MALA TECHNOLOGY ADVISORS

Independent Technology Guidance. Market Intelligence. Better Decisions.

COMPLIANCE · SOLUTION DATA SHEET

Compliance That Holds Up to Examiners, Auditors and Attackers.

Frameworks and regulators ask different questions than attackers do. MALA aligns your technology decisions to the frameworks that apply to you, from SOC 2 and ISO 27001 to HIPAA, FFIEC and NIST 800-171, and builds programs that are defensible on paper and in practice.

Risk Assessment + **Framework Alignment** + **Policies & Controls** + **Vendor Risk** + **Board Reporting**

THE CHALLENGE

Passing the audit is the start, not the finish.

Checklist compliance
Controls documented and signed off, but not effective.

Layered regulation
Industry, state and contract requirements that overlap.

Third-party risk
Vendor due diligence regulators expect but rarely see.

Changing rules
HIPAA, CMMC and AI rules moving at the same time.

OUR APPROACH

Aligned to your frameworks and your risks.

01 Assess
Run a risk assessment specific to your industry and operations.

02 Align
Map controls to SOC 2, ISO 27001, NIST CSF and sector rules.

03 Build
Develop the policies and controls you're missing.

04 Extend
Design a vendor risk program regulators expect.

05 Report
Stand up board-level reporting.

Led by former CISOs and compliance leaders who have built programs inside operating companies.

WHERE MALA HELPS

A program that's defensible, not just documented.

Risk assessment
Specific to your industry, operations and threats.

Framework alignment
SOC 2, ISO 27001, NIST CSF, NIST 800-171 and more.

Policies & controls
Written to hold up in practice, not just in audit.

Vendor risk program
Tiering, due diligence and ongoing monitoring.

Board reporting
Clear, recurring oversight for leadership.

Insurance alignment
Controls mapped to carrier expectations.

Sector expertise: HIPAA, FFIEC, GLBA, SEC/FINRA, DFARS, NIST 800-171 and FERPA.

BY THE NUMBERS

Why this matters now.

110
NIST SP 800-171 controls for defense contractors
DFARS 252.204-7012

12
security domains scored on a 0–5 maturity scale
MALA ASSESSMENT

Mid-2027
OCR's target for the final HIPAA Security Rule
HHS OCR

$0
fee to you. Paid by the vendor only if you move forward
VENDOR-SPONSORED

WHO IT'S FOR

Built for the people who own the decision.

Compliance Officer	A program mapped to the frameworks that apply.
CISO	Controls that are effective, not just documented.
Board	Recurring, defensible oversight reporting.
Regulated industries	Banking, healthcare, defense, finance and education.
Vendor managers	Third-party risk handled the way examiners expect.

THE MALA MODEL

Unbiased. Vendor-sponsored.

Our services are sponsored through strategic referral agreements with 330+ technology solutions providers, never billed to you. MALA is paid by the vendor only if you move forward with a vendor we recommend.

- **Unbiased recommendations**
  No provider pays MALA more than another qualified provider, so your requirements drive the answer.
- **Paid only if you move forward**
  The selected vendor compensates MALA, and only when you choose a recommended vendor.
- **No obligation**
  You are never required to move forward with any recommended vendor.

COMMON QUESTIONS

What clients ask first.

Q Is passing an audit the same as being secure?
No. An audit confirms requirements on a date. We also test whether controls work.

Q Do we need a dedicated compliance team?
Not necessarily. A defensible program needs a consistent inventory, tiers and review cadence.

Q Which frameworks do you cover?
SOC 2, ISO 27001, NIST CSF and sector rules like HIPAA, FFIEC, GLBA and NIST 800-171.

Q What does it cost?
Nothing. MALA is paid by the vendor only if you move forward with a recommended vendor. No obligation.

ENGAGEMENT AT A GLANCE

Frameworks	SOC 2, ISO 27001, NIST CSF and sector rules
Led by	Former CISOs and compliance leaders
Deliverable	Risk assessment, controls and board reporting
Cost to you	None. Vendor-sponsored, no obligation

RELATED Cybersecurity Data Cost Management

THE FIRST STEP

Talk to a compliance advisor. No obligation.

Bring an upcoming audit, exam or regulatory change. 30 minutes, no obligation.

Vendor-sponsored: MALA is paid by the vendor only if you move forward with a recommended vendor. No obligation to do so.

Let's simplify your next technology decision. Talk to an advisor.

Eric Anderson
eanderson@malatechadvisors.com
+1 (603) 802-2469 · malatechadvisors.com