

the FOUNDATION FOR
INFRASTRUCTURE RESILIENCE

The Certification Path

An Introduction

Foundation for Infrastructure Resilience

November 2026

Foundation for Infrastructure Resilience, Inc. ("FIR"™), a non-profit 501(c) (3) Delaware Corporation.

Our Vision

A secure and prosperous future where resilient and sustainable critical infrastructure empowers communities and safeguards our nation.

Our Mission

Improve the quality of life and help ensure the continuity of the United States by facilitating sustainable communities and resilient critical infrastructures, fortified against threats and meeting the needs of the 21st century.

Legal Disclaimer: The Foundation for Infrastructure Resilience makes no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the content of this document, third party content or references to services or information referenced or available through links herein, and further disclaims all warranties regarding any information contained herein, including any implied or express warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, arising out of any course of dealing or usage of trade, that the third-party service will be uninterrupted, error free or free of harmful components.

© 2026 Foundation for Infrastructure Resilience
All Rights Reserved

Contents

FIR Book 4: The Certification Path — An Introduction 1
About this book set, and who it is for 1
About this book 2
How this book is organized 2
Chapter 1 — What certification is, and what it refuses to claim 3
Trust but Verify 3
Conformance, not outcomes 3
Why a credential, and not just a report 3
Chapter 2 — The credentials and the path to them 4
Three tracks 4
The four credentials 4
The course path 4
The courses, by level 4
What each credential requires 5
Chapter 3 — The evidence standard 7
The evidence hierarchy 7
Verified, attested, asserted 7
Chain of custody 7
Chapter 4 — Certifying Diamond Blue 7
The certifier's posture 7
Diamond-N and the declared scope 8
What the signature means 8
Chapter 5 — The independent check 9
The Certification Panel 9
Why this matters 9
Chapter 6 — Proving it works, through exercises 10
What makes a FIR exercise different 10
Exercising what cannot be built in a drill 10
Evidence that counts outside FIR 10
Chapter 7 — Keeping it true: recertification and the registry 11
Recertification 11
The registry and the providers 11
Appendices 12
Take the next step 12

FIR Book 4: The Certification Path — An Introduction

How a community's readiness is proven, verified, and credentialed — and the people qualified to sign it.

Foundation for Infrastructure Resilience — Book 4 of the FIR introductory set. Draft of November 3, 2026.

About this book set, and who it is for

The FIR introductory set is written for people who are new to all of this. It assumes no background in emergency management, infrastructure, the military, or finance — only an interest in why a long loss of the electric grid would be so dangerous, and what can be done about it. Each term is introduced in plain words the first time it matters, and the companion *FIR Field Handbook* holds the full glossary for anything you want to look up again.

These five short books are introductions, not the full course. Each one gives a clear overview of its part of the FIR method — enough to understand it, plan with it, and know where the detail lives — but it is not a substitute for the FIR courses, which remain the version of record for instruction. A later, more detailed textbook set will carry the complete student-guide content; these introductions are the on-ramp to it. The four Foundation courses (BSE 099–102) and the free member orientation (FIR 001) cost nothing to start — browse every course and enroll at the FIR course catalog.

The set is built to be read in order:

- **Book 1, Foundations** — the problem: what a Black Sky Event is, how a community is built, who and what threatens it, and what a household can do. Everyone starts here.
- **Book 2, The Assessment Method** — how a trained assessor measures a community's readiness and turns it into a plan that can be funded.
- **Book 3, The Resilient Community** — what a community that has done the work looks like in a prolonged event: how it governs, feeds, protects, and sustains itself.
- **Book 4, The Certification Path** — how that readiness is independently verified and credentialed: the evidence standard, the Diamond Blue certification, and the people qualified to sign it.
- **Book 5, The Domains** — how each kind of infrastructure is actually hardened, sector by sector.

This is Book 4, and it is the most specialized volume so far. It is written for the reader heading toward FIR's credentials — the assessor, the certifier, the training provider — and for the official who needs to know exactly what a FIR certification does and does not promise. It assumes Books 1 and 2. Read those first.

