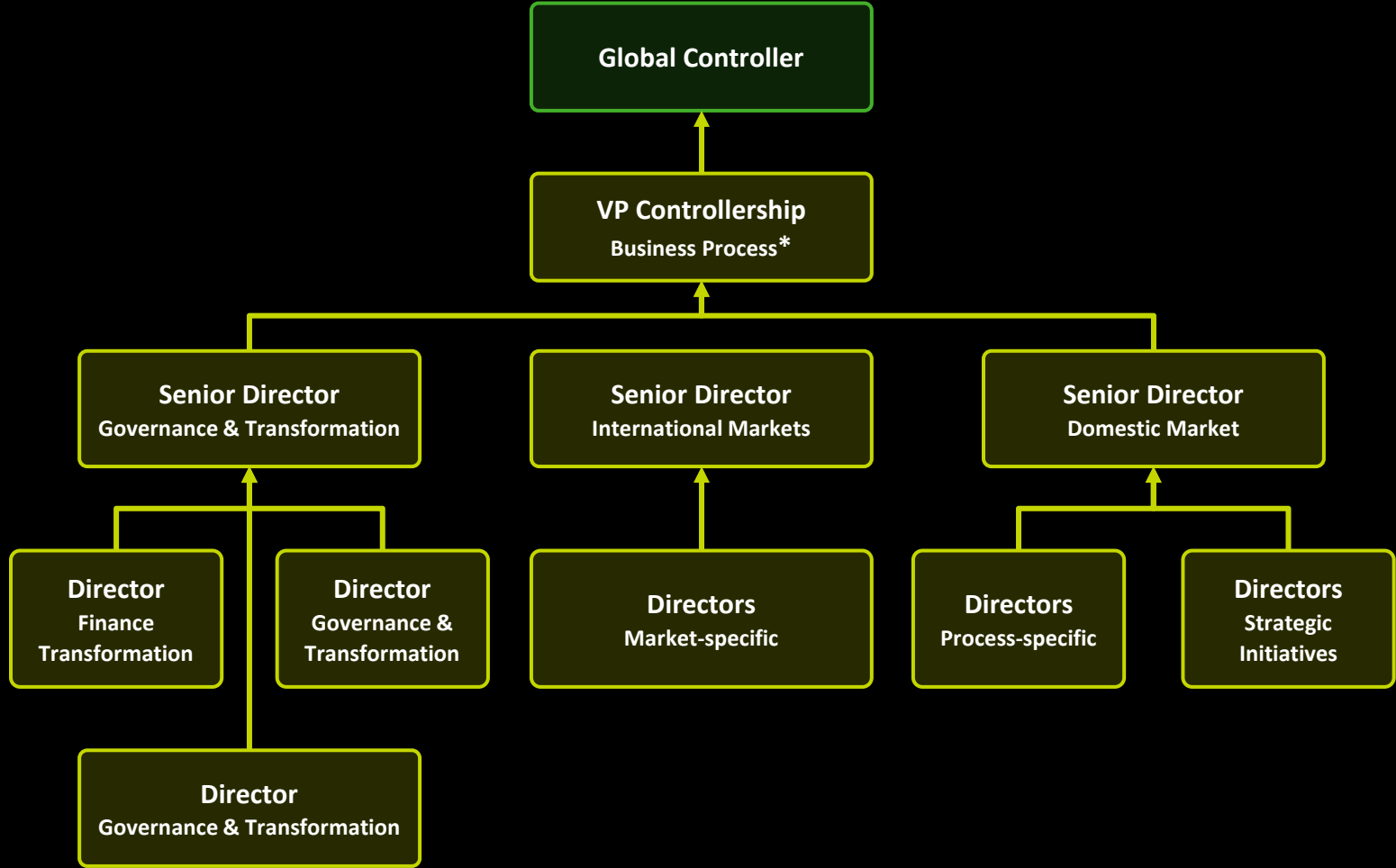
Deploying IT in the SOX environment

The placement of IT skills within a SOX program is an important decision to drive value for the program. Below we explore some typical IT skills that SOX programs should consider placing across the traditional three lines in order to drive efficacy and effectiveness of the SOX program. While many organizations typically place IT skills at the heart of both the first and third lines, expanding IT skills within the second line can have positive impact for both the efficiency and effectiveness of SOX programs and drive continuous improvement for the control program.



