Draft

The Institute of Internal Auditors

Organizational Behavior Topical Requirement User Guide

Overview of Topical Requirements

Topical Requirements are an essential component of the International Professional Practices Framework®, along with the Global Internal Audit Standards™ and Global Guidance. The Institute of Internal Auditors requires the Topical Requirements to be used in conjunction with the Global Internal Audit Standards, which provide the authoritative basis of the required practices. References to the Standards appear throughout this guide as a source of more detailed information.

Topical Requirements formalize how internal auditors address prevalent risk areas to promote quality and consistency within the profession. Topical Requirements establish a baseline and provide relevant criteria for performing assurance services related to the subject of a Topical Requirement (Standard 13.4 Evaluation Criteria). Conformance with Topical Requirements is mandatory for assurance services and recommended for evaluation during advisory services. Topical Requirements are not intended to cover all potential aspects that should be considered when performing assurance engagements; rather, they are intended to provide a minimum set of requirements to enable a consistent, reliable assessment of the topic.

Topical Requirements clearly link to The IIA's Three Lines Model and the Global Internal Audit Standards. Governance, risk management, and control processes are the main components of Topical Requirements aligning with Standard 9.1 Understanding Governance, Risk Management, and Control Processes. In reference to the Three Lines Model, governance links to the board/governing body, risk management links to the second line, and controls or control processes link to the first line. While management is represented in both the first and second lines, the internal audit function is depicted in the third line as an independent and objective assurance provider, reporting to the board/governing body (Principle 8 Overseen by the Board).

Applicability, Risk, and Professional Judgment

Topical Requirements must be followed when internal audit functions perform assurance engagements on subjects for which a Topical Requirement exists or when aspects of the Topical Requirement are identified within other assurance engagements.

As described in the Standards, assessing risk is an important part of the chief audit executive's planning. Determining the assurance engagements to include in the internal audit plan requires assessing the organization's strategies, objectives, and risks at least annually (Standard 9.4 Internal Audit Plan). When planning individual assurance engagements, internal auditors must assess risks relevant to the engagement (Standard 13.2 Engagement Risk Assessment).

When the subject of a Topical Requirement is identified during the risk-based internal audit planning process and is included in the audit plan, then the requirements outlined in the Topical Requirement must be used to assess the topic within the applicable engagements. In addition, when internal auditors perform an engagement (either included or not included in the plan) and elements of a Topical Requirement emerge, the Topical Requirement must be assessed for applicability as part of the engagement. Lastly, if an engagement is requested that was not originally in the plan and includes the topic, the Topical Requirement must be assessed for applicability.

Professional judgment plays a key role in the application of the Topical Requirement. Risk assessments drive chief audit executives' decisions about which engagements to include in the internal audit plan (Standard 9.4). Additionally, internal auditors use professional judgment to determine what aspects will be covered within each engagement (Standards 13.3 Engagement Objectives and Scope, 13.4 Evaluation Criteria, and 13.6 Work Program).

Evidence that each requirement in the Topical Requirement was assessed for applicability must be retained, including a rationale explaining the exclusion of any requirements. Conformance with the Topical Requirement must be documented using auditors' professional judgment as described in Standard 14.6 Engagement Documentation.

While the Topical Requirement provides a baseline of control processes to consider, organizations that evaluate the risk topic as very high may need to assess additional aspects.

If a chief audit executive determines that the internal audit function does not have the required knowledge to perform audit engagements on a Topical Requirement subject, the engagement work may be outsourced (Standards 3.1 Competency, 7.2 Chief Audit Executive Qualifications,10.2 Human Resources Management). Even then, outsourcing does not release the internal audit function from its responsibility for conforming with the Topical Requirements. The chief audit executive retains the ultimate responsibility for ensuring conformance. In addition, if the chief audit executive determines internal audit resources are insufficient, the chief audit executive must inform the board about the impact of insufficient resources and how any resource shortfalls will be addressed (Standard 8.2 Resources).

Performance, Documentation, and Reporting

When applying Topical Requirements, internal auditors also must conform with the Standards, conducting their work in alignment with Domain V: Performing Internal Audit Services. The standards in Domain V describe planning engagements (Principle 13 Plan Engagements Effectively), conducting engagements (Principle 14 Conduct Engagement Work), and communicating engagement results (Principle 15 Communicate Engagement Results and Monitor Action Plans).

Topical Requirements are designed to support consistent and high-quality internal audit practices. They are to be applied in conjunction with applicable local laws, regulations, supervisory expectations, and other professionally recognized frameworks, which may impose additional or more specific requirements. Internal auditors may have already developed engagement work programs and testing procedures based on these regulations and frameworks. Internal auditors should reconcile their intended third-party control testing to the Topical Requirement to ensure adequate coverage.

