

ESTABLISHING, OPERATING, AND IMPROVING YOUR 2ND LINE PROGRAM

4/26/2024

Speaker Bio – J.P. Cook



J.P. is an Associate Director in Protiviti's Internal Audit and Financial Advisory practice in Tampa, FL with over 15 years of Protiviti work experience. During his tenure he has worked in in both 2nd and 3rd line of defense with a focus on SOX, Operational Audits and Compliance. J.P. has worked in many facets of IT Internal Controls, gaining experience not only performing the day-to-day tasks but also overseeing large, multiple year engagements for both domestic and international companies.



Speaker Bio – Steve Smith



Steve is a Senior Manager within the Internal Audit & Financial Advisory practice based in the Tampa office. Steve supported the IT compliance function of a \$2 billion company in the Services sector. He assisted in developing the functions' standard operating procedures, SOX compliance processes, and reporting to executive level management. He has also worked on a number of IT SOX (ITGC/ITAC) engagements, SOC2 Readiness, Cybersecurity and risk based IT Audits. Steve has worked with clients across industries including Financial Services, Manufacturing, and Aviation.



protiviti®

Join at menti.com | use code 9546 2954

 Mentimeter

Which Line of Defense (LoD) does your role align with?



1st LoD
(Management /
Ownership)

2nd LoD
(Governance /
Compliance)

3rd LoD (Internal
/ External Audit)



Join at menti.com | use code 9546 2954

Mentimeter

What is the role of the 2nd LoD at your organization?



Strongly disagree

Risk & Control Design

Issue Management

Control Monitoring

3rd Party Risk Management / SOC Reviews

In the way

Strongly agree

Menti

Join at menti.com | use code 9546 2954

Mentimeter

What is your organization's 2nd LoD objective or value add?