Building SOX in the second line: Case studies

SOX program controllership structure: Case study 1



NOTE: The organization depicted here primarily focuses on business process controls and serves as the main point of contact for inquiries with internal and external auditors. IT risk and compliance assessments and audit support for IT general controls are managed by a separate team and are under client’s technology team and not under controllership.

WORKSTREAM PRIORITIES



Governance and Transformation

- Projects: Business process risk assessment and control implementation/assessment for multi-year, multi-market transformation projects
- SOX modernization initiatives
- Analytics
- Annual SOX scoping
- SOX certification management

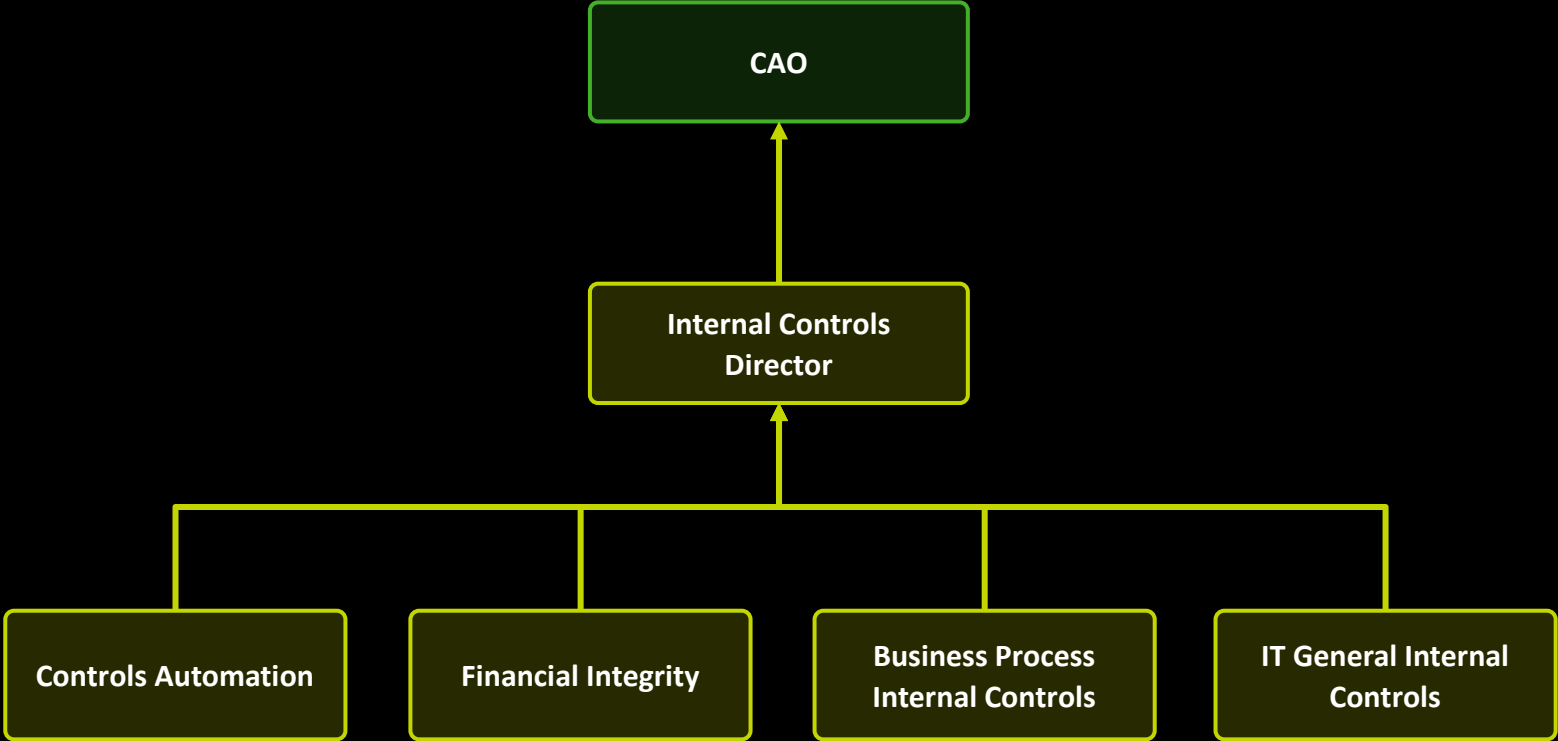
International Markets

- Projects: Business process risk assessment, control implementation/assessment for international markets (non-US)
- Steady state: Maintain controls and related documents, liaison with IA/external audit
- Market-specific SOX deficiency management

Domestic Market

- Projects: Business process risk assessment, control implementation/assessment for US market and corporate transformation projects
- Steady state: Maintain controls and related documents, liaison with IA/external audit
- US specific SOX deficiency management
- SOX assessment of other strategic initiatives (e.g., new revenue streams)