Coverage of the Topical Requirement can be documented in either the internal audit plan or the engagement workpapers based on auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions.

Quality Assurance

The Standards require the chief audit executive to develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the internal audit function

(Standard 8.3 Quality). The results must be communicated to the board and senior management. Communications must report on the internal audit function's conformance with the Standards and achievement of performance objectives.

Conformance with Topical Requirements will be evaluated in quality assessments.

Organizational Behavior

Reframing the Auditing of Culture

> The Topical Requirements use general internal auditing terminology as defined in the Global Internal Audit Standards. Readers should refer to the terms and definitions in the Standards' glossary.

The progression from considering the audit of culture as an abstract and vague topic toward a structured and precise assessment of organizational behavior represents a necessary and timely evolution within the internal audit profession. Despite widespread acknowledgment that cultural deficiencies often underlie significant control failures, this area has not gained meaningful traction in internal audit practices. Reframing auditing "culture" as auditing "organizational behavior misaligned with strategic objectives" provides a clearer, more structured, precise, and auditable foundation. As with any risk, organizations can manage this by designing appropriate controls and implementing them effectively.

The Organizational Behavior Topical Requirement adopts this philosophy, establishing minimum mandatory requirements to assess behavior when a risk assessment determines it is in the scope of review. These requirements are fully compatible with the traditional risk-based audit approach and can be applied, with minimal adaptation, across all audit functions. This companion user guide provides practical examples of how this approach can be embedded into standard audit engagements, as well as guidance on reviewing the broader organizational behavior framework or individual components. This topic's significant influence on organizational objectives demands proactive consideration and adoption.

The definitions of the following key terms are necessary to understand and apply the Topical Requirement. Given the topic's immaturity, organizations use these terms inconsistently. The definitions supplied should help users align their organizations' terminology with the terminology provided in the Topical Requirement and this user guide.

- **behavioral risk** – the risk that behavior is inconsistent with an organization's strategic objectives.
- **conduct** – behavior in relation to regulatory requirements and expectations.
- **culture** – the shared system of values, beliefs, behavior patterns, and drivers that shapes interactions, decision-making, and organizational dynamics. According to Edgar Schein, renowned psychologist specializing in this field, organizational culture is "a pattern of basic assumptions, invented, discovered, or developed by a given group, as it learns to cope with its problems of external adaption and internal integration, that has worked well enough to be considered valid and therefore is to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[1]

1. E. H. Schein, "Organizational culture," *American Psychologist* 45(2) (1990): 109-119, https://doi.org/10.1037/0003-066X.45.2.109.

- **organizational behavior** – the observable actions, decisions, and interpersonal dynamics of individuals and groups within an organization. This behavior influences performance and the achievement of strategic objectives. Simply put, organizational behavior is “the way we do things” and is considered a subset of culture.
- **values** – principles that guide how people are expected to behave.

The mandatory requirements in the Organizational Behavior Topical Requirement and the nonmandatory considerations in this user guide are divided into three sections:

- **Governance** – clearly defined baseline objectives and strategies for organizational behavior that support organizational goals, policies, and procedures.
- **Risk management** – processes to identify, analyze, manage, and monitor risks related to organizational behavior, including a process to escalate incidents promptly.
- **Controls** – management-established, periodically evaluated control processes to mitigate risks related to organizational behavior.

In addition to the Topical Requirement and this user guide, internal auditors may want to consult additional professional guidance on organizational behavior, such as the IPPF’s Global Guidance and other industry-specific resources.

Considerations

Internal auditors may use the following considerations to aid their assessment of the requirements in the Organizational Behavior Topical Requirement. The lettering of each consideration below is cross-referenced to its corresponding requirement in the Topical Requirement. These considerations are illustrative but not mandatory. Internal auditors should rely on professional judgment when determining what to include in their assessments.

For public sector internal audit engagements, it is accepted that internal auditors’ scope as defined in legislation and government structure may restrict some of this work. Internal auditors in the public sector should document such scope limitations as part of their risk assessment process to clearly communicate the tailored scope of their review.

Governance Considerations

To assess how the governance processes could be applied to organizational behavior, internal auditors may review:

A. Structured roles and responsibilities to ensure that the board maintains visibility and influence over the behaviorial dimensions of the organization. Evidence may include that:

- A governance committee:
  - Establishes and maintains a dedicated board or subcommittee(s) focused on organizational behavior with clear terms of reference linking organizational behavioral oversight to strategic delivery.
  - Conducts regular reviews of behavioral risk indicators that align with long-term business goals. Behavioral risk indicators are metrics for establishing whether action

is required to ensure behavior remains aligned with strategic objectives, related values, and organizational purpose.
    - Includes behavioral objectives in executive performance evaluations and remuneration.

