SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR REGULATED SMALL AND MIDSIZED BUSINESSES

The Continuous Compliance Playbook.

One control set for every regulation, evidence that collects itself, what auditors actually want to see and a 30 day path to audit readiness.

INSIDE THE PLAYBOOK

01 One control set
02 Evidence on autopilot
03 What auditors want
04 The 30 day path

Published by Solution Builders
Bloomington, Minnesota · www.solutionbuilders.com

30+	Top 1%	98%
YEARS	OF MSPS	CSAT

WHAT'S INSIDE

Compliance without the fire drill.

Most compliance programs run on adrenaline. An audit date lands, a spreadsheet appears and three people lose a month hunting for screenshots. It does not have to work that way. This playbook shows how to build one calm program that answers every regulator, customer and insurer, all year long.

01 **Map many regulations to one control set.**
HIPAA, PCI DSS, SOC 2, CMMC, state privacy laws and your insurer all ask for the same twenty things in different words. Map them once.
PAGE 03

02 **Automate evidence so it collects itself.**
Screenshots taken in April prove what was true in April. How to wire identity, device, scanner, backup and ticket data into evidence that is always current.
PAGE 06

03 **What auditors actually want to see.**
Scope, policies that match reality, evidence with dates, documented exceptions and proof of monitoring. The five things every auditor grades, and how to answer the questions they ask.
PAGE 09

04 **A 30 day path to audit readiness.**
Four one week sprints: scope and inventory, policies and controls, evidence and automation, then a rehearsal. Finish with a scorecard you can show your leadership team.
PAGE 12

WHO IT IS FOR
Owners, COOs, CFOs and IT leaders at companies with 25 to 500 people who answer to HIPAA, PCI DSS, SOC 2, CMMC or a state privacy law.

HOW TO USE IT
Start with chapter 01 to build your control map. Chapters 02 and 03 make it run. Chapter 04 is the 30 day plan.

READING TIME
About 25 minutes cover to cover. The framework map in chapter 01 and the 30 day plan in chapter 04 are built to print.

01

Map many regulations to one control set.

Every regulation you face was written by a different committee, and every one of them wants the same basics: know your assets, control access, watch for trouble, protect data and prove it. Build the controls once, map each rulebook to them, and audit season becomes a report instead of a project.

5
rulebooks the average regulated SMB answers to, usually with the same five people

18
controls in CIS Controls v8. Build them once and every framework maps onto them

6
functions in NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, Recover

2.7x
the cost of noncompliance compared with the cost of staying compliant

Five rulebooks. One set of controls underneath.

Lay the frameworks side by side and the pattern jumps out. Each one asks who can get in, whether devices are patched, whether anyone watches the logs, how data is protected and whether you can prove it.

Six control families, five frameworks, one map

CONTROL FAMILY	HIPAA	PCI DSS V4	SOC 2	CMMC LEVEL 2	STATE PRIVACY
Identity and access	§164.312(a), (d)	Req 7, 8	CC6.1 to CC6.3	AC, IA	Reasonable security
Devices and vulnerabilities	§164.308(a)(5), §164.310(d)	Req 2, 5, 6, 11	CC7.1, CC8.1	CM, SI, RA	Reasonable security
Logging and monitoring	§164.312(b)	Req 10	CC7.2, CC7.3	AU, SI	Breach detection duties
Data protection and backup	§164.312(c), (e); §164.308(a)(7)	Req 3, 4	CC6.7, A1.2	SC, MP	Minimization, encryption safe harbor
Governance, risk and training	§164.308(a)(1), (a)(5)	Req 12	CC1 to CC5	AT, RA, CA, PS	Data protection assessments
Incident response and vendors	§164.308(a)(6), (b)	Req 12.8, 12.10	CC7.4, CC9.2	IR, DFARS flow down	Processor contracts, breach notice

Primary anchors, not an exhaustive crosswalk. CMMC Level 2 families follow NIST SP 800-171.

How to use the map

- **Pick the backbone first.** CIS Controls v8 or NIST CSF 2.0 is the one list you run. The frameworks above become views of it.
- **Write each control once.** One policy, one owner, one evidence source, tagged with every framework reference it satisfies.
- **Treat outliers as exceptions.** FIPS validated encryption for CMMC, approved vendor scans for PCI DSS. Bolt them on, do not rebuild.