SOX program controllership structure: Case study 2

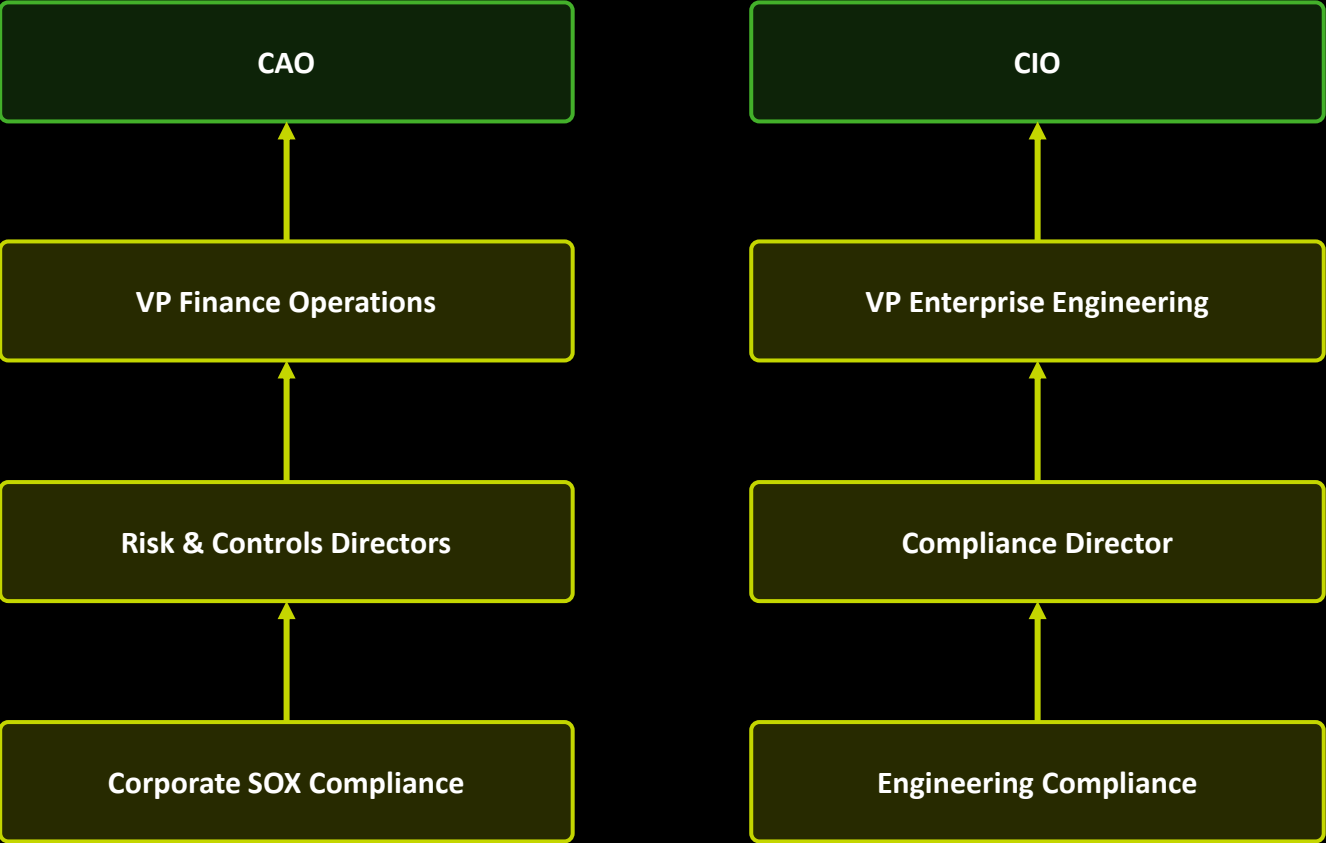


WORKSTREAM PRIORITIES



- Second-line Internal Controls Team**
 - Second-line responsibilities in this model focus primarily on SOX, with more than 40 FTEs
- Controls Automation**
 - Responsible for control automation programs, including continuous controls monitoring
- Financial Integrity**
 - Identify system implementations to determine if there is a financial impact
 - Support implementation considerations
- Internal Controls (Business Process and IT)**
 - Ownership of the GRC platform to support risk management and SOX activities
 - Focus is on SOX coordination activities, including scoping of controls, design of controls, reporting, and remediation
 - Responsible for coordinating with control owners for quarterly control self-assessments

