ETHICO

Guide to Right-Sized Enterprise Risk Management for E&C Teams

Why compliance professionals don’t need enterprise-grade complexity to achieve audit-ready risk management

Read Time: 20-25 min.

Introduction

THE OVERSELLING OF ENTERPRISE RISK MANAGEMENT

For years, compliance teams have been sold a story: effective risk management requires enterprise-grade platforms designed for Chief Risk Officers managing operational, financial, strategic, and compliance risks across multinational organizations.

The reality? Most ethics and compliance teams don't need—and can't effectively use—platforms built for enterprise-wide risk management.

According to Gartner's 2025 research, 76% of compliance leaders are prioritizing improvements to risk management approaches. Yet many are being pushed toward solutions that don't match their actual needs or resources.

You need something different.

The unsettled regulatory and legal environment now tops the list of emerging risks for organizations globally. Compliance complexity is increasing, and costs are mounting. Against this backdrop, the last thing E&C teams need is more complexity in their risk management tools.

This guide shows compliance professionals how to achieve systematic, audit-ready risk management without the overhead, cost, and complexity of enterprise platforms designed for someone else's job.

The Enterprise Trap

What enterprise risk management actually means

Enterprise Risk Management (ERM) platforms are designed to serve Chief Risk Officers and executive leadership managing risks across entire organizations:

- Operational risks: Supply chain disruptions, business continuity, vendor dependencies
- Financial risks: Market volatility, credit exposure, liquidity management, currency fluctuations
- Strategic risks: Competitive threats, M&A integration, market positioning
- Compliance risks: Regulatory violations, audit findings, policy adherence

When you're an ethics and compliance professional focused primarily on compliance risks, you're being asked to adopt a platform designed for someone else's job.

The Complexity Problem

What enterprise risk management actually means

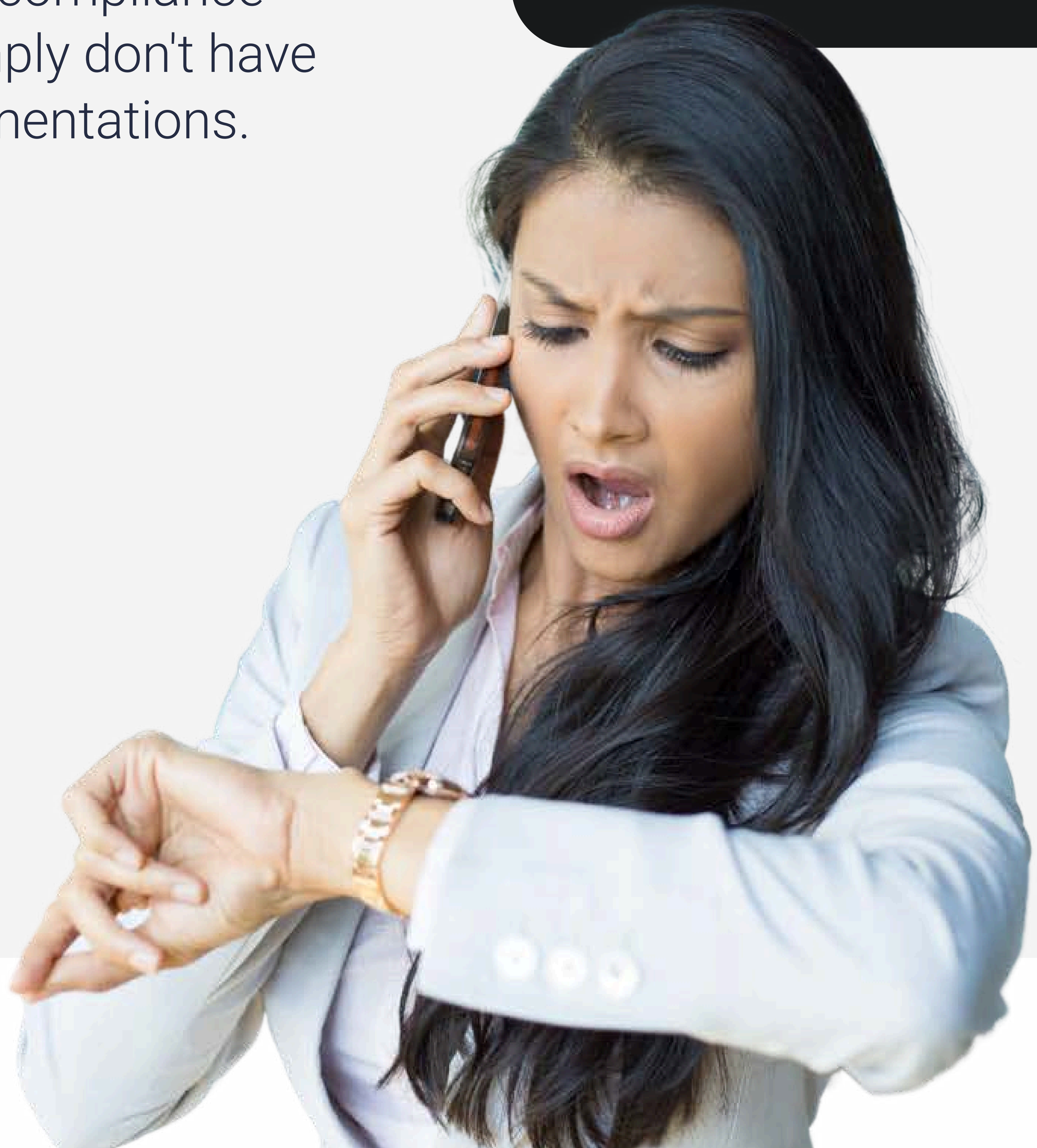
Implementing enterprise risk management platforms typically requires:

- 6-12 months for full implementation
- IT project teams managing technical infrastructure and integrations
- External consultants for configuration, customization, and training
- Ongoing system administrators to maintain the platform
- Change management programs to drive adoption across the organization
- Six-figure budgets (or higher) for licensing, services, and maintenance

According to the 2023 White & Case/KPMG Global Compliance Risk Benchmarking Survey, while 31% of organizations increased compliance budgets, 13% actually decreased them. Most E&C teams simply don't have the time, budget, or technical resources for enterprise implementations.

The Hidden Cost

While you're spending months implementing complex platforms, risks are going unidentified and unaddressed.



What E&C Teams Actually Need

Compliance Risk Assessment vs. Enterprise Risk Management

The difference isn't just semantic—it fundamentally changes what you're building and how you'll succeed.

Enterprise Risk Management focuses on:

- Risk registers for all enterprise risks across the organization
- Financial risk modeling and quantification
- Strategic risk scenario planning
- Operational risk monitoring and KRIs
- Complex risk taxonomies spanning multiple business units
- Board-level strategic reporting on enterprise exposure
- Integration with financial systems and ERP platforms

Compliance Risk Management focuses on:

- Regulatory compliance risk evaluation
- Ethics and integrity risk screening
- Workplace conduct risk assessment
- Conflict of interest identification
- Third-party compliance risk due diligence
- Audit-ready documentation demonstrating program effectiveness
- Evidence of systematic, risk-based compliance program

According to ECI's 2023 Global Business Ethics Survey, 48% of organizations report weak ethical culture. The problem isn't lack of enterprise software—it's lack of systematic approaches to identifying and addressing compliance-specific risks.