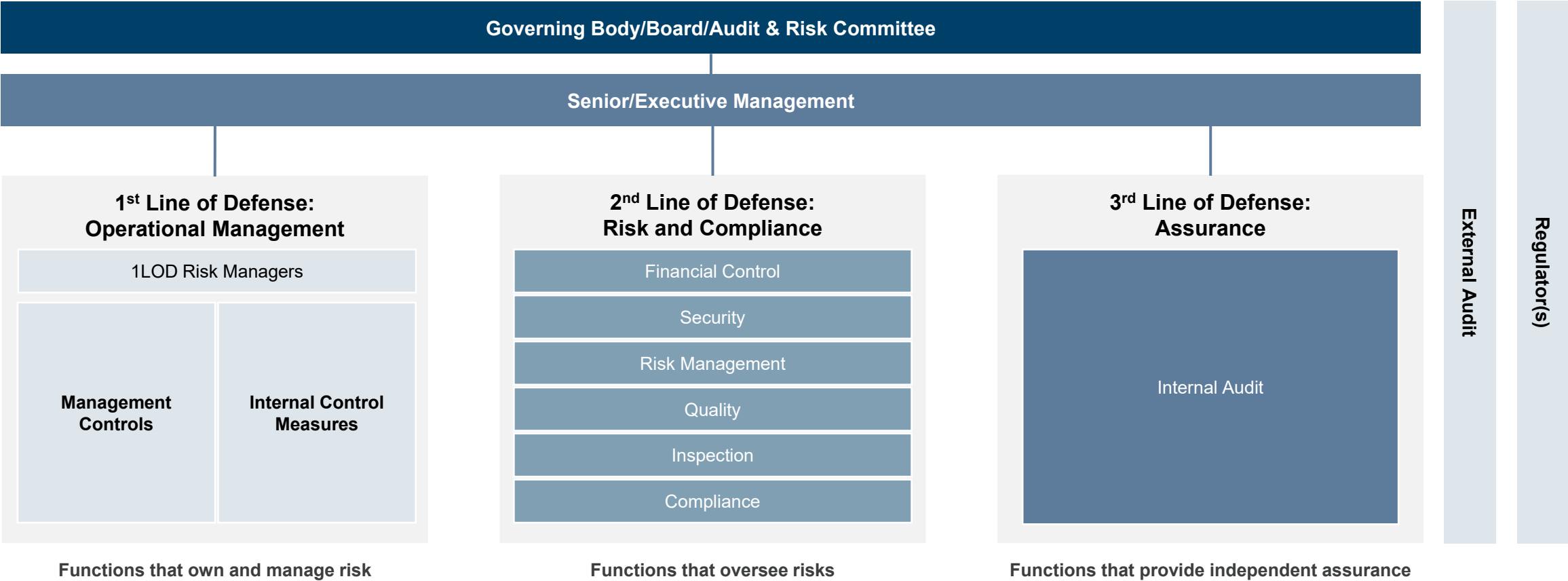




Second Line Overview

Risk Governance – Organizational Structure

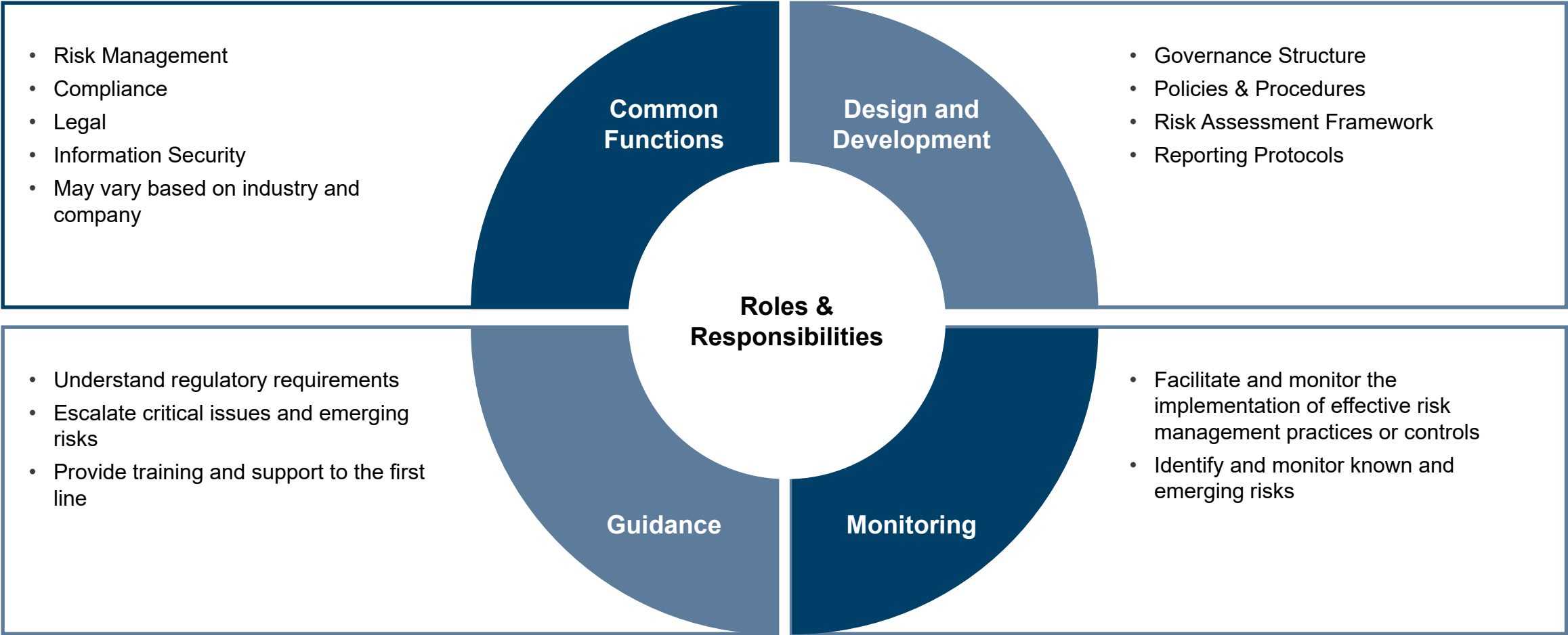
The governance structure reflects the oversight and accountability for risk issues, from individual roles and responsibilities to management committee structures and oversight by the board of directors.



Source: [IIA](#) (Institute of Internal Auditors)

Second Line of Defense Oversight Functions

The objective of the second line is to support management by bringing expertise, process excellence, and management monitoring alongside the first line to help ensure that risk and controls are effectively managed.



Establishing

Steps to Establish

Define the Objective

The overall vision and goals should be simple, clear, and aligned with the organization's risk management framework and strategic objectives.



Identify Key Functions

Determine how the second line of defense will support the risk profile of the organization, including specific workstreams or initiatives.



Develop Policies and Procedures

Design realistic policies, standards, and processes for the entire organization; develop and implement these artifacts by starting with high-impact areas.



Establish a Governance Structure

Formulate a governance structure that defines roles & responsibilities, reporting lines, decision-making processes, and accountability.



Build a Team

Identify professionals with expertise in risk management, compliance, audit, and related fields. Look for a diversity of skills and backgrounds to provide comprehensive coverage.



Implement a Risk Assessment Framework

Develop a risk assessment framework to identify, assess, and prioritize key risks faced by the organization. Utilize risk assessment tools and methodologies to quantify and prioritize risks based on their likelihood and potential impact.



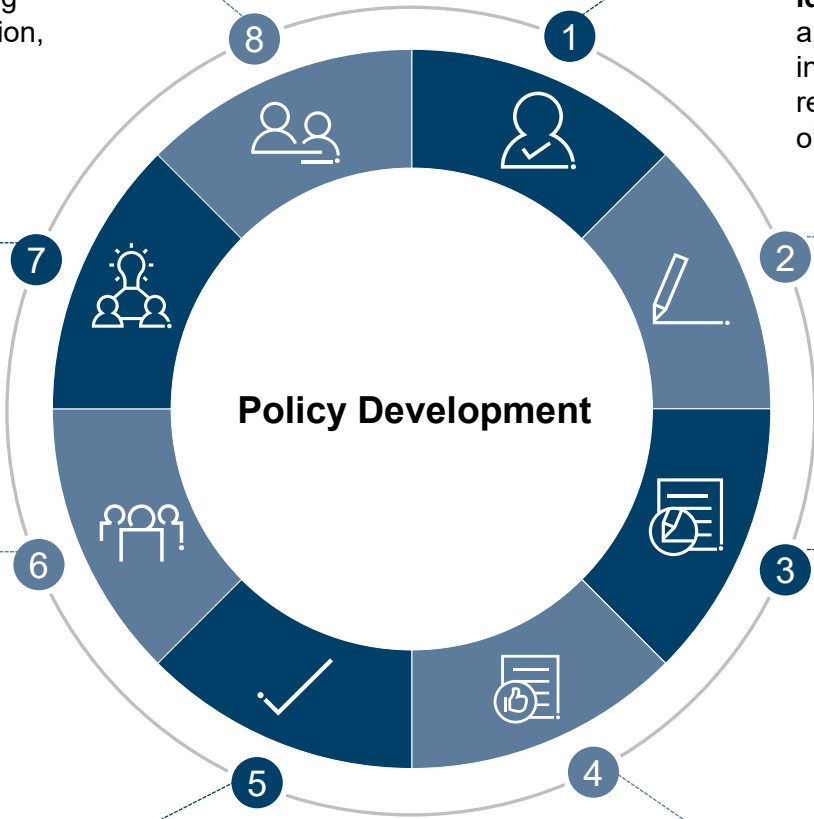
Policy Development

Review and Monitor - Establish mechanisms for ongoing monitoring, evaluation, and review of policy implementation,

Implement - Execute the implementation plan, allocating resources, assigning responsibilities, and providing necessary training and support to ensure seamless integration of the policy into organizational processes and practices.

