The audit management playbook

Table of contents

Planning

In this chapter

Planning an audit from scratch

The challenge

The IIA's latest updates to the Global Internal Audit Standards demand stronger alignment between the organization's top risks and audit activities. As a result of the call for a more risk-focused internal audit function, topics and processes with a direct link to the organization's success — including go-to-market activities, innovation, human capital, and leveraging advanced technology — are finding their way onto more and more audit plans.

Yet, many internal auditors lack either the knowledge or the subject matter expertise needed to provide assurance for activities that they have never audited before. These "checklist auditors" may scope their audit projects to include testing three or four controls, highlight exceptions in the audit report, then move on to the next audit. Recommendations made routinely constitute "internal audit recommends following the policy and procedure," and rarely provide any actionable insight to create positive change.

These actions not only fail the audit customer, but also internal audit.

The solution

Auditors who create and document custom audit programs from scratch, versus relying on checklists or template audit programs, are better equipped to perform audits over areas that are not routinely audited. And, when internal audit can spend more of its time and resources aligned with the organization's strategy and key objectives, the benefits can — and do — multiply.

What can internal auditors do to prepare a more comprehensive scope for their internal audit projects? And where can internal auditors find the subject matter expertise needed to create an audit program "from scratch"? We've collected a number of best practices that are applicable across the board when it comes to planning individual audits, no matter an audit team's size or industry.

Checklist: Planning an audit from scratch

1 Initial audit planning

All internal audit projects should begin with the team clearly **understanding why the project was put on the audit plan.**

The following questions should be answered and approved before fieldwork begins:

- ☐ Why was the audit project approved to be on the internal audit plan?
- ☐ Have you met with the business executive to determine if there have been any significant changes to the process, risk, and/or team recently?
- ☐ Have you validated that the audit is still relevant?
- ☐ How does the process support the organization in achieving its goals and objectives?
- ☐ What enterprise risk(s) does the audit address?
- ☐ Was this process audited in the past? What were the results of the previous audit(s)?
- ☐ Have any other teams, (legal, risk, compliance, IT security, controls) performed projects in this space? What have they found?

Initial document and data request list

Requesting and obtaining documentation providing **insight on how the process works** is an obvious next step. Some key documents and data to request include:

- ☐ Key business objectives for that particular line of business, risk, and process
- ☐ All policies, procedure documents, and organization charts
- ☐ Key reports used to manage the effectiveness, efficiency, and process success
- ☐ Access to key applications used in the process
- ☐ Description and listing of master data for processes being audited, including data fields and attributes
- ☐ Relevant business data, scorecards, or KPIs the business is tracking
- ☐ Data analytics, e.g., Snowflake data or analytics captured by other teams

2 Risk and process subject matter expertise

Leverage experts within the company in addition to outside subject matter experts; this can be especially helpful in large organizations where you might find resources in **different divisions, countries, or offices with the same expertise** who can provide support or insight while maintaining their independence.

Evaluate the design of the process audited using:

- ☐ Internal SMEs in different divisions, departments, or locations who can provide insight while maintaining independence
- ☐ SME from a Big 4 or other consulting firm
- ☐ Blogs: Deloitte, EY, KPMG, Protiviti, RSM, etc.

3 COSO's 2013 Internal Control — integrated framework

While used extensively for Sarbanes-Oxley compliance purposes, COSO's 2013 Internal Control – Integrated Framework can also be leveraged by internal auditors to create a more comprehensive audit program. In addition to identifying and testing control activities, **internal audit should seek to identify and test the other components of a well-controlled process.**

- ☐ Review COSO's 2013 Internal Control components, principles, and points of focus

4 Preparing for a planning meeting

Obtaining information and data about the process to be audited can happen with a combination of research and interviews. Great internal auditors know that **doing more work before meeting with process and control owners** will help minimize disruption to the audit customers and should set a positive tone for the audit. Some best practices include:

- ☐ Outline key process steps by narrative, flowchart, or both, highlighting information inflows, outflows, and internal control components
- ☐ Validate draft narratives and flowcharts with subject matter experts (if any)
- ☐ Create an initial planning questionnaire to facilitate the meeting

5 Preparing the audit program

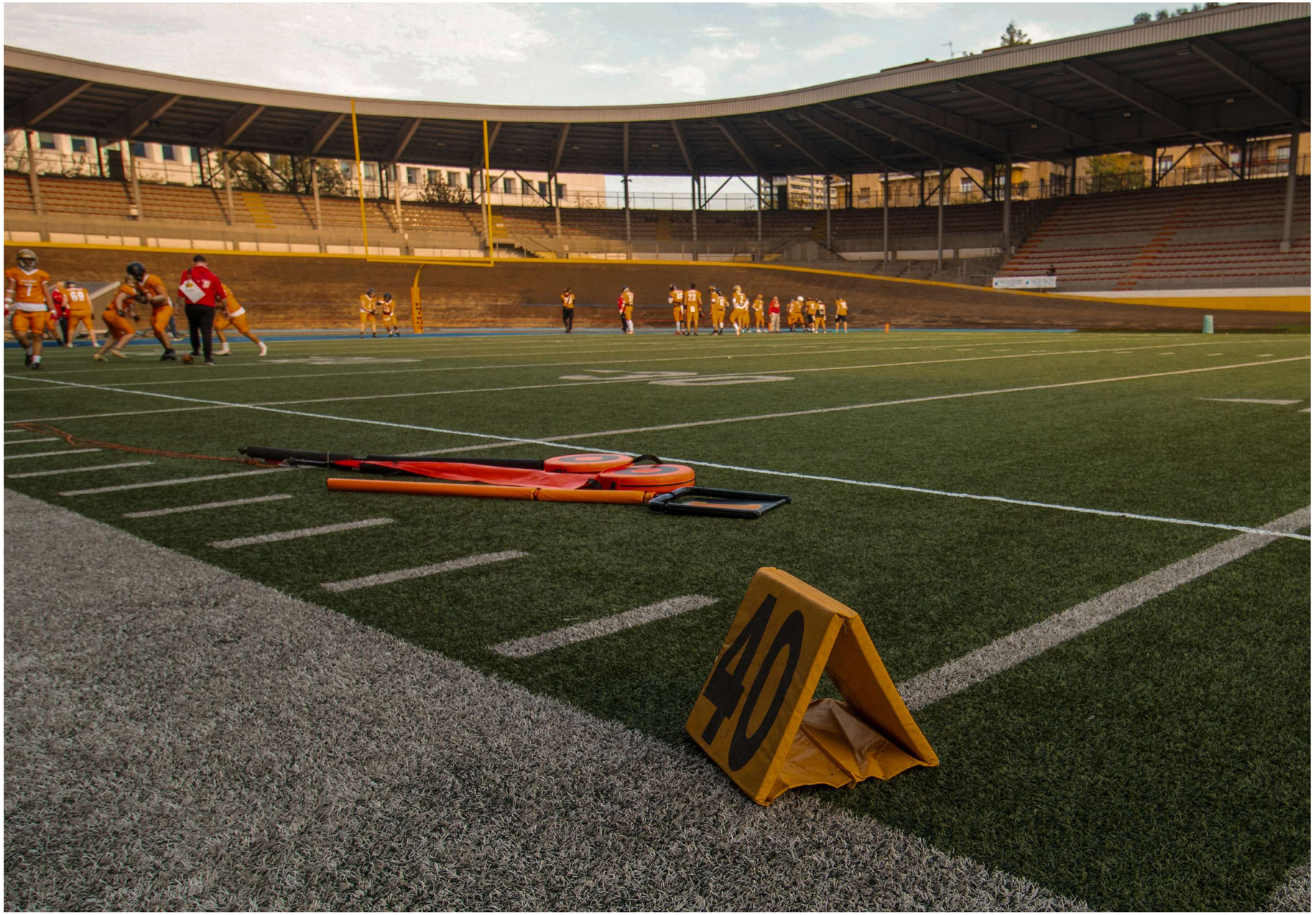
Internal audit should be keen to **capture significant activities** of everyone (employees and third parties) involved in the process, the flow of assets (tangible or intangible), and any activities and controls that prevent or detect errors from happening, including:

