STONESIGHT / EXECUTIVE WHITEPAPER

WHY COMPLIANCE FAILS

When the pressure to perform overrides
the controls meant to protect us



StoneSight
ADVISORY SERVICES

INDEPENDENT JUDGMENT. INFORMED ACTION.

01 / THE MANAGEMENT DECISION

When protection becomes optional.

Imagine a racing team introducing a new steering wheel. Its controls are more sophisticated, but difficult to operate while wearing protective gloves. The driver solves the problem by taking off the gloves. The car leaves the garage on schedule. The team gets the performance it wanted. The driver's hands are now exposed.

The inconvenience has been removed. The risk remains.

Safety requirements established by motorsport governing bodies reflect decades of experience, investigation, and engineering. Enterprise controls carry a similar inheritance. Behind requirements that now appear bureaucratic are failures involving fraud, unauthorized activity, unreliable reporting, and misplaced trust.

Yet organizations routinely make the equivalent of that driver's decision. A safeguard interferes with delivery, so someone bypasses it. The immediate objective is achieved. The protection disappears, sometimes without anyone recognizing what has been surrendered.

When management makes protection optional

Compliance can fail inside an organization that employs capable people, maintains extensive policies, and receives regular assurance. The weakness often lies in the decisions made between those formal arrangements.

“We do not need that review.” “Approve it this time.” “We cannot delay the release.”

Each instruction may appear reasonable. Together, they establish the practical authority of the control environment. Employees learn which requirements survive pressure and which yield to a sufficiently urgent request.

Management override is a recognized internal control risk. Its effects reach beyond the individual exception. When leaders repeatedly bypass requirements they have approved, they teach the organization to regard those requirements as negotiable.

There are legitimate reasons to change controls and invoke emergency procedures. Businesses need room to exercise judgment. That judgment must address the exposure being created, the safeguards that remain, the authority required, and the conditions for returning to normal operation.

An executive's willingness to proceed cannot establish that these questions have been answered. Nor can an internal acceptance of risk erase an external obligation.

The decisive issue is whether leadership understands the protection it is changing. Without that understanding, management can mistake the removal of friction for an improvement in performance.