Communicate - Develop a strategic communication plan to disseminate the approved policy to relevant stakeholders, ensuring clear and consistent messaging, and providing guidance on implementation and compliance.

Submit for Approval - Present the finalized policy document to appropriate decision-making bodies or authorities for review and approval.



Identify Need and Initiate - conduct thorough research and analysis to pinpoint the specific issue or area where policy intervention is necessary, then initiate discussions with relevant stakeholders to garner support and identify key objectives

Plan - Formulate a comprehensive plan outlining the objectives, scope, timeline, and resources required for policy development, ensuring alignment with organizational goals and compliance with legal and regulatory frameworks.

Develop and Draft - Collaborate with subject matter experts and stakeholders to draft the policy document, incorporating best practices and stakeholder input to ensure clarity, effectiveness, and feasibility

Review - Review the draft policy document to identify potential gaps, inconsistencies, and areas for improvement, seeking feedback and adjusting the policy accordingly.

Example Roles

Chief Risk Officer (CRO)/Director of Enterprise Risk Management



Role: Oversees the risk management function within the organization, providing strategic direction and leadership to the second line of defense team.
Responsibilities:

- Develop and implement the organization's risk management framework and policies.
- Identify, assess, and prioritize key risks across all business functions and activities.
- Report risk exposures and mitigation strategies to senior management and the board of directors.
- Ensure compliance with regulatory requirements and industry standards.
- Coordinate with internal audit, compliance, and other stakeholders to address risk-related issues.

Compliance Officers/Managers



Role: Ensuring that the organization adheres to applicable laws, regulations, and internal policies.
Responsibilities:

- Maintain compliance policies, procedures, and controls.
- Conduct compliance risk assessments and monitor regulatory developments.
- Provide guidance and support to business units on compliance matters.
- Conduct compliance training and awareness programs for employees.
- Investigate and resolve compliance issues and violations.

Risk Manager



Role: Identifying, assessing, and mitigating risks within specific areas of the organization.
Responsibilities:

- Conduct risk assessments to identify and evaluate potential risks.
- Develop risk mitigation strategies and action plans.
- Monitor and report on key risk indicators and trends.
- Coordinate risk management activities with business units and other stakeholders.

Control Assurance Specialist



Role: Assessing the effectiveness of internal controls and ensuring compliance with policies and procedures.
Responsibilities:

- Design, execute, and report control testing programs to evaluate the adequacy of internal controls.
- Identify control deficiencies and recommend remediation actions.
- Coordinate with internal audit and external auditors on control-related matters.

Operating

Key Activities

Risk Assessment Framework Methodology

Implementing a risk assessment framework is a critical step in establishing effective risk management within an organization's second line of defense. Below are detailed steps on how to implement a risk assessment framework, along with key considerations from management:

Define Objectives and Scope	<p>Clearly defined scope and objectives drive purposeful and focused efforts. Determine the focus areas, such as operational, financial, compliance, or strategic risks.</p> <p><u>Considerations:</u> Ensure alignment with organizational goals and priorities. Engage with key stakeholders to gather input on risk areas of concern.</p>
Identify & Assess Risks	<p>Identify potential risks within the defined scope using various techniques such as brainstorming sessions, historical data analysis, interviews with subject matter experts, and review of industry standards and regulatory requirements. Utilize risk assessment tools to evaluate risk on likelihood and potential impact.</p> <p><u>Considerations:</u> Encourage open communication and participation from all relevant departments and levels of the organization. Prioritize risks based on their potential impact and likelihood considering both qualitative and quantitative factors.</p>
Determine Tolerance	<p>Define the organization's risk appetite and tolerance levels, i.e., the amount of risk the organization is willing to accept or tolerate to achieve its objectives.</p> <p><u>Considerations:</u> Align risk appetite with the organization's strategic goals, values, and stakeholders' expectations. Establish clear thresholds for acceptable levels of risk.</p>
Mitigate Risk	<p>Develop risk mitigation strategies and action plans to address identified risks. Determine appropriate risk responses, including avoidance, mitigation, transfer, or acceptance.</p> <p><u>Considerations:</u> Prioritize mitigation efforts based on the severity and urgency of risks. Allocate resources effectively to implement mitigation measures.</p>
Monitoring and Improvement	<p>Establish a process for ongoing monitoring to track changes in risk exposure over time. Implement metrics to measure the effectiveness of risk mitigation efforts. Evaluate and improve the risk assessment framework based on lessons learned, feedback from stakeholders, and changes to the environment.</p> <p><u>Considerations:</u> Establish a cadence for regular review of the risk assessment framework. Encourage feedback for improvement from all levels of the organization.</p>
Report and Communicate	<p>Communicate risk assessment findings, including identified risks, mitigation strategies, and risk exposure levels, to senior management, the board of directors, and other stakeholders.</p> <p><u>Considerations:</u> Present risk information tailored to the needs of different audiences. Highlight risks and trends that may impact the organization's objectives.</p>

Risk Identification & Assessment

01

Identify Risk

- Utilize **established risk management frameworks** such as COSO (Committee of Sponsoring Organizations of the Treadway Commission) or ISO 31000 to systematically identify risks within the second line program, **ensuring a structured approach** that considers internal controls, compliance requirements, and industry best practices.
- Conduct interviews with stakeholders to understand business processes.



