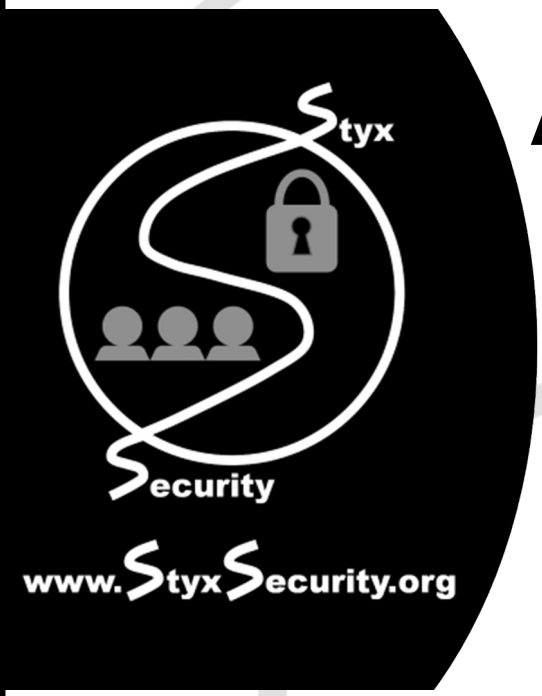

Authority, Risk & Execution

Physical Penetration Test Standards

A guide to lawful authority and due diligence for physical engagements.

PURPOSE

A reference guide for resellers and cyber-physical teams on establishing lawful authority, managing operational risk and meeting due diligence requirements. Designed for companies bundling physical operations with cyber engagements or subcontracting field work.

SCOPE

This document outlines non-negotiable requirements, including:

- Contractor expectations and issuing assignments
- Pre-engagement customer screening
- Legal and regulatory considerations
- Operational planning and go-forward authority checks

Table of Contents

Admin

Distribution Permissions

If you want to pop it into your favourite AI model and use it to cross-check your documentation and process, feel free.

Use of AI

AI was not used to create this document.

The information herein is based upon formal training, extensive reading, Styx Security’s internal documentation, experience and some hard lessons.

Intent

To ensure those sub-contracting to Styx Security are aware of our standards, to help maintain the industry reputation and to help others avoid the pain of the aforementioned hard lessons.

This is not a training manual or a substitute for comprehensive, formal training. It’s a guide to compliance and a checklist.

Disclaimer

This isn’t a training manual or a full compliance document. It is intended to assist you in creating your own compliance tools and guiding those intending to step into physical penetration testing / sub contracting work.

You will really want to consider legal review of your template documents and, if the contract is substantial, you may wish to ask for a deposit to help cover the cost of legal review of final documents.

There will be sections in this document which are not relevant at all and there will be relevant sections absent. Some of these will be made clear (like Operational Plans) and some just aren’t mentioned – this is not aimed at teaching you how to do a penetration test. You should seek proper training and not rely on this document.

Neither Styx Security nor the author are responsible for anything you do. You’re expected to take responsibility for your own actions and for being fully informed and appropriately experienced prior to undertaking work. The responsibility for physical penetration test compliance is on you, as is the safety of yourself and your team.

Introduction

This “checklist” seems really extensive because, well, *it is.*

The operational element of the physical penetration test often takes 1/10th or less of the preparation and reporting time. We are sending real people into real situations where they lack procedural protections (e.g. visitor fire evacuation protocols) to simulate criminal activity. As a result, the entire exercise must plan to safely, lawfully and morally simulate the potential recklessness and lawlessness of morality deficient criminality. All whilst being tightly controlled to legally and physically protect the contractors, client, stakeholders, public, employees and others to whom we owe a Duty of Care.

The *only* thing that separates a physical penetration test from *The Italian Job* is the paperwork and associated signatures.

Without permission, even the simplest penetration test can become trespass (best case), burglary, theft, fraud (impersonation of individuals or company representatives) and more under CMA and DPA. Civil legal ramifications abound for ground operatives, team leaders, contractors and customers. Permissions are not some perfunctory signature.

Poor contingency planning or protection of other businesses who may become collaterally involved can expose the customer organisation as much as the contractor. You’re responsible for adverse impact.