SOX program controllership structure: Case study 3



WORKSTREAM PRIORITIES



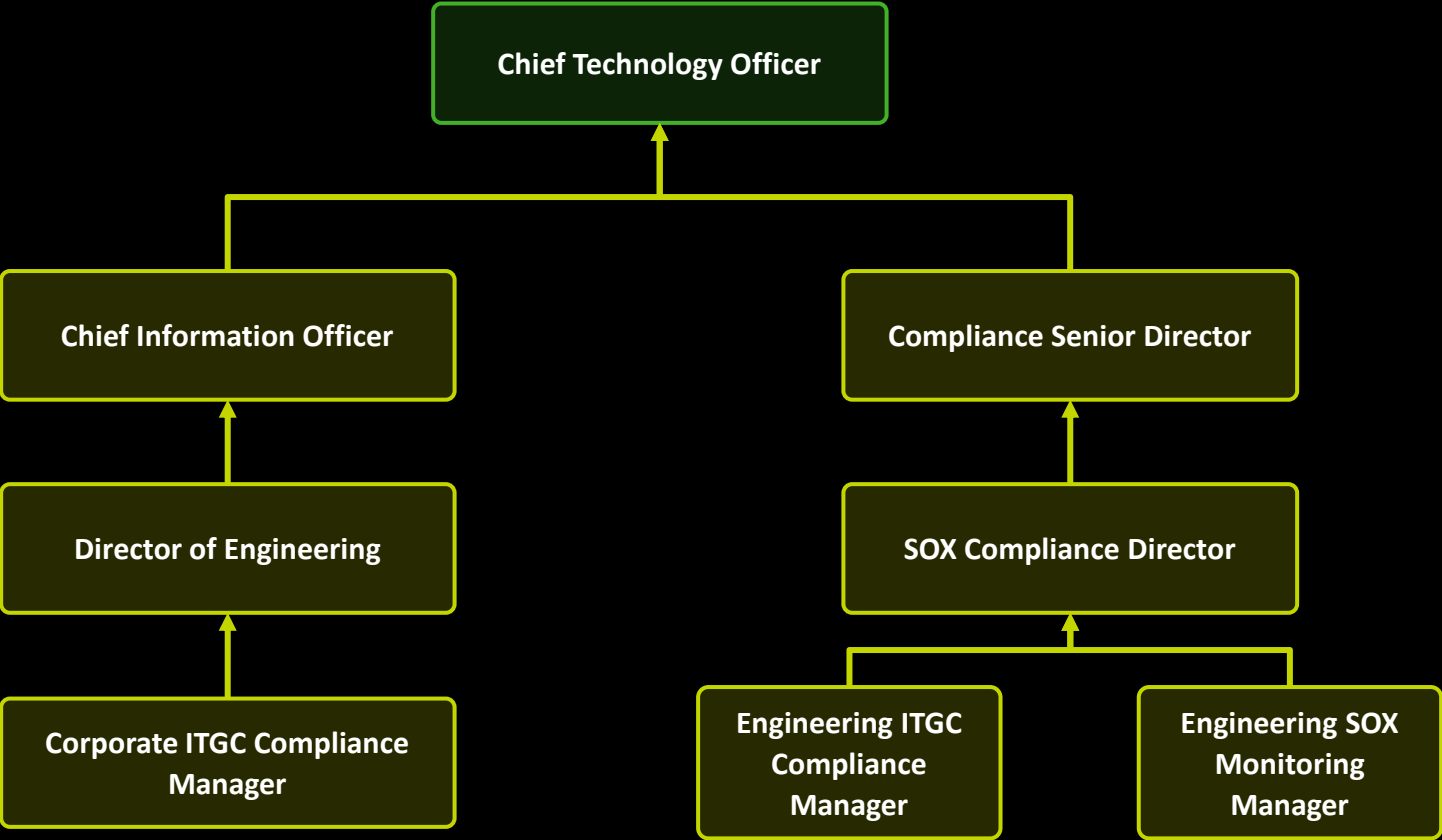
Reporting to CAO

- Revenue operations and controllership
- Work with first line to monitor risk and control activities
- Advise in the design and implementation of controls used to mitigate risk

Reporting to CIO

- Responsible for control automation programs, including continuous controls monitoring.
- Performance of user access review controls
- Identify system implementations to determine if there is a financial impact; support implementation considerations
- Maintain and rationalize list of in-scope SOX systems

IT SOX program controllership structure: Case study 4



WORKSTREAM PRIORITIES



Reporting to the CIO

- Provide oversight/checks and balances on first line
- Deliver tools and training

Reporting to the Compliance Senior Director

- Advise on development and maintenance of risk management policies and processes
- Help identify and monitor new and emerging risks
- Oversee implementation of the enterprise risk management model
- Work with Internal Audit to understand compliance requirements and design controls
- Liaison between Internal Audit and External Audit
- Assist in the design and implementation of controls
- Perform SOX readiness assessments in coordination with Internal Audit
- Lead collection of supporting evidence in response to audit requests
- Coordinate remediation efforts for identified deficiencies

