LAUNCH GRC

SOC 2 EXECUTIVE READINESS GUIDE

A practical scorecard and 90-day action plan for leaders preparing for enterprise security requirements.

100

POINT SCORECARD

Accelerating Compliance. Enabling Trust.

HOW TO USE THIS GUIDE

Readiness is an operating decision, not a paperwork exercise.

Use this guide to align leadership on scope, ownership, evidence, and timing before audit pressure exposes avoidable gaps.

Score honestly

Rate the current state, not the intended state. A control only earns full credit when it is owned, documented, operating, and evidenced.

Prioritize blockers

Focus first on gaps that affect many controls: unclear scope, missing owners, weak access management, and inconsistent evidence.

Assign one accountable owner

Give each action a named owner and due date. Shared responsibility without accountability is a common source of delay.

Validate before audit

Run a readiness review before the examination period so teams can correct evidence and control-operation issues.

EXECUTIVE QUESTION

Can we prove our controls operated consistently, not just describe them?

100-POINT SCORECARD

Score the foundations that determine audit readiness.

Rate each category from 0 to 10. Multiply the score by the weight shown, then add the weighted results for a total out of 100.

01	Scope and system description	15%	____
02	Governance and control ownership	15%	____
03	Policies and workforce awareness	10%	____
04	Identity and access management	15%	____
05	Change and vulnerability management	10%	____
06	Vendor and third-party risk	10%	____
07	Incident response and continuity	10%	____
08	Evidence collection and monitoring	15%	____

INTERPRETING THE TOTAL

80-100 Validate evidence and close targeted gaps.

60-79 Build a focused remediation plan before selecting audit dates.

Below 60 Stabilize scope, ownership, and core controls before audit preparation.

TRUST SERVICES CRITERIA

Know what the audit is designed to evaluate.

Security is required for every SOC 2 examination. Organizations add other categories when customer commitments and system functionality make them relevant.

SECURITY	Protection against unauthorized access, disclosure, and damage to systems.
AVAILABILITY	Systems remain available for operation and use as committed or agreed.
PROCESSING INTEGRITY	System processing is complete, valid, accurate, timely, and authorized.
CONFIDENTIALITY	Information designated confidential is protected throughout its lifecycle.
PRIVACY	Personal information is collected, used, retained, disclosed, and disposed of appropriately.

SCOPE RULE

Choose categories from real commitments - not from a desire to appear comprehensive.

30 / 60 / 90 DAYS

Turn the readiness decision into an operating plan.

Sequence the work so foundational decisions happen before document production and evidence collection.

DAYS 1-30

DEFINE

- Confirm system and organizational scope
- Select relevant Trust Services Criteria
- Name executive sponsor and control owners
- Complete gap assessment and risk register

DAYS 31-60

BUILD

- Approve policies and control procedures
- Remediate priority access and security gaps
- Launch vendor and incident workflows
- Train owners on evidence expectations

DAYS 61-90

PROVE

- Collect and quality-check evidence
- Test control operation and exceptions
- Complete readiness review
- Finalize audit timing with an independent CPA firm

AVOIDABLE DELAYS

Five mistakes that make readiness harder than it needs to be.

01 Starting with policy templates

Documents cannot compensate for unclear scope, missing ownership, or controls that do not operate.

02 Choosing an audit date too early

Set dates after understanding remediation effort and the evidence period required for the report type.

03 Treating evidence as a final-week task

Evidence should be defined with the control and collected throughout the operating period.

04 Ignoring vendor dependencies

Critical service providers can affect scope, commitments, availability, confidentiality, and incident response.

05 Leaving exceptions unexplained

Document the cause, impact, corrective action, owner, and closure evidence for every exception.

LEADERSHIP CHECK

Every control needs an owner, cadence, evidence source, and escalation path.

EXECUTIVE ACTION PLAN

Leave the next meeting with five decisions.

01 Name the executive sponsor and day-to-day program owner.

02 Confirm the product, people, locations, and vendors in scope.

03 Choose the report type and target timing based on customer need.

04 Approve the top remediation priorities and required resources.

05 Schedule an independent readiness review before the audit period.

Need help turning the scorecard into a practical roadmap?

wayne@launchgrc.com / 813-551-2378