The Value Drivers That Matter for Compliance

When evaluating risk management approaches, focus on these four value drivers:

01 Scale risk identification with ease and efficiency

The White & Case/KPMG survey found that 79% of organizations conduct documented risk assessments. But many struggle with consistency and participation. You need to:

- Automate risk assessments with HR-driven campaigns that target the right people
- Engage stakeholders with targeted requests, not generic surveys sent to everyone
- Customize assessments using templates designed for E&C teams
- Ensure data integrity and consistency through standardized methodologies

02 Activate your compliance team and unlock true impact

With only 56% of employees perceiving strong ethical culture (ECI 2025 U.S. Trends Report), your team can't do everything alone. You need to:

- Provide risk owners with customized views to update submitted risks
- Spend less time chasing information from busy stakeholders
- Boost team impact by offering ready-to-deploy assessments to cross-functional teams
- Alleviate duplicative requests that create survey fatigue

The Value Drivers That Matter for Compliance

When evaluating risk management approaches, focus on these four value drivers:

03 Demonstrate audit readiness and defensible program management

The DOJ's 2024 guidance update explicitly emphasizes data-driven risk detection and measurement of compliance effectiveness. You need to:

- Show regulators a targeted risk-based approach with remediation plans tied to assessments
- Document risk scoring methodologies that are defensible
- Increase program participation through simplified workflows
- Present only relevant information and questions to each audience

04 Reinforce risk culture through operational fluidity

According to Gartner, embedded controls that guide employees within workflows reduce compliance failures by 58%. You need to:

- Provide a friendly risk owner experience that encourages engagement
- Stop making compliance play IT support for every system issue
- Ensure operational fluidity with other enterprise and IT risk teams
- Enable robust integrations without requiring IT project teams

Right-Sizing Your Approach

What “right-sized” actually means

Right-sized risk management for ethics and compliance teams means:

Focused Scope Assess compliance, ethics, and regulatory risks—not operational or financial risks outside your purview. When 85% of respondents in PwC's 2025 survey report increased regulatory complexity, you need laser focus on compliance-specific risks, not dilution across enterprise risk types.

Appropriate Complexity Use tools you can implement in weeks, not months, without IT project teams. Gartner predicts legal, risk, and compliance technology spend will double by 2027—but that doesn't mean every team needs enterprise platforms.

Practical Methodology Semi-quantitative risk scoring that compliance professionals can configure themselves. You shouldn't need risk management PhDs or consultants to adjust your impact and likelihood scales.

E&C-Specific Templates Pre-built assessments for HIPAA, SOX, conflicts of interest, third-party due diligence, workplace conduct—not generic enterprise risk frameworks that you have to customize heavily.

Audit-Ready Output Visual heat maps and documentation that satisfy regulators and demonstrate program effectiveness. The DOJ wants to see data-driven risk detection—give them clear, visual evidence of your systematic approach.

The Assessment-First Approach

Start with Risk Assessment, not Risk Registers

Enterprise platforms often start with building comprehensive risk registers and cataloging every possible risk across the organization. This can take months before you conduct a single assessment.

E&C teams need a different approach that delivers immediate value:

STEP ONE

Deploy Targeted Risk Assessments

Launch assessments to relevant stakeholders based on their role, department, or location. Use HR integration to automatically target the right people without manual list management.

STEP TWO

Analyze Responses to Identify Risk Concentrations

Review incoming assessment data to identify where risks are actually concentrated. Don't assume—let your stakeholders tell you where problems exist.

The Assessment-First Approach

Start with Risk Assessment, not Risk Registers

STEP THREE

Prioritize Risks Based on Scoring

Use standardized impact and likelihood scoring to objectively prioritize which risks require immediate attention versus monitoring.

STEP FOUR

Create Remediation Plans for High-RIsk Findings

Document specific action plans for risks scoring in your high-risk zones. Assign owners, set timelines, and track progress.

STEP FIVE

Track Improvements Through Follow-Up Assessments

Re-assess the same areas over time to demonstrate risk reduction and program effectiveness.

This assessment-first approach aligns with what regulators actually want to see: evidence that you're systematically identifying, prioritizing, and addressing compliance risks.