About this book

Book 2 showed how an assessor measures a community and produces a scored claim. This book is about the step that makes such a claim worth anything to an outsider: certification. A certification is a promise, made by a credentialed professional and checked by an independent panel, that a community has actually met a standard — proven, not asserted. This book explains what FIR certifies, how it proves it, who is allowed to sign it, and how it is kept honest over time.

One idea governs everything here, and it is worth stating before the details: FIR certifies conformance, not outcomes. It certifies that an entity has met a standard's requirements. It never certifies that a community will survive a Black Sky Event, because no one can promise that. Everything in this book is built to keep that line clean — to make a FIR certification a claim an official can rely on precisely because it never claims more than it can prove.

How this book is organized

Chapter 1 — what certification is, and what it refuses to claim. Chapter 2 — the credentials and the path to them. Chapter 3 — the evidence standard. Chapter 4 — certifying Diamond Blue. Chapter 5 — the independent check. Chapter 6 — proving it works, through exercises. Chapter 7 — keeping it true: recertification and the registry.

Chapter 1 — What certification is, and what it refuses to claim

A readiness claim is only as good as the trust behind it. Anyone can say they are ready. A certification is the mechanism that lets someone who was not there — a state official, a funder, a neighboring community — believe it.

Trust but Verify

FIR's certification doctrine has a name: Trust but Verify. No claim is credited on trust alone. Each is verified to the strength the evidence requires before it is counted. The doctrine is not suspicion for its own sake; it is what makes a certification portable. When a FIR certification says a community has reached a level, it means an assessor examined the proof and an independent panel agreed — not that someone filled out a form.

Conformance, not outcomes

The single most important limit, repeated from the introduction because it is the thing most often gotten wrong: FIR certifies conformance to a standard, never an outcome. It certifies that a community has, for example, hardened its cyber vector to a defined level with evidence to prove it. It does not certify that the community will come through an actual event, because the real world holds too many unknowns for any honest body to promise that. An official reading a FIR certification should understand it as "this was proven to this standard," not "this community is guaranteed to be fine."

Why a credential, and not just a report

Book 2's assessment produces a report. A certification adds two things a report lacks: a credentialed professional whose training and standing stand behind the claim, and an independent review that the claim holds. Those two additions are the difference between an opinion and a certification, and they are the subject of the next several chapters.

Chapter 2 — The credentials and the path to them

FIR's training is organized so that a person climbs from understanding the problem to being qualified to certify a community against it. The climb runs along three tracks and four credentials.

Three tracks

The tracks sort learners by what they will actually do. Track A, Leadership, is for the people who authorize and fund resilience work — elected officials, executives, community leaders. Track B, Operational, is for the people who run a particular domain, such as energy or communications. Track C, Practitioner, is for the people who assess and certify communities. A person follows the track that matches their role, and the tracks share a common foundation.

The four credentials

Four credentials mark the path. The CRL — Community Resilience Leader — is the Track A credential, earned through the free Foundation, the companion course FIR 002, the Common Paid Core, the six governance courses, and an exam. The CRC — Community Resilience Coordinator — is the Track B credential, and it is the gateway to the two practitioner credentials above it. The CIRP — Certified Infrastructure Resilience Planner — is the Track C methodology credential, and it adds a supervised practicum, because the method has to be demonstrated under watch, not just studied. The CBRA — Certified BSE Readiness Assessor — is the summit credential, and it carries the one authority that matters most in this book: the signature on a Diamond Blue certification.

The course path

The courses stack in order. The free Foundation — BSE 099, 101, 102, then 100, about 24 hours, each final exam passed before the next course opens — is where everyone begins. The Common Paid Core (BSE 104 and three governance courses) opens CRC eligibility. A domain course matches the function a person runs. And the Diamond tier — BSE 305, 306, 307, and 308 — is the CBRA path, where a practitioner learns to certify Diamond Blue, to exercise a community, and to teach the method. Training providers themselves are credentialed through BSE 307 as FIR Authorized Training Providers, and every credential holder, provider, and instructor appears on the public FIR Practitioner Registry, so that anyone can check who is qualified.