Why one control set wins

When a new customer questionnaire or a new state law arrives, you do not start over. You map twenty new questions to controls you already run, point to evidence you already collect and answer in an afternoon.

Pick one framework to be the source of truth.

A backbone is the control list you actually operate, review and report on. Everything else, HIPAA sections, PCI requirements, SOC 2 criteria, insurance questionnaires, becomes a mapping on top of it. Two backbones fit almost every company with 25 to 500 people.

Build the common control set in five moves

01 **Inventory your obligations**

List every law, contract clause, customer questionnaire and insurance requirement that touches you. Most companies find five to eight.

02 **Choose the backbone**

CIS Controls v8 if you want prescriptive, prioritized safeguards. NIST CSF 2.0 if your board wants an outcome based story. Pick one.

03 **Map each requirement once**

Walk every obligation and tag the backbone control that satisfies it. Gaps become your remediation list. Overlaps disappear.

04 **Name an owner and an evidence source**

Every control gets a person and a system that proves it works: identity logs, device reports, scanner output, backup reports, tickets.

05 **Retire the duplicates**

Three access policies become one. Four risk assessments become one annual cycle. Fewer documents, less drift.

Choosing your backbone

	CIS CONTROLS V8	NIST CSF 2.0
Style	Prescriptive: 18 controls, 153 safeguards	Outcome based: 6 functions, 106 subcategories
Start small	Implementation Group 1, 56 safeguards of essential hygiene	A current profile, a target profile and the gap between them
Best when	IT wants a to do list it can finish	Leadership wants a maturity story it can follow
Maps to	HIPAA, PCI DSS, SOC 2 and NIST SP 800-171 through published CIS mappings	Everything, including CIS and 800-171, through NIST reference mappings

Do not build your own framework

Homegrown control lists feel flexible and age badly. Auditors know CIS and NIST, your insurer knows them, your next hire knows them. Borrow the structure and spend your energy on running it.

Sources: NIST Cybersecurity Framework 2.0 (2024); CIS Critical Security Controls v8.1 (2024); Ponemon Institute and Globalscape, The True Cost of Compliance with Data Protection Regulations (2017); HHS HIPAA Security Rule, 45 CFR 164; PCI DSS v4.0.1 (2024); AICPA Trust Services Criteria; CMMC Program Rule, 32 CFR Part 170 (2024).

02

Automate evidence so it collects itself.

Audit prep is miserable for one reason: evidence is gathered by hand, after the fact, by people who have other jobs. The systems you already run know the answers. Connect them, define what passing looks like and the evidence becomes a report you open instead of a project you dread.

$2.22M
lower average breach cost for organizations using security automation extensively

12
months in a typical SOC 2 Type II window. Evidence has to exist for every one of them

110
practices in CMMC Level 2, each needing proof that it works, not a promise that it will

5
systems that supply most of the evidence: identity, device management, scanner, backup, ticketing

The systems you already run hold the proof.

An auditor does not want your word. They want a timestamped export from the system that enforces the control. Here is where that export comes from for the six controls that show up in every framework, and what it has to contain. One export per control per month proves it operated all year.

Control, evidence, source

CONTROL	EVIDENCE THAT PROVES IT	SOURCE SYSTEM
MFA enforced for everyone	Conditional access policy export plus sign in logs showing MFA challenges	Entra ID or Okta
Devices patched and encrypted	Compliance report per device: OS version, encryption state, last check in	Intune or your RMM
Vulnerabilities fixed on time	Monthly scan with open, closed and overdue counts and closure dates	Vulnerability scanner
Backups run and restore	Job success history and a dated restore test log with times recorded	Backup platform
Access reviewed quarterly	Review tickets with approver, date and the accounts removed	Ticketing or identity governance
People trained	Completion report by user with dates and phishing simulation results	Awareness platform

Where audit prep time goes



Hunting for evidence	45%
Rewriting policies	20%
Status meetings	15%
Fixing gaps found late	12%
Time with the auditor	8%

Illustrative split of hours in a manually run program, from Solution Builders client engagements.

