Recommended Practice for Buying & Selling Compliance Technology

Version 1.0
September 2026

Integrity Bridge provides strategic & operational support for ethics & compliance teams, including the selection and configuration of compliance technology. For more information on Integrity Bridge's services please visit:

www.integritybridge.com

Integrity Bridge has established Applied Compliance, a free resource center for ethics & compliance professionals, available here:

www.appliedcompliance.com

Recommended Practice for Buying & Selling Compliance Technology

Section A: Context

Introduction

Compliance technology is the operational backbone of the modern ethics and compliance program. The whistleblower report that arrives at 2 a.m. lands in a case management system. The new third party is flagged in a screening platform. Training reaches a global workforce through a learning management system. Conflicts of interest are disclosed through a workflow tool. When the technology is well chosen and well configured, the program runs on it. When it is not, the program limps around it.

Compliance technology is also an important source of evidence of compliance risk and program effectiveness. Many operational metrics (e.g. screening false positives, investigation cycle times, training completion and disclosure patterns) draw on data held in compliance systems.

The importance of technology, and associated access to data, is recognized by prosecutors and regulators. The U.S. Department of Justice's Evaluation of Corporate Compliance Programs asks: "*How do the assets, resources, and technology available to compliance and risk management compare to those available elsewhere in the company? Is there an imbalance between the technology and resources used by the company to identify and capture market opportunities and the technology and resources used to detect and mitigate risks?*" A prosecutor evaluating a compliance program is also evaluating the technology behind it, relative to technology used by business units and other corporate functions.[1]

For these and other reasons, compliance technology has grown into a multi-billion-dollar industry, inside the still larger category of governance, risk and compliance (GRC) software. Grand View Research estimates the global enterprise GRC market, including software and services, at $72.4 billion in 2025 and forecasts 13.7% annual growth for 2026–2033.[2] Its separate third-party risk management study estimates $7.42 billion in 2023 and forecasts $20.59 billion by 2030.[3] Mordor Intelligence values corporate compliance training at approximately $10 billion in 2025, growing to $13.6 billion by 2030.[4] Compliance tech companies have gone public or attracted significant private equity investment, with all the pressures that come with that. Those pressures shape how the product is priced, how the demo is scripted, and how the renewal conversation goes.[5]

---

[1] U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (updated September 2024), available at https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

2 Grand View Research, Enterprise Governance, Risk, and Compliance Market, 2026–2033. Public market summary, updated June 2026; estimates include software and services.

3 Grand View Research, Third-party Risk Management Market, 2024–2030. Public market summary; 2023 estimate and 2030 forecast.

[4] Mordor Intelligence, Corporate Compliance Training Market (2025–2030 forecast), https://www.mordorintelligence.com/industry-reports/corporate-compliance-training-market

[5] For other resources on sourcing compliance technology, see OCEG, GRC Capability Model (Red Book), Version 3.5 (January 2024), and OCEG's companion GRC Technology resources, https://www.oceg.org/grc-technology/; GRC 20/20 Research, Becoming a Better Compliance Technology Buyer: Cutting Through the Noise (October 2024), and its Buyers Guide series, https://grc2020.com; ACFE & SAS, Anti-Fraud Technology Benchmarking Report (2026 edition), https://www.acfe.com/fraud-resources/anti-fraud-technology-benchmarking-report; PwC, Global Compliance Survey 2025, https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-

Set against that experienced seller is a compliance team that purchases technology rarely. The purchase and deployment of new compliance technology, whether for the first time or to replace an incumbent, is not for the faint of heart, and the budgetary and change-management pressures involved can themselves become a catalyst for inertia. The result is a structural mismatch: a vendor's sales team may negotiate similar deals regularly; an individual compliance buyer may have much less recent experience.

Integrity Bridge was established, in part, to help ethics & compliance teams navigate these waters. Drawing on our founder's experience as a purchaser of compliance technology and our work advising buyers, we have observed the aspirations, reality checks and frustrations of both buyers and sellers. These observations prompted us to launch buyer and seller surveys in the spring of 2026.[6] The survey responses are used here to illustrate the experiences of participating buyers and sellers, rather than to estimate how common a practice is across the market. Public research is identified separately. Our recommendations combine those sources with professional judgment and should be adapted to your company's risk, size, sector and procurement rules.

The responses reveal frustrations on both sides. Buyers described aggressive marketing tactics and vendors overpromising what their technology can do; vendors described processes that did not offer a genuine opportunity to win, and request for proposal (RFP) timelines that frequently slip. Each side's defensive behavior can feed the other's distrust: buyers hedge because they have been oversold; vendors hedge because they have been used for price discovery.

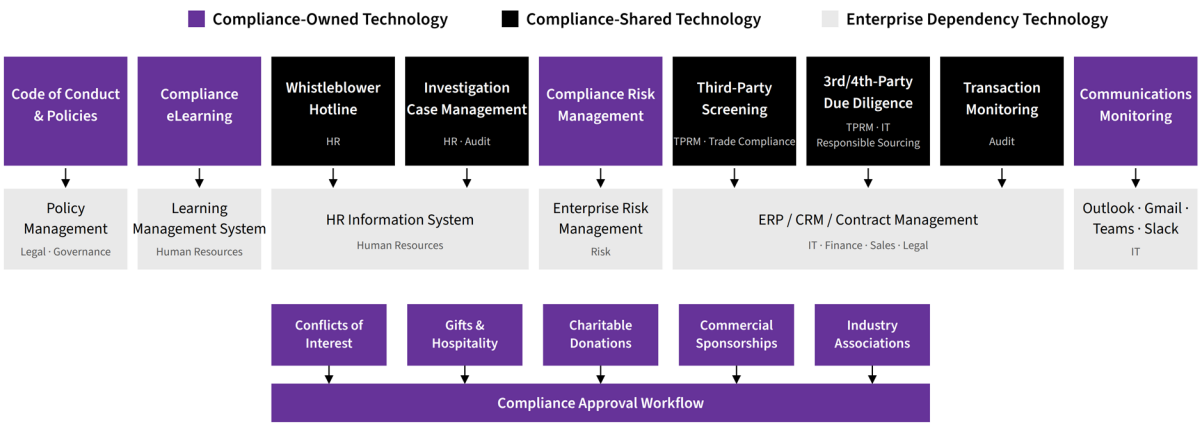
Addressing feedback from the surveys, and applying our own experience, this white paper offers a series of recommendations for compliance technology buyers organized according to the compliance tech life cycle, from the first demo through to contracting. Where appropriate, we also offer guidance to compliance tech vendors on behaviors they should continue or stop doing.

The Compliance Technology Landscape

Compliance technology, let alone "GRC," is broad and defined differently across organizations. For this white paper, we use the term for technology typically deployed to support the traditional pillars of a company's ethics and compliance program, summarized in the figure below. We exclude dedicated data privacy platforms from the product categories covered, although many recommendations apply equally to them.

survey.html; and KPMG, Global Chief Ethics & Compliance Officer Survey 2026, https://kpmg.com/xx/en/our-insights/risk-and-regulation/2026-kpmg-global-cco-survey.html.

6 Both surveys were launched in Q1 2026 and continue to remain open. To date, we have received 35 responses from 23 different compliance technology vendors (several vendors encouraged their employees to complete their own responses). We have received 52 responses from technology buyers. Survey responses were processed in accordance with Integrity Bridge's data privacy policy which was communicated to survey respondents: https://www.integritybridge.com/privacy-policy.



Budget authority and ownership of such technology often rest with the Chief Compliance Officer (CCO). However, as the figure above illustrates, responsibility for selecting and operating some products is shared with other functions. For example, third-party risk management (TPRM) can span sanctions, anti-bribery, cybersecurity, environmental and human rights risks, and extend beyond direct suppliers. Compliance teams therefore need to engage the relevant owners in IT, Procurement, Trade Compliance, Responsible Sourcing and Sustainability (without assuming that one workflow or risk score can serve every purpose).

Compliance technology may depend on enterprise resource planning (ERP), customer relationship management (CRM) and human resources information systems (HRIS) owned by other functions. Identify the owners of those systems and their data early: their participation matters to budgeting, selection, configuration and ongoing operation.

Evolution of Compliance Technology

Compliance technology has traditionally been purchased as individual point solutions: a training tool, a hotline, a screening service or a disclosure workflow. Such tools typically operated in isolation from the rest of the compliance technology stack, sometimes even from products owned by the same vendor.

Demand for better evidence of program effectiveness and workplace culture, together with customer preferences and vendor commercial strategies, has encouraged convergence. Providers strong in investigations extended into third-party risk management; training providers extended into speak-up and investigation case management. In our experience, the early results were mixed: investment and management attention were diverted away from core products to develop new ones, and the new products were often sub-standard.

Artificial intelligence has since changed the economics of product development: it has significantly reduced the barriers to, and the time and cost of, new product development, making a fully integrated, data-enabled suite of compliance products a realistic proposition. And it has done so, as much for new entrants, unburdened by the product-development baggage of the incumbents, as for the incumbents themselves.

AI is also extending compliance technology deeper into the compliance workflow itself, with a corresponding reduction in the burden on compliance teams. Investigation case management is the clearest example. Until recently, most platforms served as little more than a document depository for investigation materials. Several compliance tech providers now support the full lifecycle of an investigation, including the agentic preparation of investigation plans, interview plans and draft reports.

For all that promise, adoption of AI within compliance programs remains broad but shallow. Recent industry surveys report that most compliance teams already use AI tools in some form, yet only around

one in four has a strong governance framework for that use,[7] and fewer than half of the programs using AI can explain how it improves outcomes.[8] Investment intent nonetheless remains strong: PwC's Global Compliance Survey 2025, drawing on 1,802 executives across 63 territories, reports that 82% of companies plan to invest more in technology to automate and optimize compliance activities.[9] In third-party risk management, the category with perhaps the most to gain, adoption of AI-enabled screening and automated reporting remains at an early stage. The reasons are instructive for buyers and vendors alike: a black-box trust deficit, fear of more false positives rather than fewer, fragmented and legacy technology estates, and data hygiene. AI is only as good as the data foundations beneath it; a buyer cannot layer AI on top of a disorganized compliance program and expect magic, and a vendor should not promise otherwise.[10]

These capabilities come with additional complexity, particularly as to configuration. Buyers now face extensive choices about workflows, access, data and automation, without sufficient internal resources to resolve them. Vendors have traditionally been reluctant to close this gap with consulting services, for fear of undermining their value multiplier as a technology platform. This configuration and deployment gap between compliance tech vendors and buyers is one of the reasons Integrity Bridge was established.