- Board reporting frameworks:
    - Provide insights into behavioral risk indicators using structured dashboards (for example, staff engagement, incident trends, customer satisfaction, values-based recognition).
    - Integrate culture-related metrics into strategic performance reporting at the board level.

- Stakeholder feedback mechanisms, such as surveys, allow:
    - The board to receive direct input on behavioral alignment with values and strategy from employees, customers, and other stakeholders.
    - Feedback to help shape strategic direction and behavioral interventions.

B. Effective management of organizational behavior occurs through clearly defined accountability across the organization. The board is ultimately accountable for ensuring that the organization promotes and sustains behavior aligned with its strategic objectives, including setting clear expectations for conduct, overseeing behavioral risk reporting, and challenging management where misalignment is detected. Evidence may include that:

- The board:
    - Approves the organization's behavioral risk appetite and key cultural objectives.
    - Requires regular reporting on indicators of behavioral risk (for example, trends, incident patterns, whistleblower themes).
    - Holds executive management to account for cultural performance through mechanisms such as incentive structures and "tone at the top."
    - Meets with second and third line functions on matters relating to behavioral risk escalation, gaps in oversight, and the sufficiency of remedial actions.

- Business units and operational management embed behavioral expectations into daily operations, ensuring that decisions, communications, and team dynamics reflect the organization's stated values. This may include taking ownership for:
    - Modeling desired behaviors and maintaining a psychologically safe environment.
    - Implementing controls that influence behavior, such as recruitment, reward, communication, and leadership routines.
    - Proactively identifying and escalating behavioral risks as they emerge in operational settings.
    - Mitigating behavioral risk that is a consequence of misaligned behavior within their teams and the need for controls (formal and informal).

- Risk, compliance, human resources, and related oversight functions design and maintain the organization's behavioral risk framework, including.

- Defined roles and responsibilities for behavioral oversight.
- Escalation pathways and data analytics processes.
- Dashboards, thematic analyses, and periodic assessments to provide forward-looking insight into behavioral conditions across the organization.
- The ability to challenge practices where incentives, communications, or leadership behaviors diverge from stated goals.
- Consultation on all material changes to people-related controls, governance frameworks, or strategic transformation initiatives that may influence culture.
- Review of emerging trends from incident reports, audit findings, and other assurance mechanisms that indicate behavior-related issues.

C. Governance process that ensures behavioral oversight, regular monitoring, evaluation, and the alignment of behavioral patterns and strategic objectives. The process may include:

- Using a dashboard to provide key datapoints from sources such as employee satisfaction and integrity survey results, attrition and absenteeism rates, speak-up channel content, incident data, and performance and innovation metrics. Characteristics of an effective organizational behavior dashboard include:
  - Defined threshold values to identify behavior improvement opportunities.
  - Separation of behavioral data (such as speak-up data) from driver data (such as clarity of roles and responsibilities) and outcome data (such as customer complaints).
  - Combined quantitative data, such as from surveys, with qualitative data, such as from focus groups and speak-up channels.
- The board understanding how current aspects of organizational behavior could be addressed to enhance organizational effectiveness and performance. These aspects comprise how:
  - Decisions are made, including seeking different perspectives and challenges.
  - Employees communicate with each other, including voicing concerns and expectations.
  - Employees collaborate, including across teams and when managing conflict.
  - Employees respond to failure, for example, by learning from mistakes or responding with blame or denial.
  - Middle and senior management leadership behavior impacts the other behavioral categories (for example, how leaders respond to mistakes and how they invite challenge in decision-making).
  - Strategy and the business model drive decision-making, codes of conduct, incentives/disincentives performance management.
- The board requiring a continuous learning system that identifies improvement opportunities and actively and measurably addresses them by:
  - Using evidence-based insights based on actual employee behavior.

- Focusing on what is known to be happening within the organization rather than what is intended or desired.
- Assessing a mix of qualitative and quantitative data, often acquired by surveys, speak-up channels, confidential conversations, and focus groups.
- Applying the insights to determine actions that will strengthen and address certain aspects of organizational behavior.
- Incorporating an action plan to combine targeted interventions in critical areas (for example, communication strategy, training, leadership development, and team-level discussions).