The courses, by level

Steve's note here was to lay out the courses and what each credential needs. The authoritative, current catalog — with prices, prerequisites, and enrollment — lives at the FIR course catalog online; the summary here is the map, not the fine print.

The free Foundation is four short courses taken in order: BSE 099 (Why This Matters — Orientation), BSE 101 (Individual Readiness), BSE 102 (Household Readiness, Tier 0H), and BSE

100 (Source Discipline & Methodology). FIR 001 (Member Orientation) and the free companion courses FIR 002 (Making the Case) and FIR 003 (Find Your Path) sit alongside them.

The Common Paid Core is the shared "survive for months" body that everyone past the awareness level takes, and the gateway to the CRC: BSE 104 (Food Systems and Agricultural Resilience), GOV 106 (Why Consolidation), GOV 107 (Community Readiness and Governance), and GOV 108 (the Consolidation Framework and the Diamond-N practicum).

The governance courses carry the Book 3 material in depth: GOV 110 (Resilience for Decision-Makers), GOV 111 (Back to Work — re-employment and the guild transition), GOV 112 (Contracting for Contingency), GOV 113 (Local Scrip, Barter and the Credit-Ledger Economy), GOV 114 (Legal Protections for Emergency Responders), and GOV 210 (Rule of Law Under Stress).

The domain courses match the function a person runs, grouped by area: energy and utility (BSE 103, OT/SCADA Security Fundamentals, and BSE 105, Shadow Grid & Energy Independence); communications (BSE 111, Community Communications, ARES/HF); logistics (BSE 112, Stockpile & Supply Chain); critical-infrastructure research (BSE 106, Community Critical Infrastructure Research, and BSE 110, Shadow Infrastructure Survey & Community Carrying Capacity); and health and medical (BSE 113, Post-BSE Community Health & the Disease Environment, and BSE 114, Post-BSE Veterinary & Animal Health).

The assessor methodology is the Book 2 material as a course sequence: BSE 201 (the FIR Resilience Framework), BSE 202 (Compliance Standards — the ten dimensions and the rubric), BSE 203 (Roadmap Development), BSE 205 (Threat Posture & Kill Chains), BSE 206 (Advanced OSINT for Critical Infrastructure Assessment), BSE 204 (Military Mutual Aid & DSCA), and BSE 207 (Funding Architecture & Self-Funding Strategy), with the tool-orientation course BSE 109.

The Diamond tier is the CBRA path: BSE 305 (Diamond Blue Certification), BSE 306 (Community Economic Framework and Tier 0S Delivery Architecture), BSE 307 (the instructor and training-provider course), and BSE 308 (Exercise Design and Recertification Architecture).

What each credential requires

Each credential is earned by completing a defined set of these courses, with a proctored exam and, for the practitioner credentials, supervised work. In summary:

- **CRL (Community Resilience Leader)** — the Leadership-track credential: the free Foundation, FIR 002, the Common Paid Core, all six governance electives (GOV 110, 111, 112, 113, 114, and 210), and the CRL exam.
- **CRC (Community Resilience Coordinator)** — the Operational-track credential and the gateway to the practitioner credentials: the Foundation, the Common Paid Core, up to four domain courses of the candidate's choice, the Fundamentals Evidence packet, and the CRC exam.

- **CIRP (Certified Infrastructure Resilience Planner)** — the Practitioner methodology credential: the CRC first, the gate courses GOV 110 and BSE 106, the full assessor methodology (BSE 109 and 201 through 207), a supervised assessment practicum, and the CIRP exam.
- **CBRA (Certified BSE Readiness Assessor)** — the summit credential, carrying Diamond Blue signature authority: the CIRP first, the Diamond tier (BSE 305–308), a portfolio review of at least two completed assessments, and an oral board.

The CRC, CIRP, and CBRA exams each require the Fundamentals Evidence submission. Because the catalog evolves — courses are added, and prices and prerequisites change — the online FIR course catalog is the version of record for exactly what each credential requires today.

Chapter 3 — The evidence standard

Certification lives or dies on evidence. The whole apparatus of credentials and panels exists to apply one disciplined idea: a claim is credited only at the strength its proof can carry.

