EDUCATIONAL MATERIAL | GOVERNANCE & COMPLIANCE

Compliance programs: from policy to practice

An educational guide and discussion checklist on governance, risk management, and operational controls for small and mid-sized businesses.

AUTHOR | Kaique Ruan Dourado Cabral · VERSION 2.0 · 20 OCT 2026

Why written policies are not enough

A company may have a code of conduct, documented procedures, and training while those materials fail to guide day-to-day decisions consistently. The challenge is understanding the connection between formal design, responsibility, available resources, observable practices, and responses to problems. The gap between “having a policy” and “being able to demonstrate how it works” is this guide’s starting point.

References are guidance, not a seal of approval

The DOJ publishes guidance about reviewing corporate compliance programs in the specific context of federal prosecutors’ work. It addresses design, implementation, and practical operation; it is not a universal checklist or certification scheme for small companies. NIST separately publishes voluntary guidance, including cybersecurity resources tailored to smaller organizations. Neither source replaces analysis of a business’s own risks, legal obligations, and circumstances. [P1] [P2]

The reader’s objective

Identify topics to discuss among leadership, operations teams, and appropriately qualified professionals. This material does not measure maturity, effectiveness, compliance, residual risk, or performance. The presence or absence of a single procedure does not by itself establish whether a program is adequate.

The guiding question is not merely “what document exists?” but “what happens when the organization needs to act?”

01 | LEADERSHIP & STRUCTURE

Governance, accountability, and business risks

Responsibility and leadership support

A compliance program rests on human decisions: who notices problems, who assesses them, who may recommend changes, and how significant issues reach leadership. A small business may combine roles, but still needs to understand potential conflicts and limits of authority. Naming a responsible employee does not prove that the person has adequate time, independence, or resources. DOJ guidance discusses leadership commitment, autonomy, and resources in its own program-evaluation context. [P1]

Understanding risks arising from actual activities

Relevant risks vary between subscriptions, e-commerce, in-person services, critical vendors, and international activities. A generic risk list does not replace knowledge of business processes, markets, and operational changes. A risk review may need revisiting when products, vendors, jurisdictions, or sales channels change; the significance of any fact requires professional context.

Policies suited to real work

A policy can be technically sound yet hard for decision-makers to understand or use. It may assign responsibilities that do not match the company's systems or ways of working. An effective discussion should connect language, training, workflows, and communication channels without assuming that every organization needs the same volume or format of documentation.

For a technical discussion: stated responsibilities and observable routines can be compared without assigning scores or ratings. Examples of actual decisions, internal records, and management explanations help establish context, but their sufficiency requires professional assessment.

> Hypothetical situation. A policy requires marketing approval before campaigns launch, but a vendor publishes new advertisements directly. A policy exists, yet its actual operation calls for examination. The situation does not, on its own, establish program ineffectiveness or a legal violation.

02 | PEOPLE & THIRD PARTIES

Training, reporting concerns, and vendors

Training tied to real decisions

General training may create a shared vocabulary without helping employees recognize role-specific issues. Its educational value depends on audience, responsibilities, and how regulatory or operational developments reach the right people. Attendance alone does not prove learning or compliant behavior; evaluating later conduct requires appropriate observation and analysis.

Reporting channels, follow-up, and trust

Channels for questions and concerns should be understandable and connected to people who can consider the facts. Their design raises issues of confidentiality, appropriate information handling, and the ability to escalate sensitive matters. No reports should not automatically mean no problems; more reports do not necessarily mean a weaker program.

Third parties and oversight limits

External marketers, payment vendors, logistics providers, and technology contractors may perform critical steps in an organization's operations. Contracts and written commitments do not, on their own, establish how those services operate. The FTC emphasizes attention to cybersecurity risks involving vendors that can access sensitive information; the appropriate depth of review depends on the relationship and risk. [P3]

For a technical discussion: attendance logs, communications, manuals, and employee accounts are different evidence sources. None alone demonstrates learning, culture, or effectiveness. Interpretation must consider the purpose of a control and the decisions it is meant to guide.