D. Policies and procedures addressing behavioral risk protocols are established, periodically reviewed, communicated effectively, and integrated into business operations and decision-making. The policies and procedures cover ethics, human resources, compliance, risk, operations, and decision rights. The board should ensure:

- Behavioral expectations are formally articulated in relevant policies (such as a code of conduct and/or policies on ethics, human resources, incentives, and the delegation of authority). Such policies should define acceptable and unacceptable behavior with practical examples, aligned to the organization's risk appetite.
- Risk management functions map behavioral expectations to key operational processes — such as hiring, performance reviews, onboarding, and client management — ensuring they are reflected in daily decisions. Assurance reviews should test how these expectations influence actual behaviors and report to the board accordingly.
- The board seeks and receives assurance that the organization's policies are accessible and clearly communicated through multiple channels (for example, intranet, training, town halls). Embedding case studies and decision trees helps contextualize behavioral expectations. Dashboards can track comprehension and usage metrics.
- All behavioral policies and procedures are subject to a scheduled review cycle and updated in response to incidents, survey findings, or regulatory changes. Second line functions should maintain a lessons-learned register to identify gaps emerging between behavior and strategic objectives.
- The board receives regular updates on policy coverage, clarity, and effectiveness. The second line should analyze breaches, policy impacts, and alignment with desired behaviors. Policy effectiveness should be reviewed through qualitative feedback and behavioral risk indicators.

Risk Management Considerations

To assess how risk management processes are applied to organizational behavior, internal auditors may review whether:

A. A behavioral risk management process is clearly defined and includes behavioral characteristics critical to meeting strategic objectives. At a minimum, risk management should demonstrate the following characteristics:

- Roles and responsibilities align with enterprise risk and governance frameworks and reporting lines enable independence and influence.

- Authority to challenge decisions and escalate behavior-related risk issues without fear of retribution or dilution.
- Independence from operational management with direct access to senior leadership and the board.
- Access to multi-source behavioral risk data that is relevant, timely, and triangulated across sources. This data includes both structured (such as survey results, policy breaches) and unstructured forms (for example, speak-up reports, focus group insights). Data sources include human resources (such as attrition, retention, and survey data), whistleblowing, customer complaints, and audit findings.
- Use of data analytics to identify trends, anomalies, and emerging risks.
- Use of dashboards and risk indicators to inform management and board reporting.
- Use of behavioral risk indicators tied to organizational objectives.
- Conducting or outsourcing reviews of the root cause of conduct failures and cultural misalignment.
- Familiarity with both formal and informal drivers of behavior (for example, incentives, psychological safety, and leadership tone).
- Senior leaders' credibility and trust with operational teams, combined with the ability to influence decision-making in real time.
- Active involvement in the design and review of controls related to human resources (for example, incentives, hiring, and training).
- Advisory role in strategic change programs and transformation initiatives.
- Engagement with business leadership to shape culture through influence, not just enforcement.
- Ongoing collection and analysis of data, which may include:
  - Employee engagement and well-being surveys.
  - Recognition and reward data for values-driven behavior.
  - Whistleblower reports and complaints.
  - Customer feedback, highlighting both satisfaction and dissatisfaction.
  - Performance appraisals, reflecting collaboration, integrity, and innovation.
- Use of data analytics to identify vulnerabilities and detect trends.
- A clearly defined process for prompt escalation of risks and behavior that do not align with strategic objectives.
- Oversight of the determination and execution of management action plans to address risks and reinforce required behaviors.

B. Timely monitoring processes for organizational behavior that include reporting results to stakeholders. Examples of risk indicators in the behavioral, driver, and outcome categories and reportable deficiencies include:

- Decision-making: A lack of effective challenge or insufficient inclusion of different perspectives.
- Communication: Inadequate attention given to the issues reported by individuals.
- Collaboration: Fragmented work environments in which employees focus on their own work only.
- Responding to shortcomings: Placing blame and exacting punishment for unintentional mistakes.
- Leadership: Demanding performance without offering understanding when goals are not met.
- Formal drivers: Unclear roles and responsibilities or conflicting targets.
- Informal drivers: Low psychological safety or ineffective dynamics among the three lines.
- Performance data: Excessive customer complaints or stagnating innovation or digitalization.
- Human resources data: High levels of attrition and absenteeism and low levels of satisfaction in survey results.

Risk and legal data: High number of investigations, policy breaches, or alerts and situations narrowly averted.