Real-World Example: From Spreadsheets to Systematic

Healthcare Compliance Director

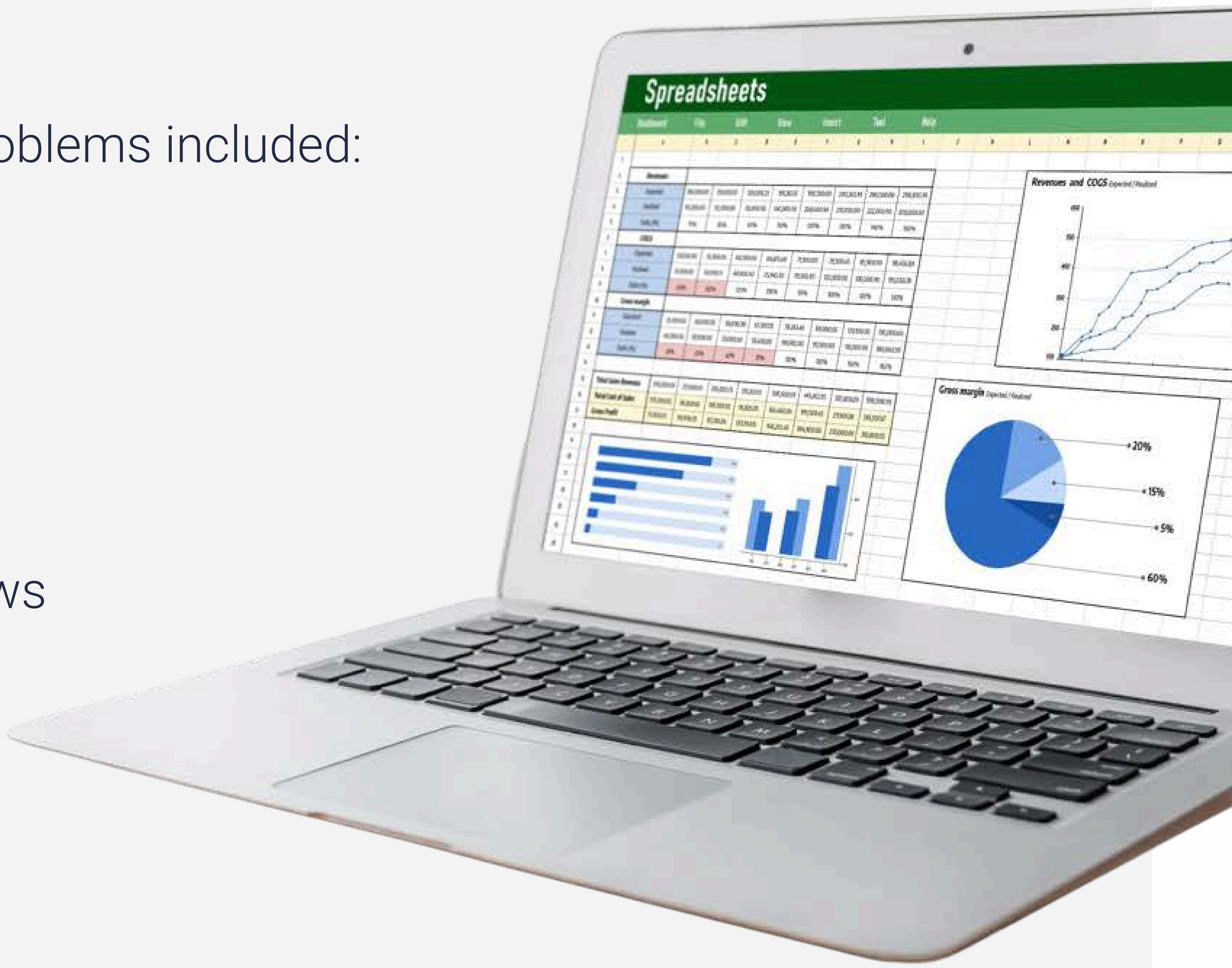
The Challenge

A mid-sized healthcare system's compliance director was using spreadsheets to track HIPAA risk assessments across 12 facilities. Leadership questioned whether the compliance program was truly risk-based. The annual board presentation consisted of manually created charts that took weeks to prepare and were out of date by the time they were presented.

Previous Approach

Annual spreadsheet sent to department heads asking about risks. Problems included:

- Inconsistent responses with no standardized methodology
- No way to track who hadn't responded without manual follow-up
- Difficult to aggregate results across facilities
- No visual representations of risk concentrations
- Impossible to trend year-over-year changes
- Leadership couldn't understand risk severity from spreadsheet rows



The Challenge

A mid-sized healthcare system's compliance director was using spreadsheets to track HIPAA risk assessments across 12 facilities. Leadership questioned whether the compliance program was truly risk-based. The annual board presentation consisted of manually created charts that took weeks to prepare and were out of date by the time they were presented.

Right-Sized Solution

Deployed HIPAA compliance risk assessment template with standardized impact/likelihood scoring. Used HR integration to automatically target assessments by role and location. Configured the system themselves in under two weeks.

Results After 30 Days:

- Launched first assessment in 2 weeks (vs. 2-3 months for spreadsheet coordination)
- 87% participation rate vs. 52% with spreadsheets
- Generated risk heat map for board presentation showing risk concentrations by facility
- Identified 3 critical risk areas requiring immediate remediation
- Demonstrated systematic, audit-ready risk methodology when regulators visited
- Compliance director spent time analyzing risks instead of chasing spreadsheet responses

The Difference Focus on **compliance risk assessment,** not enterprise complexity.

When You Might Actually Need Enterprise Risk Management

Enterprise Platforms Have Their Place

Be honest about whether you're the right audience for ERM platforms. You might genuinely need enterprise risk management if:

You're the Chief Risk Officer (not Chief Compliance Officer Your title includes "risk" and you're responsible for ALL enterprise risks—operational, financial, strategic, and compliance. You report to the CEO or CFO on enterprise-wide risk exposure.

Your Budget Supports Six-Figure Investments You can allocate $100,000+ for software licensing annually, plus implementation costs, plus dedicated system administrators. This doesn't strain your compliance budget.

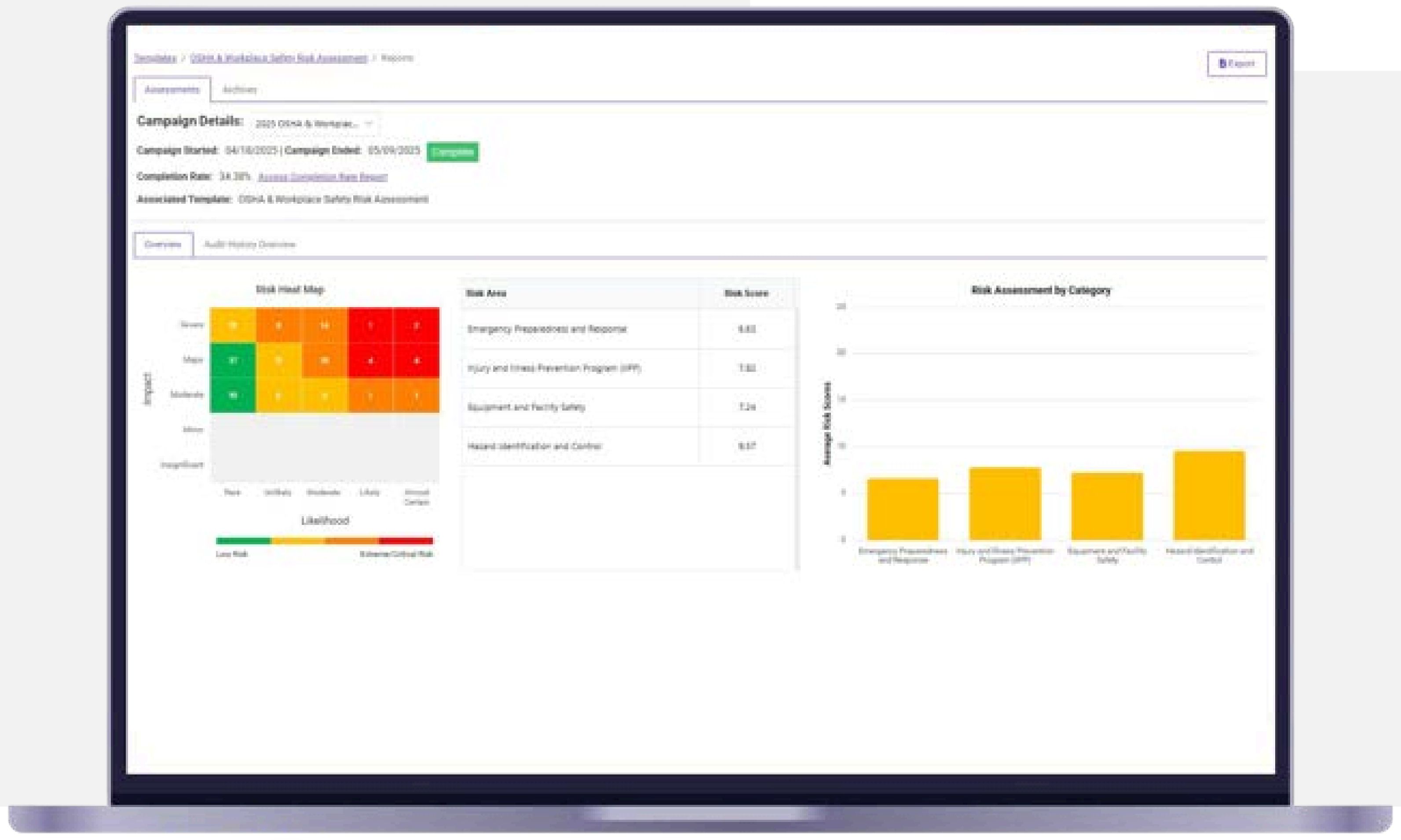
Your Organization Has a Dedicated Risk Management Team You have staff specifically focused on operational risks, business continuity, strategic risks, and financial risks—not just compliance. Multiple people work full-time on risk management.