- ☐ Process objectives
- ☐ Process risks
- ☐ Controls mitigating process risks
- ☐ Control attributes, including:
  - ☐ Is the control preventing or detecting a risk event?
  - ☐ Control frequency (daily, weekly, monthly, quarterly, etc.)
  - ☐ Does the control mitigate a fraud risk?
  - ☐ Is the control manually performed, performed by an application, or both?
  - ☐ An initial assessment of the risk event (e.g., high, medium, or low)
- ☐ Testing procedures for controls to be tested during the audit, including:
  - ☐ Inquiry, or asking how the control is performed
  - ☐ Observation, or physically seeing the control be performed (if possible)
  - ☐ Inspection, or reviewing documentation evidencing the control was performed
  - ☐ Reperformance, or independently performing the control to validate outcomes

6 Audit program and planning review

Audit programs, especially those for processes that have never been audited before, should have **multiple levels of review and buy-in** before being finalized and allowing fieldwork to begin. Before the audit kicks off, receive approval from:

- ☐ Internal Audit Manager or Senior Manager
- ☐ Chief Audit Executive
- ☐ Subject matter expert
- ☐ Management's main point of contact for the audit (i.e., audit customer)



Key metrics to track in your audits and audit plan

As internal audit faces perennial pressure to cut costs, it remains critical for the department to prove its value as a contributor to business goals. Performance metrics communicate the effectiveness of internal audit activities and their alignment with organizational objectives.

What sets good metrics apart from the rest?

Key performance indicators (KPIs) are quantifiable measurements that demonstrate the effectiveness of an individual, department, or organization in achieving key goals. Clearly defining goals and tracking meaningful KPIs provide valuable evidence that internal audit activities support the organization's strategic objectives.

Checklist: Key metrics to track in your audits

Audit milestones to track

Planning

- ☐ % of respondents who completed pre-audit questionnaire
- ☐ Announcement memo sent on time (X days prior to fieldwork)
- ☐ Align audit scope and map to audit universe

Fieldwork

- ☐ Kick-off/opening meeting completed
- ☐ Evidence collection completed
- ☐ Periodic audit status meetings with key stakeholders completed
- ☐ Budget to actual hours spent of fieldwork
- ☐ Hours spent per auditor

Reporting

- ☐ Preliminary findings communicated
- ☐ # of high/medium/low issues reported
- ☐ % of issues closed as of final report issuance
- ☐ Net number of repeat findings
- ☐ Recommendations communicated
- ☐ Management action plans documented
- ☐ Final report issued timely

Follow-up

- ☐ % of audit issues resolved
- ☐ Audit feedback survey sent
- ☐ QA results completed

Metrics to track in an audit plan

- ☐ % of audit plan completed
- ☐ # of unplanned engagements
- ☐ Average days to complete audit
- ☐ Outstanding audit issues
- ☐ # of repeat audit findings
- ☐ % of audit recommendations accepted
- ☐ # of training/continuing education hours
- ☐ % of audit team utilized
- ☐ Customer satisfaction score
- ☐ % of risks covered
- ☐ % of audit universe covered
- ☐ # of new controls identified during process analysis
- ☐ # of new risks identified during risk/control gap analysis

Pro tips

- Use weekly check-ins with management to communicate identified issues, fieldwork status, and milestones.
- Set a timely target to issue your final report, e.g., within 30 days of completing fieldwork.
- For customer satisfaction results, identify the percentage of surveys returned and if scores are improving year over year.
- Identify your percentage of risks audited based on your risk assessment.

Covering critical risk areas

Is your audit plan sufficiently covering critical risk areas?

A well-rounded audit plan will not only meet Sarbanes-Oxley (SOX) or other compliance requirements, but will also reflect an enterprise-wide scope and coverage of risks.

Cybersecurity

Recommended audit projects:

- Data encryption
- Access management policies and controls
- Data penetration testing with vendors
- Business Continuity Plan (BCP)
- Patch management policies
- Employee information security training

Culture and ethics

Recommended audit projects:

- Digital ethics (how consumer information is managed and protected across the enterprise)
- Succession planning
- Gender and racial discrimination

Data privacy

Recommended audit projects:

- General Data Protection Regulation (GDPR) enforcement
- Consumer consent

Data governance

Recommended audit projects:

- Data quality: data migration procedures, data management procedures in the event of acquisitions, data quality standards
- Data analytics: policies and procedures of data analytics functions, proper storage and ownership controls for data repositories and self-service platforms, data access controls

Third-party risk

Recommended audit projects:

- Background checks
- Third-party risk management
- Contract management
- Right-to-audit clauses
- Monitoring and compliance

Managing the internal audit function

Consider:

- Team development initiatives to build engagement and connectedness throughout the organization
- Continuous education for your team members to upskill
- Thinking outside of the box for recruiting, backfilling, and succession planning
- Diversifying engagements to promote talent retention

Fieldwork

In this chapter

Tips for turning audit clients into allies

The challenge

As planning transitions into fieldwork, it is important to consider the perspective the internal auditor persona carries. Too often, internal audit carries a reputation as the regulator, or “bad cop” of the company, a group more interested in uncovering problems in departments than giving credit for good work. This negative perception can create apprehension and color the expectations of audit clients, especially those who have never been audited before.

The solution

Audit clients who understand internal audit’s objectives and how they fit into the bigger picture will have more realistic expectations for the engagement and be more likely to provide helpful information, such as where the risks and issues actually are. When audit clients feel understood, comfortable, and on the same page as internal audit, they will become better collaborators. This drives better audit results and helps internal audit be more effective in providing the organization with the tools it needs to mitigate risk.

Tips for turning audit clients into allies

Turning audit clients into allies should be a year-round effort. We've collected tips to consider incorporating in every stage of an audit project.

Planning

- Communicate with stakeholders/process owners well in advance of the audit (exception: unannounced audits).
- Provide clear dates, and stick to them. Don't push back meetings or announce unexpected meetings.
- Be mindful of the client's location and time zone. Conduct planning calls during the client's working hours.
- Leverage an audit management solution to facilitate communication with clients and streamline document requests.

Fieldwork

- Lay out a clear and concise plan for communicating with clients during the opening meeting, including dates of meetings, check-ins, and the closing meeting.
- Schedule a weekly meeting with the main point(s) of contact to review the working results as the project progresses.

Reporting

- Ensure stakeholders and points of contact have been briefed on preliminary audit findings in advance of the closing meeting.
- If cross-functional teams are involved, brief them on the findings prior to the closing meeting.
- Come to the closing meeting prepared with draft management action plans.