The evidence hierarchy

FIR ranks proof on five rungs, strongest first. Exercised is the strongest — the capability was run, under observation, in a drill or a real event. Below it is demonstration — it was shown to work on request. Then inspection — a qualified person examined it directly. Then documentation — it exists on paper. And weakest, narrative — someone described it. These five rungs map onto the 0-to-5 scores from Book 2, so that a high score is not a matter of opinion but of where on this ladder the proof actually sits. A capability that has only been written down cannot be scored as though it had been exercised.

Verified, attested, asserted

A second distinction runs alongside the hierarchy, about who stands behind a piece of evidence. Evidence is verified when the assessor or another qualified party directly examined, tested, or observed it. It is attested when a responsible party formally stated it to be true. It is asserted when it was simply said, with nothing behind it. An assessment that quietly treats an assertion as a verification is exactly the failure Trust but Verify exists to prevent.

Chain of custody

Because a certification may be relied on by people far from the community, every piece of evidence carries a chain of custody: an unbroken record of who produced it and who verified it, from the moment it was collected to the moment it was signed. The chain of custody is how Trust but Verify is demonstrated rather than merely claimed — it lets a reviewer, or a court, follow any single claim back to its source. The deliverable that carries all of this is the scorecard: the declared scope, the ten dimensions against the three vectors, every cell a 0-to-5 evidenced score, each vector set at its weakest dimension.

Chapter 4 — Certifying Diamond Blue

Most certifications in the FIR system are per-vector levels — a cyber Gold, a physical Silver. The summit certification is different, and it is what the CBRA credential exists for: Diamond Blue, the certification that a community can operate as a functioning limited society through a prolonged event.

The certifier's posture

A Diamond Blue certification is demanding by design, and the certifier approaches it with a particular posture: skeptical, evidence-first, and unwilling to credit anything that has not been proven to the standard the hierarchy requires. The certifier reads the community's structure before scoring it — placing it in the dependency stack, scoring governance and workforce directly rather than assuming them — and then scores each vector and its underlying

dimensions against the declared scope, setting each vector at its weakest dimension and never averaging across them.

Diamond-N and the declared scope

Two numbers anchor a Diamond Blue certification. The first is Diamond-N, the days of supply the community can sustain under its tightest constraint, counting every category of consumable at once — fourteen marginal, thirty adequate, sixty resilient — and credited only once a vector is hardened to its survivable threshold. The second is the declared scope: exactly what the community put forward as Diamond-ready, which is therefore exactly what must be exercised and proven. A community may declare a hardened command core or the whole municipality; whichever it declares, the certification covers that and never silently more.

What the signature means

When a CBRA signs a Diamond Blue certification, the signature means a specific thing: that all three vectors in the declared scope reached Diamond, that the community (or subset) demonstrated the ability to function as a limited society, and that the evidence for all of it was verified to the standard. It does not mean the community is guaranteed to survive. The Prudence Notice from Book 2 still applies to every claim below community-wide Diamond Blue, and the honesty it enforces is the whole point of the signature's value.

Chapter 5 — The independent check

A certification signed by the same person who did the assessment is only as trustworthy as that one person. FIR does not rely on a single signature for its highest certifications. It adds an independent check.

The Certification Panel

Every Diamond Blue package, before any award, is reviewed by the FIR Diamond Blue Certification Panel: certified assessors who had no role in the engagement. Their independence is the point — they have no stake in the outcome and no relationship to defend. The panel does one of two things. It concurs, and the certification is awarded. Or it remands, returning the package with named defects that must be addressed. What the panel never does is re-score the assessment, waive a requirement, or soften a finding. It is a check on whether the standard was met, not a negotiation over the standard.

Why this matters

The risk the panel guards against is the oldest one in any inspection system: the sole assessor who, over time, grows close to the communities being assessed and begins — even without meaning to — to see the best in them. An independent panel breaks that drift. It is also why assessor-shopping, a community quietly seeking out a more lenient assessor, is treated as a red flag rather than a convenience. The certification is worth something precisely because it cannot be talked down.

Chapter 6 — Proving it works, through exercises

The strongest rung on the evidence hierarchy is "exercised," and for a reason: a plan that has never been run is a hypothesis. The Diamond tier includes a whole course (BSE 308) on how to design and run the exercises that turn a plan into proof.