You Have Existing IT Infrastructure Your organization already supports enterprise applications like SAP, Oracle, or similar platforms. You have IT teams experienced with complex integrations.

You're a Multinational Corporation You require complex risk aggregation across business units, countries, and legal entities. You're consolidating risk data from dozens of subsidiaries with different regulatory environments.

If this describes your situation, enterprise platforms may be appropriate. They're built for your use case.

For everyone else—which is most E&C teams—right-sized compliance risk assessment delivers better results faster and more cost-effectively.



Campaign Details: 2025 OSHA & Workplac...

Campaign Started: 04/18/2025 | Campaign Ended: 05/09/2025 Complete

Completion Rate: 34.38% Access Completion Rate Report

Associated Template: OSHA & Workplace Safety Risk Assessment

Risk Area	Risk Score
Emergency Preparedness and Response	6.83
Injury and Illness Prevention Program (IIPP)	7.82
Equipment and Facility Safety	7.24
Hazard Identification and Control	8.57

The Compliance Team's Risk Management Maturity Path

Build Your Program Progressively

Understanding where you are and where you need to be helps clarify what tools you actually need.

Level 1 - Ad Hoc (Where most teams start)

Characteristics:
- Spreadsheets tracking risks inconsistently
- No standardized methodology
- Reactive responses only—assessments happen when auditors ask
- Difficult to demonstrate program effectiveness
- Leadership questions risk-based approach

Move to Level 2 with right-sized risk assessment software

Level 2 - Developing (Target for year 1)

Characteristics:
- Systematic assessments with regular cadence
- Standardized impact/likelihood scoring
- Visual reporting that leadership understands
- Documented methodology that's defensible
- Beginning to identify risk trends

Strengthen with remediation tracking and trending

Level 3 - Defined (Target for year 2-3)

Characteristics:
- Regular assessment cycles covering all major risk areas
- Established methodology that stakeholders understand
- Audit-ready documentation readily available
- Integration with broader compliance program
- Year-over-year risk trending showing improvements

According to the ECI survey, organizations with strong ethical culture have significantly lower rates of misconduct. Level 3 maturity contributes to this cultural strength by making risk management systematic rather than sporadic.

Enhance with control management and policy integration

Level 4 - Managed (Advanced state)

Characteristics:
- Integrated risk and compliance program
- Quantified effectiveness metrics
- Continuous improvement processes
- Risk data informing resource allocation
- Predictive risk analytics beginning

The Compliance Team's Risk Management Maturity Path

Build Your Program Progressively

Understanding where you are and where you need to be helps clarify what tools you actually need.

Level 5 - Optimized (Mature state)

Characteristics:

- Predictive risk analytics identifying emerging risks
- Full integration with enterprise systems
- Risk intelligence driving strategic decisions
- Advanced automation and AI capabilities
- Industry-leading program maturity

The key insight: Most E&C teams should focus on reaching Level 3 before considering enterprise platforms. Right-sized risk assessment gets you there without the complexity and cost of enterprise tools designed for Level 4-5 organizations.
Gartner research shows that 76% of compliance leaders are prioritizing improvements to risk management. But improvement doesn't mean complexity—it means moving from Level 1 to Level 3 with appropriate tools.

Key Capabilities for Right-Sized Risk Management

What Your Compliance Risk Assessment Tool Must Do

When evaluating tools, use this checklist to ensure you're getting what compliance teams actually need:

Essential Capabilities

- □ **Deploy assessments quickly:** Launch new assessments in days, not months
- □ **Target by role/ department:** Use HR data to automatically reach the right stakeholders
- □ **Configure scoring yourself:** Adjust impact and likelihood scales without IT support

Valuable, Non-Essential

- □ Integration with case management systems
- □ Remediation plan tracking with workflows
- □ Risk register capabilities for documentation

Probably Don't Need

- □ Financial loss quantification models (unless you're in financial services with specific requirements)
- □ Monte Carlo simulation capabilities
- □ Operational risk KRIs across business units
- □ Complex risk appetite frameworks at enterprise level

These capabilities directly support the four value drivers: **scaling risk identification, activating your team, demonstrating audit readiness, and reinforcing risk culture.**

Key Capabilities for Right-Sized Risk Management

Essential Capabilities

- □ **Generate visual heat maps:** Automatically create risk visualizations for leadership
- □ **Provide E&C templates:** Access pre-built assessments for common compliance risks
- □ **Track participation:** Monitor response rates and send targeted reminders
- □ **Create audit documentation:** Generate reports demonstrating systematic methodology
- □ **Support branching logic:** Show conditional questions based on previous answers

Valuable, Non-Essential

- □ Control management functions
- □ Policy acknowledgment tracking
- □ Third-party risk due diligence workflow

Probably Don't Need

- □ Enterprise risk taxonomy management
- □ Strategic scenario planning modules
- □ Boardroom-level strategy risk dashboards

Choose tools based on what you'll actually use daily, not what sounds impressive in vendor demos.

Avoiding the Feature Bloat Trap

More Features ≠ Better Risk Management

Enterprise platforms tout hundreds of features. The question is: how many will your 3-7 person compliance team actually use?

Features E&C Teams Rarely Use

- Financial risk modeling: Unless you're in treasury or finance, you don't need to model currency exposure or interest rate risk
- Operational KRIs: Real-time monitoring of manufacturing defects or supply chain metrics isn't your job
- Strategic scenario planning: "What if we acquire a competitor?" is an executive team question, not a compliance risk assessment
- Complex taxonomy management: Maintaining enterprise-wide risk category structures across business units
- Board strategy modules: Strategy presentations with competitive positioning analysis

Features E&C Teams Use Daily:

- Simple assessment deployment: Create and launch new assessments quickly
- Visual risk reporting: Heat maps and dashboards leadership can understand immediately
- Template libraries: Pre-built assessments for HIPAA, SOX, conflicts, third parties
- Participation tracking: See who's responded, send reminders, monitor completion
- Remediation documentation: Track what you're doing about high-risk findings

The bloat trap: Vendors demonstrate impressive features you'll never use. You pay for capabilities designed for Chief Risk Officers managing $10B+ organizations. Your 5-person team struggles with complexity instead of identifying risks.

The right-sized alternative: Tools focused on compliance risk assessment that your team can actually master and use effectively.