Annual risk assessment

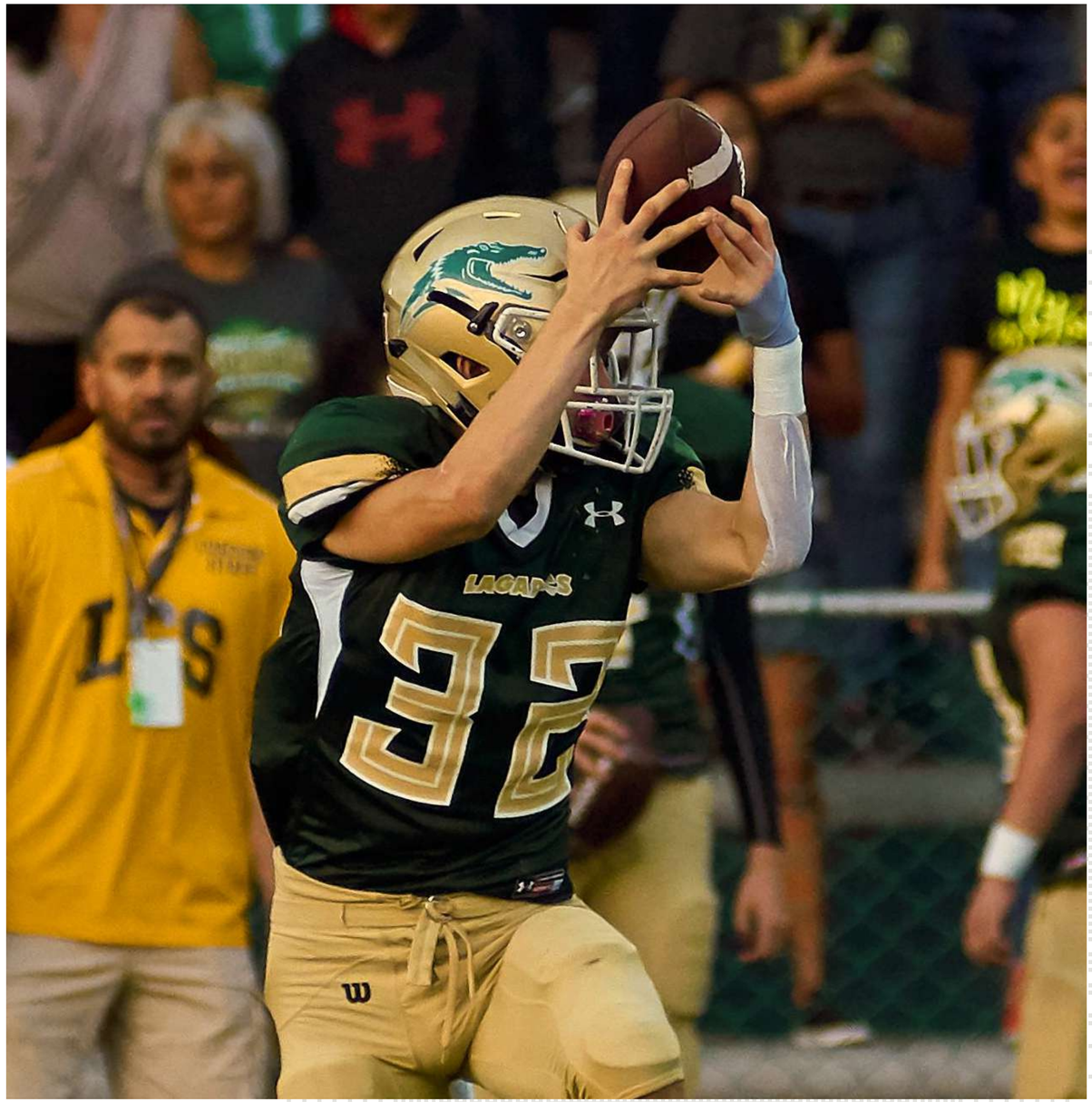
- Meet your key stakeholders face to face to build rapport and break the ice prior to querying them on their risk areas.

Off-cycle/ throughout the year

- Get to know your regular audit clients well when you're not in the middle of an audit or requesting help from them. Meet with them to get coffee and learn about their lives. By establishing a genuine interest and investment in the relationship, you'll be building allies rather than adversaries.

Audit evidence collection checklist

Collecting evidence is one of the most important elements of any audit, but it can cause confusion, frustration, and even regulatory violations if the documentation is not handled properly. While IIA Standard 2330 describes good evidence as “sufficient, reliable, relevant, and useful information to achieve the engagement’s objectives,” auditors also have to consider how to request, collect, and properly store the documentation. The content, organization, and format of workpapers may vary by organization and the nature of the engagement, however, it is important to achieve documentation consistency. The following checklist will help you apply best practices when collecting audit evidence.



Checklist: Audit evidence collection

This checklist includes three sections with best practices for handling evidence during different stages of the audit. Depending on your industry, you may work with both hard copy documents and/or electronic files. We have included recommendations for both scenarios, as well as tips for those working in a hybrid environment.

1 Requesting and tracking evidence

Requesting and tracking the status of evidence manually can be time-consuming. Be specific when creating your tracker, or use purpose-built software to automate these tasks.

- ☐ Identify the appropriate, reliable source for audit evidence.
- ☐ Decide if the evidence can be self-collected or if you will need assistance.
- ☐ If evidence cannot be obtained internally, determine if an external organization or third party may provide the evidence.
- ☐ Be specific in requesting evidence within date ranges in line with audit scope.
- ☐ Clearly communicate which data to include if the evidence is extracted from a system.
- ☐ Log all relevant data regarding the request.
  - ☐ Document name
  - ☐ Description
  - ☐ Contact name for the request
  - ☐ Time and date sent
  - ☐ Follow-up attempts
- ☐ Consider jurisdictional restrictions related to data and document movement across borders.
- ☐ Request all screenshots to include date and timestamps.
- ☐ Files should be sent through approved, protected channels with encryption as needed.

2 Gathering and handling evidence

Consider the chain of custody and data security when gathering and handling either hard copy or digital evidence.

Hard copy evidence

- ☐ Pick up original documents and maintain custody.
- ☐ Keep documents well organized.
- ☐ Do not leave documents in plain view and practice maintaining a clean desk.
  - ☐ Protect data in open office environments.
  - ☐ Apply data protection to the home office as well.
- ☐ Store hard copy documents (original and copies) in locked drawers.
- ☐ When working with hard copy originals, scan or copy the documents so these are not compromised.
- ☐ Redact or return any documents with personally identifiable information (PII) that are not needed as evidence. Document the methods used to gather the evidence with enough detail to facilitate reperformance.

Digital copy evidence

- ☐ When using audit management software, deliver digital evidence directly to the audit.
- ☐ Do not leave documents open and unattended and practice maintaining a clean desktop.
  - ☐ Protect data in open office environments and in your home office as well.
  - ☐ Consider using privacy screens for laptops.
  - ☐ Do not work with sensitive data on unsecured Wi-Fi.
- ☐ Data should be encrypted in transit and at rest (stored in a database).
- ☐ The database should be backed up, encrypted, and stored offsite in case of disaster.
- ☐ Access to evidence in the audit should be restricted to the audit team and administrators.

3 Using and disposing of evidence

When the audit is finished, make sure the final evidence is scanned into the file, originals are returned, and copies are destroyed appropriately.

- ☐ Update the tracking sheet/system.
- ☐ Evaluate the information received to determine if it is accurate and complete.
- ☐ Reference the evidence in context within the working papers.
- ☐ Remove any documents that were not needed and not referenced from the audit file.
- ☐ Return original documents and destroy any copies that do not need to be retained for evidence.
- ☐ Note if audit evidence is placed on a legal hold requiring retention.
- ☐ Destroy files according to the audit data retention policy (physical and digital copies).

4 Support audit evidence collection with technology

While managing the process manually with spreadsheets and following up through email is possible, we have more effective methods available to us today. Technology makes a huge difference in audit evidence collection and management. Following the best practices outlined in the Audit Evidence Collection Checklist and enabling the process with technology will improve your ability to collect, gather, and use the documentation in the most effective way possible.