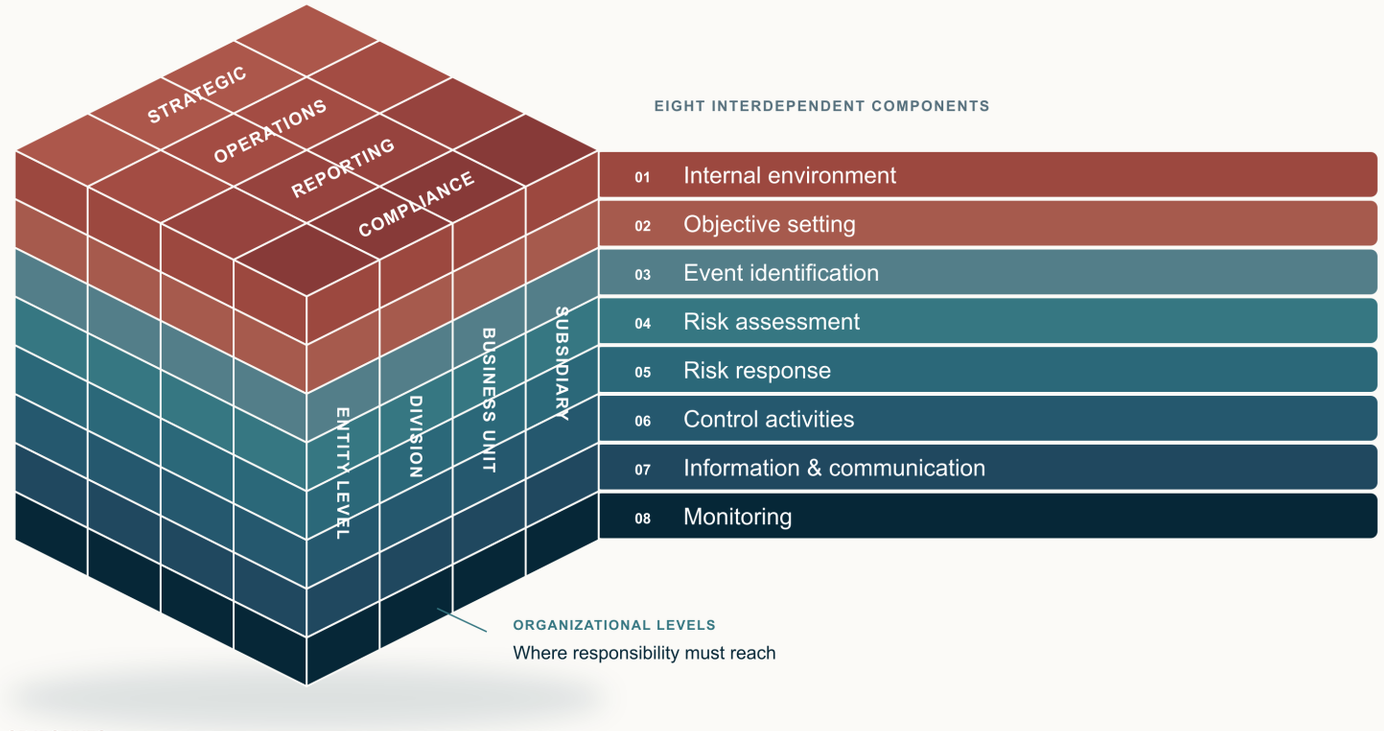
02 / PURPOSE AND OWNERSHIP

People perform the action and miss the purpose.

A control can survive in documentation long after its purpose has disappeared from organizational memory.

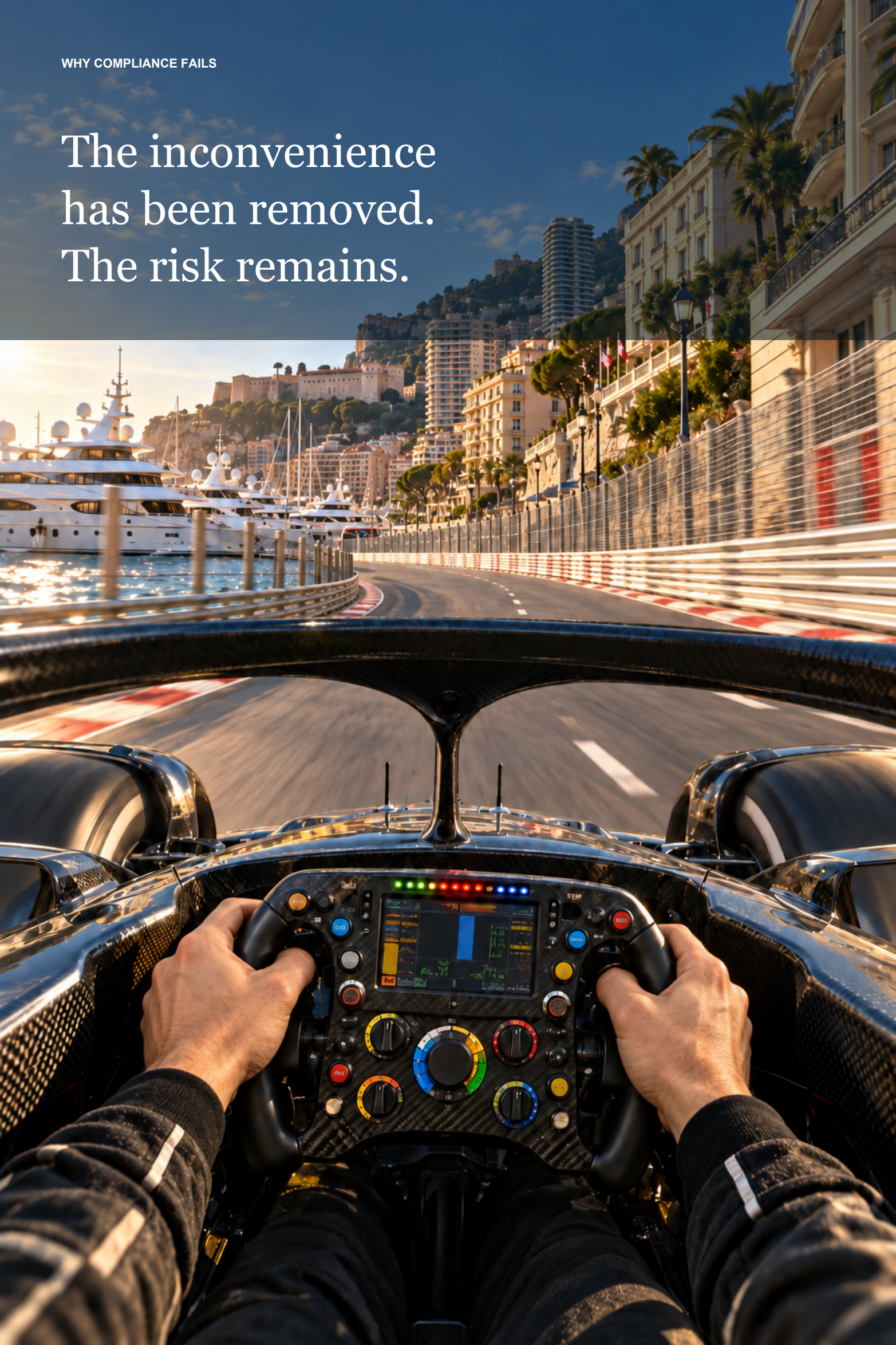
An executive brings familiar requirements from a previous employer. A manager inherits a review. An administrator receives a recurring task. Everyone recognizes the activity; fewer can explain the failure it is intended to prevent or the decisions that depend on it.