More recently, compliance tech vendors are pivoting back towards services. Configuration support is increasingly recognized as a driver of client satisfaction (and therefore retention) and of new technology use cases within the client (and therefore revenue). Vendors are establishing internal centers of excellence staffed by former compliance officers who understand the daily work of their peers; "forward deployed engineers" are being embedded within clients; and technology deployment partnerships are being established with specialist consultants, such as Integrity Bridge.

Purpose & Scope of this White Paper[11]

Through our own experience, and that of survey respondents, we have identified several recurring frustrations with the compliance tech buying and selling experience.

For buyers, the frustrations begin long before any RFP exists. The marketing arrives uninvited - cold calls to mobile phones, contact details sourced from data brokers, LinkedIn chasers that follow unanswered emails - and too often continues after a clear "no." When the conversation does start, the selling can run ahead of the product: coverage claims that do not survive the deep dive, AI capabilities described in the abstract, functionality promised that cannot later be demonstrated. Buyers described *"being promised what can't be delivered"* as the most corrosive vendor behavior of all, because it is discovered only after the contract is signed, when the switching costs have moved to the buyer's side of the table.

Buyer frustration continues into the selection process. RFP questions are ignored or answered with boilerplate and marketing decks, making bids nearly impossible to compare. Demonstrations stray from

[7] Compliance Week & KonaAI, AI & Compliance Survey 2026: Adoption Is High; Governance and Controls Lag (survey of 193 compliance leaders), https://www.complianceweek.com/resource/ai-compliance-survey-2026-adoption-is-high-governance-and-controls-lag/. The underlying survey results report, How Ethics & Compliance Teams Are Adopting Artificial Intelligence (AI) Tools (January 2026) is cited below as the "CW/KonaAI Survey."

[8] LRN, The Next Leap: 2026 Ethics & Compliance Program Effectiveness Report, https://lrn.com/resources/2026-program-effectiveness-report

[9] PwC, Global Compliance Survey 2025 (survey of 1,802 executives across 63 territories), https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

[10] CW/KonaAI Survey (see note above), Qs 11 and 14: 41% of respondents agreed or strongly agreed that they trust AI-driven outputs for ethics and compliance decisions; 66% expect agentic AI to be applied in semi-autonomous workflows or autonomous risk detection within 12 months.

[11] AI disclosure statement: This white paper is the proprietary work of Integrity Bridge, LLC. It was manually drafted over several months based on our experience and that of survey respondents. AI was utilized to (a) undertake research; (b) process survey responses (with personal identifiable information removed beforehand) and (c) make editing suggestions, some of which were accepted. As such, this white paper may contain AI drafting artifacts. Any errors or omissions are entirely our own.

what was asked. And after go-live, the team that sold the platform gives way to ticket queues and support that must be chased.

The deepest frustration of vendors is the process that was never real: the RFP written around a pre-selected vendor, the invitation issued to satisfy a procurement rule, the market test run to sharpen an incumbent's renewal pricing. Estimates of how often bidding processes are effectively pre-decided ranged, across the vendor responses, from *"not the norm"* to *"greater than 50%."* Close behind sit the "blind" RFP that arrives with no prior engagement, and the package itself: hundreds of generic procurement and security questions, a compliance section that reads as though written from outside the function, and response deadlines of ten to fourteen days for a bid that will take 30–50+ hours to prepare, followed by weeks of buyer silence.

Then the deadlines slip (*"ALL THE TIME"*), the selection criteria stay opaque and, too often, the outcome is never communicated at all; several vendors reported being simply ghosted. Even a win can sour at the last: legal teams engaging after commercial agreement to reopen settled points, or procurement returning for a further discount after final pricing was accepted. What vendors ask for, in short, is not a guaranteed win; it is a process they can rely on.

This white paper addresses these frustrations with recommended practices for buyers and vendors. It covers the entire technology acquisition lifecycle from initial business case development and budgeting through to contracting with the newly selected vendor. *Configuration* of selected technology is outside the scope of this white paper but will be addressed in its own white paper in Q1 2027.

Section B: Compliance Technology Strategy & Planning

Development & Maintenance of a Compliance Tech Strategy

The appropriate selection and configuration of compliance technology is critical to the design, execution and continuous improvement of an effective ethics & compliance program. Most corporate functions will develop a clear technology strategy, and compliance should be no different; compliance technology is not simply a budget line item to be revisited every year. We recommend the development of a documented compliance technology strategy that:

- aligns with the company's long-term business and technology strategy (e.g. new products, markets, mergers, acquisitions & divestments).
- identifies potential triggers for changes in the strategy and/or individual vendor. These may include changes in related enterprise technologies, future M&A, group-wide reductions in budget, expiry of incumbent contract terms, acquisition of an incumbent vendor (or the sunset of its product), a vendor service failure or data-security incident, and new regulatory requirements that change the scope of screening, diligence or monitoring.
- identifies anticipated changes in compliance program design, which will affect compliance technology requirements.
- clarifies which technology is in scope, and who owns the budget for, and has responsibility for, the selection and management of each vendor.
- tracks the functionality offered by the company's current vendor versus what is being offered in the market.
- identifies dependencies on other enterprise systems.
- identifies the owners of relevant systems, data and underlying processes, together with system dependencies, planned lifespan and success measures.
- assesses how the strategy aligns with management expectations as to the use of artificial intelligence, including pressure to bring technology use-cases in-house and/or integration with the company's Large Language Model (LLM) services.
- addresses the risks of AI-enabled compliance technology before purchase, including where human approval is required and how performance will be tested.
- compares Compliance's access to data, expertise and technology with that available elsewhere in the business and assesses whether resources are proportionate to its risks and responsibilities.[12]

A documented compliance technology strategy has several benefits. It can be proactively shared with key stakeholders such as the Chief Information Officer and Chief Financial Officer for pre-budget cycle feedback and support. It helps to frame subsequent return on investment (ROI) pitches and budget requests as part of that broader compliance and enterprise technology strategy. Finally, it ensures that the compliance function is well prepared when the aforementioned triggers are activated, and changes in compliance technology are required. Treat the strategy as a living document: refresh it annually ahead of the budget cycle, and immediately after any trigger event.

While outside the scope of this white paper, we also recommend developing a similar strategy for (a) internal and public source data that support such systems; and (b) other compliance service providers, such as providers of enhanced due diligence and forensic services.

[12] U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (September 2024) https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl

Navigating the Annual Strategy, Planning & Budget Season

Ethics & Compliance typically submits an annual budget like every other function. When justifying this budget, a Chief Compliance Officer faces several challenges:

- Compliance budgets are small relative to IT and most other corporate functions, which makes every technology line item proportionately more visible.
- The connection between the technology, commercial outcomes and operating costs may be indirect or difficult to quantify.
- The technology is often not fully understood by senior management.
- Technology funding is often tied to an annual cycle; missing it may delay the initiative unless an exception or in-year investment route is available.
- A bottom-up budget may subsequently face an across-the-board reduction, requiring difficult choices about priorities.

For these reasons, the annual budget season is often viewed by compliance professionals with trepidation. There is no silver bullet to this challenge. However, we suggest several ways to maximize the likelihood of your budget ask surviving intact.

Demonstrate Understanding of the Company's Long-Term Strategy

Many companies have a rolling long-term strategic plan. This strategic direction is critical to an ethics & compliance function's risk assessment, its program design and by extension its budget. Your Executive Leadership Team (ELT) sponsor (e.g. General Counsel, Chief Compliance Officer) should have access to these materials (e.g. presentations to the ELT, annual board strategy day presentations), and your own presentations should explicitly acknowledge that strategic direction.

Align with Other Corporate Functions

Proactive engagement with other corporate functions is critical. Where the execution of compliance processes impacts their operations, other heads of functions have a vested interest in your technology (e.g. procurement, sales, travel & expenses). This can range from ensuring you have other heads of function as allies at the table, to sharing technology costs where such technology serves dual purposes (e.g. expense management technology serves to manage both costs and risks). Having the opportunity to review and align with (often very sophisticated and data-driven) strategy and budget presentations of your function peers can help to further enrich and align your own presentations.

Develop the Multi-Year Narrative

What program and cost-related themes can you highlight in your presentation? Can you demonstrate continuous improvement of your ethics & compliance program over the years, against a budget that is flat or even declining in real terms? For new compliance technology introduced in the past year, are there performance indicators that you can cite to demonstrate impact on program cost or efficiency?

Demonstrate Cost Management Empathy

If your company is going through challenging financial circumstances, are you proactively suggesting ways in which to cut the compliance budget? Have you ranked those cost reduction opportunities? Can you provide grounded assessments of the potential impacts of such reductions, so that management can make an informed decision? In our experience, the proactive proffering of cost reduction opportunities at the outset of the budget season will be happily accepted by management but may not prevent the aforementioned request to unilaterally cut budgets further.

Buy, Build or Assemble?

Any business case must also survive the build-versus-buy question, and the distinction is blurring. As one CCO respondent put it, the distinction is in part illusory: *"even in a build scenario you are using a tool of some sort that you did not make."* A third option is assembly: configuring tools the enterprise already licenses for intake, approvals and reporting where requirements and volumes permit. Existing licenses may lower incremental license fees, but security, configuration, testing, support and ongoing ownership still have costs.

AI is expanding the possibilities for internal development. Buyer respondents reported internal discussion of whether *"basic screening services can be met via a good set of prompts and an enterprise generative AI license,"* and in-house AI agents for routine, no-judgment tasks; in the CW/konaAI Survey, a third of adopters reported custom-built AI solutions against 43% using the AI features of third-party platforms.[13] The limits are equally clear. Buyers themselves regard certain product types as *"out of reach in most build scenarios, such as screening and hotline services"*: proprietary data assets, the independence expectations attached to speak-up channels, and defensible audit trails are not assembled from prompts. Build also carries costs the enthusiasm rarely budgets: one respondent whose firm prefers building conceded that it *"takes forever,"* and in-house tools accrue maintenance costs and suffer from a lack of a continuous-improvement roadmap that vendors typically maintain.