Tech tip

Audit management systems include evidence request and management features to facilitate creating, sending, and following up on requests. Incorporating automation and technology is the next step to maximize the efficiency of your testing program.

10 best practices for fieldwork execution

Once fieldwork commences, scope creep and delays due to information obtained during walkthroughs can be common roadblocks. Many of these speedbumps during fieldwork may be avoided by observing the following best practices:

1. Set expectations early.

Setting and managing expectations with the client up front is key and helps prevent scope creep. When documenting the audit scope within an engagement letter, include an escalation and approval to expand your scope in the event any additional necessary procedures are identified during testing.

2. Schedule recurring status update meetings.

Proactively schedule status update meetings (ideally weekly) throughout fieldwork with all stakeholders to give updates on testing status, delays, and potential findings. This ensures the final audit report will be a summary of discussions you've already had and will help avoid last-minute surprises.

3. Have walkthroughs prior to fieldwork.

Walkthroughs should occur prior to fieldwork and before audit document request lists are sent to the client. Delays in audits usually happen when additional documentation is requested because of new information obtained during walkthroughs. Testing attributes should also be documented after walkthroughs once you have a clear understanding of the process.

4. Begin fieldwork when all requests are met.

Communicate to audit clients that the original fieldwork timeline assumes all requested support is obtained by the first day of fieldwork. If there are any delays in obtaining PBCs, remind the client that the engagement timeline will be impacted.

5. Test complex areas and prior findings first.

When determining which sections to test first, always start with complex areas and areas where there were prior audit findings. These areas are most likely to result in findings and will be most heavily scrutinized, so it is important to leave ample runway for follow-up discussions.

6. Communicate all potential findings as soon as they are confirmed.

All findings should be communicated, vetted, and agreed upon with management prior to the closing meeting so there will be no surprises. Since findings usually result in additional testing procedures as part of the confirmation process, identifying and communicating potential findings early helps ensure ample time to test if needed.

7. Be in sync with the audit client.

When presenting findings in the closing meeting, lead with "As we discussed..." before getting into the details. This helps both your audit team and the audit client feel in sync as they communicate, leading to a smoother report issuance process.

8. Keep an audit log.

9. Give yourself time to follow up.

Ensure workpapers are reviewed with ample time left for follow up with the client. Ideally, all testing should be complete before moving into the reporting phase of an audit.

10. Rotate for fresh eyes.

If you have a standardized audit program for different audit categories, try rotating out team members. A good balance is to have at least one subject matter expert recurring on the audit while rotating out the others. This will ensure a fresh set of eyes to help find overlooked issues.

Reporting

In this chapter

Best practices for audit report writing

An audit report should be a living, breathing document created throughout an audit engagement. Starting the audit report at the end of an engagement compromises your ability to consider the messages you want to deliver as you plan the audit and note potential findings during fieldwork, possibly leading to a stale report.

A great audit report clearly communicates the objectives, scope, and findings of an audit engagement, and in doing so, motivates its readers to take internal audit's recommended actions. In this section, we will cover best practices for writing effective audit reports that achieve their desired outcome.

Tips for writing an effective executive summary

1. Know your audience.

Understand who will receive the report. The executive summary should give an overview of the detailed report that resonates with every executive officer who reads it, so it is important to understand your organization's culture. Some organizations may be more cross-functionally collaborative, while others will be more compliance-oriented. Not every stakeholder will be a technical subject matter expert. For example, if your report is going to the CFO and you have IT audit findings, ensure that the issue can be understood by a non-technical audience.

2. Cut the fluff.

The executive summary should be 1-2 pages at most. Aim for brevity as much as possible. Consider the best way to summarize each point, as there will be more takeaways in the detailed report. Wherever possible, use numbers and percentages to help drive points home. Eliminate any unnecessary descriptive adjectives and adverbs.

3. Explain it to the company.

Whether the audit report is presented to members from operations or IT, the executive summary should be written so that every individual can easily understand the terminology and sophistication level of the writing. A good rule of thumb is to explain every point in a way that all levels of experience and expertise at your company would understand. Focus on high-level and strategic insights rather than the technical details.

4. Make it digestible.

For any key point, bring the reader's attention to the information as concisely as possible. Identify your key takeaways or messages, then leverage visual formatting to draw your audience's eyes to your insights.

Tech tip

Optro's generative AI capabilities can provide a jumping off point for drafting executive summaries to save your team time and ensure that escalations and key tasks never fall through the cracks. In Optro, you can also document your executive summary for easy access in the Overview page and even pull the executive summary into your automated reporting with Microsoft Word-Based Reports.

Pro tips

- Stay away from using overly sophisticated vocabulary or technical jargon. If someone needs a dictionary to understand your summary, this hurts the readability of your report.
- Avoid acronyms and functionally esoteric terms not everyone in the organization will understand.
- For important ideas or concepts that are difficult to digest, try using analogies. When done correctly, this facilitates understanding and can help drive the point home.
- Use bullet points wherever possible.
- Tables, graphs, and charts tend to be more effective in illustrating a finding than a block of text.
- If you can use a number or percentage to describe a fact, do so. This is particularly important when discussing key findings, critical risks, or trends.
- Circle or highlight the key points you want to convey, as well as **bold**, underline, *italicize*, or use color.

Writing the detailed report

Depending on the audit, expectations set during the opening meeting, and the findings, the contents of the detailed report may vary from organization to organization. **If there were more findings and complexity in the audit than anticipated, you may need to include more detail.** The contents of the detailed report are as follows:

BACKGROUND, OBJECTIVE, AND OVERVIEW OF THE AUDIT AREA REVIEWED

Focus areas, auditable entities impacted, risks being addressed, etc.

SCOPE AND APPROACH

What is included in the audit and how is it being addressed?

AUDIT PERIOD

What date range does the audit cover?

FINDINGS SUMMARY

- Issues or process improvement opportunities
- Observation themes and trends

DETAILED FINDINGS

- Includes the five C's of observations: Criteria, Condition, Cause, Consequence, and Corrective Action Plans/ Recommendations
- Organized into logical categories (department, process, risk area, etc.) and by rating or priority
- Evidence to support findings
- Implications and impact of findings

Tech tip

In Optro, you can use Microsoft Word-Based Reports to auto-generate audit reports that include key details about an audit, including issues data.

Keys to writing a digestible audit report

1. Reference everything.

Avoid unverifiable claims and make sure to bridge any gaps of information by referencing where you obtained key facts and figures.

2. Include a reference section.

Use of indices, appendices, and tables in this section is very helpful.

3. Use figures, visuals, and text stylization to make the report as digestible as possible.

- Numbers and percentages. If you can put a number behind a fact or use a percentage to describe it, do so.
- Circle or highlight the key points you want to convey, as well as bold, underline, italicize, or use color to draw attention to key facts and figures.
- Use tables or graphs to summarize and draw attention to key trends or important data, wherever possible.

4. Note key statistics about the entity audited in the background/overview (if applicable).

This puts things in perspective and gives context and relevance to your audit findings.

5. Note any positive themes or observations and things that are working well.

6. Ensure every issue in detailed observations includes the five C's of observations:

Criteria, Condition, Cause, Consequence, and Corrective Action Plans/ Recommendations.

7. Detailed observations are also a good place to include any additional facts and figures.

Ensure your observations are supported with proper evidence and the impact of your findings is clearly stated.

8. Always perform a quality assurance check.

Seek someone who is not directly connected to the audit so they can provide fresh eyes. If possible, ask someone from the department or function audited to review the report as well.

