



GHOST
PROTOCOL

SO

THE FIELD LIBRARY

GROUND RULES

THE SHARED LANGUAGE OF ASSURANCE

Standards and Compliance

Why standards exist, the frameworks, PCI and regulated data, compliance versus security, and the audit.



Ghost Protocol (Pvt) Ltd · Colombo · ghosts.lk

Security internship training · The Field Library · Edition 1 · 2026

THE GHOST PROTOCOL FIELD LIBRARY · GROUND RULES

Standards and Compliance

Why standards exist, the frameworks, PCI and regulated data, compliance versus security, and the audit.

Ghost Protocol (Pvt) Ltd · Colombo

The Field Library, Edition 1 · 2026

Copyright 2026 Ghost Protocol (Private) Limited. All rights reserved.

Sold as a PDF for the buyer's own reading. Please do not share or resell the file.

The library

The Field Library is a whole shelf, not one book. The Core Path is the spine everyone reads. The rest is depth and breadth, taken on as the work calls for it. The shelf is complete now, and you are reading the one marked here.

A · THE CORE PATH

O The Oath BUILT

I Groundwork BUILT

II The Web BUILT

III The Wider Field BUILT

IV The Work BUILT

V The Craft BUILT

B · DEEP TRACKS

AI and Agents BUILT

Reading Code BUILT

Internal and Active Directory BUILT

The Web, Deeper BUILT

Cloud and Containers BUILT

Mobile and APIs BUILT

Reverse Engineering BUILT

Hardware and the Edges BUILT

C · THE OPERATIONS

Red and Purple Team BUILT

OSINT and Recon BUILT

Report Writing Mastery BUILT

The Consulting Craft BUILT

Bug Bounty BUILT

D · THE OTHER SIDE

Detection and Response BUILT

Threat Hunting and Forensics BUILT

Hardening and Architecture BUILT

E · THE GROUND RULES

The Law, Deeper BUILT

Standards and Compliance YOU ARE HERE

Ethics and Disclosure BUILT

F · COMPANIONS

The Reference Pack BUILT

The Lab Workbook BUILT

Case Files BUILT

The Bestiary BUILT

The Glossary and the Ledger BUILT

Contents

- Opening 5
- 1** Why Standards Exist 6
- 2** The Frameworks 10
- 3** PCI DSS and Regulated Data 15
- 4** Compliance versus Security 19
- 5** The Audit and the Evidence 23
- Worked answers 27

The word that means nothing alone



The email asked one question, the way these emails do: "Are we compliant?" Blink wanted to answer yes and move on.

BLINK "They have a firewall and a policy document. So, compliant. Yes?"

SOL "Compliant with what, measured how, attested by whom? A standard is a shared language, so a client, an auditor, and you all mean the same thing by one word. That is its whole value, and its whole danger: a tick in every box describes a system that passed an audit, not a system that is safe. Learn the frameworks so you can speak them. Never mistake the map for the ground."

Wurm's eye settled on a control marked "in place" that no one had tested in a year.

WYRM "map. not ground."

So the book is the language of assurance: the frameworks, the regulated data, the audit, and the exact gap between a box ticked and a control that would actually hold.

CHAPTER ONE

Why Standards Exist

A standard is a shared language of assurance, the thing that lets a client, an auditor, and you mean the same word when you all say "secure". This chapter teaches you to read that language, and to see exactly where you stand in it.

Volume 0 gave you the one law: you test only what you are authorised, in writing, to test. This volume is about the paper on the other side of the engagement, the frameworks a client is measured against and the report you hand an auditor. None of it changes how you find a flaw. All of it changes whether your finding is believed, filed, and acted on. A tester who cannot speak this language does good work that dies in a meeting. A tester who can turns the same finding into evidence an auditor signs.

Assurance is a claim that needs a witness

A client says "we are secure". On its own the sentence carries no information. Secure against whom, doing what, measured when, judged by what bar? The word only starts to mean something when all three parties in the room agree in advance on what would count as proof. That shared agreement, written down so it cannot drift mid-argument, is a standard. It is not a magic property a system either has or lacks. It is a dictionary the client, the auditor, and the tester all read from, so that a claim can be checked instead of merely asserted.