02

Assess Risk

- Conduct thorough risk assessments using predefined criteria such as **likelihood and impact** to evaluate the significance and urgency of identified risks.
- Employ **qualitative and quantitative** risk analysis techniques, including risk matrices and scenario analysis, to assess the potential consequences and likelihood of occurrence associated with each identified risk.



03

Control Risk

- Develop and implement a tailored set of controls and mitigation strategies aimed at addressing the specific characteristics and root causes of identified risks.
- Ensure that controls are designed to prevent, detect, and mitigate risks effectively, aligning with organizational objectives and regulatory requirements.
- Quantify risk tolerance using metrics or thresholds



04

Review Controls

- Establish a systematic process for monitoring and reviewing implemented controls to ensure their ongoing effectiveness and relevance.
- Conduct periodic audits, assessments, and reviews of control activities to identify any gaps, weaknesses, or emerging risks, enabling timely adjustments and enhancements to maintain control effectiveness



Control Design, Evaluation, Monitoring



Control Design - Crafting frameworks and procedures to mitigate risks and enhance compliance. This includes establishing clear control objectives, designing control activities **tailored to specific risks**, and implementing mechanisms for monitoring and enforcement. The design process should integrate input from stakeholders, leverage industry best practices, and consider the **organization's capabilities** unique risk profile and **regulatory requirements** to ensure effectiveness.



Control Evaluation - Assessing the design and operating effectiveness of control activities. This involves conducting reviews and assessments to verify whether controls are adequately **designed to address** identified risks and whether they are **operating effectively**. Evaluations could include various methods such as testing, sampling, and analysis of control documentation and operational data to provide assurance over the control environment. These could be evaluated by the **third-line or external parties**.



Control Monitoring – Continuous oversight to detect deviations from established control objectives and identify emerging risks or vulnerabilities. This includes establishing monitoring protocols, employing automated tools and technologies for continuous monitoring, and conducting periodic reviews and audits. Monitoring efforts should be proactive, responsive, and adaptive, enabling timely detection of control deficiencies or breakdowns and facilitating corrective action to mitigate potential impacts on the organization.

Advising, Training, Awareness



Training Programs – On an annual basis, utilize a variety of training methods, including in-person sessions, online modules, and interactive workshops, to accommodate diverse learning preferences and ensure maximum engagement and retention.



Advisory Service - Utilize a dedicated advisory service that provides employees with timely guidance and support on navigating the complexities of the second line program and addressing compliance-related issues