Perhaps the most sobering survey response for compliance tech vendors was provided in relation to the buy-versus-build question: *"the biggest reason I have considered build is the extreme difficulty of doing a successful implementation when you buy. I'd rather work through challenges with co-workers than deal with a vendor."*

The call to action follows for each side. For buyers: treat a build or assembly option as a bid like any other: subject it to the same total-cost discipline as a vendor proposal (build effort, security review, maintenance, key-person risk and an accountable owner for the tool's lifetime), and revisit the decision at the same trigger events that would prompt a vendor review. For vendors, the message is more pointed: the build-versus-buy contest is no longer won at the demo; it is won at implementation and in the first year after go-live. Every improvement in how technology is sold, scoped and delivered narrows the gap that tempts a compliance officer to conclude that colleagues are easier to work with than vendors.

Building the Business Case & Budget for New Compliance Technology

If the budget-setting season for an ethics & compliance function's entire budget occurs in Q4 of the preceding fiscal year, building the business case for new compliance technology must begin much earlier.

Is it new Compliance Technology or a new Technology Vendor?

The development of a business case and budget differs significantly between the acquisition of new compliance technology versus the switching out of an existing vendor.

When switching technology vendors, the business case for needing the relevant technology has already (and hopefully) been proven. However, company inertia to switching technology providers must be overcome, particularly when there are costs and potential disruption associated with the switch. There is always the risk that initiating a discussion on vendor switching may re-open the build-versus-(re)buy debate, particularly in the age of AI.

For new compliance technology, much depends on management perceptions of the need for it and what is currently used to manage the process. Traditional areas of compliance technology such as third-party risk management, hotline & investigations, disclosures and training are generally accepted by

[13] CW/konaAI Survey, Q 3: 33% of respondents reported custom-built AI solutions in ethics and compliance work, against 43% using the AI features of third-party compliance platforms.

management as a requirement of doing business. In addition, the sensitivity of the information being handled and the complexity of associated workflows and enterprise system integrations often pre-empts management desire to operate an in-house solution. For other types of compliance technology, such as policy management and communications/transaction monitoring, business case development may require greater education of management as to why it is needed, and why the existing solution (e.g. SharePoint for policy management, ad hoc transaction tests by Internal Audit) no longer suffices.

What is the Trigger?

For a vendor switching scenario, the trigger is typically the anticipated expiration of the contract term and perceived dissatisfaction with incumbent pricing or performance. But there are other trigger scenarios:

- New enterprise technology forces a rethink in relation to the existing compliance technology vendor. For example, a company is planning to introduce a new ERP platform that will support high volume third-party screening. The compliance team no longer requires their existing TPRM platform to support such screening, limiting their go-forward requirements to enhanced due diligence.
- The company intends to expand the use of compliance technology, and the incumbent cannot support this expansion. For example, a company would like to use its speak-up platform for Code of Conduct allegations to also support human rights-related grievances made by company employees, supplier employees and members of the local community.
- A de-merger is prompting one or both to-be-separated companies to reflect on whether it wishes to continue with the existing technology vendor.

As indicated above, maintaining a compliance technology strategy in which potential triggers (and trigger responses) are identified can enable Compliance to quickly and effectively respond in scenarios that are often time-pressured.

What is the current Total Cost of Ownership?

To fully develop a business case for new compliance technology, the total cost of existing technology and/or processes needs to be mapped. This is not simply the compliance tech vendor's annual platform license fee:

- How many compliance tech vendors are currently providing the same service? In our work, we often see duplicative services especially in relation to third-party screening and due diligence services, both within the compliance function and across other functions (e.g. Credit, Finance, Procurement, and Sustainability). What is the total cost of those services? This number in and of itself may come as a surprise to management and may be the only argument needed for change.
- Are there other third-party technology costs associated with the operation of the compliance technology? For example, is there middleware between the compliance tech vendor and company systems? Is a technology deployment consultant needed to manage application programming interface (API) connections between tech vendor and company?
- How many full time equivalents (FTEs) are needed to administer the current platform, review its outputs and support users? How much time do other users spend on the process?
- Are additional third-party service providers (e.g. managed screening, enhanced diligence, forensic investigators) currently needed for the process that the compliance technology platform supports? What are their annual costs?
- Are metrics available on the performance of the compliance process that the technology supports? These current-state metrics are very important (i) in building an objective data-driven business case

for change; and (ii) post-acquisition of the compliance technology, (hopefully) demonstrating the cost savings and process improvement the investment has led to.

- If there is no current platform, how much time is the compliance team spending on manual workarounds (e.g. spreadsheets, shared inboxes and ad hoc reporting), and what does that time cost (in full-time employee equivalent)?

What is the anticipated Total Cost of Technology Acquisition and Operation?

This is inevitably tied to the development of the business case (including ROI), more on which to follow. For now, we focus on the headline cost items associated with the acquisition of new compliance technology:

- Annual cost of the new compliance technology platform.
- Initial set-up costs for new compliance technology platform, including one or multiple technology integrations (e.g. via API).
- Costs associated with an outgoing provider, including any lawful early-termination charges and agreed data-export or transition fees. Include any offset contribution offered by the new vendor only if it is documented.
- Consulting fees associated with compliance technology configuration and deployment, and migration of data from incumbent to new provider.
- Internal charges from other functions (e.g. IT, project management).
- Data cleansing fees.
- Temporary or permanent data storage fees (e.g. fees for aggregating company data from multiple ERPs; fees to temporarily or permanently archive data previously held by an incumbent technology provider).
- How many FTEs are expected to be needed to manage the new platform? How much time will users spend in the new platform?
- Will the new platform preclude the need for or reduce the dependency on third-party service providers? For example, will an AI-enabled screening service reduce current dependency on human-led managed screening services? Will an agentic AI investigation platform reduce current outside spend on forensic or other investigation services?
- If the new platform uses AI, what usage units drive the price: tokens, documents, searches, agents or transactions? Model normal and peak use, retries and human review, and confirm limits, overage rates and spending alerts.
- Change management fees, including training.

In putting these cost estimates together, it is important to document any anticipated changes in scope of use of existing versus new compliance technology; for example, in relation to technology switching, is a "lift and shift" anticipated or will the new technology offer greater functionality that will alleviate the burden on the ethics & compliance team?

Be alert, too, to a structural expectation gap flagged by vendors: platforms bought a decade ago often carry legacy pricing far below today's rates for equivalent scope. One respondent estimated that such clients *"are paying 20% of the price that they would if they purchased today"*; so a budget anchored to the incumbent's renewal line may find replacement quotes jarring.

Building the Business Case

The detailed costings and performance work described above will go a significant way to building the business case for new compliance technology. It will demonstrate to finance and other decision-makers that your proposal is objectively grounded in data.

New regulatory developments may serve as a catalyst for the acquisition of such new compliance technology. For example, the focus of the U.S. Department of Justice on data analytics from 2019 led to the launch of several new transaction monitoring platforms.[14] Forced-labor-related import bans and requirements for modern slavery due diligence led to the development of new supply chain mapping and screening tools.[15]

However, we caution against placing too much value on the reduction of known compliance risks. Assessing inherent and residual compliance risk is challenging in and of itself, let alone assessing the impact of one tool to manage such risk. Vendor and buyer respondents alike were candid in their feedback that demonstrating compliance ROI is inherently hard. One survey respondent also noted that "*we fight against the unseen - sometimes risk goes up because we're finally tracking it*." While enhanced identification of actual risk should be seen as a positive thing, this response indirectly alludes to management's wariness of compliance technology being *too good.*

Further away from the Compliance ROI sun are other value indicators that may be cited in a compliance technology business case:

- Impact on workplace culture and employee retention (e.g. improvements to speak-up/investigation case management technology increasing employee confidence that their concerns will be addressed and in a timely manner).
- Improvements in employee, customer and vendor satisfaction with a related business process (e.g. third-party onboarding).
- Speed and cost of producing evidence for regulators, monitors, auditors and customers, where reliable records can be retrieved and reconciled more efficiently.

But care must be taken here not to over-promise and under-deliver. The better approach is to identify the performance metrics by which new compliance technology is to be assessed, and report on those metrics post-acquisition.

For compliance officers looking to build this discipline, Ethico's Ethicsverse "MBA" masterclass series on running compliance like a business, and its companion session on calculating and demonstrating compliance ROI are a helpful resource.[16]

AI-Specific Budget & Acquisition Considerations

AI may deserve a separate budget line where it introduces distinct usage charges, testing requirements or operational risks. In the CW/konaAI Survey, roughly a quarter of respondents planned to devote 25% or more of their compliance technology budget to AI tool development and operation over the next twelve months, while one in eight reported having no compliance technology budget at all. Budget for evaluation, integration, data preparation, oversight and ongoing monitoring as well as access to the model.

---

[14] The ECCP's June 2020 update introduced prosecutor questions on compliance personnel's access to company data and the use of data analytics; the September 2024 update (see note above) expanded them, including how companies measure the accuracy, precision, or recall of the data analytics models they rely on.

15 See, e.g., the Uyghur Forced Labor Prevention Act, Pub. L. No. 117-78 (2021), and U.S. Customs and Border Protection's UFLPA enforcement resources, https://www.cbp.gov/trade/forced-labor/UFLPA. Similar tooling followed the German Supply Chain Due Diligence Act (LkSG) and related mandatory due diligence regimes.

[16] Ethico, Ethicsverse "MBA" masterclass series (How to Run Compliance Like a Business), https://ethico.com/masterclass/; Ethico, Calculating, Understanding, Demonstrating & Leveraging ROI, https://ethico.com/ethicsverse-episodes/webinar-calculating-understanding-demonstrating-leveraging-roi/. Integrity Bridge is an independent compliance consultant and receives no commission from Ethico.

Among teams already using AI in ethics and compliance work, the realized benefit reported almost universally is efficiency: reduced manual work, followed by improved analytics and faster decision-making; fewer than half report cost savings, and fewer than half agree they are satisfied with the performance of the AI tools their organization uses.[17] Anchor the business case in time returned to the team and improved decision quality, define the success metrics up front, and treat cost savings as an outcome to be reported, not a promise to be made.