This is the same move you already make with a vulnerability. "The site is broken" is a feeling. "An unauthenticated GET to `/api/orders/1004` returns another customer's order" is a claim with a witness: anyone can send the request and read the response. A standard does for a whole organisation what a reproduction does for a single bug. It replaces "trust me" with "here is the thing you can check".

Three people who need the same dictionary

Picture the three roles, because the rest of this volume is about keeping them honest with each other. The **client** is buying assurance, usually because someone above them, a customer, a board, a regulator, asked for it. The **auditor** is the independent party who decides whether the assurance is real, and who puts their own name on that decision. The **tester**, which is you, produces evidence the auditor weighs. If each of those three used a private definition of "secure", every engagement would end in an argument no one could win. The standard is what they share so they do not have to.

Hold on to the direction of travel, because people get it backwards constantly. You do not decide the client is compliant. The auditor does, and only the auditor. You produce evidence toward named controls, and you produce it so plainly that the auditor can act on it without a translation step. The whole of your value in this room is that your evidence is true and legible. The moment you reach past that and start certifying compliance yourself, you are doing someone else's job and staking your name on a judgement that is not yours to make.

Control, requirement, criterion: the words Frameworks Use

Frameworks are built from small named units, and the names matter because auditors file by them. A **control** is a safeguard, something an organisation puts in place to reduce a risk: access reviews, encryption at rest, a tested backup. A **requirement** is a control a standard says you must have, often numbered so it can be cited exactly. A **criterion** is the thing an assessor judges you against. The units differ between frameworks, and that difference is not decoration. It tells you what a finding of yours can and cannot be mapped to, which is the whole subject of Chapter Four.

When you write a finding, you will later tag it with the control it is evidence for. That tag is only worth something if you used the framework's own identifier, spelled and versioned the way the framework spells it. A control written in your own words is a paraphrase an auditor has to double-check. A control written as the standard's exact reference is one they can file.

Two shapes of standard: prescriptive and risk-based

Standards come in two shapes, and knowing which one you are holding tells you how your finding maps into it. A **prescriptive** standard states, close to line by line, what must be true: encrypt this, scan that, test on this cadence. PCI DSS is the clearest example, and Chapter Three is spent inside it. A finding against a prescriptive standard maps cleanly, because the standard already named the thing you broke.

A **risk-based** standard, by contrast, does not hand you a checklist. It tells the organisation to run a process, decide what matters for its own context, put controls in place, and prove those controls operate. ISO/IEC 27001 and SOC 2 are this shape, and Chapter Two lays them out. Here a single finding of yours rarely "fails" one line. Instead the whole act of testing is evidence that a process, vulnerability management, is running and producing results. Map a finding into a risk-based standard the way you map it into a prescriptive one and you will overstate what you proved. The shape of the standard decides the shape of the claim.

Where you Fit, and where you stop

Put it together and your position is small, clear, and worth defending. You test what you were authorised to test. You confirm each finding the way Volume II taught, so that it survives a challenge. You map each confirmed finding to the control it is evidence for, in the framework's own language, with the edition named. You state plainly what your test did not cover. Then you stop. The auditor reads your evidence, weighs it with everything else they gather, and reaches the compliance decision. The client gets the assurance they were buying. You never signed the word "compliant", and because you never signed it, your name is still worth something the next time you hand over a report.

**SOL SAYS**

Learn the frameworks so you can stop thinking about them. A standard is a shared language, and a language is only useful because it lets two people who have never met agree on what a sentence means. It does not do your judging for you, and it is not a shield you hold up to make a weak finding look strong. The reason to know ISO from SOC 2 from PCI cold is so that when you write a finding, it lands in the auditor's world already filed, and the only thing left to discuss is the thing that actually deserves discussion: whether it is true, and how much it matters.