C. Processes to ensure that deviations between expected and observed behaviors are identified and communicated to those with the authority and ability to act. Internal auditors may review that:

- Effective communication is timely, evidence-based, and supported by analysis of underlying drivers and root causes.
- The design and operating effectiveness of communication efforts avoid superficial fixes, reputational damage, or repeated failures.
- Information is gathered and synthesized from multiple sources, including employee feedback, whistleblower reports, audit findings, and incident reviews.
- Structured analysis techniques — such as thematic reviews, behavioral science models, and root cause frameworks — go beyond surface symptoms and identify underlying drivers of misalignment (for example, unclear incentives, low psychological safety, or ineffective tone at the top).
- Gaps are presented not simply as compliance breaches or isolated incidents but as events with behavioral root causes reflecting cultural, systemic, and/or leadership issues.
- Communications highlight what happened and why, drawing on quantitative and qualitative data to support conclusions.
- The organization separates behavioral patterns, vulnerabilities arising from behavioral drivers, and organizational outcomes (for example, performance impact, stakeholder trust), enabling behavior and its drivers to be addressed. Findings are communicated to the right audience, at the right level of detail:

- Operational managers for immediate process correction.
- Senior leadership for resource allocation, messaging, and tone.
- The board or relevant committees for oversight and strategic implications.

- Visual and narrative tools such as dashboards, heat maps, or case summaries explain findings and support recommendations and/or action plans.
- Implications for risk exposure and the resilience of the control environment are included in process reviews.
- The communication of gaps is tied to remedial actions and monitored for completion.
- The outcomes of interventions are assessed and shared, completing the learning cycle.
- Communications are free from undue influence and align with established escalation protocols, preserving the independence and credibility of assessments.

D. Gaps between expected and actual behaviors are resolved in a structured and participatory manner to ensure that remediation is grounded in stakeholder insight, tracked to completion, and evaluated for effectiveness. Internal auditors may review whether:

- The resolution process meaningfully involves the stakeholders closest to the issue, such as operational managers, human resources, business partners, employee representatives, compliance advisors, and affected individuals or teams. Their input ensures that actions are:
  - Contextually grounded: sensitive to the operational realities and informal norms that may have contributed to the gap.
  - Credible and accepted: more likely to be supported and embedded if the actions are shaped by those directly involved with the actions.
  - Constructively challenging: enabling candid reflection on contributing leadership behaviors, control design weaknesses, or group dynamics.
- Stakeholder input is solicited, synthesized, and incorporated into action plans. Feedback mechanisms may include interviews, focus groups, survey diagnostics, and other methods.
- Resolution actions are documented, with defined ownership, timeframes, and success criteria:
  - Actions are proportionate to the severity of the issue.
  - Where necessary, actions target the formal drivers (for example, policies, incentives) and informal drivers (for example, psychological safety, team dynamics).
  - Where multiple functions are involved (for example, human resources for training, risk management for controls), cross-functional delivery and accountability are coordinated and clarified.
- Progress is tracked to completion, ensuring that commitments are fulfilled and sustained. This includes:
  - Maintaining a behavioral issue/action register or equivalent mechanism.

- Holding regular check-ins with action owners to verify status.
- Escalating delays, partial completions, or resistance to appropriate governance forums.

- The effectiveness of the resolution in closing the gap and reducing behavioral risk is assessed. This may involve:
  - Reassessing behavioral risk indicators after implementation.
  - Gathering feedback from affected stakeholders on changes observed.
  - Testing for shifts in behavior via observation, survey, or audit techniques.
  - Adjusting actions or adding reinforcements where outcomes remain weak or ambiguous.

Control Process Considerations

To assess how control processes are applied to mitigate the risk that organizational behaviors are not aligned with strategic objectives, internal auditors may review:

A. Behavioral risk reviews to understand the risk driven by current organizational behavior (that is, the potential unintended consequences of how things are done). Examples of such reviews are assessments of projects after they are completed, root cause analyses, and reviews of detailed operations in practice.

B. Structured feedback processes to understand what mechanisms management uses to communicate behavioral expectations (for example, town halls, email, meetings between individuals and their supervisors) and the effectiveness of the management tone on behavior within an organization. This can be done by evaluating the processes that capture and analyze employees' perceptions and understanding of board and senior management messages. Internal auditors can help organizations continuously refine their communication strategies and help ensure that the tone from the top resonates effectively across all levels by reviewing key controls such as:
   - Regular surveys, interviews, and focus group discussions with employees, inquiring about the clarity, consistency, and impact of leadership communications and yielding quantitative and qualitative data on how well the messages are being received and understood at various levels of the organization.
   - Open channels for anonymous feedback, allowing employees to share their honest opinions without fear of reprisal. These channels should be facilitated through digital platforms that enable real-time feedback and suggestions. Data derived from these channels should be analyzed to check whether the tone at the top is well understood among employees at all levels.
   - Feedback from senior management meetings collected through surveys, interviews, focus groups, minutes, and anonymous channels to ensure senior management is aware of ineffective communications, misunderstandings, or areas needing improvement. Senior management demonstrates that employee input is valued by actively responding to and acting on the feedback. When this does not happen, employees may become less inclined to provide feedback due to a sense of resignation.