How Compliance Technology Vendors Can Help

Nearly all compliance technology vendors who participated in the survey indicated that they support early business case and budget development for prospective clients: the (often unspoken) quid pro quo being that the tech vendor will be invited to participate in any RFP in the future. Compliance tech vendors would much prefer to be involved at this early stage than to go through an RFP process only to be told that the project is on hold due to a lack of budget approval. One vendor respondent reported fielding budget-support requests more than fifty times a year; another noted that such requests often arrive *"disguised as an RFQ."*

Depending on where a prospective client is in the budget process, compliance tech vendors can provide:

- Early value hypothesis.
- Generic ROI indicators and development of customer-specific ROI models.
- Case studies that achieved measurable regulatory, performance and cost ROI.
- Budget ranges around use cases, expected volume, configuration needs, integrations, and deployment complexity.
- Support for internal budget approval requests for management.

Vendor-supported ROI models may contain optimistic assumptions. Ask for the underlying baseline, scope, implementation cost and measurement period, and test them against your own data. Buyer respondents cautioned against generic claims that technology will "pay for itself." Such a conclusion should follow from a supportable model, rather than precede it.

Integrity Bridge helps chief compliance officers build the case before it is needed: compliance technology strategies, current-state cost baselines, budget and ROI models for new technology, and CFO and board-ready materials informed by our experience as a former buyer and as an independent adviser that neither takes nor pays vendor commissions.

Securing In-Principle Technology Approval

Compliance technology typically requires several layers of in-principle approval before it becomes a line item in next year's budget:

- **The budget owner**: often, but not always, the Chief Compliance Officer or General Counsel. Alternatively, in some companies, all technology is managed as part of the Chief Information Officer's budget. Depending on the company's delegation of authority (DOA) thresholds, and the anticipated spend commitment, approval may also be required of someone more senior than the budget owner.
- **IT**: for compliance technology that requires integration with enterprise systems (e.g. ERPs, CRM, HRIS), IT approval is typically needed to ensure that the project is in their own technology

[17] CW/konaAI Survey, Qs 8 and 9: 84% reported improved efficiency/reduced manual work; 41% reported cost savings; 44% agreed or strongly agreed they are satisfied with AI tool performance.

deployment roadmap and related costs (integrations, data storage) are budgeted by them. For AI-enabled technology, IT's gatekeeping role is often doubled: in nearly half of organizations, primary responsibility for overseeing the use of AI sits with IT rather than compliance, so the purchase must also clear the company's AI governance process alongside the usual security and architecture reviews.[18]

- **The executive sponsor:** the member of the Executive Leadership Team who will likely be presenting (and defending) the technology business case on your behalf during budget season.

Each of these approvers may have pre-defined processes for reviewing significant budget/technology proposals. Find the people who administer those processes on behalf of the approvers and learn from the successes and failures of those who have come before you. Also, each of these stakeholders is a person before they are an approval gate, and your engagement style should be tailored accordingly. Some want the detailed cost build; some want the risk narrative; some mainly want to know that their peers are comfortable; the key is to know this well in advance and prepare accordingly.[19]

Beyond the approvers is an important sub-group of potential allies in your quest for budget approval: the future users and beneficiaries of the technology beyond ethics and compliance. For example:

- Internal Audit might support the business case for a new transaction monitoring platform because it shortens their time to audit and reduces dependency on outside resources. Procurement may similarly support the proposal, particularly if the technology can identify inadvertent overbilling as well as fraud.
- HR might support AI-assisted intake and case management if testing demonstrates an accessible reporting experience and better investigation support, with human escalation, confidentiality and appropriate safeguards for affected employees.
- The Sustainability Officer might support the acquisition of supply chain mapping technology because, in addition to helping to manage modern slavery and environmental risk, it can support scope 3 emissions calculations.

Given the number of approvers and other interested stakeholders, start early with informal engagement. Develop the narrative over time:

- you are assessing a particular element of the ethics & compliance program, including its technology.
- you have identified potential opportunities from new investment or from switching providers.
- the analysis is maturing.

By the time the formal request arrives, the proposal should be familiar, evidence-based and ready for challenge. Early engagement should inform the decision without pre-empting the required approvals. One CCO respondent described *"playing the long game"*: *"planting the seed early"* and building advocacy across budget cycles, including by *"finding multiple use cases or other functions that will benefit from the service."*

[18] CW/konaAI Survey, Q 13: IT holds primary responsibility for overseeing AI use in 47% of organizations, against 26% for ethics and compliance.
[19] Ethico, How the Enneagram Can Make You a Better Compliance Professional (Ethicsverse episode), https://ethico.com/ethicsverse-episodes/enneagram-personality-framework-compliance-ethics-professionals/.

Section C: Compliance Tech Marketing

Compliance technology is rarely bought when it is marketed. A compliance tech purchase now almost always traces back to an impression formed long before any RFP existed: a peer's recommendation, a conference conversation, a white paper that taught the reader something. Most of the evaluation happens without the vendor in the room, which makes what a vendor leaves behind (content, reputation, references) the value-add marketing.

Based on feedback from the buyer survey, and our own experience, Chief Compliance Officers and other compliance tech buyers:

- place substantial weight on their peer network. One buyer respondent described positive peer discussion of a vendor as sufficiently rare that, when it happens, people start taking notes.
- are interested in learning about new developments in compliance technology but are not always in the market for new compliance technology.
- appreciate product marketing that addresses the day-to-day challenges they face, with reference to actual case studies.
- value useful surveys, substantive papers and practical resources such as buyers' guides, sample RFPs and budget calculators over generic product marketing created by AI.
- need support building the business case and budget approval request for new compliance technology (see Section B).
- enjoy small vendor events that provide buyers with an opportunity to engage with their peers.
- respond well to formats that compress discovery. One buyer respondent singled out "speed dating"-style introduction sessions as "*fairly effective*": many vendors, short slots, and no obligation.
- may value events that combine peer discussion with short, pre-agreed vendor meetings, provided the format and any conditions of free attendance are clear.
- place greater value on references provided by compliance tech clients than those of compliance consultants or paid-for promoters.

Buyers also place weight on vendors' conduct towards them and their teams, including respect for privacy and communications preferences. Compliance technology vendors should:

- think very carefully about the use of "cold" emails, including those sent using contact lists obtained from conference producers.
- for "warm" emails, consider the volume and frequency. One respondent in the buyer survey suggested that compliance tech vendors observe the "*three attempts then six months of silence*" rule.
- think even harder about cold calling a potential compliance tech buyer. These are invariably coming through to the buyer's mobile phone, likely at the most inconvenient of times. One buyer respondent went further: "*organizations with dedicated sales staff doing cold calls are usually offering a stale product*."
- apply the marketing and privacy rules relevant to the recipient, jurisdiction and channel. US CAN-SPAM rules cover B2B commercial email; Canadian CASL generally requires consent or a relevant exception, identification and an unsubscribe mechanism. UK corporate email rules differ from those for sole traders, and use of named business contacts still engages data-protection rules. EU electronic-marketing rules also depend on national implementation. Assess tracking pixels separately.[20][21][22] One CCO respondent reported receiving cold calls from vendors "*whose marketing departments got my data from a non-compliant data broker*", which was "a non-starter".

20 UK ICO, Business-to-business marketing. Regulatory guidance on UK GDPR and PECR, including corporate subscribers, objections and tracking pixels

21 US FTC, CAN-SPAM Act A Compliance Guide for Business. Regulatory guidance; commercial email rules also apply to business-to-business email.

22 Canadian Radio-television and Telecommunications Commission, Spam and malware. CASL regulatory guidance on consent, identification and unsubscribe requirements; exceptions must be assessed.

- never lie about meeting a compliance tech buyer at an event, or refer to a prior conversation that never happened.
- avoid disparaging competitors.
- be precise about AI claims. Marketing that overstates what a model does or stays silent on training data, human oversight, and failure modes is being read by an audience professionally trained in skepticism. Overclaiming AI capability to compliance officers is not merely ineffective; it is disqualifying.
- resist the temptation to go around a "no." Contacting other members of the buyer's team after the compliance officer has declined, or escalating to the general counsel or the CEO, is remembered, and not fondly. A "not now" is a statement about budget cycles and priorities, not an invitation to find a more receptive audience.
- ensure that any referral commissions paid to consultants for client introductions are fully disclosed (see Section D below);
- follow the buyer's gifts and hospitality rules and avoid gifts or entertainment that could compromise, or appear to compromise, an active selection process.

There is a common thread running through all of this. A compliance tech vendor's marketing is a live early demonstration of its own compliance culture. A vendor that scrapes contact data, ignores an unsubscribe request, invents a prior conversation, or disparages a competitor has told a compliance officer everything they need to know about how it will behave as a processor of the company's most sensitive data. The inverse is equally true: a vendor that markets with restraint, candor, and disclosed interests has passed the first, and arguably the most critical, due diligence test the buyer will run.

Section D: Planning for New Compliance Technology

With in-principle budget approval secured (Section B), attention turns to planning the technology acquisition. This requires understanding the company's procurement process, setting a realistic timetable, identifying credible bidders and designing a clear RFP package.

Understanding a Company's Procurement Processes

In our survey, Compliance tech vendors report that while buyers have a firm understanding of the technology they wish to acquire, they are often less familiar with company procurement processes that must be followed. Specifically:

- when the acquisition of technology above a specific $ threshold requires competitive sourcing (e.g. minimum of 3 bidders);
- whether the company mandates use of an e-sourcing platform (e.g. Ariba or Coupa) through which the RFP must be issued and bids received;
- whether there is a sole-source exception; and
- who are the required approvers for this $ spend/technology.

As compliance professionals who encourage or require employees to follow business processes, compliance tech buyers should practice what they preach. Fully understanding a company's procurement process can also yield multiple benefits:

- a company's source-to-pay process is one of the most important fraud and anti-bribery & corruption controls. Understanding how it works can help compliance teams identify potential controls gaps and/or opportunities to better align with compliance processes.
- conducting an RFP can help you to become a more informed purchaser, identify new improvements for your compliance process and lead to a more successful deployment.
- if there is an objectively justified reason to select one vendor, seek any permitted sole-source approval and document the rationale. Do not use a competitive process to create the appearance of a choice already made.
- vendor estimates of how often bidding processes are effectively pre-decided or market-testing ranged from "not the norm" to "greater than 50%"; a spread that says as much about how poorly buyers signal genuine intent as about the practice itself.
- colleagues in Procurement and IT remember a compliance team that respected their process; that goodwill is repaid when Compliance later needs an exception handled at speed.