■ EXERCISE

Pick one product you use that has a "trust" or "security" page: a bank, a SaaS tool, a payment app. Read what it actually claims. Note each standard it names, and for each one write down, in a sentence, what that claim asserts and what it does not. A page that says "SOC 2 Type II" is claiming an independent party watched a set of controls operate over a period; it is not claiming the product has no bugs. A page that says "PCI compliant" is claiming something narrower still, about cardholder data only. You are training the reflex to hear a compliance claim and immediately ask what is inside it, because that is the reflex an auditor and a careful buyer both have.

■ VERIFY IT

"We are ISO 27001 certified" is a checkable claim, not a mood. A real certification has a certificate, an accredited certification body that issued it, an expiry, and, the part people forget, a **scope statement** that names exactly which part of the organisation was certified. A company can hold a genuine certificate whose scope is one data centre and one product line, while the thing you were hired to test sits entirely outside it. Before you repeat anyone's certification as cover for anything, read the scope. A certificate you have not read the scope of is a sentence you have not verified.

■ ON YOUR FEET

A prospect emails you: "We just need a quick pentest so we can be SOC 2 compliant by the end of the month." Two things in that sentence are worth gently correcting before you quote anything. What are they, and how do you say it in a way that builds trust rather than sounding like you are lecturing a paying client?



WHAT WYRM KEEPS

A standard is a shared language of assurance: the dictionary a client, an auditor, and a tester read from so a claim can be checked instead of asserted. You produce evidence toward controls. The auditor decides compliance.

- Frameworks are built from named units: a control is a safeguard, a requirement is a control you must have, a criterion is what an assessor judges you against. Tag findings in the framework's own identifier, versioned.
- Standards come in two shapes. Prescriptive standards (PCI DSS) name the thing you broke, so a finding maps line to line. Risk-based standards (ISO 27001, SOC 2) ask for a process you must prove operates, so the test is evidence the process runs.
- A certification claim has a scope statement. Read it before you rely on it: a genuine certificate can cover a part of the organisation that is not the part you were hired to test.
- You never sign "compliant". You confirm, map, name your gaps, and stop. The auditor owns the verdict, and your restraint is what keeps your evidence worth reading.

CHAPTER TWO

The Frameworks

The four names you will meet on nearly every engagement: ISO/IEC 27001 and 27002, the NIST Cybersecurity Framework, the CIS Controls, and SOC 2. What each one is for, who asks for it, and why they overlap on purpose.

A client rarely asks for one framework in isolation. They are chasing a customer's question-naire, a tender requirement, a board's demand, and those arrive in different dialects. This chapter gives you the four you will meet most, with the editions named so you can cite them without guessing. Read them as instruments with different jobs, not as rivals. Most of them are measuring the same handful of good practices from different angles, which is exactly why one honest finding of yours can be evidence across several at once.

ISO/IEC 27001 and 27002

ISO/IEC 27001 is the international standard for an **information security management system**, an ISMS: the documented process by which an organisation decides what it needs to protect, assesses its risks, puts controls in place, and keeps improving them. It is certifiable. An accredited certification body audits the organisation and issues a certificate with a defined scope, which is the scope state-ment Chapter One told you to read. The current edition is ISO/IEC 27001:2022, which replaced the 2013 edition and restructured its control annex. A client will hold "27001 certified" out as the heavyweight credential, and international and enterprise buyers ask for it by name.

Its companion, ISO/IEC 27002:2022, is not certifiable and is often confused with 27001. The distinc-tion is worth keeping straight: 27001 is the management system you are certified against; 27002 is the guidance that describes each control in detail, the reference you reach for when you want to know what a control actually means. The 2022 edition of 27002 organises its controls into four themes, which is a useful map to carry.

THEME	WHAT IT COVERS
Organisational	Policies, roles, supplier relationships, incident management
People	Screening, awareness, responsibilities, conduct after leaving
Physical	Secure areas, equipment, media, clear desk and screen
Technological	Access control, cryptography, logging, secure development, testing

When your web finding maps into ISO, it almost always lands in the technological theme, under tech-nical vulnerability management and secure development. You are rarely evidence about the organisa-tional or people themes, and saying so plainly is part of honest mapping.

The NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a voluntary framework, not a certification. It gives an organisa-tion a shared structure for describing and improving its security posture, built around a small set of