One enterprise. Three dimensions of control.



COSO Enterprise Risk Management framework (2004). Historical model, redesigned for StoneSight.

The inconvenience has been removed. The risk remains.



03 / PRESSURE AND ASSURANCE

From procedure to exposure.

The resulting weaknesses are familiar:

• Controls are copied before the organization's risks are understood.

• Ownership is assigned without establishing competence or capacity.

• Completion is accepted without evidence of meaningful scrutiny.

• Exceptions remain open after their original justification expires.

• Changes in personnel remove the explanation behind the procedure.

An access review illustrates the problem. A manager signs the report because the names look familiar. The evidence is retained. The control is recorded as complete. Nobody establishes whether those people still need the privileges they hold.

The organization has evidence of an approval. Whether it has meaningful protection depends on the judgment exercised before that approval.

The same weakness affects executive reviews, reconciliations, change authorization, and supplier oversight. A person who understands only the required action cannot reliably recognize when the action has ceased to serve its purpose.

The Friday night exception

An engineer is restoring a service late on Friday. The device works with its default credentials. Policy requires changing them, but doing so introduces additional configuration and testing. The engineer wants the service restored and the weekend to begin.

The system returns to operation. The credentials remain.

This is how an apparently minor compromise can become an enduring exposure. Monday brings another incident. The deployment is already reported as complete. The unfinished safeguard has no clear owner, deadline, or visibility.

The engineer may be conscientious and technically skilled. Those qualities do not resolve the gap between restoring functionality and completing the protection the business expects.

Experience matters here. Someone accustomed to an informal operating environment may not recognize why independent approval, controlled access, or timely evidence is essential in a different organization. A senior title or technical certification does not establish that understanding.

Management must also examine the conditions it creates. If workloads, staffing, and delivery expectations make proper execution consistently difficult, workarounds become predictable. An organization that relies on exhausted employees voluntarily returning to unfinished safeguards has designed fragility into its operations.

The answer requires controls that people understand and can execute within the demands of the job.

04 / INDEPENDENT SCRUTINY

Assurance can become detached from reality.

A review performed too late can lose the very value that justified its frequency.

A weekly examination intended to detect unauthorized activity promptly cannot provide that protection when several months of activity are reviewed just before an audit. Retrospective work may identify problems and support remediation. It cannot restore the earlier opportunity to intervene.

Organizations must distinguish testing historical performance from recreating its appearance. Auditors can examine past evidence. Control owners cannot manufacture reviews that never occurred and present them as timely execution.

Pressure to produce a clean result can obscure this distinction. Missing evidence becomes a documentation problem. A missed control becomes an administrative oversight. Repeated deferrals become accepted practice. Each description can soften the significance of what actually happened.

Internal audit must be able to challenge that account. Its credibility depends on competence, objectivity, access, and the ability to communicate uncomfortable findings. Management ownership of controls and independent examination of those controls must remain distinguishable.

External auditors may use internal audit work after evaluating its quality and the competence and objectivity of those performing it. Responsibility for the external audit opinion remains with the external auditor. Familiarity with the team cannot replace that evaluation.

For leadership, the question is whether assurance remains capable of changing a decision. If findings cannot affect priorities, funding, deadlines, or executive behavior, the organization should examine what its investment in assurance is accomplishing.

What supports the score?

ILLUSTRATIVE MATURITY PROFILE



ASSESSED

4.0

SAMPLE GOAL

4.5

Illustrative profile using custom five-point scores across NIST CSF functions. NIST CSF Tiers use a separate four-tier structure.

WHY THE CONTROLS EXIST

Failures, reforms and the assurance disciplines we inherit

—— Solid: direct response ····· Dotted: broader development

FAILURE OR PRESSURE	REFORM OR STANDARD
1929–1933 Market collapse & exposed abuses	**1933–1934** **Securities Acts & SEC** Disclosure and independent audit
1970s Corporate bribery & hidden payments	**1977** **Foreign Corrupt Practices Act** Books, records and internal accounting controls
1980s Fraudulent financial reporting	**1985 · 1987 · 1992** **COSO formed · Treadway report** COSO Internal Control Framework
1990s Reliance on outsourced processing	**1992** **AICPA SAS 70** Assurance over service organization controls
2001–2002 Enron · WorldCom Andersen's collapse	**2002** **Sarbanes-Oxley (SOX) · PCAOB** Accountability, controls and audit oversight
2008 Madoff investment fraud	**2009** **SEC custody rule amendments** Stronger safeguards for client assets
2000s–2010s Broader demand for service assurance	**2011** **SSAE 16 / SOC 1 · SOC 2** Financial reporting and trust services assurance

CYBERSECURITY & GOVERNANCE: INTERTWINED

2005
NIST SP 800-53
Security control catalog

2014
NIST CSF 1.0
Cybersecurity risk framework

2023
SEC cybersecurity disclosure rules
Form 8-K Item 1.05: material incidents
Regulation S-K Item 106: risk and governance

2024
NIST CSF 2.0
Explicit Govern function

New technology. Inherited responsibilities.

