Your NAID AAA cybersecurity requirements, handled before your next audit.

One question sets your scope. Then you choose how much of the writing you do yourself.

i-SIGMA added cybersecurity requirements to NAID AAA certification effective October 1, 2026, and your first audit after that date is where they get enforced. What you have to do comes down to one question, so start there and read only the path that applies to you.

START HERE

Do you hold an overwriting or degaussing endorsement?

Your answer decides everything below. Read one path, not both.

IF NO

Path A. Cybersecurity policy work only.

You need the cybersecurity policy set under 1.29 and the server and network access controls under 2.1.

IF YES

Path B.

- Cybersecurity policy work
- Server and network access controls
- 7.4 Workstation Access Control procedures
- 7.5 Identity Access Management procedures
- An annual Security Risk Analysis under 3.2

PATH A · NO OVERWRITING OR DEGAUSSING ENDORSEMENT

SELF-SERVE

The Toolkit.

You write the documents from our template set.

You get templates for acceptable use, password management, incident response and physical access control for your servers and network equipment, plus a tailoring guide, a checklist of every specification point, and the acknowledgment form. You write the parts that describe your own operation.

$750

one time · Word files, one site, no updates, no support

DONE FOR YOU — RECOMMENDED

The Module.

We write them for you and map each one to the specification the auditor inspects.

The toolkit policies and procedures, the annual signed-agreement language and the training amendments, all written to your operation. We write the set for one site and you may adapt it for your other locations.

$2,950

one time · policy work, one site

PATH B · OVERWRITING OR DEGAUSSING ENDORSEMENT HOLDERS

Part one. The documents. Choose one.

SELF-SERVE

The Toolkit, upgraded.

Everything above plus template language for the 7.4 workstation access control procedure, the 7.5 identity access management methodology and the training acknowledgment. You write the sections describing your own environment.

$1,250

one time · Word files, one site, no updates

DONE FOR YOU

RECOMMENDED

The Module, plus endorsement scope.

The Module as described above, plus:

- An intake call with your IT owner
- The 7.4 Workstation Access Control procedures drafted to the physical, logical and administrative controls you run
- The 7.5 Identity Access Management procedures drafted to the methodology you run

$4,950

one time · policy work plus endorsement work

Part two.

The Security Risk Analysis.

Required annually under 3.2.

$5,995

per year · one NAID certified facility

Beacon Ascent verifies six controls every year: least privilege, multi-factor authentication, antivirus, firewall, endpoint detection and patch management. It closes with documented evidence of an acceptable security review by a competent third-party security expert, as 3.2 requires.

- **3.2 requires a competent third party, on the record.** For twelve months after the report, we answer your i-SIGMA auditor's questions about it at no charge.
- **It runs in parallel with Part one.** The analysis looks at what is running on your network, not at what the documents say, so it does not wait on the policy work.

Already have a current analysis covering the six controls, reviewed and accepted by a competent third-party security expert? Bring it to your audit. You do not need this.

One analysis covers every network operating at the certified facility, physical or virtual. Where more than one certified location runs on the same network, a single report can cover them all, with each location named and each LAN included.

If your ISO 27001 certificate covers the environment in scope, much of the evidence may already exist and the price may drop to $3,995 per year.

ABOUT BEACON ASCENT

Beacon Ascent focuses on information security and AI management systems. It shares common ownership with Greeneye Partners and keeps a separate scope. Neither firm reviews the other's work, and that separation is what lets Beacon Ascent act as the independent third party under 3.2.

Beacon Ascent performs the annual comprehensive Security Risk Analysis required under 3.2.

beaconascent.com

WHICH PATH IS RIGHT FOR YOU

CHOOSE THE TOOLKIT IF

You have an in-house IT owner with real time to spend, you are comfortable writing the sections that describe your own environment.

No customization, no specification mapping and no support. Budget your IT manager's hours alongside the $750 or $1,250 before you decide.

CHOOSE THE MODULE IF

You would rather buy the finished result than the template set, and you want the documents to match the way your operation runs.

You get documents written to your operation, a crosswalk the auditor can follow, and our name on the work. If you hold an endorsement this is where the difference matters most, because 7.4 is inspected against what is installed.

What the Module buys

ONE

Documents written to your operation.

Your facility layout, your access process, your training material and your acknowledgment form, drafted for the way you run, not blanks for you to fill in.

TWO

A crosswalk the auditor can follow.

Every document mapped to the specification it satisfies, so the auditor confirms compliance in minutes instead of hunting through a binder. That hunt is where findings come from even when the work was done.

Next step

Two minutes on the intake form tells us your endorsement status and the path you want. We confirm your scope, tell you which parts apply, and send the quote.

EVERYONE STARTS HERE

The intake form

Pick your path and we quote it. About two minutes.

Start the intake form →

ONLY NEED A SECURITY RISK ANALYSIS?

The SRA Readiness Check

Five minutes. Your IT owner or managed provider will have most of the answers.

Start the Readiness Check →

Questions before you start? Call either of us.

GREENEYE PARTNERS · POLICY WORK

Nicole Delich · nicole@greeneyepartners.com
(952) 457-4018

BEACON ASCENT · SECURITY RISK ANALYSIS

Tom Delich · tdelich@beaconascent.com
(952) 381-5898