9. Avoid blame — state the facts.

Aim to preserve the relationship with the auditees by being as objective as possible and avoiding blame. Simply state observations and recommended actions.

10. Rotate for fresh eyes.

Avoid soft statements when making recommendations (such as "Management should consider...") and opt for solid recommendations and calls to action instead.

Checklist: Audit reporting

- ☐ Work off a findings sheet that has been discussed and agreed to by management.
  - Tech tip: leverage Optro's issue management tracking capability.
- ☐ Every detail in the report correlates to what is captured in your issue repository.
- ☐ Use bullet points wherever possible and keep them concise for readability.
- ☐ Remove all unnecessary adjectives and adverbs.
- ☐ Highlight/circle/bold/italicize major takeaways.
- ☐ Use numbers or percentages to describe facts wherever possible.
- ☐ Use tables or graphs to summarize key information wherever possible.
- ☐ The report contains clear references, indices, and appendices.
- ☐ All verifiable claims are annotated.
- ☐ All annotated claims map to a reference.
- ☐ Remove soft/indirect recommendations (such as "Management should consider...") and replace them with direct language recommending corrective actions.
- ☐ Remove blaming/inflammatory statements (such as "Management failed to..."). Instead, state the issue and the recommended corrective action.
- ☐ Check spelling: use Microsoft Word or Google Docs spell-check tools.
- ☐ Check readability: use the Flesch Reading Ease or Flesch-Kincaid Grade Level tests.

Issue management

In this chapter

Optimizing your issue management program

How quickly issues are remediated is a sign of how effectively an organization is managing risk, because this:

- Indicates issues identified are relevant to the organization.
- Illustrates how efficiently the business is operating.
- Demonstrates the business' receptiveness to change and risk tolerance.

The challenge

Often, different business functions may be performing duplicate issue tracking activities using inconsistent methodologies. Multiple issue logs in varying formats tracking similar outcomes create inefficiencies for all stakeholders involved, including issue owners being asked to provide the same information to various groups at different times. Such practices limit the organization's ability to achieve a holistic view of issues, resulting in inefficiencies such as poor data quality and incomplete organizational impact analysis, lack of issue prioritization and clear accountability, and unclear issue closure processes.

The solution

Invest in optimizing your issue management program. Doing so can reduce duplicate efforts across assurance groups, improve data quality, and raise closure rates — leading to cost savings and increased audit effectiveness. The following are best practices for building a well-rounded issue management program.

8 tips for building a well-rounded issue management program

1. Standardize

Apply a standardized risk rating and issue identification framework across departments that capture and identify issues. Bring multiple issue stakeholders together to prevent duplicate administrative work. This strengthens the ability to report on issues uniformly across the business, correctly identify root causes, and assign the appropriate remediation action plans to issue owners.

- Framework examples include: the five C's (Criteria, Condition, Cause, Consequence, Corrective action plans), an issue rating scorecard, or a custom methodology.

Tech tip

Optro's generative AI capabilities provide a starting point for drafting issue, risk, and control descriptions. The drafted text can be easily shortened, lengthened, or refined for clarity by the AI and edited by a trained practitioner before it is accepted and published.

2. Connect

The standard issue rating framework should mirror the way the business is evaluating risks by connecting to the organization's ERM framework. If issues are being uniformly managed across the organization, there is more opportunity to perform trend analysis and identify enterprise-wide themes on why issues are occurring — increasing the business's likelihood of proactively addressing those themes and preventing issues from reoccurring.

Tech tip

Optro helps standardize and centralize issue identification, follow-up, and reporting with an issue repository that ties issues directly to your risk universe. Drive risk-aware audit activities with real-time risk assessments and increase ownership with automated issue remediation workflows.

3. Set the tone

Strive for executive buy-in and a supportive tone at the top. A united executive leadership team that promotes a standard issue methodology helps embed issue management into risk culture across the organization. For example, align performance feedback and compensation to issue management metrics to incentivize early issue identification and implementation of corrective actions.

8 tips for building a well-rounded issue management program *cont'd*

4. Automate

Automated issue-tracking software helps auditors easily validate issue identification and follow up with issue owners during remediation. An audit management solution should:

- Enforce the issue management methodology. Apply a standardized issue rating and identification framework. If no framework exists, introduce and formally establish one during the implementation process. This ensures consistent organization-wide adherence to the standard methodology for managing issues.
- Have a validation workflow. The solution automates the issue follow-up process, letting auditors initiate an automated workflow that sends notification reminders to issue owners.
- Have agile reporting capabilities. Issues should be automatically reportable any time they are logged, and status should update in real time as issues move through the remediation process (validated, outstanding, overdue).

5. Report

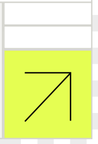
Provide different levels of reporting to department leaders, the executive team or risk committee, and the board of directors. Department leaders directly influence issue remediation, the executive team or risk committee has the power to provide the full scope of issues and identify issue themes, and the board should be aware of issues at a high level so that it can help enforce issue remediation.

Metrics to address in these reports are:

- Issues identified by department
- Issues identified by root cause
- Issues that are repeatedly identified
- Outstanding issues

Tech tip

With Optro's highly visual and configurable dashboards and reports, you can stay on top of key findings, monitor action plan status, and track the overall audit plan progress.



6. Analyze

Perform frequent analysis of issues to create awareness of lessons learned from past identified issues. In order to proactively prevent past identified issues from reoccurring, this should be done on a continuous basis, not as a point in time exercise.

8 tips for building a well-rounded issue management program *cont'd*

7. Lead

While different functions track issues, internal audit is optimally positioned to lead an enterprise issue management program due to its independence and unique view into issues across different areas of the business. The benefits of a streamlined enterprise issue management process include:

- Improved issue reporting to executives and the board.
- Improved risk management in the organization due to better identification of issue themes, leading to proactive deficiency prevention.
- Prevention of duplicate administrative work being performed across multiple teams or departments — this also reduces costs.
- Improved assurance that issues were corrected as management expected, due to internal audit's independence and objectivity.

8. Collaborate and consult

Once issues have been identified and successfully remediated, take the opportunity to train and educate stakeholders on the history of the issue to create awareness around how to prevent it from reoccurring in the future. This important step offers an opportunity for internal audit to put on its consultant hat and provide further value to the business in an otherwise routine process.

Checklist: 8 Tips for building a well-rounded issue management program

1 STANDARDIZE.

Apply a standardized risk rating and issue identification framework consistently across the organization.

2 CONNECT.

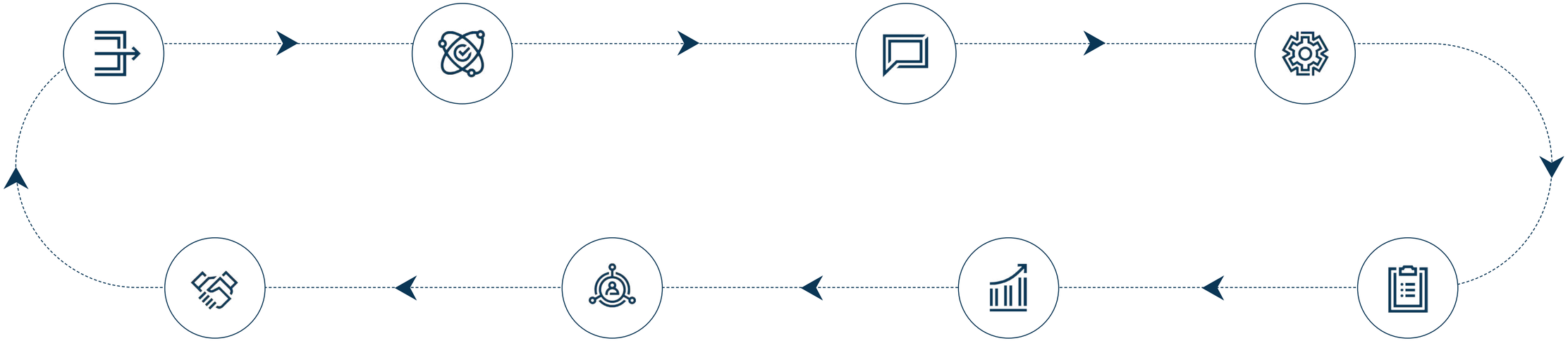
Connect your issue management to the organization's ERM framework.