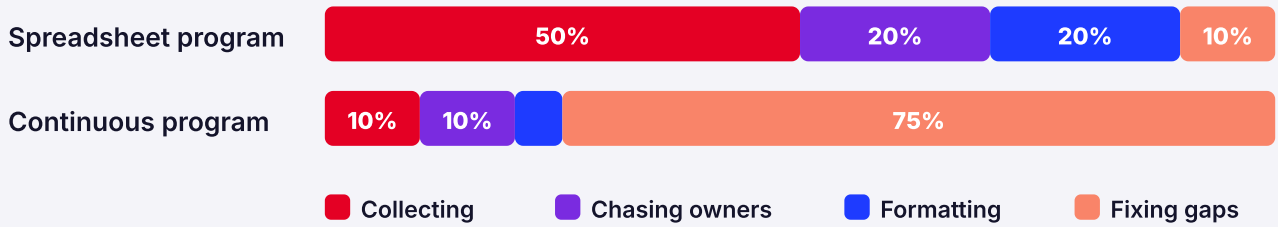
Screenshots are the enemy

A screenshot proves what one screen showed on one day. Exports, logs and system reports prove the control ran continuously. Prefer anything with a timestamp and a record count.

What changes when the evidence flows all year.

Automation does not remove the work. It moves the work from collecting and formatting to reviewing and fixing, which is the part that makes you safer. The shift below is what we see when a program goes from spreadsheet to continuous.

How compliance hours get spent, per audit cycle



Illustrative share of hours. Total hours also fall, usually by more than half, once exports replace hand collection.

Turn it on in four steps

1. **Connect the five systems**
   Identity, device management, vulnerability scanner, backup and ticketing feed a compliance platform or a shared evidence library.

2. **Define what passing means**
   Every control gets a test with a number: MFA coverage 100%, patch age under 14 days, restore tested within 90 days. Pass or fail, no judgment calls.

3. **Route failures to tickets**
   A failed test opens a ticket with an owner and a due date. Compliance work becomes normal IT work.

4. **Review exceptions monthly**
   Thirty minutes, one list. Approve, extend or fix. Anything older than 90 days gets escalated.

14
days of maximum patch age in a typical passing test for critical updates

90
days is the longest a documented exception should live before someone senior signs it again

A platform helps. The discipline matters more.

Compliance automation platforms earn their keep once you face two or more frameworks. But a shared library, five scheduled exports and a monthly review deliver most of the benefit for a fraction of the effort.

Sources: IBM Cost of a Data Breach Report 2024 (savings from extensive security AI and automation); AICPA guidance on SOC 2 Type II examination periods; CMMC Model 2.0, Level 2 (110 practices). Hours split is illustrative, from Solution Builders client engagements.

SOLUTION BUILDERS®

03

What auditors actually want to see.

Auditors are not trying to catch you. They are trying to form an opinion they can sign their name to, in the hours they have. Make that easy and the audit gets shorter and friendlier. Make it hard and every answer earns a follow up question.

5
Trust Services Criteria in SOC 2. Only Security is required, the other four are your choice

12
requirements in PCI DSS v4, every one of them fully in force since March 2025

700+
large healthcare data breaches reported to HHS in 2023, a record year

15%
of breaches involved a third party, which is why vendor questions are on every audit

Auditors grade five things. Fire drills deliver one.

Every audit, whatever the framework, comes down to the same five questions. Companies in fire drill mode usually answer only the third one, with a folder of screenshots. Always ready companies answer all five from systems they run anyway, and the auditor samples dates you did not pick.

01 **Scope**

What systems, people, locations and data are in the audit, and what is deliberately out. A tight, defensible scope is the single biggest time saver.

02 **Policies that match reality**

Written rules that describe what you actually do. Auditors test the gap between the document and the practice. A short, true policy beats a long borrowed one.

03 **Evidence with dates**

System generated proof that each control operated across the whole period, not on the day you remembered to check.

04 **Exceptions, documented**

A legacy server without MFA is a finding. The same server with a risk acceptance, a compensating control and an expiry date is a managed exception.

05 **Proof of monitoring**

Evidence that someone looks: alert reviews, monthly exception meetings, ticket trails. This is what separates a program from a project.

What they are really asking

Underneath every question is one: if something went wrong, would you have known, and would you have acted? Answer that with evidence and most of the follow up questions never arrive.

Before the kickoff call

- **Send the scope first.** A one page system list with the boundary drawn saves the first two hours.
- **Name one point of contact.** Requests go to one person who routes them. Auditors notice chaos.
- **Share the exception register early.** Known gaps presented by you are managed risks. Found by them, they are findings.

> **The best audit evidence is the evidence you would collect even if no auditor existed.**
>
> SOLUTION BUILDERS COMPLIANCE PRACTICE

Six questions every auditor asks, and what to show.