What makes a FIR exercise different

Ordinary emergency exercises tend to rehearse a single hazard — a flood, a chemical spill — over a short horizon, and they assume the cause is natural. A Black Sky Event is none of those things, so a FIR exercise is built differently. It is grounded in a deliberate, multi-domain adversary rather than a single accident. It stresses the cascades and dependencies from Book 1, not just one broken thing. It exercises the Tier 0S governance and economic machinery from Book 3 — the council deciding, the ledger settling, the gate screening — not only the physical response. It runs toward a sustainment horizon of weeks and months, not hours. And it holds everything to the Trust but Verify evidence standard. The difference is the point: generic drills do not prepare a community for the event these books are about.

Exercising what cannot be built in a drill

Some things cannot be stood up for real in an exercise — a community will not actually issue scrip or man a gate for a test. FIR's answer is to exercise the decision and the written governance plan that allows that decision, not the installation: the people who would run those functions work through the real choices under observation, without physically building anything. The same applies to the hardest vector. A community that cannot fully prove its EMP/GMD hardening in a drill can still exercise it by declaration and records inspection — stating which electronics are hardened and operating from that shielded core — which is honest about what was and was not tested. EMP/GMD hardening evidence must be in writing, such as equipment specifications, installation records, and electrical inspections.

Evidence that counts outside FIR

Exercises also produce evidence that bodies outside FIR recognize, and a good certification captures it in the forms those bodies use — for example, the after-action report and improvement plan that federal exercise programs expect. This matters because a certification is most useful when its evidence can travel into the grant applications, the state reviews, and the standards processes where resilience work is actually funded and recognized.

Chapter 7 — Keeping it true: recertification and the registry

A certification is a statement about a moment. Communities change, threats change, and equipment ages, so a certification that is never revisited slowly stops being true. The last piece of the path is how FIR keeps a certification accurate over time.

Recertification

Recertification is a narrower engagement than the first certification, but it is held to the same strict standard, and it runs each cycle. It does one of three things on exercised evidence: it holds the certification as it stands, it holds it with conditions that must be met, or it reverts it to a lower level when the evidence no longer supports the claim. Recertification is deliberately unsentimental — a certification earned three years ago is not a certification today unless the evidence still carries it. Cycles are aligned to a common anniversary so that a community's certifications stay in step rather than drifting apart.

The registry and the providers

Two public structures keep the whole system legible from the outside. The FIR Practitioner Registry lists every credential holder, every authorized training provider, and their instructors, so that anyone relying on a certification can confirm the people behind it are qualified. And training itself is credentialed: an organization becomes a FIR Authorized Training Provider through BSE 307, and its instructors are qualified there, so that the method is taught consistently wherever it is taught. Together the registry and the provider system are what let a certification signed in one place be trusted in another.

That is the certification path, end to end: a credentialed professional, a disciplined evidence standard, an independent panel, proof through exercise, and recertification that keeps it true — all of it built to support a claim an outsider can rely on, and none of it claiming more than it can prove.

Appendices

The reference material for this book — the glossary of record, the course field cards, and the sources — is gathered in the companion *FIR Field Handbook* rather than repeated here, so that one document stays the single source of record. The certification, evidence, and credential terms used above are defined there in full, with the courses that own them (principally BSE 201–203 and the Diamond tier, BSE 305–308). Where this book and the Handbook ever differ on a definition, the Handbook governs; where either differs from the online courses on instruction, the course governs, and the difference should be reported for correction.

Take the next step

This book is a free introduction. To learn the method in full — and to earn FIR's credentials — take the courses, which are the version of record for instruction. The full credential path — CRL, CRC, CIRP, and CBRA — and the exact courses each one requires are laid out in Chapter 2; earned credentials appear on the public FIR Practitioner Registry. Whatever your path, the four Foundation courses (BSE 099, 101, 102, and 100) and the free member orientation (FIR 001) are the place to start, and they cost nothing. Browse every course and enroll at the FIR course catalog, and learn more about FIR at fir.foundation.