Contacts: Deloitte's SOX Center of Excellence



Patty Salkin
Managing Director
psalkin@deloitte.com
+1 609 806 7279



Sandra Teixeira
Managing Director
sateixeira@deloitte.com
+1 914 564 4040



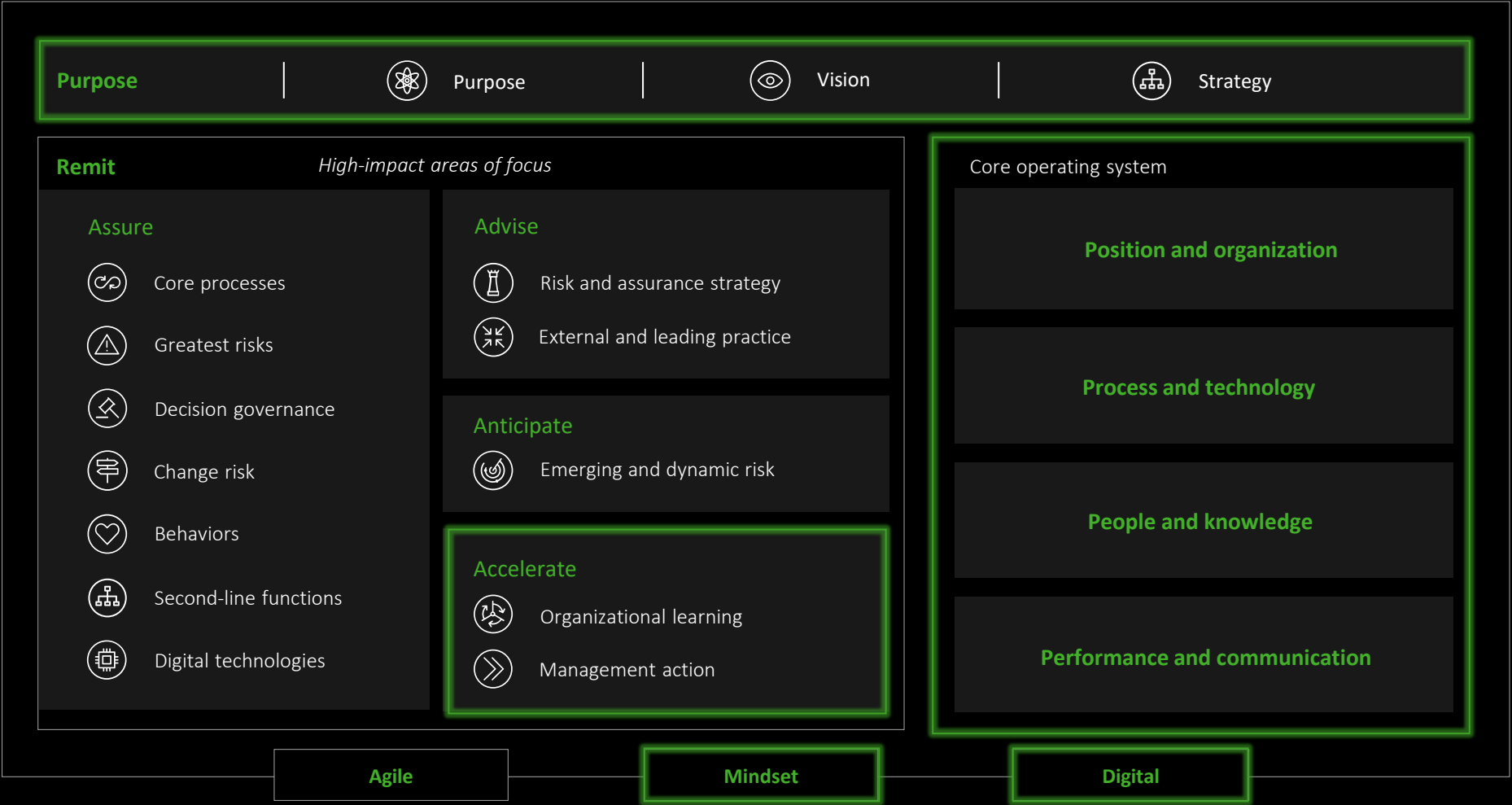
Jack Dean
Senior Manager
jacdean@deloitte.com
+1 703 251 3775



Will Gullette
Senior Manager
wgullette@deloitte.com
+1 469 644 5379

Appendix: Deloitte's Internal Audit 4.0 Model

Purpose driven, digitally powered



What's new?

Starts with purpose, aligning Internal Audit's role and remit with the organization's purpose, a new orientation for many functions.