There is also a quiet cost to not knowing the machinery: inertia. One vendor respondent described compliance teams that *"get interested in a product, meet with vendors, then go and find out how the procurement process works - and then decide that the effort/risk of procuring a new tool exceeds that of staying with the incumbent."* The procurement process should be a gate, not a deterrent, and it is far less daunting mapped in advance than discovered mid-enthusiasm.

How often a formal process applies varies by segment. One vendor respondent estimated that roughly 60% of its enterprise engagements run through a formal Procurement-led RFP, while the substantial majority of mid-market purchases are sourced through less formal proposal processes. The disciplines in this section apply to both; only the paperwork is lighter.

Accountabilities

As explained in Section B above, Supply Chain/Procurement is often the gatekeeper for enterprise-wide "indirect" spend.[23] In some companies, the procurement of technology hardware and/or software is delegated to the company's IT department. Compliance may therefore need approvals from other functions even when it owns the budget and is accountable for the intended compliance outcome.

This is not to say that Compliance should wholly delegate responsibility for acquiring compliance technology to Procurement and/or IT. Vendors report, and we see, chief compliance officers who disengage once procurement takes the file, reappearing only at the end to discover that the selected platform cannot meet their requirements. The best outcomes happen when procurement manages process discipline, but compliance remains active in defining use cases, evaluating demos and validating workflow fit.

When planning a compliance tech procurement process, consider the following:

- Which function is responsible for the procurement of technology?
- Will the function assign a dedicated sourcing manager to manage the procurement process?
- Who are the other stakeholders who need to be involved during (i) the procurement process; (ii) AI, cyber security, data privacy and other due diligence; (iii) contract negotiations; and (iv) commercial and contract approvals?
- Who is going to be the point person in Compliance? Will that person own the vendor relationship post-acquisition?
- Does the company offer project management support throughout the entire technology acquisition and deployment lifecycle? If not, should Compliance consider retaining a consultant to support? (See Using a Consultant to Support Compliance Technology Acquisition below)

Managing the Project Timeline

Tech vendor survey respondents universally reported frustrations (quote: "*ALL THE TIME*") with slipping deadlines at each stage of the tech procurement process (pre-RFP, RFP, contract negotiations, deployment). Timetable delays also have a compound adverse effect if a company has an existing tech provider with a fast-approaching renewal-notice deadline. Vendors recognize that this is often beyond the control of Compliance teams, but nonetheless feel that steps can be taken to manage the risk of delay:

- Above all else, re-validate that in-principle budget approval to acquire the new compliance technology is secured before commencing the RFP.
- Work with Procurement to develop a realistic RFP timetable, and ensure the Compliance point person is able to meet their obligations in that timetable.
- If there is an incumbent, work backwards from its renewal-notice deadline. Allow time for approvals, testing, migration and contingency. Any contract overlap should be proportionate and budgeted; do not give notice until continuity and an achievable transition route are established.
- Reserve slots in any mandatory IT/AI/data privacy approval processes and assemble the information approvers need in the required format; relevant steering committees may meet infrequently so it is important to get on their schedule.
- Notify the Legal Department well in advance of anticipated contract support.
- Sequence the Non-Disclosure Agreement (NDA) step (see Design of the RFP below) ahead of the intended RFP release date.

[23] Indirect spend is procurement of goods or services that are <u>not</u> used in the manufacture of a company's goods or provision of a company's services. Direct spend is procurement of raw materials needed to manufacture a company's goods. Compliance tech is considered indirect spend, unless the company is providing compliance tech services itself.

Finally, if deadlines are expected to slip, communicate this to vendors as quickly as possible so that they can update their own resource planning.

Identification of Potential Bidders

As explained in Section A, Compliance technology is developing at a rapid pace. AI is reducing the barriers to entry, meaning that newer players are challenging the incumbents. Identifying who to invite to a competitive sourcing process is a critical first step.

If a compliance team has developed the recommended Compliance Tech Strategy, they will have developed a firm view of what technology they require in the short, medium and long term. This is important because it can and should directly affect who you invite to bid for compliance technology that addresses your short-term requirements.

For example, consider third-party risk management. A company's short-term priority may be to switch providers of third-party screening services. Their medium-term priority might be to implement a new anti-bribery & corruption due diligence workflow and procure "boots on the ground" due diligence services. Longer term, they are planning to undertake ESG-related due diligence on their extended supply chain and will likely need supply chain mapping support. Knowing this upfront can directly inform who a tech buyer invites to bid for the initial third-party screening services, and reduce the risk of technology proliferation later on.

Tech vendor survey respondents recommended that buyers should avoid:

- delegating the task of identifying RFP invitees to Procurement/IT (quote: "*often misses the mark*").
- inviting so many vendors that the buyer cannot give each a credible evaluation.
- inviting a vendor purely to benchmark pricing for an incumbent negotiation. Vendors describe learning after the fact that they were leverage and declining that buyer's next, genuine invitation.

To help identify potential bidders, consider the following sources:

- Seek recommendations from other compliance teams. One buyer survey respondent noted that peer referral is "*so rare that any vendors [that] are discussed positively that when that happens … people will start taking notes*."
- An independent compliance consultant with relevant buying and configuration experience can help assess vendors against the company's program maturity and enterprise systems. Verify both that experience and any relationships with recommended vendors.

Integrity Bridge offers this service, which can range from high-level guidance on vendors in the market (business development) or in-depth matching of potential vendors against a client's requirements (contracted engagement)

- Technology analyst reports can help explain a market. Review their scope, inclusion thresholds, evaluation date and methodology, and distinguish independent research from sponsored listings or paid promotion. Use them as a discovery aid, then test fit against your own requirements.
- Treat AI-generated vendor lists as provisional: verify vendor identity, availability, relevant product documentation and claimed functionality. A vendor's own documentation is a starting point; material capabilities still require demonstration or testing.
- If attending a compliance conference, use the exhibit hall to test your market scan against your requirements (see Section C). An hour among the booths is one of the cheapest market scans available, and vendor conversations are more candid in person than in a discovery call.

Convert the long list into a manageable field of credible bidders. Three to six may be a useful planning range, depending on the market, project complexity and procurement rules. Beyond that, vendors suggested that *"things can get confusing for the buyer, which may lead to a bad decision, or worse, buying on price alone."*

To narrow to the shortlist, we recommend the following:

- Compliance tech vendors cite splitting the procurement process into a formal two-stage process of a Request for Information (RFI) and an RFP as best practice used by sophisticated technology buyers. The RFI enables buyers to validate which tech vendors are best able to meet their requirements and ensures that the subsequent RFP is targeted. A separate formal stage may be unnecessary for a small or well-understood purchase, and will likely extend your technology acquisition timetable.
- Review vendor websites to assess their features and industry sectors against your own requirements.
- Participate in initial vendor demonstrations, and (to avoid multiple email follow-ups) provide them with an honest assessment of (i) whether they are likely to be invited to bid; and (ii) when the RFP is likely to commence.
- Do not let the RFP be a vendor's first contact with you. Vendors treat "blind" RFPs, arriving with no prior interaction, as a red flag, and will often no-bid or under-resource them. Several also cautioned that an RFP alone is too thin an instrument to evaluate a vendor: in one respondent's words, proper vetting means *"5+ hours on a call, asking questions and looking at technology, especially 'under the hood'."* One vendor respondent was categorical about blind invitations: *"if there is no engagement, good providers won't bid."*

Time spent upfront on this vendor research not only helps buyers to identify the right prospective bidders, but can directly inform the scope and requirements of the subsequent RFP.

Using a Consultant to Support Compliance Technology Acquisition

In our survey, compliance tech vendors and buyers identified several benefits of using a consultant to support the technology selection process:

- Consultants can assess the effectiveness of the existing compliance program element (e.g. policy management, training administration, third-party screening, investigations management) and recommend improvements to the *process* before configuration in the *technology*.
- As indicated above (*Identification of Potential Bidders*), consultants possess market knowledge across a fast-moving vendor market, and can help to cut through the AI hype.
- They can support or lead the preparation of the RFP bundle, including a clear articulation of the client's vision, use cases, technical requirements, constraints (e.g. multiple enterprise systems, data quality) and selection criteria.
- Consultants can help project manage the technology sourcing and deployment process; by bringing project management discipline they can ensure that the project timetable remains on track.
- Consultants can ensure that changes to both compliance process and technology configuration take advantage of the selected vendor's functionality (i.e. not just a "lift and shift").
- If a consultant is to be used, include the fee in the business case and budget approval from the outset; one buyer respondent said they would consider a consultant *"especially if I could build the cost in up front to my internal proposal/approval process."*

Conversely, vendor survey respondents expressed frustration with consultants who play the role of gatekeeper, limiting direct access to the operational, technical and executive stakeholders who will make the final selection decision and ultimately own the outcome. Buyers also raised concerns with consultants who:

- delegate the project to junior associates with limited experience of the market or underlying compliance process.
- add cost and delay through over-engineering workflows.
- recycle generic evaluation templates rather than adapting to the client's actual processes and enterprise systems.
- field generalist teams without compliance tech specialization. Several vendor respondents reported that large, non-specialized consultancies slow processes down, while specialized consultants in the space work best.

A particularly sensitive issue is consultants' actual or perceived conflicts of interest. These may include:

- Payment of commission when a vendor is (i) invited to participate in an RFP; and/or (ii) selected by the buyer at the end of an RFP.
- Consultants being separately retained by a vendor (e.g. for product design, go-to-market support) and this engagement not being disclosed to a tech buyer.
- A consultant's vendor selection recommendation being influenced by the amount of consultant support needed for technology deployment.

While survey participants were mixed as to the appropriateness of commission payments, there was universal support for transparency. We recommend tech buyers require the disclosure of any pre-existing relationships with compliance tech vendors including those that result in the payment of commission, referral, consulting and/or speaking fees. However, disclosure does not by itself make every conflict acceptable.

Integrity Bridge neither requests nor receives commission or other sales-related payments. Any prior or existing contractual relationship (e.g. speaking engagement) with a prospective tech vendor is fully disclosed to the client. Recommendations as to which tech companies to include in an RFP and which bidder to ultimately select are objective and strictly guided by the requirements of the client.