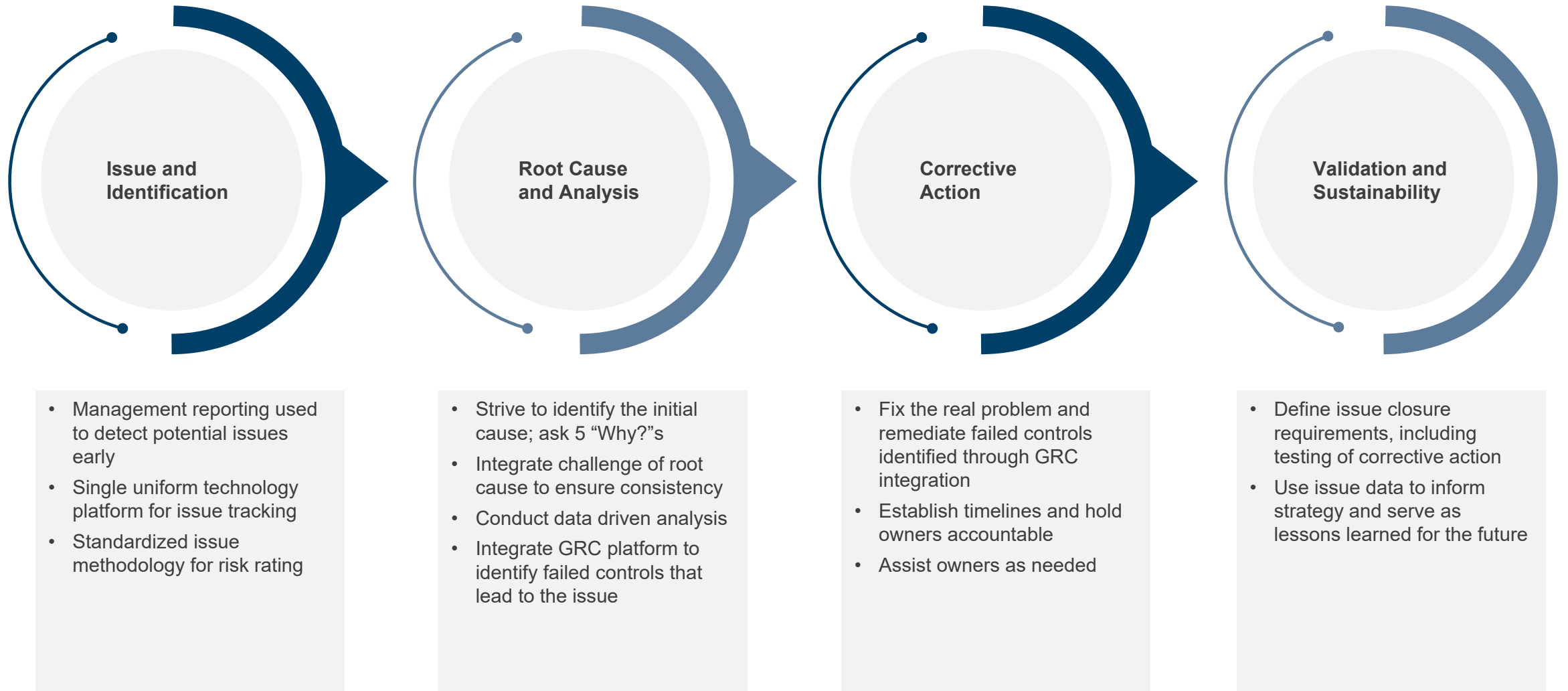


Real Scenarios - Incorporate real-life examples, case studies, and success stories into awareness initiatives to illustrate the relevance and impact of the second line program on day-to-day operations and organizational goals.



Identify Needs – Assess needs within employee roles and levels within the organization. This ensures that each individual receives relevant and targeted instruction on the specific aspects of the second line program relevant to their responsibilities

Issue Management Lifecycle Components



Reporting



Stakeholder Communication

Establishing clear channels of communication with stakeholders to facilitate timely dissemination of reports, address inquiries, and solicit feedback for continuous improvement.

Technology Automation

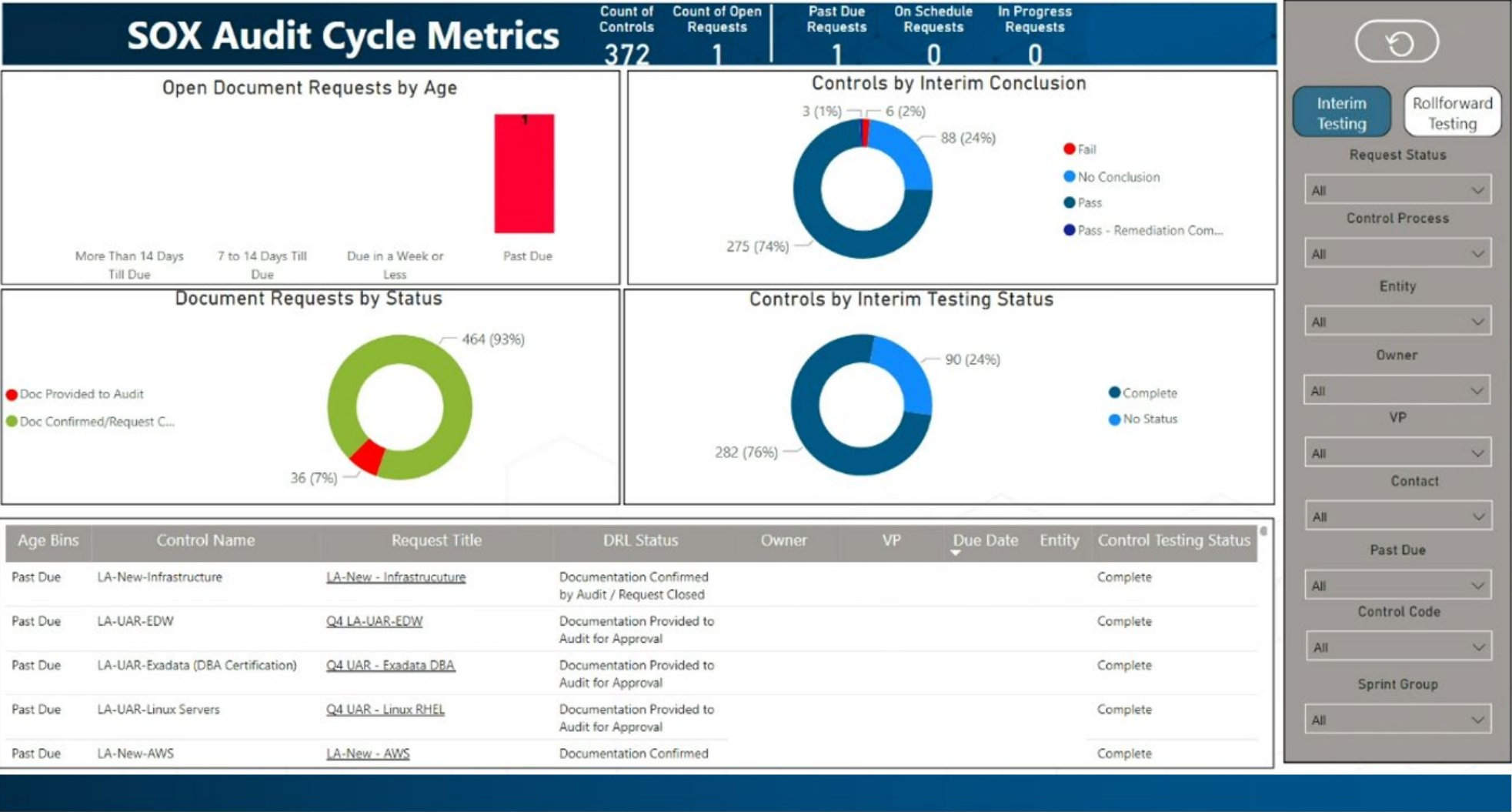
Leveraging technology and automation tools to streamline reporting processes, enhance data accuracy, and minimize manual effort.