The Cost of Complexity

Hidden Costs of Enterprise Platforms for Small Teams

When considering enterprise platforms, look beyond software licensing to understand true total cost of ownership:

Direct Costs

- Software licensing: $30,000 - $500,000+ annually depending on users and modules
- Implementation services: $100,000 - $200,000 for configuration and customization
- System administrator salary: $80,000 - $120,000 annually for dedicated admin
- Training and change management: $30,000+ for initial training and ongoing support
- Maintenance and upgrades: 15-20% of licensing fees annually

Annual Total: $150,000 - $700,000+ for small to mid-sized organizations

Indirect Costs

- 6-12 months before seeing value: While implementing, risks go unidentified
- Compliance team time diverted: Your limited staff becomes system administrators instead of compliance professionals
- Opportunity cost: Delayed risk identification means delayed remediation
- Low adoption rates: Complex systems require constant re-training and support
- Consultant dependency: Every configuration change requires expensive consultants
- IT resource drain: Your IT team has more critical priorities than supporting your risk platform

Throwing money at complex platforms doesn't equal better risk management.

Right-Sized Alternative

- Implementation in weeks: Use existing staff without IT project teams
- Transparent pricing: Know exactly what you're paying with no hidden costs
- No dedicated administrator: Compliance team manages the system themselves
- Immediate value: Start identifying risks from day one, not month 12
- Focus on risk mitigation: Invest resources in addressing risks, not managing software

The question isn't just "Can we afford this platform?" but "Can we afford to divert our limited compliance resources to system administration instead of compliance work?"

Building Your Business Case

How to Justify Right-Sized Risk Management to Leadership

Different stakeholders care about different aspects of risk management tools. Tailor your business case accordingly:

For CFOs (Cost Justification)

- "We can achieve audit-ready, systematic risk management for a fraction of enterprise platform costs. Instead of $200,000+ in implementation and licensing, we're looking at implementation in weeks with our existing staff and predictable costs. This lets us invest savings in actual risk remediation rather than software complexity."
- Key points:
  - Total cost comparison over 3 years
  - No IT project costs
  - No dedicated administrator salary
  - Faster time to value means earlier risk identification

For Audit Committees (Regulatory Compliance)

- "Our approach provides documented, systematic risk assessment methodology that satisfies DOJ expectations and regulator requirements without unnecessary complexity. We're focusing on demonstrating program effectiveness through data-driven risk detection—exactly what the 2024 DOJ guidance emphasizes."
- Key points:
  - Audit-ready documentation
  - Defensible methodology
  - Visual risk reporting for board presentations
  - Evidence of systematic, risk-based approach

Building Your Business Case

How to Justify Right-Sized Risk Management to Leadership

Different stakeholders care about different aspects of risk management tools. Tailor your business case accordingly:

For IT Leadership (Technical Requirements)

- "This is a cloud-based tool requiring no IT implementation project, no infrastructure investment, and no ongoing system administration. We're not creating another system for your team to support. The vendor handles all technical infrastructure, security, and maintenance."
- Key points:
  - No IT project team required
  - No infrastructure costs
  - No ongoing support burden
  - Cloud-based with vendor-managed security
  - Faster time to value means earlier risk identification

For Chief Compliance Officers (Program Effectiveness)

- "We can demonstrate program effectiveness and identify risks without diverting our small team to managing complex software. This lets us focus on compliance work rather than becoming system administrators."
- Key points:
  - More time for compliance work
  - Systematic risk identification
  - Better stakeholder engagement
  - Improved board reporting
- According to PwC's 2025 Global Compliance Survey, 47% of compliance professionals cite organizational complexity as limiting effectiveness. Don't add software complexity to organizational complexity.

Implementation Roadmap

From Decision to Value in 30 Days

One of the biggest advantages of right-sized tools: speed to value. Here's a realistic 30-day implementation roadmap:

Compare this to 6-12 month enterprise implementations where you're still in configuration phase after 30 days.

WEEK ONE

DAYS 1-2

- Platform setup and user provisioning
- Admin training on platform basics
- Security and access configuration

DAYS 3-5

- Review template library
- Select starting assessments (recommend 2-3 for first cycle)
- Configure risk scoring methodology (impact/likelihood scales)
- Create initial contact lists using HR data integration

Foundation

WEEK TWO

DAYS 6-8

- Customize assessment questions and branching logic
- Configure automated reminders and communications
- Set up role-based targeting rules

DAYS 9-10

- Test assessments with pilot group (5-10 people)
- Refine questions based on pilot feedback
- Finalize launch communications

Customization & Testing

WEEK THREE

DAYS 11-12

- Launch first assessment campaign
- Monitor initial participation rates
- Respond to stakeholder questions

DAYS 13-17

- Send automated reminder communications
- Review incoming responses in real-time
- Begin preliminary risk analysis
- Identify high-risk findings requiring immediate attention

Launch & Monitor

WEEK FOUR

DAYS 18-20

- Complete risk analysis as responses close
- Generate risk heat maps showing concentrations
- Create remediation plans for critical risks

DAYS 21-25

- Prepare leadership presentation with visual risk reporting
- Present findings to compliance committee or executive team
- Assign remediation owners and timelines

Analysis & Reporting

DAYS 26-30

- Document lessons learned from first assessment
- Plan next assessment cycle
- Begin tracking remediation progress

30-DAY DELIVERABLES

- 2-3 completed risk assessments
- Visual risk heat map identifying priorities
- Documented remediation plans for high-risk findings
- Established methodology for ongoing assessments
- Demonstrated value to leadership

Common Objections Addressed

"But Won't We Outgrow a Right-Sized Tool?"

Q: What if we need enterprise risk management capabilities later?
A: Most E&C teams never need full ERM. Think about your role: Are you actually going to manage operational risks like supply chain disruptions? Financial risks like currency hedging? Strategic risks like M&A target evaluation?

If your organization grows to the point where they hire a Chief Risk Officer managing all enterprise risks, they'll bring their own tools. Your compliance risk assessment remains valuable for E&C-specific needs. You don't need to buy enterprise tools "just in case."

According to Gartner, 76% of compliance leaders prioritize improving third-party risk management—a compliance-specific function, not an enterprise risk function. Focus on doing compliance risk assessment excellently, not mediocre enterprise risk management.

Q: Won't stakeholders expect enterprise-grade sophistication?
A: Stakeholders care about results, not software complexity. A clear risk heat map showing your compliance priorities with documented remediation plans is infinitely more impressive than talking about your platform's 500 features while struggling to produce useful reports.

The ECI survey found that 72% of employees who observe misconduct report it. Your job is creating cultures where risks are identified and addressed—not demonstrating software sophistication.

Common Objections Addressed

"But Won't We Outgrow a Right-Sized Tool?"

Q: How do we ensure our methodology is defensible in audits?
A: Defensibility comes from:

- Standardized impact/likelihood scoring applied consistently
- Documented methodology explaining your approach
- Audit trails showing who assessed what and when
- Regular assessment cycles demonstrating systematic approach
- Clear remediation tracking for identified risks

Platform complexity doesn't make methodology more defensible—documentation and consistency do. Right-sized tools provide audit trails and documentation without unnecessary complexity.

Q: What about integration with other systems?
A: Best-of-breed tools that integrate effectively serve E&C teams better than monolithic platforms trying to do everything. You can integrate compliance risk assessment with:

- Case management systems through standard APIs
- HR systems for automated targeting
- Policy management platforms
- Learning management systems
- Disclosure management tools

You don't need everything in one enterprise platform. According to PwC, 49% of compliance professionals use technology for 11+ activities. They're using multiple integrated tools, not single monolithic platforms.