The question is rarely the point. The auditor is listening for whether the answer comes from a system or from memory. Here are the six that appear in nearly every HIPAA, PCI DSS, SOC 2 and CMMC engagement, with the answer that ends the conversation.

AUDITOR ASKS	FIRE DRILL ANSWER	ALWAYS READY ANSWER	HAND OVER
Who has admin rights?	**"Let me pull a list."**	**Quarterly access review, last run six weeks ago.**	Review ticket and current admin export
How do you know devices are patched?	**"Auto update is on."**	**97% within 14 days. Three exceptions, all ticketed.**	Device compliance report, exception tickets
Where is your last risk assessment?	**"It is from 2022, mostly still valid."**	**Annual cycle, refreshed in Q1, register with owners.**	Risk register and sign off
What happened in your last incident?	**"Nothing major has happened."**	**Two phishing events, contained in minutes, lessons logged.**	Incident log and post incident notes
Which vendors touch our data?	**"IT keeps a list somewhere."**	**Vendor register with data classes and annual reviews.**	Vendor register, signed agreements
Can you restore from backup?	**"Backups run nightly."**	**Quarterly restore drill. Last one took 3 hours 40 minutes.**	Restore test log with times

AUDIT SEASON

The fire drill

- Evidence gathered in a three week scramble before the auditor arrives.
- Policies rewritten the night before to match what is actually happening.
- Findings are surprises, discovered by the auditor.
- Everyone involved quietly dreads next year.

ALWAYS READY

Continuous compliance

- Evidence exports on a schedule. Audit prep is opening a folder.
- Policies reviewed annually and short enough that people follow them.
- Findings are known exceptions with owners and expiry dates.
- The audit is a two day conversation instead of a quarter long project.

Sources: AICPA Trust Services Criteria (2017, revised 2022); PCI Security Standards Council, PCI DSS v4.0.1 (2024); HHS Office for Civil Rights breach portal, 2023 reports of 500 or more records; Verizon 2024 Data Breach Investigations Report (third party involvement).

SOLUTION BUILDERS®

04

A 30 day path to audit readiness.

Thirty days will not make you perfect. It will make you ready: a defined scope, a control map, evidence that flows and a rehearsal that found the gaps before the auditor did. Here is the plan, week by week, with room for an owner next to every item.

4
one week sprints: scope, controls, evidence, rehearsal

220K
defense contractors and subcontractors that CMMC is expected to reach

2025
the year Minnesota's own consumer privacy law took effect, on July 31

24
items on the checklist. Score yourself on page 14

Define the scope, then build the control map.

The first two weeks are about decisions, not tools. You decide what is in scope, which backbone you run and who owns each control. Most of this is meetings and documents, which is exactly why it never gets done without a deadline.

WEEK 1

Scope and inventory

Obligations listed, systems and data inventoried, scope boundary drawn

WEEK 2

Policies and controls

Backbone chosen, control map built, owners named, policies trimmed

WEEK 3

Evidence and automation

Exports scheduled, tests defined, failures routed to tickets

WEEK 4

Rehearsal and governance

Mock audit run, exception register live, monthly review booked

5 to 8

obligations most companies discover in week one, including ones nobody owned

1

owner per control. A name, not a department

30 min

monthly review that keeps the program alive after day 30

Week 1: Scope and inventory

- List every obligation: laws, customer contracts, insurance requirements, card brand rules. Note the next audit or renewal date for each.
- Inventory systems, data stores and SaaS apps. Flag where regulated data (PHI, card data, CUI, personal data) actually lives.
- Draw the scope boundary. Separate the systems that touch regulated data from the ones that do not.
- Name an executive sponsor and a program owner. Compliance without a sponsor loses every scheduling fight.
- Pull the last audit report or questionnaire. Every open finding goes on the list.
- Check your cyber insurance application against reality. Anything you attested to is now a control.

Week 2: Policies and controls

- Pick the backbone: CIS Controls v8 or NIST CSF 2.0. Write the decision down with the reason.
- Map each obligation to backbone controls. Mark gaps red, partials amber, covered green.
- Assign one owner per control. One name, not a department.
- Collapse duplicate policies into one set. Aim for a policy a new hire would actually read.
- Define the exception process: who approves, which compensating control, when it expires.
- Book the monthly compliance review for the next 12 months. Thirty minutes, standing agenda.

Then make the evidence flow, and rehearse.