Continuous Improvement

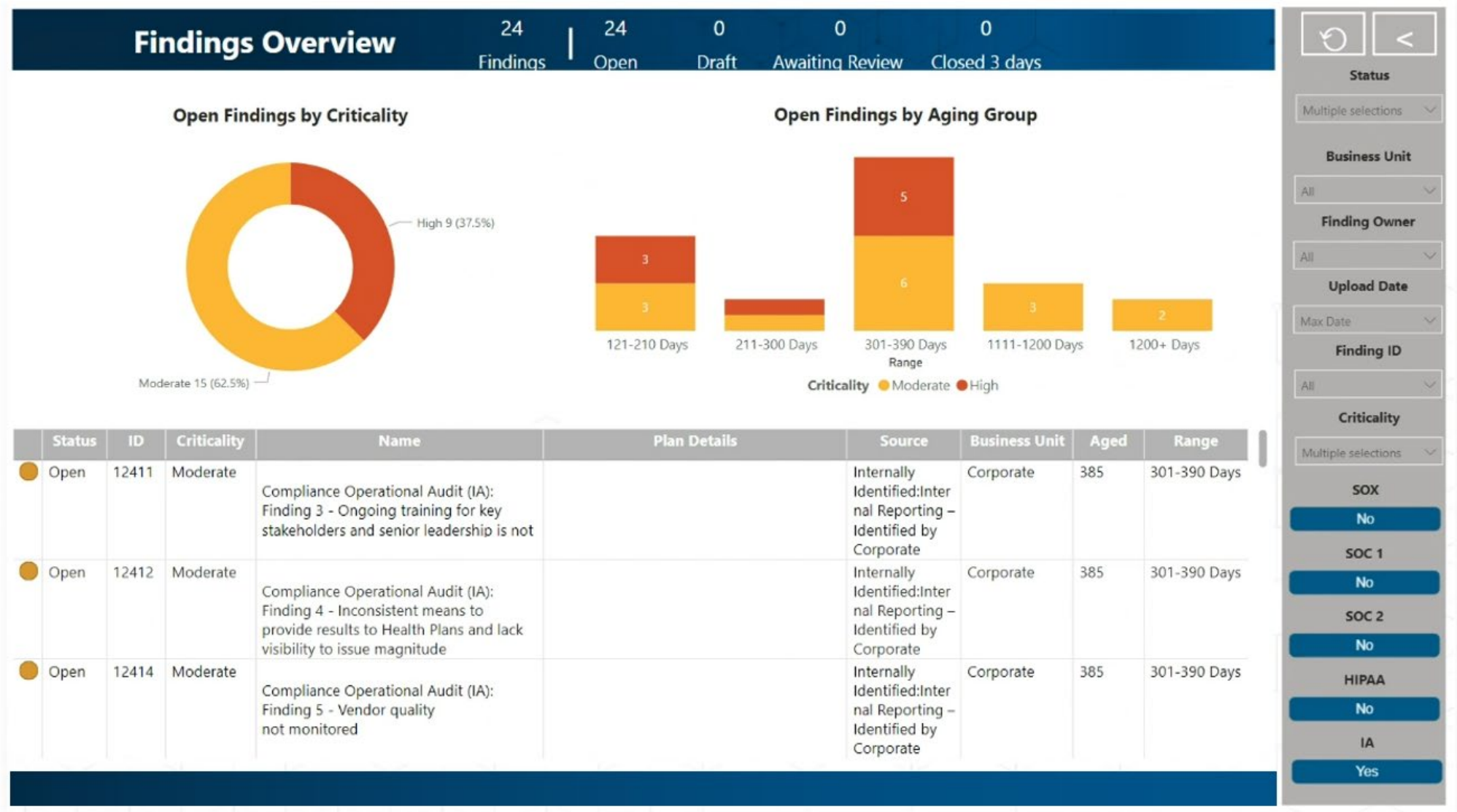
Establishing mechanisms for ongoing monitoring, evaluation, and enhancement of reporting practices based on feedback, lessons learned, and emerging trends or requirements.



Reporting



Reporting



Join at menti.com | use code 9546 2954

 Mentimeter

Does your 2nd / 3rd LoD have good relationships with 1st LoD?



Yes

No

Unsure



Join at menti.com | use code 9546 2954

 Mentimeter

What drives good relationships with 1st LoD?



transpiration
leader bold inspiration
creative
fast focus



Importance of communication with first line and third line

First Line

- **Effective communication** between the first and second lines ensures alignment of objectives, priorities, and expectations. Clear **communication channels** enable the first line to understand risk management requirements and expectations, facilitating collaboration in implementing controls and addressing identified risks.
- First line communication **enables timely reporting** of emerging risks, incidents, and control deficiencies to the second line. This ensures that risks are promptly identified, assessed, and escalated as necessary, **enabling proactive** risk management and decision-making to mitigate potential impacts on the organization

- Communication between the third line and the second line provides **independent assurance** on the effectiveness of risk management and control activities. Through regular dialogue and reporting, the third line gains insight into the second line's oversight processes, enabling it to assess the adequacy of controls and provide objective assurance to senior management and stakeholders.
- Third line communication ensures that senior management and **governance bodies are informed of significant risks** and control issues identified by the second line. This **enhances transparency** and accountability in risk management, enabling senior leaders to make informed decisions and allocate resources effectively to address key risk