Integration With Your Compliance Program

Risk Assessment as Foundation, Not the Entire House

Right-sized risk assessment should integrate with your broader compliance program, not replace it entirely.

Risk Assessments Feeds Into:

- Annual compliance work plans: Prioritize activities based on identified risk concentrations
- Training needs analysis: Focus training on areas showing knowledge gaps or risk
- Monitoring and auditing: Direct audit resources to high-risk areas
- Resource allocation: Justify staffing and budget requests with risk data
- Board and leadership reporting: Present data-driven risk priorities

Risk Assessments Connects With:

- Case management: Route high-risk findings into investigation workflows
- Policy management: Identify policy gaps requiring new or updated policies
- Disclosure programs: Validate disclosed relationships against risk assessment findings
- Hotline reports: Compare reported issues to risk assessment concentrations
- Third-party due diligence: Risk-assess vendors before detailed due diligence

Risk Assessments Supports With:

- DOJ guidance compliance: Demonstrate data-driven risk detection and program effectiveness measurement
- Audit readiness: Provide documentation of systematic, risk-based approach
- Cultural reinforcement: Show stakeholders that their input drives program priorities
- Continuous improvement: Track risk score improvements year-over-year

The DOJ's 2024 guidance update emphasizes measuring compliance effectiveness and data-driven risk detection. Risk assessment provides the foundation for both.

You don't need everything in one platform. Best-of-breed tools that integrate effectively serve compliance teams better than trying to do everything in monolithic enterprise systems.

Measuring Success

How to Know Your Right-Sized Approach Is Working

Define success metrics before implementation so you can demonstrate value to leadership:

Adoption Metrics (Are people actually using it?)

- Assessment participation rates >75% (vs. 40-60% with spreadsheets)
- Time to launch new assessments <1 week (vs. weeks or months)
- User satisfaction scores from participants
- Percentage of stakeholders completing without reminders
- Time savings vs. manual spreadsheet processes

Program Effectiveness (Are we identifying and addressing risks?)

- Number of risk areas identified and successfully remediated
- Year-over-year risk score improvements in reassessed areas
- Percentage of high-risk findings with documented remediation plans
- Time from risk identification to remediation completion
- Correlation between risk scores and actual compliance issues

Measuring Success

How to Know Your Right-Sized Approach Is Working

Business Value (What's the impact?)

- Compliance team hours redirected from administration to strategic work
- Positive audit/examination feedback specifically mentioning risk methodology
- Leadership engagement with risk reporting (board presentations, executive discussions)
- Regulatory violations prevented through proactive risk identification
- Cost savings vs. enterprise platform alternatives

Cultural Indicators (Are we changing behavior?)

- Stakeholder feedback on assessment process
- Unsolicited risk reports from empowered employees
- Improved speak-up culture metrics
- Decreased retaliation concerns (ECI found 46% who report misconduct experience retaliation)
- Increased perception of ethical culture strength

According to the White & Case/KPMG survey, 79% of organizations conduct documented risk assessments. But conducting assessments doesn't equal effective risk management. These metrics help you demonstrate actual effectiveness, not just activity.

Taking Action on Right-Sized Risk Management

Three Steps to Get Started

Step 1: Assess Your Current State

Ask yourself:

- How are you conducting risk assessments today? (Spreadsheets? Ad hoc conversations? Annual surveys?)
- How much time does your current approach require? (Factor in coordination, follow-up, analysis, reporting)
- Are you getting audit-ready documentation? (Could you produce systematic risk methodology documentation tomorrow if regulators asked?)
- Can you easily generate leadership-ready reports? (Or does board reporting require days of manual chart creation?)
- Do you have year-over-year trending? (Can you show whether risks are improving or worsening?)

Be honest about current state gaps. According to Gartner, regulatory complexity now tops emerging risks. Your current approach may have worked before, but does it scale for today's environment?

Step 2: Define Your Requirements

Clarify what success looks like:

Risk Coverage:

- What compliance risks must you assess? (Regulatory, ethics, conduct, conflicts, third-party)
- How frequently? (Annual, quarterly, continuous monitoring)
- Who needs to participate? (All employees, specific roles, certain departments)

Capabilities:

- What features do you actually need daily? (Not what sounds nice—what you'll use)
- What integrations matter? (HR data, case management, other compliance tools)
- What reporting do stakeholders expect? (Heat maps, trend analysis, remediation tracking)

Taking Action on Right-Sized Risk Management

Three Steps to Get Started

Resources:

- What can you implement with existing staff? (No IT projects, no dedicated admins)
- What's your realistic timeline? (Weeks not months)
- What's your budget? (Including hidden costs like time and opportunity cost)

Step 3: Choose the Right Tool
Evaluate options against your requirements:

Implementation Speed:

- Can you launch first assessment within 30 days?
- Does vendor provide implementation support or are you on your own?
- Are templates pre-built or must you create everything custom?

Ease of Use:

- Can compliance team manage without IT support?
- Is interface intuitive or require extensive training?
- Can you make configuration changes yourself?

E&C Specific Capabilities:

- Are assessment templates relevant to compliance teams?
- Does scoring methodology make sense for compliance risks?
- Are reports designed for compliance stakeholders vs. enterprise risk committees?

Pricing Transparency:

- Are costs clear and predictable?
- Any hidden fees for implementation, training, support?
- What happens as you grow—reasonable scaling or price jumps?

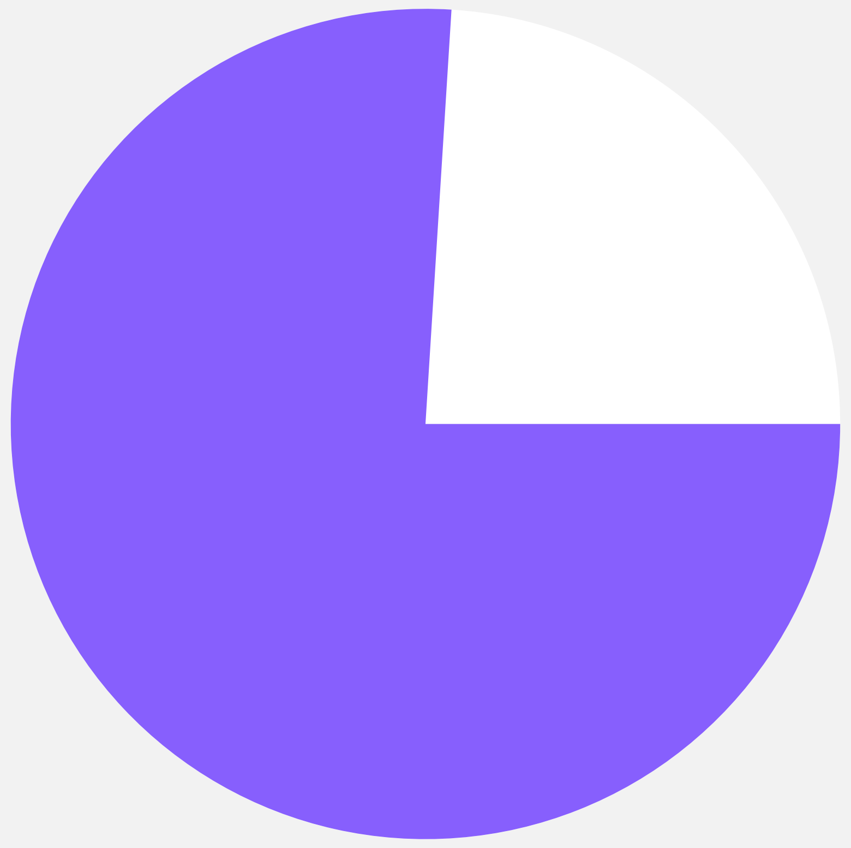
IT Requirements:

- Cloud-based or requires internal infrastructure?
- Standard integrations or custom development needed?
- Vendor-managed security or your IT team's burden?