Weeks three and four turn the map into a running program. Evidence starts arriving on a schedule, and a mock audit finds the gaps while they are still cheap. Count your completed items across all four weeks and score yourself.

Week 3: Evidence and automation

- [ ] Schedule exports from identity, device management, scanner, backup and ticketing into one evidence library.
- [ ] Write a pass or fail test for each control, with a number: MFA coverage, patch age, scan closure, restore date.
- [ ] Route every failed test to a ticket with an owner and a due date.
- [ ] Run the first full evidence cycle. Anything collected by hand goes on the automation backlog.
- [ ] Start the exception register. Every known gap gets a risk owner, a compensating control and an expiry date.
- [ ] Turn on retention: keep evidence for the audit period plus one year.

Week 4: Rehearsal and governance

- [ ] Run a half day mock audit. Someone outside the team asks the six questions from chapter 03.
- [ ] Fix the quick wins. Anything under four hours of work gets done this week.
- [ ] Brief leadership: scope, control map, evidence status, open exceptions and the plan for the rest.
- [ ] Update the vendor register and chase the missing agreements.
- [ ] Freeze the control map and policies as version 1.0. Change control applies from here.
- [ ] Put next quarter's restore test, access review and phishing simulation on the calendar.

_____ / 24

Score yourself

Count the items you have fully completed across all four weeks and write the number here.

What your score means

ITEMS DONE	WHERE YOU STAND
0 to 8	Fire drill territory. An audit today would be a scramble and a surprise.
9 to 16	Getting there. You know your gaps, but evidence still depends on people remembering.
17 to 24	Audit ready. Keep the monthly review and let the evidence speak for you.

Keep it running

Readiness decays. A monthly 30 minute review of failed tests and open exceptions is what keeps day 31 from turning back into day 0.

Sources: CMMC Program Rule, 32 CFR Part 170 (effective December 2024) and the DoD estimate of about 220,000 affected companies; Minnesota Consumer Data Privacy Act (effective July 31, 2025); CIS Controls v8.1 Implementation Groups; NIST CSF 2.0 Quick Start Guides.

Compliance that is continuous, not seasonal.

Solution Builders has supported regulated Minnesota businesses since 1995. Our compliance practice maps your obligations to one control set, automates the evidence and runs the monthly review, backed by 50+ engineers and a SOC 2 Type II audit of our own.

R

Resilient

Tested backups and recovery plans that satisfy HIPAA contingency and SOC 2 availability criteria.

I

Integrated

Identity, device management and ticketing wired together so evidence flows on its own.

S

Secure

Managed security, 24/7 monitoring and compliance support for HIPAA, PCI DSS, SOC 2 and CMMC.

E

Evolving

AI adoption with data governance built in, so new tools never break your compliance story.

01

Compliance Readiness Snapshot

A 30 minute conversation. You leave knowing your obligations, your biggest gap and what to do first.

FREE · 30 MINUTES

02

Compliance Gap Assessment

Three weeks: scope, control map against your frameworks, evidence inventory and a prioritized 90 day plan.

FIXED FEE · 3 WEEKS

03

Managed Compliance Program

The control set, evidence automation, monthly reviews and audit support, run for you all year.

MONTHLY · ONGOING

Find out how ready you are in 30 minutes.

Book a free Compliance Readiness Snapshot with a Solution Builders solution architect. No pitch, just a clear read on where you stand and what to fix first.

Book my readiness snapshot

THE SHORT VERSION

Three things to remember.

If this playbook disappears into a drawer, keep these three ideas. They are the difference between companies that survive audits and companies that stop dreading them.

01 **One control set answers every rulebook.**

HIPAA, PCI DSS, SOC 2, CMMC and state privacy laws overlap almost entirely. Build the controls once and map each framework to them.

02 **Evidence should come from systems, not people.**

Scheduled exports from identity, devices, scanners, backups and tickets prove controls ran all year. Screenshots prove one afternoon.

03 **Readiness is a monthly habit.**

Thirty days gets you ready. Thirty minutes a month reviewing failed tests and open exceptions keeps you there.

SOLUTION BUILDERS®

START THE CONVERSATION

www.solutionbuilders.com

(952) 854-8188 · 1550 American Blvd East, Suite 900, Bloomington, MN 55425
Your technology partner since 1995

Book a free assessment

© 2026 Solution Builders, Inc. All rights reserved. Product names and marks are the property of their respective owners. Figures marked illustrative are planning estimates, not guarantees.