- Feedback on senior management performance is integrated into their performance reviews to continuously monitor the reception of leadership directives. This reinforces the importance of leadership messages and ensures they are reflected in day-to-day operations.

C. Escalation within an organization is encouraged for early risk identification and mitigation and to establish a psychologically safe environment where employees feel comfortable reporting issues without fear of retaliation. Internal auditors can review key controls to help enhance effective risk management such as:

- Easy-to-use feedback mechanisms, including direct reporting and anonymous options, internal and external hotlines, surveys, suggestion boxes, and digital platforms to allow confidential reporting and capture issues that individuals may hesitate to report openly.
- Well-defined and easy-to-understand processes for reporting issues, with multiple direct and anonymous internal and external channels, and efforts to promote employee awareness. Characteristics of reporting channels should include:
  - Confidentiality assurances, protecting the identities of individuals who report issues.
  - Strict no-retaliation policies that are clearly communicated and consistently upheld to protect individuals who report issues.
  - Communication back to individuals who report issues, regardless of the reason or outcome.
  - Regular organizationwide summaries of issues reported in the past and their outcomes to show that issues are reported and acted upon and to ensure transparency about the actions taken to address feedback.
- Regular communication from management emphasizing the importance of open communication and reporting issues and demonstrating how management itself models such behavior.
- Regular training sessions emphasizing the importance of psychological safety, encouraging individuals to report issues, and providing guidance on how to escalate issues appropriately. The training should be repeated periodically to reinforce the desired behaviors over time.
- Informal rewards, such as verbal or written appreciation and public recognition, for individuals who report issues.
- Regular reviews of the escalation process to ensure its effectiveness and efficiency, including soliciting employee feedback to identify and promptly address barriers to reporting.
- Communication about the resolution of the feedback to prevent resignation among employees.

D. Incentive-disincentive programs align with the organization's desired behaviors and strategic objectives and are communicated. Internal auditors may review controls such as:

- Incentives — both monetary (for example, bonuses, promotions) and nonmonetary (for example, recognition, development opportunities) are aligned with strategic objectives and linked to the demonstration of the desired behaviors.
- Balanced performance review criteria incorporate how objectives are achieved (for example, collaboration, integrity, and customer-centered) as well as more traditional achievement metrics (such as financial targets).
- Incentive criteria and disincentive thresholds are clearly defined, consistently applied, and subject to review by management or human resources to avoid bias and unintended outcomes.
- Cross-functional groups validate consistency and fairness in incentive decisions across business units.
- Consequences for misconduct and cultural breaches include clear, proportionate disincentives (for example, bonus reductions and promotion blocks), with actions explained and documented to ensure transparency.
- Nonmonetary recognition programs highlight employees who model cultural values, such as ethical decision-making and psychological safety.
- The impacts of incentive programs are routinely assessed through employee feedback and behavioral metrics to refine or rebalance reward mechanisms. Incentive programs should be evaluated and adjusted to ensure:
  - The goals are not too narrow or too broad.
  - The goals are achievable.
  - The short-term goals do not undermine long-term outcomes.
  - Acceptable levels of risk-taking are articulated.
  - Safeguards are implemented to ensure ethical behavior while attaining goals (for example, leaders as exemplars of ethical behavior, making the cost of cheating far greater than the benefit, and strong oversight).
  - The goals are tailored to individual abilities and circumstances while preserving fairness.
  - Team goals do not contradict individual goals.
  - Intrinsic motivation is assessed, and management recognizes that some goals may curtail intrinsic motivation.
  - The organization's ultimate goals are considered, and the type of goal (for example, performance or learning) is assessed for appropriateness.
- The organization integrates positive reinforcement and corrective actions to cultivate proactive organizational behavior that aligns with its strategic objectives and regulatory requirements. Key controls should include:
  - Regularly assessing the effectiveness of communication and training programs to ensure employees understand the importance of reporting issues and the consequences of noncompliance and feel encouraged, instead of fearful, to report issues.

- Monitoring and reporting systems track compliance and identify potential underreporting issues.
- Disciplinary actions are applied consistently and fairly and are neither so harsh that they discourage reporting nor so lenient that they fail to deter unethical behavior.
- Feedback mechanisms that allow employees to report issues anonymously are regularly reviewed to ensure they are effective and encourage honest reporting.