Third Line



Improving

Continuous Improvement Strategies and Performance Measurement

01

Leadership Support and Commitment

- Resource allocation
- Communication Channels
- Advocacy and Influence (i.e., CEO/CFO endorsement on quarterly townhall of second line defense on effective risk management)

02

Cross-Functional Collaboration and Knowledge Sharing across 3LOD

- Collaboration Framework (Roles/Responsibilities)
- Joint Risk Assessment
- Feedback/Lessons learned

03

Benchmarking Against Industry Standards

- Performance Gap Analysis (i.e., compare current state to best practice/industry)
- Maturity assessments

04

Adopt Agile Principles

- Agile methodologies (Scrum, Kanban)
- Cross functional teams

05

Integration of Technology for Efficiency

- GRC tools
- Automation opportunities (i.e., enhance Risk Assessment (s) routine tasks and processes to improve efficiency and accuracy)
- KPIs/KRIs

Innovative Technologies and Tools for Enhancement – Integrated Risk Management Platform



Enhanced Visibility: A comprehensive view of risks across the organization, consolidating data from various sources into a centralized dashboard. This enhanced visibility enables second-line teams to identify emerging risks, trends, and interdependencies more effectively, facilitating proactive risk mitigation strategies and informed decision-making



Streamlined Processes: Automating routine tasks such as risk assessments, compliance monitoring, and incident management. By eliminating manual efforts and reducing administrative burden, second-line teams can focus on strategic initiatives, accelerate response times, and enhance overall efficiency.



Improved Collaboration: These platforms facilitate collaboration and communication among second-line teams and other stakeholders by providing a centralized platform for sharing information, insights, and updates. Through features such as document sharing, task assignment, and discussion forums, team members can collaborate more effectively, fostering a culture of transparency and accountability.



Real-Time Reporting and Analytics: Reporting and analytics capabilities enable second-line teams to generate customized reports and dashboards in real-time. By accessing timely and accurate data, stakeholders can gain actionable insights into risk trends, performance metrics, and compliance status. Empowering informed decision-making at all levels of the organization.



Regulatory Compliance: Integrated Risk Management Platforms help ensure regulatory compliance by providing tools and frameworks to track regulatory requirements, assess compliance gaps, and monitor remediation efforts. By centralizing compliance-related activities and documentation, second-line teams can demonstrate adherence to regulatory standards more effectively

Innovative Technologies and Tools for Enhancement – Control Automation



Increased Efficiency

Control automation streamlines repetitive and time-consuming tasks within the second-line program regarding control testing. By automating control testing, teams can allocate resources more efficiently, reduce manual errors, and focus on higher-value activities.



Enhanced Accuracy

Automation ensures consistent execution of control activities, minimizing the risk of human error and enhancing the accuracy of control testing. By leveraging predefined rules and algorithms, control automation eliminates inconsistencies in data interpretation and reporting, leading to more reliable insights and decision-making.



Compliance Assurance

Control automation helps ensure compliance with regulatory requirements and internal policies by enforcing consistent adherence to control standards and protocols. By automating control testing assessments and documentation processes, organizations can demonstrate compliance more effectively during audits and regulatory inspections, reducing the risk of non-compliance.



Technology Accelerator Platform (TAP)

Accelerate work with an automation and analytics platform.

Leveraging next-gen technologies like custom scripting and RPA, TAP enhances Protiviti's efficiency, deepens engagement insights, supports SOX controls, business process analytics for any ERP, IT General Control testing, and technical audit assessments.

protiviti | Technology Accelerator Platform

Welcome to TAP

The Protiviti Technology Accelerator Platform (TAP) is a self service application that provides users from all solutions the ability to reduce time and effort on tedious tasks via automation.

Click to Begin

- Accelerators
- Find your TAP Champion
- Product Information

View in Action

INTRODUCING

Technology Accelerator Platform

protiviti
Global Business Consulting

More

Request Client Demo
Complete [this form](#) to request a client demo.

Questions or issues?
Contact us at TAP@Protiviti.com

Have an idea?
Submit it to TAP [here](#).

*TAP usage transfers client data to Protiviti servers. Please review client contracts and local data privacy laws to validate TAP submission is appropriate. For any questions, reach out to your Managing Director and/or TAP@protiviti.com. 2023 Protiviti Inc. All Rights Reserved.

SOX

TAP enhances SOX testing with efficient IT general control tests, in-depth business process analytics, and versatile accelerators such as automated SOX Risk Assessment and SOC Report Analyzer accelerators.

Business Process Analytics

TAP's analytics accelerators provide immediate insights, revealing audit findings that might otherwise go unnoticed. They encompass key areas such as general ledger, payroll, accounts payable and integrate with any ERP system.

IT Controls / Assessments

Our accelerators streamline audit testing for critical IT areas, enhancing efficiency in evaluating logical access, firewall configurations, database and operating system assessments, privileged access management, and network security, leading to faster and more comprehensive audits.

TAP Accelerators

Automated ITGC, Standard Business Process Analytics, and SOX control testing

With 35+ accelerators and growing, TAP can accelerate your audits and test full populations, leading to continuous auditing.