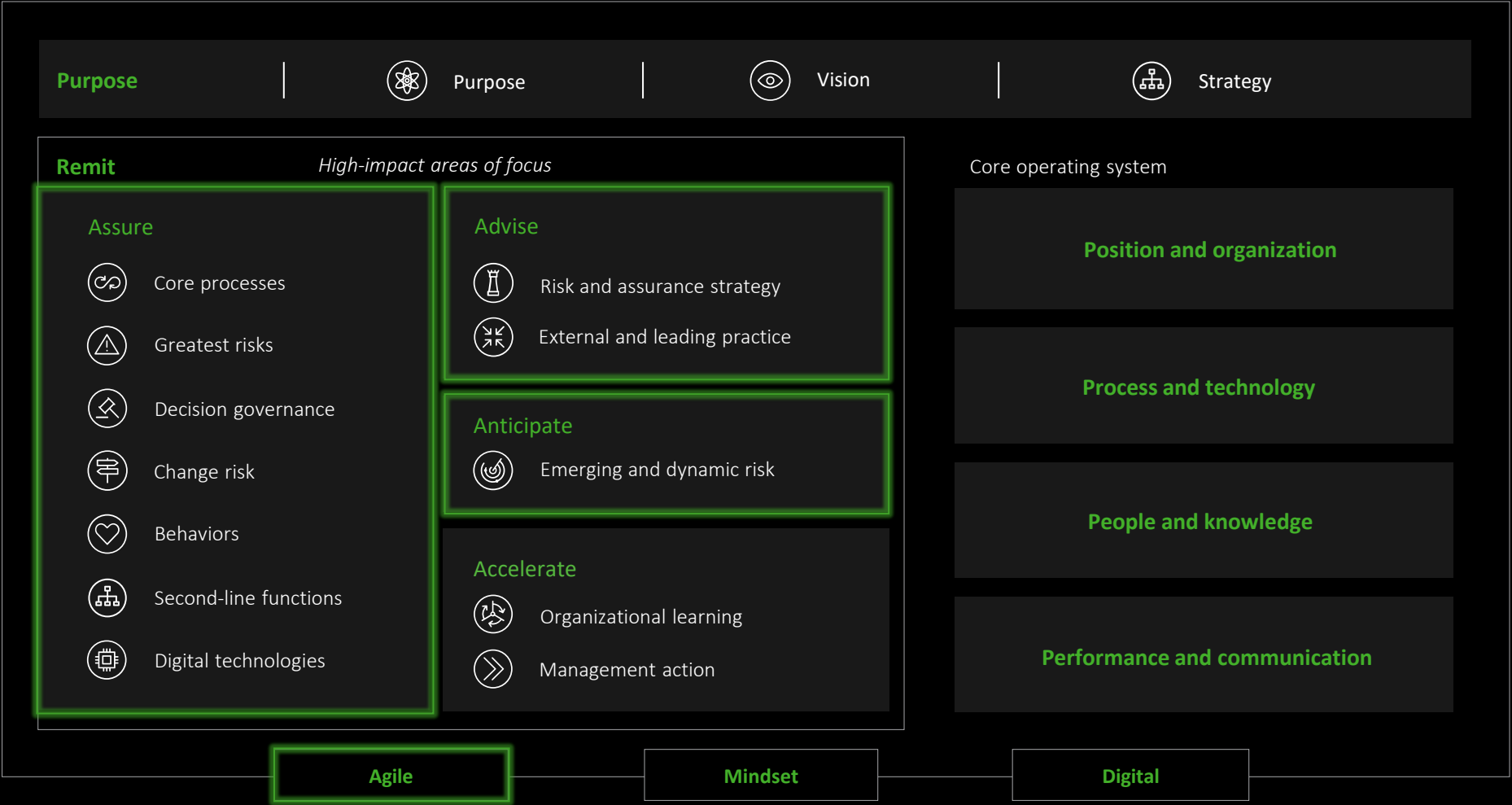
Challenges Internal Audit functions to add Accelerate (a fourth "A") to the remit to support organizational learning and management action in ways that match today's pace of change.

Fully embraces the use of digital technologies across the life cycle to help drive insights, collaboration, quality, and productivity.

Promotes a continuous improvement mindset that enables agility and digitalization through encouraging purposeful and structured focus on incremental improvement.

Outlines the key principles and building blocks that functions need to consider as they design, build, and evolve their operating models.

Purpose driven, digitally powered



What stays the same?

Assurance
At the core of Internal Audit's role, remit, and value; providing organizations the confidence to grow responsibly.

Advice
Timely and helpful advice to help management through challenge, insight, external perspectives, and an objective point of view.

Anticipation
Forward looking, driving sustainable and future-focused improvements in risk, governance, and control.

Agility
Embracing agile principles, values, and mindsets to drive high performance, continuous improvement, innovation, and stakeholder engagement.



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.