E. The organization's issue management process identifies behaviors that are misaligned with strategic objectives and escalates them when necessary to create a management action plan to mitigate the risk of poor outcomes. Internal auditors can review key controls for effective behavioral change interventions, such as:

- Evidence-based approaches: The action plan incorporates evidence-based approaches to changing behavior, grounded in behavioral science, behavioral models, and change management. If the approach is not explicitly based on a specific behavioral change model, the approach should combine intervention strategies for:
  - Communication: Consistently raising awareness among employees and management about the necessity for behavioral change and motivating them to embrace and support the transformation.
  - Employee training and development: Investing in training programs tailored to different roles, equipping employees with necessary skills and behaviors through workshops, e-learning, and continuous development opportunities. This includes learning and being able to effectively implement the new skills and behaviors required to achieve the changes desired by the organization.
  - Management development: Managers at all levels consider how to enable and demonstrate behavioral changes in daily situations. This may include management adjusting its own behavior to help staff feel more comfortable implementing new behaviors, directly requesting that employees implement new behaviors, and encouraging learning and requesting training on the skills and behaviors still needed. Leadership programs and coaching can refine skills and confidence.
- Consistent reinforcements in daily situations: Individuals need support, encouragement, and regular reminders to develop new behaviors and integrate them into their daily work routines.
- Congruent reinforcement: An intervention plan should be aligned across leadership messaging, processes, systems, coaching, and informal feedback mechanisms to reinforce the desired change. This alignment removes uncertainty and confusion, ensuring that employees understand the desired behavioral changes, how to adopt them, and their importance.
- Targeting the drivers of behaviors: Sustainable behavioral change requires addressing the underlying drivers (see Risk Management, section C) of behaviors rather than only the behaviors themselves.
- Measurement: Measuring the progress and effectiveness of interventions helps determine whether they are achieving the desired impact and whether adjustments are needed. Regular updates act as positive reinforcement and provide stakeholders with

progress information. An effective measurement approach combines qualitative and quantitative methods, such as surveys and interviews, and provides a comprehensive understanding of progress.

F. Training programs intended to influence behavior are explicitly linked to defined behavioral expectations or risk appetite statements. Examples of training topics include ethics, compliance, leadership, inclusion, risk awareness, and decision-making. Internal auditors may review that training programs are:

- Reflective of desired conduct and attitudes and include clear, documented learning objectives.
- Based on behavioral evidence or incident learning (for example, audit findings, root cause analyses, and feedback mechanisms).
- Delivered to all relevant role groups, with tailored modules for senior management, line managers, and staff.
- Mandatory where relevant (for example, high-risk processes, regulated responsibilities, and control roles).
- Refreshed regularly, with content reviewed at least annually to ensure relevance and effectiveness.
- Designed to:
  - Incorporate real-world scenarios or case studies to make behavioral expectations tangible.
  - Use techniques that engage learners (for example, storytelling and reflective questioning).
  - Actively involve senior management to indicate the tone at the top and encourage employees to adopt behavioral changes.
- Include impact and assurance controls that:
  - Track completion of mandatory training and report on exceptions.
  - Measure behavioral impact and retention through informal surveys, simple tests, or observation-based assessments.
  - Capture participant perspectives and training effectiveness through structured feedback processes.
  - Ensure training content is aligned with risk frameworks and control requirements and includes formal review and sign-off processes.

G. Hiring processes align with the organization's behavorial expectations and incorporate behavioral competencies. Internal auditors may review control features such as:

- Tools enable the assessment of candidates' alignment with the organization's values, including structured interview guides and scenario-based questions.
- Behavioral interviews and peer feedback are used to assess traits such as empathy, ethical judgment, and accountability.

- Recruitment advertisements and employer branding reflect the organization's cultural aspirations to attract culturally aligned candidates.
- Feedback mechanisms enable the assessment of recently hired individuals' cultural integration so that misalignments can be addressed early.
- Documentation (for example, scoring frameworks and interview records) demonstrate consistent decision-making hiring criteria are applied.
- Human resources and senior management review hiring patterns for risks, such as favoritism, bias, or failure to uphold behavioral standards.
- Hiring and promotion policies are regularly reviewed for consistency with organizational values and effectiveness in practice.

Appendix A. Practical Application Examples

Example 1: Standalone review of the organization's behavioral framework

The internal audit function initiated a stand-alone review of an organization's overarching framework to evaluate its design and operational effectiveness in managing behavioral risk. The scope of this engagement covered the governance structures, risk management activities, and behavioral controls that underpin alignment across the organization.