Design of the RFP

The RFP package is a two-way instrument. It is how a buyer specifies what it needs, and it is also the single strongest signal a vendor receives about whether this buyer is worth the substantial investment a serious response consumes. A coherent, specific, well-governed package attracts the strongest bidders and their best teams; a vague or boilerplate-heavy one invites either a no-bid or boilerplate in kind. The components below reflect what both survey populations, and our own experience, identify as separating the packages that get answered well from the packages that get declined.

Context

In our experience, this is the most important part of an RFP and yet is the part that is often missing. A complete narrative of a company's current state and future technology vision enables tech vendors to offer a *solution* rather than a *product*. This summary should include the following:

- What are the current compliance and enterprise technology solutions?
- What are the compliance processes and technology workflows that underpin existing technology? What use cases is the technology intended to address? Consider attaching existing policies, procedures and process maps to the RFP as appendices (NB: see NDA section below).
- What is the company's organizational structure and how does that affect requirements? (e.g. business units or regions with their own unique workflow requirements).

- What are the current volumes (e.g. employees, third parties, policies, investigations, training modules)?
- What is the level of compliance and enterprise master data quality? (vendor quote: "*buyers who share a realistic picture of their data maturity get a more accurate commercial proposal*.").
- What is the current output of the existing process and technology? As one respondent put it, buyers send out an RFP "*looking for [a] tool to do ABC and that does not define the true process - and the true process shows itself during implementation*"; the same respondent reported that every one of its clients requests post-go-live changes traceable to design work that was never done. Another vendor framed the point structurally: "*you are digitizing processes, but sourcing processes rarely outline what is to be digitized*."
- What are the current challenges that you are looking for new compliance technology to address?
- If replacing an incumbent, describe the reasons and the conditions for switching, subject to confidentiality commitments. Be clear whether retaining or improving the incumbent remains an option. A genuine competition does not require a promise to switch.
- What are the expected system integrations and data flows?
- What internal constraints will shape deployment (e.g. an ERP migration in flight, a change freeze, limited IT resourcing, works council or data privacy approvals required in key jurisdictions)?
- In summary, what is your future compliance technology vision?

Technical Section

The technical section forms the substantive backbone of the entire RFP. It sets out the design specifications unique to the compliance technology in question. While Procurement may own the overall design and formatting of an RFP, Compliance should own the technical section; if the section reads like Procurement wrote it, vendors notice and will calibrate accordingly, typically not in the buyer's favor.

Defining the unique requirements of each type of compliance technology is outside the scope of this paper. At a higher level:

- What are the features of existing compliance technology that need to be replicated?
- What additional features are needed?
- What master data needs to be captured?
- What enterprise systems need to be connected to the compliance technology? For inputs, outputs or both?
- What analytics capability is needed and what metrics need to be reported on? Can data and metrics be exported?
- How does the system manage reporting, audit trail and regulator, public and company reporting requirements?
- What configuration must be achievable by the compliance team itself, without vendor professional services or IT change requests? One vendor respondent called this the deepest source of buyer regret: *"the number 1 regret I hear is going with a system that isn't self-service, and then they can't adapt the program without change requests and fees"*.
- What language and localization requirements apply (user-interface languages, translated content, regional data formats)?
- Can users with disabilities and those using mobile devices or low-bandwidth connections complete the critical tasks?
- Where AI functionality is requested, specify the outcome it must serve rather than asking for "AI" in the abstract. Vendors note that many RFPs *"mention AI simply because it is a buzzword,"* rather than connecting the capability to a workflow or a measurable outcome.

- What operational measures should be included in the service-level agreement (SLA), and which program outcomes remain the buyer's responsibility? (See Section F, *Contract Negotiations*.)

In defining your requirements, consider classifying and scoring each according to its importance. Is the requested feature mandatory, a nice-to-have or for information purposes only (i.e. because it might be needed in the future)?

One of the most common complaints made by compliance tech buyers, and which we regularly observe, is tech vendors failing to follow RFP instructions and answer questions in the required format. Efforts by vendors to obfuscate, particularly where their responses are weak, are counterproductive as they frustrate efforts by buyers to compare responses. To manage this risk, buyers should consider controlling answers as well as the questions. For example, for each technology feature, require a vendor to select from one of the following:

- Yes: Available in the current release as standard.
- Yes: Available through configuration.
- Yes: Available through a named third party or integration.
- No: Not currently available but on the vendor's roadmap.
- No: Not available and no committed development plan.

In addition to features-based questions, we also recommend including open-ended scenario-based questions. For example, for a third-party screening platform: "*a sanctioned party is added to a watchlist overnight - walk us through, screen by screen, how the alert is surfaced, who is notified, and how the resulting case is escalated, documented and closed*." For an investigations case management system: "*our hotline receives a report implicating a senior executive - show us how case access is restricted, how the workflow differs from a routine matter, and what the audit trail records*." Questions of this kind force vendors to demonstrate the workflow rather than affirm the feature and expose the difference between a capability that exists and one that merely appears on a slide.

Pricing

To compare proposals consistently, define the cost breakdown and the scope to which it applies. Common components include:

- Base product pricing per year.
- Third party data services (e.g. screening data sourced by TPRM workflow providers).
- AI/data analytics add-ons or other "premium" features.
- System integrations (API).
- Platform configuration services.
- Bulk data migration from incumbent technology provider.
- Managed services, post-deployment.
- Other charges (vendor required to specify).
- Annual price escalators.

Vendors should be asked to

- price on a set of volume-based assumptions defined by the buyer (number of third parties, employees, volumes).
- provide volume-based pricing thresholds, particularly if volumes are expected to change during the contract term (e.g. due to M&A activity).

Fixed fees can be appropriate where scope, volumes, dependencies and acceptance criteria are sufficiently defined. The problem is asking a supplier to price unresolved requirements or risks it cannot reasonably control. This can be an ineffective and counter-productive method of exerting cost pressure:

- credible bidders may decline, delay their bid or price defensively.
- a single total may conceal exclusions and assumptions unless a breakdown is required.
- delivery quality may suffer if the agreed resources and outputs are unclear.
- uncertainty may return as contingency pricing, disputed exclusions or change requests.

Vendor Qualification

Qualification helps to identify capability or compliance red flags that disqualify vendors at an early stage. While qualification is recognized by vendors as an important component of an RFP, they cite the need for proportionality; too often, the modest technical section prepared by a compliance function is dwarfed by the 300-question template IT security questionnaire. Proportionality has a market consequence too: one vendor observed that heavy questionnaire burdens *"disproportionately favor the larger, more established players"* screening out precisely the newer entrants that AI is bringing to market (see Section A).

IT Security

Agree with IT at the outset what security diligence is genuinely needed at each stage. For shortlisted bidders, the essentials are independent assurance reports, hosting and support locations, material subcontractors and incident history. Then read what you are given. A SOC 2 Type II report is an attestation over a defined period and scope, not a certification: check the exceptions, and the controls the customer is expected to operate. An ISO/IEC 27001 certificate covers a defined organizational scope; it does not prove that each product is secure.[24] Save the deep dives (architecture review, penetration-test remediation, resilience testing) for the preferred bidder. Staged diligence should reduce duplication, not defer disqualifying issues.

Data Privacy

Whose data? For what purposes? Shared with whom? Processed where? Determine controller and processor roles, lawful grounds for processing, safeguards for sensitive or criminal-offence information, retention rules, and support for individuals exercising their rights. Agree the required processor terms and assess international transfers on the facts; regional hosting alone does not resolve every access or transfer issue.

Artificial Intelligence

Which features use AI, which model or provider (and version) sits behind each, what data goes in, what comes out, and what the system is permitted to do with it? Ask where human review is required and how changes to models and features are controlled. The NIST AI Risk Management Framework[25], NIST Generative AI Profile[26] and CLAIR's AI Vendor Due Diligence Questions[27] are useful reference materials.

Test failure modes that matter in compliance work. How does the system keep one customer's data from surfacing for another? How does it handle misleading source material, or instructions embedded in an uploaded document? Can it flag unsupported assertions and material omissions, perform consistently across languages and groups, and abstain and escalate when it should?

Where an AI agent is permitted to act, be specific: which tools and records it may touch, where approvals sit, what limits and logging apply, and how quickly the automation can be suspended. Sensitive actions (releasing an allegation, closing a material case, changing a screening rule) should

24 AICPA & CIMA, System and Organization Controls suite of services. SOC 2 is an examination and reporting framework, not a product certification; the report scope and findings matter.
25 NIST, AI Risk Management Framework 1.0. January 2023; voluntary framework. The NIST resource page states that revision is underway.
26 NIST AI 600-1, Generative Artificial Intelligence Profile. July 2024, sections 2–3, especially confabulation, data privacy, human–AI configuration and pre-deployment testing. Voluntary guidance.
27 CLAIR, AI Vendor Due Diligence Questions, listed in its AI Governance Resources. https://www.joinclair.com/resources.

require defined human authorization, and a fallback process must survive the failure of the model or its provider.

Finally, have Legal assess the rules that apply to the actual use case and to each party's role. Under the EU AI Act, obligations turn on intended purpose, risk classification and whether a party is a provider or a deployer; a generic "AI compliant" claim is not an answer. Record the applicable implementation timetable in the procurement file.

Ethics & Compliance

Is the vendor prepared to certify compliance with the company's Supplier Code of Conduct? Screen the vendor as you would any third party through your own TPRM process. Secure Supplier Code certification, anti-bribery representations, and modern slavery and supply-chain disclosures proportionate to the relationship.

Financial Resilience

Most compliance tech vendors are privately held, so publicly available information is thin. Assess resilience proportionately and directly: ownership, whatever financial information the vendor will share, dependence on key people, product-support commitments and concentration in subcontractors. The question behind the questions is simple: will this vendor still exist, and still be investing in this product, at renewal? A smaller vendor may well be the right answer with appropriate safeguards; size alone is neither assurance nor a disqualifier.