3 SET THE TONE.

Strive for executive buy-in and a supportive tone at the top.

4 AUTOMATE.

Leverage automated issue-tracking software.



5 REPORT.

Provide different levels of reporting to issue stakeholders.

6 ANALYZE.

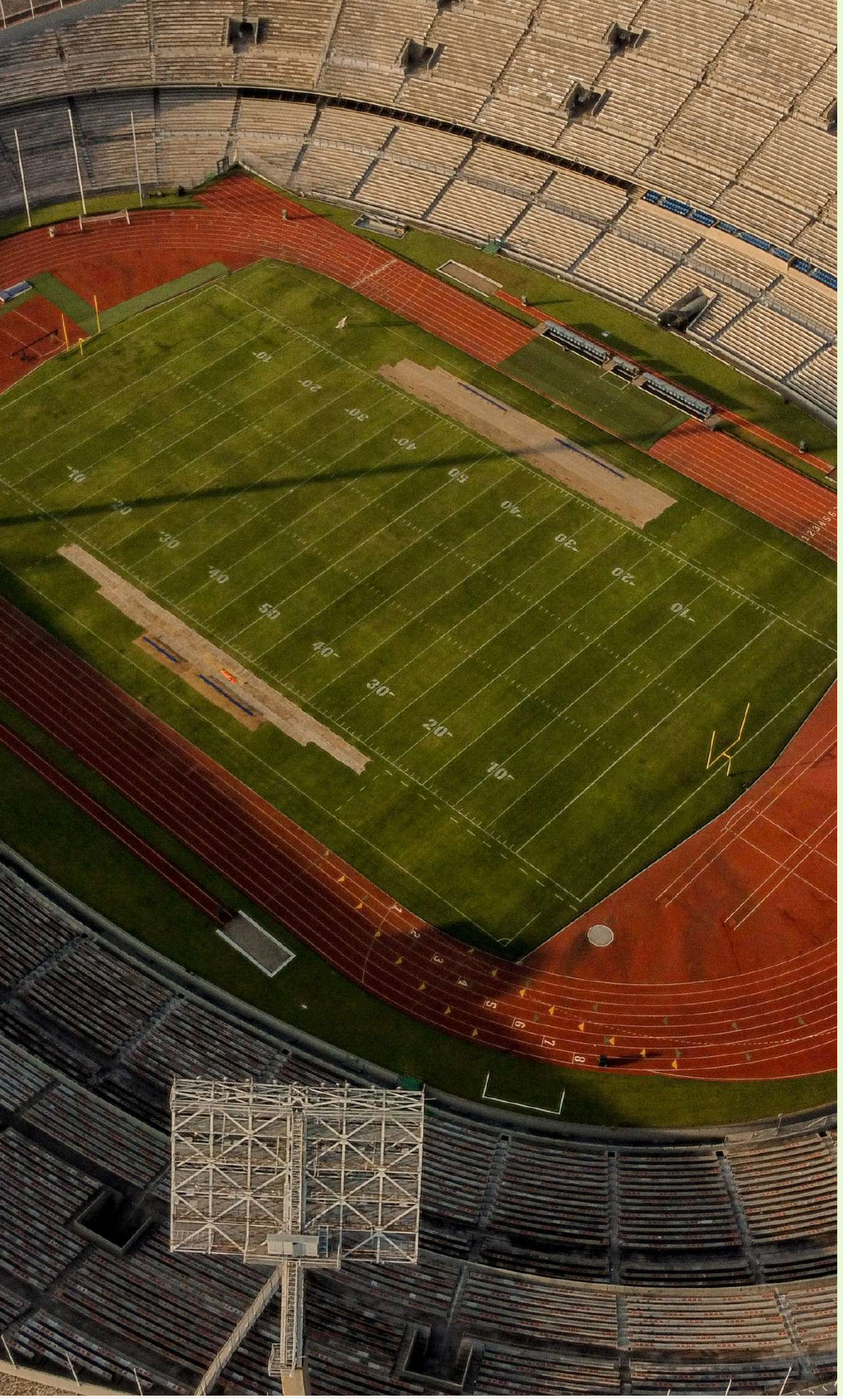
Perform frequent analysis to proactively prevent past identified issues from reoccurring.

7 LEAD.

Let internal audit lead your issues management program due to its independence and unique view across the business.

8 COLLABORATE & CONSULT.

Train and educate issue stakeholders to help prevent issues from reoccurring.