TECHNOLOGY AUDIT & ADVISORY			GENERAL	
APPLICATIONS	CYBERSECURITY	CHANGE MANAGEMENT	OTHER TOOLS	
S4 BASIS Testing Workday Configurable Controls Application Access Comparisons & Analytics	Firewall Assessments Privileged Access Management Analysis Active Directory Domain Assessments OS/DB Security & Benchmarking Analysis	ServiceNow Change Management Extraction & Testing	Tickmarking Automation DRL & RCM Generator Teams Planner Board Generator Optical Character Recognition Deliverable Key Word Search	
CLOUD & EMERGING TECH	INFRASTRUCTURE	LOGICAL ACCESS	SOC REPORT ANALYSIS	
AWS Well Architected Framework (WAF) Azure Well Architected Framework (WAF)*	Privileged Access & Passwords Testing for: <ul style="list-style-type: none"> Active Directory Windows AS400 Linux SQL Oracle Database 	Terminations User Provisioning	SOC Report Text Extraction and Analysis Templates	

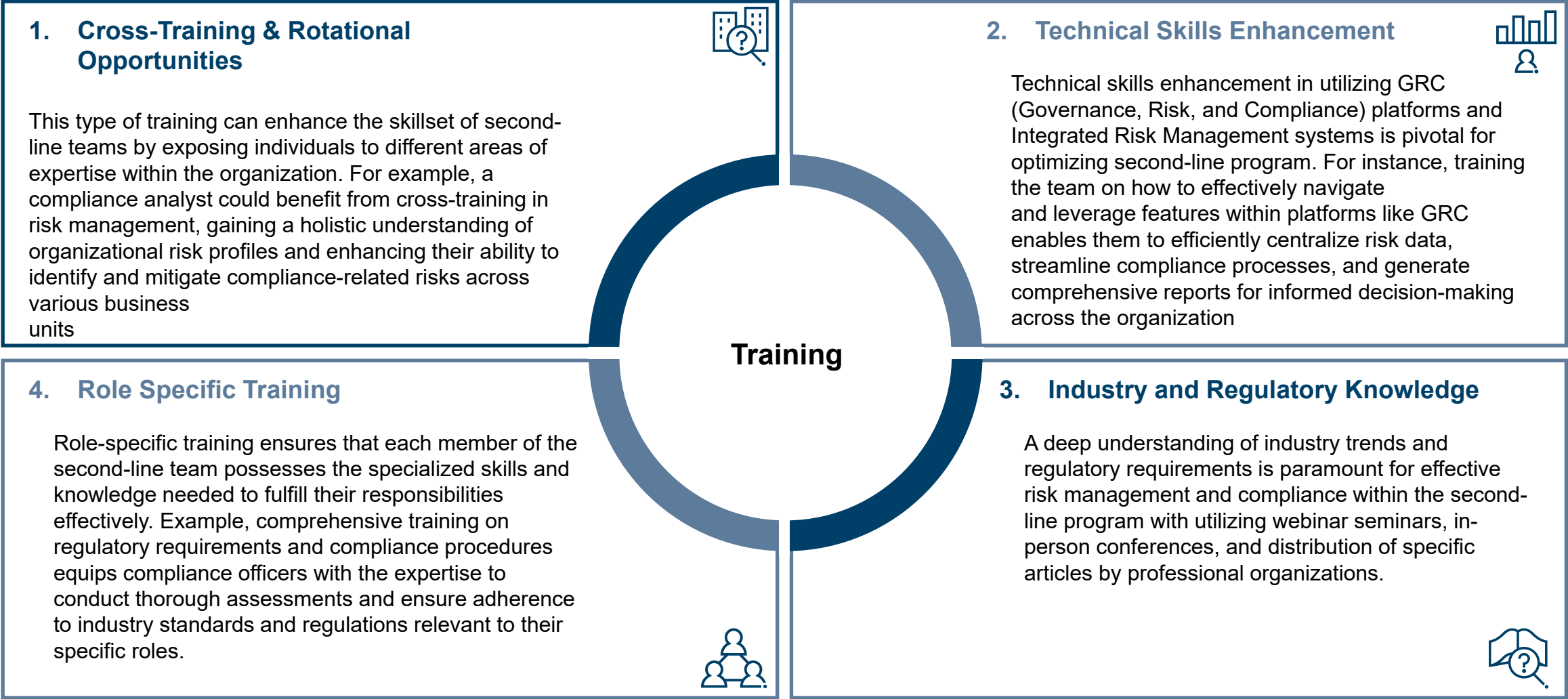
BUSINESS PROCESS AUDIT & ADVISORY		PRODUCTS & TOOLS	
STANDARD ANALYTICS	RISK ASSESSMENT AUTOMATION	CUSTOM DEVELOPED SOLUTIONS	DEVELOPMENT TOOLS
<ul style="list-style-type: none"> Payments Payroll General Ledger Travel & Expenses Revenue* Pricing* 	SOX Risk Assessment Automation & Templates	User Access Review Automation ERP Analytics Analysis & Dashboards Issues Management Audit Lifecycle Management* Controls Recertification & Analytics*	Alteryx UI Path PowerAutomate PowerBI PowerApps ProcessAdvisor Tableau Python Celonis PowerShell SQL and More...

AI Considerations



Future Ready Internal Audit - Are You AI Enabled?

Staff Training and Professional Development



Key Takeaways

- Establish a foundation for the second line guided by clear objectives, a well-defined governance structure and supporting roles to set the team up for success.
- Guide the function with a prescriptive risk assessment framework that defines processes for identifying, assessing, and controlling risk effectively.
- Continuously improve the second line function via coordination across lines of defense, promoting feedback, and enabling innovative technologies.

Q&A

protiviti®

Face the Future with Confidence®

TAMPA CPE DAY

June 14, 2024

7:30 a.m. – 5:00 p.m. ET

Shanna and Bryan Glazer JCC

[Register](#)