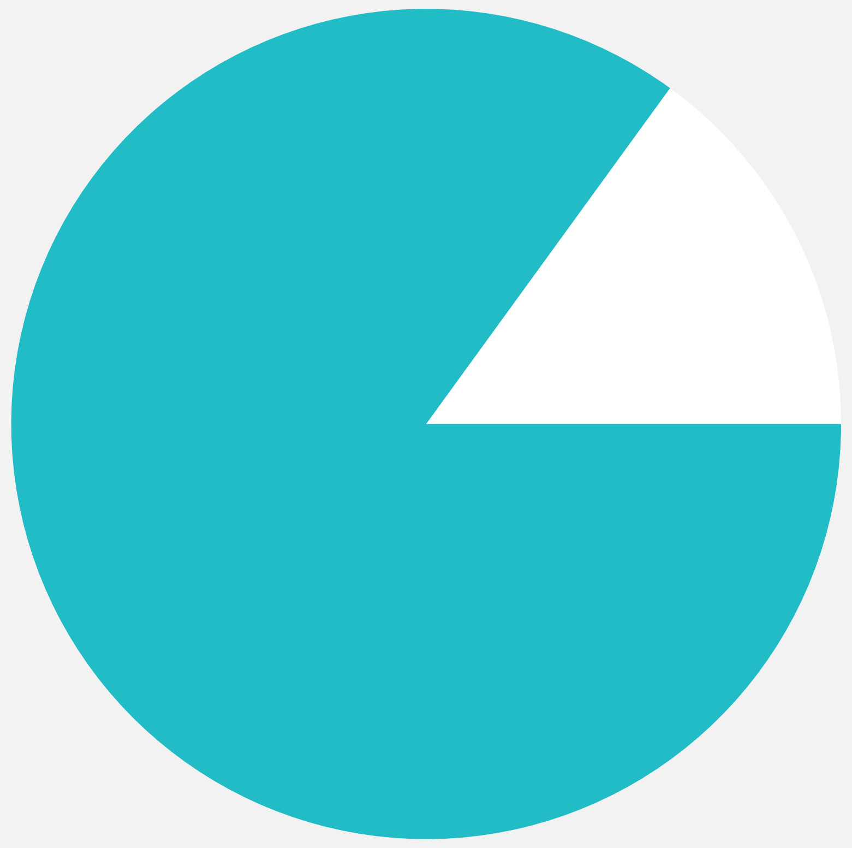
Conclusion: Enterprise Problems Don't Require Enterprise Solutions

Ethics and compliance teams deserve risk management tools built for their specific needs—not scaled-down versions of enterprise platforms designed for Chief Risk Officers managing all enterprise risks.

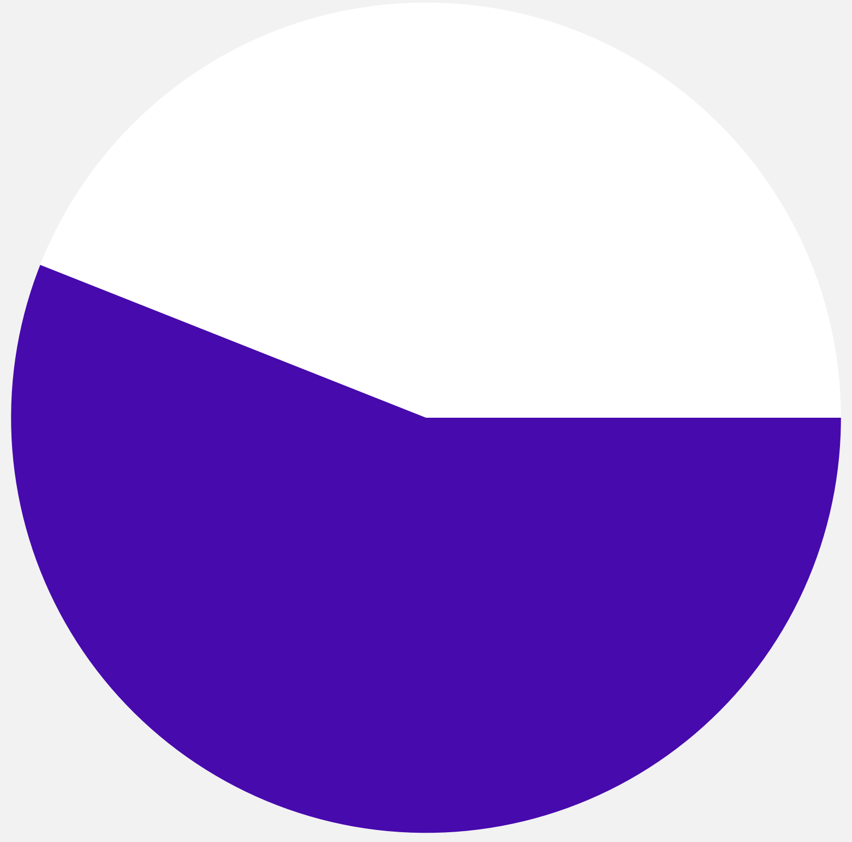
76% of compliance leaders prioritize improving risk management (Gartner)