Internal auditors assessed whether responsibilities for behavioral oversight were clearly defined and free from conflicts of interest. The team reviewed the board's terms of reference and verified that the board had received regular reporting on behavioral risk indicators, such as survey results and speak-up trends. The review included evaluating whether culture-related policies, such as those governing whistleblowing and ethical conduct, were routinely updated and enforced.

Internal auditors also assessed risk management elements, starting with the behavioral risk management framework maintained by the second line, focusing on whether it identified key behavioral risk drivers (such as low psychological safety or misaligned performance targets). The assessment emphasized how the organization tracked and addressed the variance between expected and observed behaviors, including whether behavioral anomalies were escalated and addressed systematically.

The control environment was examined to determine whether formal processes supported behavioral expectations. The auditors evaluated hiring protocols for values-based assessment, whether the onboarding content was aligned with the norms of the organization's culture, and the extent to which incentives (monetary and nonmonetary) were reviewed for unintended consequences. Training programs, speak-up channels, leadership messaging, and data analytics used to detect behavioral concerns were also tested.

This engagement provided a comprehensive view of how behavioral risk is managed at an organizational level and formed the basis for recommending enhancements to the organization's behavioral infrastructure.

Example 2: Thematic Review of Incentive Practices

This audit engagement focused on assessing how the organization's incentive frameworks influence behavior and whether they align with the organization's purpose, values, and regulatory expectations. The internal audit function selected this theme due to increasing concerns about misconduct risk and emerging evidence of pressure-based behaviors in business units.

The review began by evaluating the governance arrangements for designing and approving incentive schemes. The audit function assessed whether those responsible for implementing governance decisions, such as human resources or remuneration committees, had formal oversight of the design of incentives and whether their work received independent review by risk, compliance, or audit functions.

A risk management perspective was applied to understand whether the development of incentive structures included a consideration of their behavioral implications. The auditors explored whether the organization had tested scenarios or analyzed behavioral risks in relation to its reward schemes. They also reviewed whether behavioral key performance indicators, such as collaboration scores, were tracked and used to assess outcomes.

Control testing covered a range of mechanisms designed to shape reward-related behaviors. These included balanced scorecards incorporating performance criteria that measured achievements and how they were achieved, the application of malus (a penalty or reduction in pay) and/or clawback provisions, and the existence of 360-degree feedback processes. Auditors also examined training provided to line managers on delivering behavioral feedback and explored nonmonetary recognition schemes that rewarded values-based conduct.

Throughout the engagement, internal auditors sought to identify whether incentive practices could unintentionally drive undesirable conduct, such as excessive risk-taking, taking shortcuts, or reluctance to escalate issues. Recommendations were made to improve transparency, embed values-based goals more consistently, and strengthen independent reviews of second-line management during its process of designing rewards.

Example 3: Integration into a Traditional Audit – Cyber Risk Management

In this example, the internal audit function integrated behavioral risk considerations into a traditional engagement to assess cyber risk management. Recognizing that many cyber failures are due to not just technical issues but also human behavior, the auditors embedded reviews of behavior throughout the engagement.

The engagement began by assessing the extent to which behavioral risk was acknowledged within the governance of cyber resilience. Auditors reviewed the board and senior management's oversight of the cyber strategy, looking for evidence that the bodies were monitoring and discussing behavioral alignment, such as compliance with secure practices or leadership modeling of secure behavior, with strategic objectives.

In terms of risk management, the team evaluated whether the organization's cyber risk assessments considered human factors. This included assessing whether behavioral data (for example, the frequency of phishing test failures, system access breaches, or low training completion rates) were used to monitor and escalate risk. The engagement also investigated whether the root cause of previous security incidents had been determined to identify potential behavioral drivers, such as unclear accountability or management tone.

Control testing focused on behavioral design and secure operations. Auditors reviewed whether behavioral screening was included in hiring processes for roles with privileged access. Incentive

structures were assessed to see whether they encouraged secure online practices or inadvertently prioritized risky behavior over safety. Cybersecurity training was also evaluated to determine whether it was engaging, refreshed regularly, and included simulations that tested behavioral responses to phishing and social engineering.

Finally, the engagement looked at how management reinforced secure behaviors through communication and whether employees felt comfortable reporting unsafe cyber behavior. An organizational culture that encouraged employees to speak up was considered a critical enabler of resilience.

The inclusion of behavioral aspects within this cyber audit led to deeper insights and useful recommendations, strengthening the organization's capacity to manage risk in one of its most critical domains.

About The Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information www.theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

July 2025