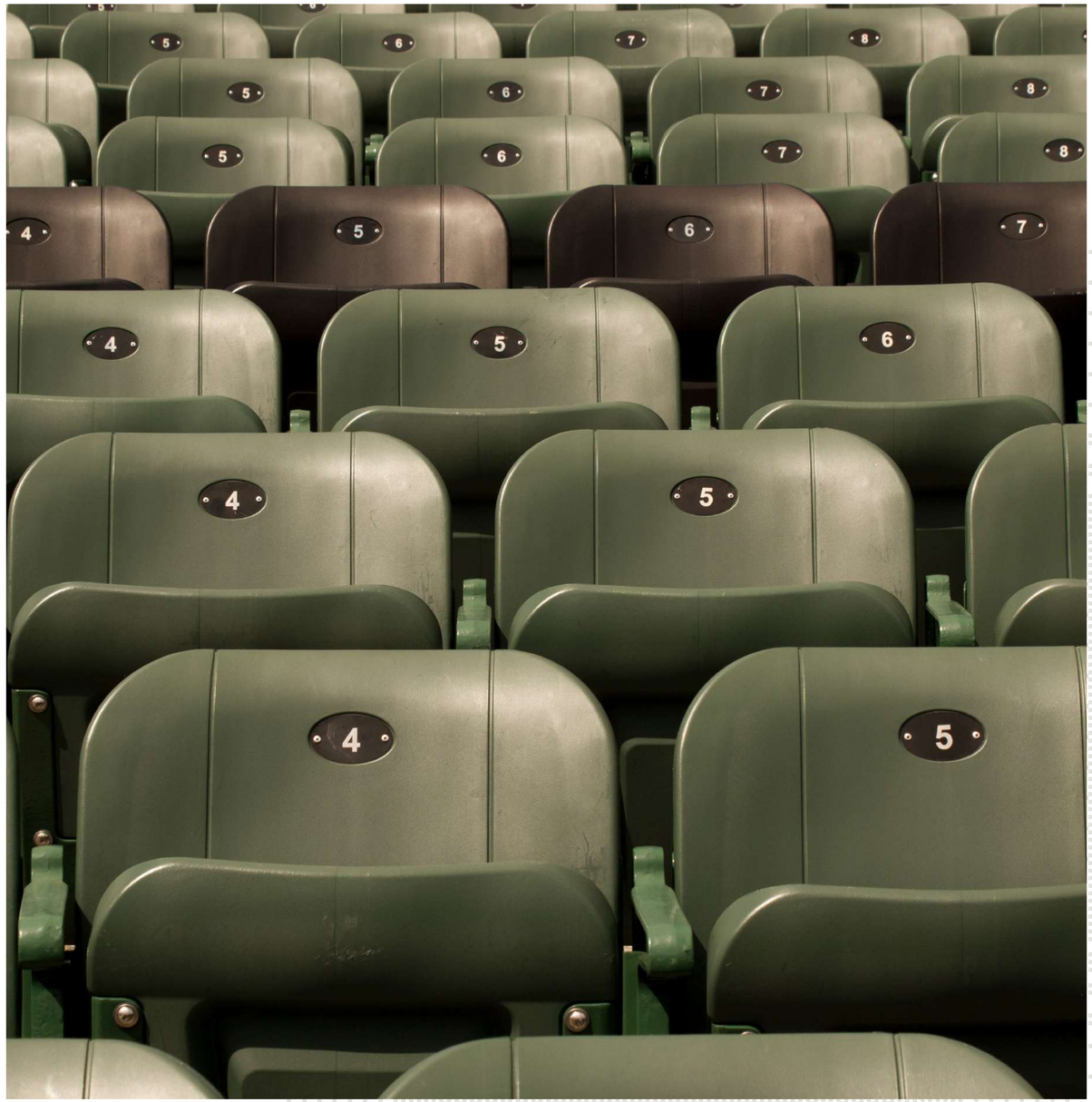
Scaling

In this chapter

Scaling with AI and other advanced technologies

Since Microsoft Excel was first introduced in the late 1980s, the business landscape has undergone significant technological advancements that have improved the way internal auditors perform their jobs. In particular, the rise of **AI, advanced analytics, and technologies purpose-built to connect audit, risk, compliance, InfoSec, and ESG teams** enable these groups to perform their activities more efficiently and effectively than ever before.

The effect of these technologies on the internal audit industry is apparent anywhere you look. When technology is successfully deployed, teams benefit from improved efficiency and collaboration, better risk insights, and more comprehensive and accurate testing results. Technology's critical role as a capacity multiplier for auditors is even reflected multiple times throughout the updated IIA Standards. Of particular note is Standard 10.3's language requiring **CAEs to communicate the impact of technology limitations on the internal audit function to the board and senior management**. Examples of evidence of conformance with Standard 10.3 include a technology section in the internal audit strategic plan or any other documented technology plans.



AI's role: Driving efficiency and accuracy across GRC teams

Technology solutions that employ machine learning (a subset of AI that uses algorithms to train on data and make recommendations or predictions) and generative AI (a subset of machine learning that generates content learned from the data on which it's trained) offer the most compelling current evidence for AI's ability to accelerate and enhance assurance-related activities.

Generative AI, where the AI can provide content creation and suggestions as a user types in the interface, is being used to automate a wide range of activities involving writing. Areas where GenAI has accelerated and enhanced audit programs include:

- Compliance activities, such as writing control requirements and control details
- Assurance activities, such as creating audit descriptions and worksteps
- Risk management activities, such as creating risk descriptions
- Governance activities, including narrative writing and report writing
- Issue/exception creation activities used across GRC functions

Machine learning (ML) models, which use algorithms trained on available data to emulate logical decision-making, are being used for activities such as generating intelligent recommendations based on user data, as well as detecting intrusions and malicious behavior. Areas where ML models have accelerated audit, risk, and compliance processes include:

- Suggesting mapping between controls and framework requirements
- Suggesting mapping between issues and controls, risks, and audit worksteps
- Uncovering duplicate issues in your GRC environment
- Audit or assessment evidence reuse
- Anomaly detection in controls testing

89% of organizations plan to use AI despite anticipated challenges like data privacy concerns, according to Optro's survey of over 500 InfoSec, audit, risk, and compliance leaders for *The Connected Risk Report*. Our research reveals that **two-thirds** of organizations that have integrated some form of AI into their risk management processes report **increased efficiency, time savings, and better data analysis and insights.** Additionally, over **50% of respondents** have experienced **increased data accuracy and reliability and enhanced risk detection and mitigation.** These benefits demonstrate AI's potential to streamline audit, risk, and compliance processes, allowing organizations to identify and address risks more effectively while reducing manual workloads.

Tech tip

Purpose-built generative AI solutions, such as Optro's native AI capabilities, can streamline, automate, and improve the accuracy of your internal audit program.

- **Instantly generate control, risk, and issue language.** The drafted text can be easily shortened, lengthened, or refined for clarity by the AI and edited by a trained practitioner before it is accepted and published.
- **Generate executive summaries of internal and external audits** that uncover insights and high-priority action items. Save time and ensure that escalations and key tasks never fall through the cracks.
- **Uncover insights in your data to connect risks and impacted controls**, suggest mapping between controls and framework requirements, uncover duplicate issues, and more.
- **Leverage Intelligent Staffing** to accelerate staffing decisions, meet new IIA Standards, and assign the best resources for an engagement with auto-generated recommendations based on your team's skills and qualifications.
- **Leverage Cross-Audit Summary** to automate the consolidation of audit context, findings, and trends into a single, executive-level report.

To learn how Optro can help your team work faster and smarter with AI-powered insights and intelligent recommendations to augment your capabilities and business impact, schedule a tailored demo today.

89%

of organizations plan to use AI

Advanced analytics' role: Driving more accurate testing

Advanced analytics, involving the autonomous or semi-autonomous examination of data or content using sophisticated techniques and tools, enable auditors to ask insightful questions about their business and test full populations instead of just a sample. Advanced analytics' value lies in their ability to provide more accurate testing results with significantly greater efficiency, uncover reoccurring issues in high-risk areas, enhance collaboration across all three lines of defense, and improve continuous auditing.

Out-of-the-box analytics solutions, such as Optro Analytics, can streamline data management and drive efficiency, scalability, and alignment across teams.

- Perform full population SOX testing for greater assurance. Improve the accuracy and performance of your SOX work.
- Streamline internal audit and compliance programs and testing. Automate evidence collection and testing, and perform continuous auditing with audit context, workflow certification, and version control to improve the accuracy and performance of your audit and compliance work.
- Centrally manage all of your analytics and automation. Build your governance program around automation and analytics with Optro's centralized data hub.

Tech tip

Optro provides the flexibility of our native, no-code audit analytics solution or the seamless integration with your preferred, best-in-class analytic applications to provide your teams with unparalleled control, scalability, and team efficiency.