Selected milestones. Laws, regulators, frameworks and assurance standards serve different roles.

Sources: SEC · COSO · AICPA · PCAOB · NIST

05 / CYBERSECURITY AND GOVERNANCE

An intertwined responsibility.

The accompanying timeline shows how failures and changing business dependencies shaped today's expectations of control and assurance. Cybersecurity developed alongside those disciplines and is now deeply intertwined with them.

A privileged account can affect financial information. A rushed migration can weaken segregation of duties. A discontinued review can remove evidence on which another function relies. The security implications and the governance implications arise from the same operating decisions.

Technical expertise is essential, but enterprise responsibility requires a wider view. Practitioners must understand what existing controls protect, which obligations they support, and who depends on their continued operation.

The SEC's 2023 cybersecurity disclosure rules make that connection explicit. For covered domestic registrants, Form 8-K Item 1.05 generally requires disclosure within four business days after determining that a cybersecurity incident is material, subject to specified exceptions. That determination must occur without unreasonable delay after discovery.

Regulation S-K Item 106 also requires disclosures concerning cybersecurity risk management, strategy, and governance. Technical events therefore require coordinated judgment across Security, Operations, Finance, Legal, and executive leadership.

The ability to make those judgments depends on information reaching the right people promptly. A security team cannot supply reliable enterprise assurance when exceptions are hidden, escalation is discouraged, or management's understanding rests on controls that exist only in documentation.

Cybersecurity inherits responsibility for understanding this architecture as well as defending the systems within it.

2023 / SEC CYBERSECURITY DISCLOSURES

Form 8-K Item 1.05
Material cybersecurity incidents

Regulation S-K Item 106
Risk management, strategy and governance

06 / THE LEADERSHIP IMPERATIVE

Keep the protection when the business changes.

Returning to the cockpit, the engineering challenge is to make the steering wheel usable while preserving the driver's protection. The business equivalent is to adapt controls without casually surrendering their purpose.

Some controls deserve simplification. Others need automation, different ownership, better information, or additional resources. The decision should follow an examination of the exposure and the protection required.

At StoneSight, we focus on that relationship: what leadership believes is protected, what people actually do, and what evidence supports the difference. We examine whether controls fit the business, whether owners understand their responsibilities, and whether management decisions reinforce or undermine execution.

That requires continuity through leadership changes. A departing owner should leave more than a procedure: the successor needs the rationale, dependencies, outstanding exceptions, and authority to act. Leaders should expect people to explain those connections and demonstrate the work. They should also ask which controls are routinely bypassed, why the shortcuts persist, and whether reported completion reflects actual performance. These conversations expose the distance between the operating model management approved and the one employees use when nobody is watching and delivery takes precedence.

The test comes under pressure, when the system is down, the deadline is close, and proper execution is inconvenient.

Management's job is to make the controls work at the speed of the business, and to recognize when speed is being purchased by quietly removing protection.

Make the controls work at the speed of the business.

SOURCES / SELECTED REFERENCES

Evidence behind the perspective.

01 / FIA
Protective clothing guidance

02 / PCAOB
AS 2201: Internal control over financial reporting

03 / The Institute of Internal Auditors
Global Internal Audit Standards

04 / PCAOB
AS 2605: Consideration of the internal audit function

05 / SEC
2023 cybersecurity disclosure rules, Release No. 33-11216

06 / COSO
Internal control and enterprise risk management history

07 / U.S. Senate / SEC
Pecora investigation and securities reforms

08 / SEC
Foreign Corrupt Practices Act and accounting controls

09 / SEC
Sarbanes-Oxley implementation and audit oversight

10 / SEC
2009 custody rule safeguards following investment fraud

11 / GAO / AICPA
SAS 70 (1992); expanded SOC reporting (2011)

12 / NIST
SP 800-53 (2005) and Cybersecurity Framework 2.0 (2024)

PUBLICATION NOTES

Original racing and harbor illustrations depict fictional racing scenes along a developed coastline. They are editorial illustrations, not photographs of an actual event or reproductions of a real world circuit. COSO artwork depicts the historical 2004 ERM model. Timeline milestones are selective; laws, regulators, frameworks and assurance standards serve different roles.

© 2026 StoneSight Advisory Services, LLC. All rights reserved.


Move forward.
Keep the protection.
stonesightadvisory.com
STONESIGHT
ADVISORY SERVICES