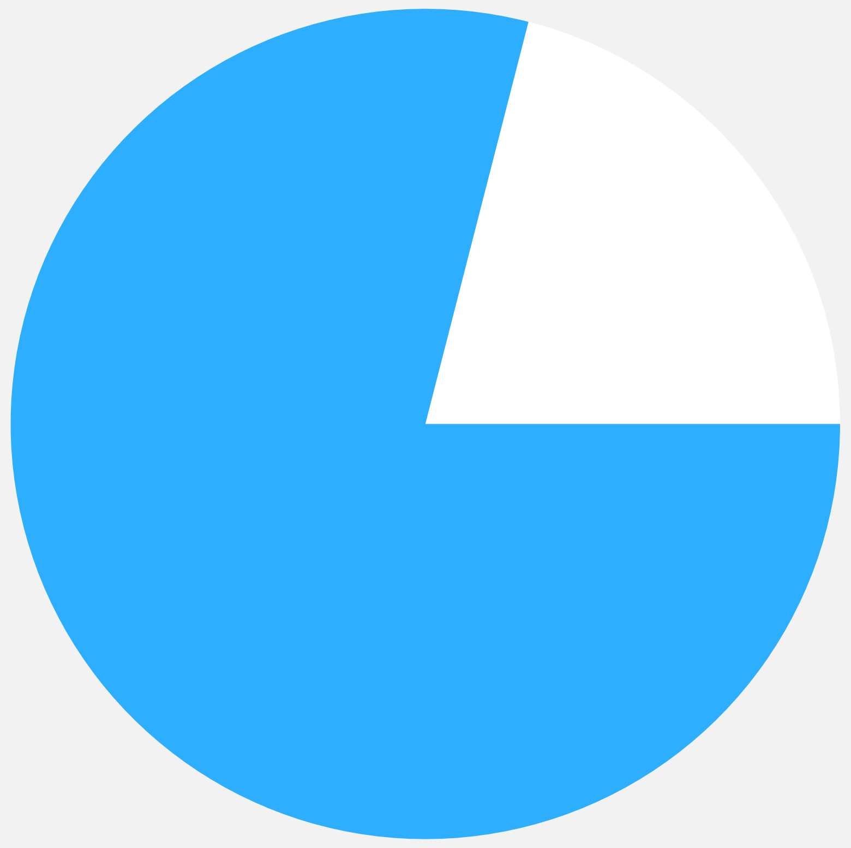
85% of organizations face increased regulatory complexity (PwC)



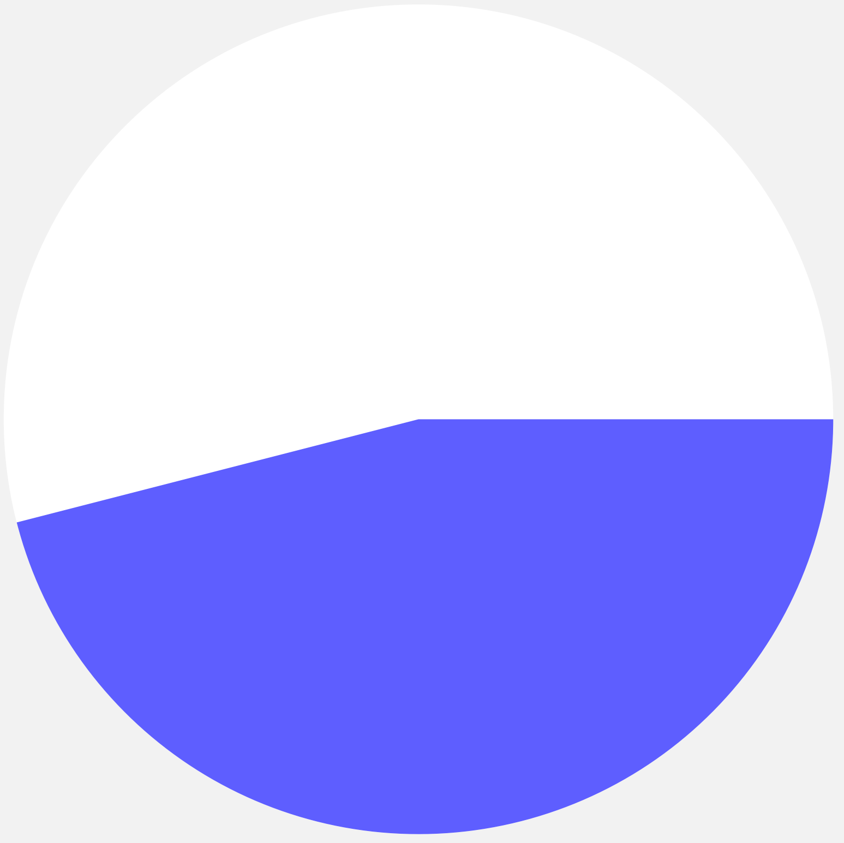
Only 56% of employees perceive strong ethical culture (ECI)



79% of organizations conduct documented risk assessments (White & Case/KPMG)



46% of employees who report misconduct experience retaliation (ECI)



These challenges require systematic, effective risk management—not enterprise complexity.

Right-sized risk management means:

✓ **Getting value in weeks, not months:** Start identifying risks immediately instead of spending quarters implementing complex platforms
✓ **Using tools your team can manage:** Focus on compliance work, not system administration
✓ **Focusing on compliance risks:** Address regulatory, ethics, and integrity risks—not all enterprise risks
✓ **Achieving audit readiness:** Demonstrate systematic methodology and data-driven effectiveness to regulators
✓ **Investing in risk mitigation:** Allocate resources to addressing risks, not managing software complexity
✓ **Reinforcing risk culture:** Make risk identification easy and engaging, not burdensome and complex
✓ **Activating your compliance team:** Distribute work appropriately across stakeholders instead of overwhelming compliance with implementation
✓ **Scaling risk identification:** Automate assessments and leverage HR data to reach the right people efficiently

The question isn't whether you need risk management—of course you do. Regulators expect it, auditors look for it, and effective compliance programs require it.The question is whether you need risk management built for someone else's job, or risk management built for yours.

Enterprise Risk Management platforms are powerful tools—for Chief Risk Officers managing operational, financial, strategic, and compliance risks across large organizations with dedicated teams and substantial budgets.

Compliance Risk Assessment tools are practical solutions—for ethics and compliance professionals managing compliance-specific risks with small teams and limited resources who need to demonstrate program effectiveness without enterprise overhead.

Choose tools that match your role, your resources, and your actual needs. Choose right-sized risk management built for compliance professionals.

About Ethico

Purpose-Built Risk Assessment for Ethics & Compliance Teams

Ethico provides right-sized risk assessment tools designed specifically for ethics and compliance professionals who need systematic risk management without enterprise complexity.

SCALE RISK IDENTIFICATION

- Deploy professional risk assessments in weeks using HR-driven campaigns
- Customize assessments easily with extensive E&C template library
- Engage stakeholders with targeted requests, not generic surveys
- Ensure data integrity through standardized methodologies

ACTIVATE YOUR COMPLIANCE TEAM

- Provide risk owners with customized views to update submitted risks
- Reduce time spent chasing information from busy stakeholders
- Offer ready-to-deploy assessments that reduce duplicative work
- Boost team impact by distributing work appropriately

DEMONSTRATE AUDIT READINESS

- Show regulators targeted, risk-based approaches with clear documentation
- Generate visual risk heat maps automatically for leadership presentations
- Track remediation plans tied directly to risk assessment findings
- Increase program participation through simplified workflows

REINFORCE RISK CULTURE

- Provide friendly risk owner experiences that encourage engagement
- Ensure operational fluidity with robust integrations
- Stop making compliance play IT support
- Make risk identification easy, not burdensome

Ready to explore right-sized risk management for your compliance program?

- Request a personalized demo
- Download E&C assessment template examples
- Speak with a compliance risk assessment expert
- See how we've helped compliance teams like yours

Contact: www.ethico.com