Support Model

Ask now about the support model you will live with after go-live: the cumulative experience of the client-facing team, named support contacts versus anonymous ticket queues, escalation paths, and post-launch enablement. One vendor respondent warned that a solution that looks good in a demo but has inadequate support *"can result in buyers' remorse."* Similarly, a buyer respondent reported that ticket systems without a human relationship are *"extremely annoying from a customer perspective."*

Exit & Offboarding

Require bidders to describe offboarding in the proposal: export formats, content, timing, fees, continued access and transition assistance. Include attachments, metadata, audit trails, workflow configuration and decision records, subject to third-party rights. Test a sample export and reconciliation; a CSV file of selected fields may not preserve a usable investigation record. Buyer respondents highlighted exit commitments, while a vendor observed that *"how a vendor behaves on the way out says as much about them as how they behave on the way in."* Make the incumbent part of the same discipline: establish what your current vendor's export utility produces before migration is scoped, and require bidders to prove theirs during evaluation. In one vendor's words: *"a lot of companies get surprised at this point that their vendor doesn't have a good export utility ... everyone misses it, and it's really important."*

Glossary of Terms

To avoid misunderstandings, and to ensure that comparisons between vendor proposals can be made, we recommend including a glossary of key terms that are used throughout the RFP. Terms that mean different things to different vendors (e.g. "continuous monitoring," "ultimate beneficial owner," "false positive," "implementation," "total cost of ownership") are cheap to define and potentially expensive to leave ambiguous.

Selection Criteria

To ensure an objective selection process, competitive sourcing best practice involves defining and proactively communicating your evaluation criteria. This includes:

- identifying which RFP requirements are scored versus information-only.
- clearly communicating the penalties for vague or incomplete responses.
- the scoring mechanics (pass/fail, %).
- the weighting between scored measures.
- how many bidders have been invited, and what the down-selection stages and decision timeline look like.

Pre-defining your evaluation criteria and scoring methodology, and controlling the manner in which bidders provide answers, enables the easier preparation of scorecards.

Bidding Timetable

Bidders should be provided with a reasonable timeframe within which to ask questions, schedule demonstrations and submit their response; if you anticipate your selection decision taking several weeks or even months, a two-week deadline for RFP responses is unreasonable (but, per the vendor survey, does happen). Finally, if the submission deadline is pushed back for one bidder, it should be adjusted for all. As a rule of thumb, allow no less than three to four weeks for a substantive package, with a published window for clarification questions inside it.

Non-Disclosure Agreement

Before the RFP and supporting materials are provided, bidders should be asked to sign an NDA. The NDA should restrict use of RFP materials to bid preparation only and require return or confirmation of destruction of such materials in the event of an unsuccessful bid. Address AI explicitly: identify which tools, if any, may process the materials and on what terms; prohibit unauthorized disclosure, training or reuse.

The NDA should also be mutual: in the demonstrations and clarifications that follow, vendors will disclose roadmap and pricing information that is confidential in the other direction. Guard that direction with equal care: bidders' pricing, roadmaps and proprietary materials must not circulate beyond the evaluation team. Vendor respondents reported commercial information shared in bids finding its way to competitors.

Integrity Bridge supports compliance teams with the preparation of RFP packages for various types of compliance technology including communications monitoring, policy management, speak up & investigations, third-party screening & diligence, transaction monitoring and training. These packages are tailored to a client's existing and planned compliance processes.

Section E: Participation in the RFP

The RFP is out. What follows is the phase both sides experience as the deal itself: qualification, questions, demonstrations, hands-on testing and, finally, the response. It is also where the planning described in Sections B and D pays for itself, or fails to. The disciplines below are addressed to both sides of the table, because both are being evaluated: bidders on whether they can be trusted to deliver, and the buyer on whether this is a process worth a serious vendor's best team.

Buyer Qualification

Vendors also assess potential buyers and invitations to bid. Survey respondents indicated that each RFP can often require 30–50 hours of investment from each bidder, sometimes more. Compliance tech vendors maintain their own "no-bid criteria" that ensure consistency when deciding whether to make that resource investment.

Factors that can positively influence a vendor on that decision to bid, and how many resources they invest, include:

- Early, substantive engagement can help a vendor understand the opportunity. Where prior contact is restricted or has not occurred, a clear briefing can serve the same purpose.
- Evidence that budget for the compliance tech has been approved in principle.
- Sophistication of RFP materials, including the weighting of the compliance substantive section versus others.
- Involvement of the compliance team, and any other decision makers, during early engagement with a prospective bidder. Vendors read involvement as intent: an engaged compliance team "*signals that they are looking for improvement and change*"; an absent one "*typically signals they are looking to check a box or drive down the cost of their technology.*"
- The buyer's demonstration that the competition is genuine and that switching is feasible if a challenger offers the best outcome. One vendor respondent stated: "*if we're simply being invited to fill out the dance card, we often decline*."
- A named executive sponsor and a stated decision date.
- Signals of sophistication. Marks of a sophisticated buyer were a willingness to engage, an articulated longer-term vision, the ability to *"speak to the actual problems, pains, and focus on outcomes,"* and a grasp of *"the change management process and time it takes to implement."* One respondent added that the clearest tell is a buyer who can *"define all the areas that their current platform has failed and articulate exactly what they need,"* adding that this is *"very rare."* The red flags are the mirror image: *"a tick box of features with price being the driving factor and unrealistic timelines."*

Buyer-Bidder Communications During the RFP

A tech buyer's competitive bidding process may require buyers to limit communications with prospective bidders:

- All communications with vendors during the RFP should involve the RFP lead, typically a member of Procurement. Several vendors counseled against prohibiting any contact with the compliance team, noting that this can result in more generic bids.
- Any communications that could affect bidder scoring should be in writing.
- Where a material clarification is given to one bidder, it should be circulated to all.
- Do not receive gifts or hospitality during the RFP process.
- Keep a log of material communications with bidders.

- Decline "one-off" conversations in which a bidder seeks insider information. One buyer respondent said plainly that the attempt itself *"lacks integrity,"* and it is remembered at scoring time.

Bidder Clarifications

Even with a perfect RFP, bidders should be expected to have questions. Bidders should be afforded a window during which questions can be posed. To minimize delay, it is important that the buyer's RFP lead has internal stakeholders lined up ready to answer bidder questions. Ideally, all questions received from bidders and their responses are aggregated into one Q&A document to ensure that each bidder is receiving the same information (while respecting confidentiality obligations to bidders). Similarly, if a question exposes a genuine gap or error in the RFP, correct the package for every bidder.

Meetings & Demonstrations

In the ordinary course, a bidder will expect, at a minimum, the opportunity to meet and showcase their technology to the buyer. If a bidder is disqualified before this stage, this is as likely a function of poor bidder identification as it is a poor-quality response from a bidder. In the event of rejection at this time, a bidder should be provided with clear and honest feedback as to why.

Meetings between the buyer and bidders require careful planning on both sides. For buyers:

- Communicate the same expectations of the purpose and content of the meeting to all bidders: for example, what compliance problem is being solved, which workflows matter most, what evaluation criteria will be used, and what concerns need to be addressed.
- All buyer attendees should have read the materials beforehand.
- If there are potential differences of opinion between buyer stakeholders, seek to address those internally beforehand; in survey responses, multiple vendors reported having valuable meeting time taken up by arguments between buyer stakeholders. One vendor described becoming *"the therapists in the room"* when a large group of decision makers could not agree on their own needs; another recalled a procurement officer abandoning a TPRM RFP altogether because the stakeholders kept fighting.
- Ensure decision makers are in the room: this means not only Compliance and Procurement, but also the budget holder (if different), operational process owners, relevant technical stakeholders, and any executive sponsor or business leader who is ultimately accountable for successful deployment.
- Ensure the physical or virtual meeting room is appropriately set up for the demo.
- Allow enough time for the agreed use cases and questions. A focused 60–90-minute session may suit an initial evaluation; complex workflows or technical diligence may need separate sessions.
- Schedule bidder meetings close together, the same week where possible, so comparisons are made while memory is fresh, and score each session against the pre-agreed evaluation criteria rather than general impressions.
- Signal engagement: cameras on, questions asked, follow-ups raised live rather than sent as a list a week later. Vendors calibrate their seriousness to the buyer's: "*attendees having their cameras on indicates engagement*."
- Evaluate the company as well as the software. One vendor respondent observed that buyers increasingly *"care only about functionality and price. In doing so, they are flying blind on important strengths and weaknesses of the vendor"* such as the delivery team and the support model.
- Buyer stakeholders should provide feedback to the RFP lead immediately after the meeting, while it is still fresh in their mind.

For Compliance tech bidders, meetings with a buyer are not just an opportunity to sell the compliance technology. To secure internal approval, compliance teams must involve busy and likely distracted employees from other functions. The performance of bidders during these meetings can reflect positively or negatively on the internal reputation of the compliance team. Bidders should:

- send a short survey or agenda request in advance to gather the buyer's context and arrive prepared. Buyer respondents singled the practice out for praise, alongside honest, industry-specific materials that highlight *"what they do best"* while *"being honest about any gaps."*
- prepare from the RFP pack, not the pitch deck: explicitly reference the buyer's stated volumes, workflows and pain points.
- bring the team that will implement the technology.
- treat meetings with a buyer as a working evaluation rather than a one-way scripted demo; the questions asked by a bidder are just as impactful as any demo.
- follow buyer's direction (buyer survey response: "*show what was asked and not what wasn't.*").
- use a case study to walk through the technology workflow.
- close with clarity: restate what was asked, what was shown, and what remains open, and confirm the follow-up in writing.

Following the meeting, bidders should promptly provide any supplementary information requested by the buyer. This does not necessarily need to be in written format; we have seen several vendors follow up with recorded demonstrations of specific walkthroughs of the compliance technology in action, which are usually well received by buyers.

The RFP lead should close the loop after the demonstration with a definitive status and timeline for the remainder of the RFP. Many vendors responding to the survey expressed frustration with lengthy periods of radio silence following a meeting.

Sandbox Access

Compliance tech vendors report that AI, whether used in their product or not, has increased buyer requests for hands-on testing of the platform in a sandbox environment. Vendors were mixed as to the perceived value of sandbox environments relative to the resources needed to set them up. Several were concerned that an unconfigured sandbox has the potential to misrepresent the product. All vendors expressed frustration with buyers who request sandbox access but are too busy to use it.