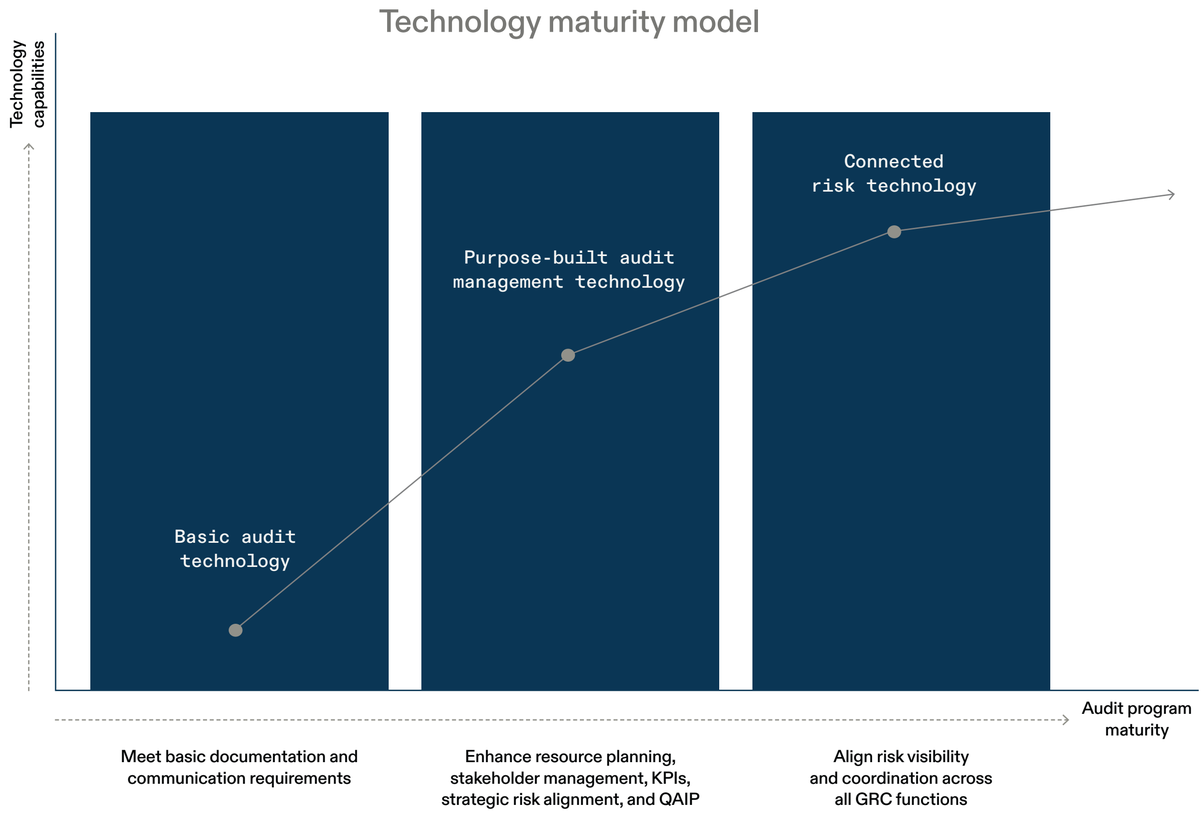
Scaling with connected risk

A connected risk approach aims to strengthen cross-functional collaboration and create greater risk visibility by uniting previously siloed audit, risk, and controls data. **Connected risk — sometimes referred to as integrated risk management** — enables audit, risk, and compliance teams to work smarter through leveraging enabling technologies that connect teams, unify data, and automate processes. Internal audit is well-positioned to take the lead. Indeed, a 2024 Optro survey of audit leaders found that CAEs indicated **integrated risk management as the #1 area in which they should have more responsibility.**

The Technology Maturity Model illustrates the progression of audit efficacy in correlation to increasing technological capabilities. **The three categories of technological capabilities described in the visual are:**

1. Basic audit technology. Typically used as a document repository and leveraged to streamline testing and maintain an audit trail via workflow automation.
2. Purpose-built audit management technology. Specifically built for and used by audit stakeholders and often includes advanced technologies such as AI and analytics to help streamline audit processes, e.g., resource planning, stakeholder management, KPI tracking, strategic risk alignment, and QAIP.
3. Connected risk technology. Centralizes data, workflows, and collaboration across all audit, risk, compliance, and control functions, as well as regulators and other third parties. Has built-in or integrated analytics and AI capabilities, enabling audit teams to leverage AI insights and recommendations on their data, surface and manage more risk, improve team efficiency and collaboration, and increase frontline ownership.

As organizations move along the technology maturity model toward connected risk, they will drive improved risk ownership and empower their business to make better decisions. While choosing to embark on a connected risk initiative takes significant time and effort, it is an undertaking that reaps benefits every step of the way, e.g., a universal risk register, less duplicative assurance efforts, reduced audit fatigue, and improved risk ownership. As you progress, remember that each small milestone is an improvement and should be celebrated as a win. Like most progressive initiatives, iteration, patience, and keeping the big picture in mind are essential for success.



Leading the way forward

What sets great audit teams apart are forward-thinking leaders who prioritize the use of capacity-multiplying technologies such as AI, advanced analytics, and connected risk solutions, enabling their auditors to focus on more value-add projects and better collaborate across the three lines.

Leveraging the best practices provided in this playbook — in addition to harnessing the power of the advanced technologies described — will pave the way to more optimal productivity, collaboration with other assurance stakeholders, and value-add capabilities.

When done hand in hand, under careful and mindful audit leadership focused on connected risk, such practices can drive efficiencies and value to the organization that multiply year over year.

Tech tip

An IDC White Paper, sponsored by Optro, found the following productivity gains for customers using Optro's connected risk platform:

- 45% increase in productivity.
- 50% increase in stakeholder engagement.
- 281% three-year ROI.

To learn how Optro can elevate your audit, risk, compliance, InfoSec, and ESG programs with a modern, cross-functional approach to managing risk, schedule a tailored demo today.

About Optro

Optro is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 50% of the Fortune 500 leverage Optro to move their businesses forward with greater clarity and agility. Optro is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte. Explore how to transform risk into opportunity at Optro.ai or request a personalized demo today.

Contributors

Michelle Brown

Michelle is an Implementation Project Lead at Optro. An experienced auditor with a Masters in Accounting and an EY alumnus, Michelle has spent nearly a decade specializing in compliance audits with a focus on data protection, information privacy, and technology risk.

Christian Burich

Christian is a Customer Success Manager at Optro. Prior to joining Optro, Christian spent five years in the IT Audit/ GRC space, specializing in information technology audits, cybersecurity, SOX, and regulatory compliance.

Cristi Cao

Cristi is a Director of Product Solutions at Optro. Prior to Optro, Cristi served as an Internal Audit Advisor in city government.

Aaron Dillon

Aaron is the Director of Product Management for Automation & Intelligence at Optro. Aaron has ten years of experience developing B2B SaaS solutions and building platform products.

Ali Glickstein

Ali is an Account Executive at Optro. Prior to joining Optro, Ali spent seven years at JPMorgan Chase and three years at a commercial real estate firm, with her most recent role being VP of Operations & Strategy and ESG Program Lead.

Daniel Green

Daniel is a Regional Director of Product Solutions at Optro. Daniel started his career at PwC, and served as a Senior Internal Auditor in the electronics industry.

Key Perry

Key is a Product Solutions Manager at Optro. Prior to joining Optro, she served as a SOX Compliance Manager at Azenta Life Sciences and an Internal Audit Supervisor at Waters Corporation. Key specializes in process transformation and automation.

Weston Prohaska

Weston is the Analytics Content Manager for Optro Analytics. Weston is a licensed CPA and has 6 years of experience in professional services, with a strong focus in data analytics and automation in the accounting and finance space.

Christina Ramos

Christina is a Senior Manager of Implementation and Professional Services at Optro. Prior to Optro, Christina spent 10 years at Deloitte as an external auditor focused on PCAOB audits, including two years as a PCAOB advisor in Japan.

Ryan Saw

Ryan is a Manager of Scale Customer Success at Optro. Prior to joining Optro, Ryan spent three years with Moss Adams in the advisory practice, specializing in SOX compliance and operational audits.

Jorge Solis

Jorge is the Director of Product Management for OpsAudit at Optro. Jorge has over ten years of product management experience helping deliver customer-centric solutions for a variety of industries.

Vi Tran

Vi is a Product Marketing Manager at Optro. Prior to joining Optro, Vi served as an external auditor at PwC, Internal Controls Senior Analyst at Targa Resources, and Associate Manager at The Siegfried Group.

Aaron Wright

Aaron is a Director of Audit Solutions at Optro. Before joining Optro, Aaron was an Internal IT Audit Advisor at Cardinal Health.