> Hypothetical situation. Staff received training on escalating repeated customer complaints, but a system categorizes every contact under an uninformative generic label. Training may have taken place, yet the workflow may prevent recurring patterns from being recognized.

03 | PRACTICAL PERFORMANCE

Monitoring, response, and continuous improvement

A program must be observed in operation

Formal approval does not establish effectiveness. The question is whether procedures are understood and used and whether important problems reach responsible decision-makers. Reviewing practices may involve records, decisions, interviews, and suitable evidence; no single measure proves effectiveness in every area.

From incidents to an understanding of causes

An event may arise from a system error, weak communication, commercial pressure, unclear procedures, individual misconduct, or several factors together. Before recommending standardized fixes, an organization should understand the nature and reach of the problem. DOJ guidance discusses root-cause analysis and remediation, but does not provide an automatic formula for every business. [P1]

Changing operations and technology risks

Growth, remote work, and dependence on digital vendors can alter an SME's exposure. NIST CSF 2.0 provides a voluntary language for discussing Govern, Identify, Protect, Detect, Respond, and Recover in cybersecurity. NIST's small-business introduction is not a compliance assessment and cannot guarantee protection against incidents. [P2] [P4]

For a technical discussion: issuing a recommendation and implementing it are different events. Records of the initial issue, decisions about change, and later observations may support discussion of organizational learning without creating an automatic maturity rating.

> Hypothetical situation. A business resolves billing mistakes repeatedly but never examines the interaction among contracts, invoicing, and support. Each correction matters; understanding the program also means considering what the organization learned from the pattern.

04 | GUIDED REFLECTION

Questions for a governance discussion

Eight introductory prompts

1. Can leadership explain which compliance concerns are relevant to the current business model?
2. Do formal responsibilities match available people and resources?
3. Are practices reconsidered as products, vendors, or markets change?
4. Are there known differences between written policies and how teams actually work?
5. Does training connect with decisions and questions employees encounter?
6. Can important concerns reach responsible leaders without depending on one person's initiative?
7. Can the organization recognize recurring problems and discuss possible underlying causes?
8. After a change, is there a way to observe whether it worked as expected?

Why these prompts do not yield a result

They are invitations to discuss, not variables in an assessment instrument. Answers without context may mean different things depending on industry, scale, risk, resources, and applicable obligations. A program is not "mature" or "effective" because it receives a particular number of positive answers here.

Where professional assessment begins

Individualized review may require examining actual governance, documentation, records, conflicts, materiality, legal duties, and implementation, including when to refer questions to U.S.-licensed lawyers or other specialists. This publication does not prescribe corrective actions or replace that work.

From document to practice: educational questions support dialogue; professional assessment interprets context.

REFERENCES | SCOPE | VERSION

Official sources and limits of use

[P1] U.S. Department of Justice, Evaluation of Corporate Compliance Programs (September 2024)

https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl

Guidance for prosecutorial assessment, not a universal compliance checklist or certification.

[P2] NIST SP 1300, Cybersecurity Framework 2.0: Small Business Quick-Start Guide (2024)

https://doi.org/10.6028/NIST.SP.1300

Voluntary introductory guidance for smaller organizations.

[P3] FTC, Cybersecurity for Small Business

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity

Risks involving vendors, data, and digital infrastructure.

[P4] NIST, Cybersecurity Framework 2.0 for Small Business

https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

Public reference framework and small-business cybersecurity resources.

Methodological note. DOJ ECCP discusses topics that may matter in certain prosecutorial evaluations of corporate programs; it is not a general mandatory standard. NIST CSF 2.0 is voluntary guidance. Citation does not indicate DOJ or NIST review, endorsement, or certification. This publication is not an audit, maturity rating, effectiveness diagnosis, individualized consulting, or legal advice. Specific matters require appropriately licensed or qualified professional review.