Buyers, for their part, read refusal the other way: one CCO respondent reported that a sandbox or test reports are almost always offered and that *"not doing so is a red flag."* The tension is best resolved with a guided, purpose-built environment:

- Vendors should establish a standard workflow within a sandbox environment that showcases their features. Where appropriate, consider using a case study with synthetic data.
- The sandbox should have a data export feature to enable buyers to test how platform data can be incorporated into their compliance analytics and reporting.
- Supplement the sandbox environment with explanatory notes concerning functionality and AI/data safeguards. A hybrid of a sandbox environment is a guided walkthrough of the platform with these explanatory notes built in.
- Buyers should agree data safeguards before access is granted: synthetic or anonymized data only unless the data privacy agreement (DPA) and security review have already been completed.
- Agree a timeframe for access to the sandbox, and milestone markers where vendors and buyers can provide feedback.
- Test against your own workflows. One vendor respondent, arguing against taking RFP answers on trust, urged buyers to *"actually try and test the system yourself - not just a generic sandbox, but something tailored to your workflows ... pick a use case that is important and make sure it not only works, but is intuitive."*

Responding to the RFP

The RFP response is the final act. *How* bidders respond to the RFP is just as important as the substantive content. A poorly crafted RFP response, which makes it hard for a buyer to compare against other responses, will be consciously or subconsciously penalized.

Given that compliance tech vendors respond to multiple RFPs each month, one would think that this is a well-drilled exercise, with consistent quality of responses. However, buyers suggest otherwise. We recommend the following:

- Prepare a self-standing executive summary that the RFP lead can share with decision makers.
- Address the buyer's stated problem, vision and goals. Where these are unclear, seek clarification and identify assumptions rather than substituting your own.
- Compliance tech vendors have the privilege of seeing hundreds of client compliance processes in action. Don't just focus on technology attributes; provide feedback on a buyer's existing substantive process, and how your technology can help.
- Demonstrate industry-specific experience through technology configurability, case studies and client references.
- Closely follow RFP instructions:
  - answer the questions that were asked, in writing, in the buyer's structure.
  - answer questions with pre-determined response keys correctly. A "Roadmap" response with an expected date is credible; a "Yes" that turns out to mean "configurable, later, at additional cost" will significantly undermine trust later.
  - complete mandatory fields. Don't leave cells blank, hedge with "to be negotiated" or provide generic marketing decks in lieu of answers.
  - if a mandatory requirement cannot be met, say so and propose the nearest alternative.
  - tailor answers to the right stakeholders (e.g. the technical section for Compliance, commercial for Procurement).
- Proactively disclose scope and assumptions.
- Identify upfront what is needed from the buyer for a successful deployment.
- Provide a transparent pricing structure with a clear cost component breakdown.
  - Price the buyer's stated volume scenarios exactly as defined.
  - Clearly identify variables and ranges that affect pricing (e.g. number of employees, third parties, investigations, policies).
  - Separate one-off costs (implementation, migration, integrations) from recurring fees and state the assumptions behind each.
  - Keep the proposal valid for the agreed period. Submit revised offers only through the stated process, showing changes in scope, assumptions and price clearly.
- Provide a realistic implementation roadmap including platform configuration, system connectivity and data migration from incumbents. Identify the implementation team.

Section F: Vendor Selection and Contracting

The value of a well-designed RFP becomes apparent at selection. Clear functional requirements and input from the relevant technical specialists help distinguish demonstrated capability from marketing claims. Security and privacy diligence can identify disqualifying gaps, while an appropriately weighted scorecard supports comparison among otherwise similar bidders.

Selection

Selection Committee

We recommend that a distinction be made between (i) the working group that is responsible for developing the selection recommendation; (ii) other stakeholders who need to be consulted prior to finalizing the recommendation; and (iii) the ultimate decision maker(s):

- Compliance and Procurement should be responsible for reviewing responses and developing the selection recommendation.
- Other functions, particularly those responsible for due diligence and future deployment, should be consulted (e.g. data privacy, IT).
- Re-validate who is the budget holder, the required approver (per the company delegation of authority) and the person authorized to sign the contract (not always the budget holder).

Bid Evaluation

It might seem trite but it is important for buyers to carefully read bidder responses! One vendor survey respondent provided the anecdote of a Fortune 50 buyer rejecting a vendor for "missing" functionality it had demonstrated and documented.

We also recommend the following:

- Keep bidders up to date with the review timeline, particularly if delays are likely.
- Follow the pre-defined scoring methodology and document the review.
- Where more than one member of the Compliance team is involved in the RFP, each member should score independently before conferring.
- Where a response contradicts what was demonstrated, reconfirm with the bidder before scoring it down.
- Consult with other stakeholders to identify any technical red flags.
- Keep price in perspective. One vendor respondent observed that where value is demonstrated, price is rarely the determinant within a reasonable band (*"if you're within 20% it's usually okay"*). Be wary of Procurement placing more emphasis on a price vs capability gap.
- Weight substance over polish. Compliance buyers naturally gravitate to the user experience but, as one vendor respondent cautioned, that is how people buy *"a new house because it has a fresh coat of paint and new countertops but failed to inspect the plumbing, electrical, HVAC."* The data model, security architecture and system integrations are the technology plumbing.
- Hold structured reference calls with two or three clients of comparable scale and sector: implementation experience versus what was sold, support responsiveness, and what they would do differently. Ask the vendor for a client who left; the answer, either way, is informative.
- Meet the named implementation team and validate delivery assumptions before signature: methodology, resourcing, timeline, data migration approach, training and enablement materials, and the post-go-live support model.

- If retaining a reserve bidder during diligence and contracting, explain its status, the remaining uncertainty and how long the proposal is expected to remain valid. Do not imply that two bidders have both won.
- Prepare an executive summary of the evaluation for the ultimate decision maker(s).

Award

Once a decision has been made, vendors benefit from a clear yes/no response. Several vendors reported never being informed of the final decision; they were simply ghosted. Also:

- tell bidders as soon as they are eliminated at any stage, rather than only at the end.
- all vendor survey respondents were keen to receive concise feedback on the main factors behind the decision (vendor response: "[*w]e are all adults and can handle bad news.*"). One vendor survey respondent requested live feedback: "*a 20-minute conversation … is genuinely valuable … the default is a templated rejection email that tells you nothing*." The courtesy flows both ways: one buyer respondent offers every losing bidder a feedback call and finds that "*often this is not taken up*."
- for losing bidders, buyers emphasized the importance of losing gracefully. The conduct of a losing bidder can directly inform whether they are invited to a future opportunity. Buyer survey respondents cited disparaging the (suspected) winner as being counterproductive.

Contract Negotiations

Relief at completing the selection process can be short-lived as the sobering reality of contract negotiations hits both sides. Survey respondents identified the following recurring points of contractual contention:

- Limitation of liability (vendor survey response: "*just stop asking for unlimited liability*").
- Indemnification and insurance.
- Termination for convenience.
- Service credits versus termination rights for persistent SLA failure.
- Data-protection obligations, including retention, legal holds and deletion.
- Use of company and vendor intellectual property.
- Publicity, logo and case-study rights.
- Security obligations.
- Unusually broad audit terms.
- 90–120-day payment terms.
- Auto-renewal mechanics and renewal price escalators.

To reduce delays and preserve the agreed outcome, Compliance should work with Procurement and Legal on the following:

- Ideally, in-house counsel is one of the stakeholders who has been involved throughout the RFP. If not, ensure they are fully briefed on what the technology does and provide them with a copy of the successful bidder's RFP response. Vendors report "*legal teams engaging for the first time after commercial agreement, effectively reopening settled points*."
- Where personally identifiable information is to be processed, involve the in-house data privacy counsel if there is one so that the data privacy agreement can be prepared (and the data privacy impact assessment completed if it hasn't already been).
- Establish whether the successful bidder will be required to use the company's contract template for software. Buyer protection is important but recognize that a draft contract on buyer paper heavily weighted in favor of the buyer will likely lead to significant delay during negotiations.

- Use the contract form appropriate to the technology being acquired. Don't shoehorn compliance tech into a consulting services template. Vendors are blunt about the mismatch: *"contracts drafted for large enterprise software vendors (or worse, industrial companies) being applied unchanged to specialist SME providers - the provisions simply don't fit."*
- Participate in those negotiations between Procurement/Legal and the vendor to avoid discussions going down rabbit holes.
- Use scheduled negotiation calls or meetings with authorized decision makers to resolve material issues versus email.
- Ensure that scope, pricing and assumptions in the draft contract closely track the vendor's final RFP response.
- Price the known unknowns honestly (master-data quality was the most-cited in the tech vendor survey).
- Agree implementation milestones, dependencies, responsibilities and objective acceptance tests for configuration, integrations and migration.
- Negotiate an associated service-level agreement including key performance indicators for the operation of the technology and any associated managed services.
- Define governance upfront for change orders and associated costs.
- Proactively address what happens in the event of termination in relation to, for example, data ownership and export and the provision of transition assistance.
- Do not re-open pricing after final agreement. The same discipline the buyer expects of vendors (Section E) applies in reverse: vendors cite *"procurement pushing for discounts after final pricing has been agreed and accepted"* as a practice that undermines trust, just as the relationship begins.

Section G: Concluding Remarks

This white paper has followed the arc of a compliance technology purchase from strategy to signature: the market and its frustrations (Section A); the strategy, budget and business case that precede any acquisition (Section B); the marketing conduct that builds (or burns) credibility long before an RFP exists (Section C); the planning, bidder identification and RFP design that determine most outcomes before the first bid is received (Section D); conduct of the RFP itself, on both sides of the table (Section E); and the selection and contracting practices that convert a good process into an optimal outcome (Section F).

If there is a single thread running through the survey responses and our own experience, it is that the compliance technology market runs on trust. Buyers ask vendors to market honestly, answer what was asked, disclose limitations and price transparently. Vendors ask buyers to run genuine processes, share real context, keep to their own timetables and deliver outcomes with honest feedback. These are similar values that compliance professionals ask of their own organizations every day. A profession that evaluates conduct for a living should expect its own purchases, and its own sales, to model it.

Contract signature is a milestone, not evidence that the investment has succeeded. That is also dependent on the appropriate configuration and deployment of the technology, a subject which will be the focus of a separate white paper in early 2027.

Providing Feedback on this White Paper

We hope this white paper is helpful. We would love to receive feedback! You have two options:

- Add comments to this paper and send them to info@integritybridge.com
- Complete the survey for buyers or sellers, both of which remain open and can be accessed by scanning the relevant QR code below. The surveys cover both selection and configuration of compliance technology.

Buyers

Vendors