For a simple “proof we can get in”, social engineering penetration test, most of this is really simple and handled by templates. But it must all be covered and the legal ramifications for failure are significant.

There are companies who are half-arsing this stuff and getting away with it. And they’ll continue to get away with it and undercut those doing it properly… right up until something goes wrong. Market yourself as protecting your customer with your diligence. Being a “visitor” is rarely enough and clients seeking quick-fix loopholes should be avoided.

My strong advice is to do this properly or pass on it. After this, you’ll see why I often urge customers to reconsider a physical pen test and look to adversarial assessments instead. I’d rather spend their money testing controls than navigating authorities, risk assessments and juggling stakeholders.

Phil Smith – Director

The Summary “Up Top”

This document is detailed, but not complex. You will find it easier to keep the contracts you’re likely to take in mind as you extract the elements most relevant to you. Template this and it’ll save you time in future.

Compliance in a Few Lines

Risk:

Have I identified all the risks, controlled what I can and created sensible and simple contingency plans that will survive contact with reality?

Authority:

Has everyone who might sue, or have us arrested, signed letters of authority based on approval of the final operational plan? Can the chain, from informed consent to signing method, stand up in court?

Consent:

Has anyone who might be directly / indirectly affected, or erroneously call police, been informed and given written consent if needed? Are leased equipment owners, nearby businesses, licensed IP, etc considered?

OPORDs:

Does my Operational Order allow the least experienced person on my team to perform their role with no other direction, tell them the limits of the granted authority and say when (and how) to quit?

A Note on OPORDs (Operational Order)

This is different to a military Operations Order, although it achieves the same goal. The name is slightly different for a good reason. We're civilians operating within the law, in a civilian context and have access to resources (emergency services, food, power etc) where the military have to plan for self-sufficiency in austere environments (CAS/MEDEVAC, trauma hospitals, etc). This document doesn't cover OPORD or Operational Plan creation, but here are some tips to control mission creep and associated risk.

Don't over complicate an OPORD – these are an art and need to be detailed enough to inform but short enough to memorise. Get the intent part correct and simple as this will allow your ground team to adapt and proceed with the objective when things go wrong. Find someone covered by the NDA, but not involved in planning, to review your OPORD.

Keep it simple. If you have three contingencies with subtly different triggers, I *guarantee you* each one of your ground team will pick a different one. That's your fault. **It has to work under stress, with no-comms and when things are going wrong.**

Styx Security uses a variant of IMMARCH, which is a civilian policing approach. This is closer to the reality in which we are operating than the military approach, which can lead to focus on areas which need be one line or entirely absent.

Sub-Contractor Expectations

A physical penetration test requires a lot of work prior to execution. It is not enough to have a vague plan and then sub-contract someone for the day or two of the operation, landing them with the risk, but no planning or risk controls. They'll walk, muttering about prison food.

Expectations for Operational Day Subs

1) All the prep work, risk assessment, operational plan and authorities will be done, dusted, granted and available to check *in advance*.

2) An operational order (OPORD) shall be issued which detail the risks and controls, objectives, the overall plan, the individual's place within it, authorised TTPs, scope, abort conditions, comms plans and so on.

3) A letter of authority shall be issued satisfying them, and potentially others, of full lawful authority for the operation. <u>You must be able to supply, in advance, any information reasonably required for them to satisfy themselves of full lawful authority for their due diligence.</u>

4) If you're not paying them to report, you will be paying them for debrief time post-op and you should make the most of this. Contractors will expect to hand over notes, surveillance logs, photos / video footage and have a debrief immediately after exfil (I suggest recording this as it's just easier). If you want a written report from each, you can expect this time to be billed to you. Ultimately, you'll be getting raw data, a contemporaneous record of events, and reporting yourself.

Summary

A sub-contractor can plan and run your test, but you'll be paying them for this work as there's a lot of it, much of it compliance. They may or may not have templates that speed it up. You'll be expected to review anything contractual and put things into your branding / stationery before forwarding to the client. If just contracted for operational days, they will expect this to be done by you. If OPORDs and authorities aren't squared away in advance, they must (and *absolutely will*) walk – usually whilst charging you for a last minute cancellation.

If OPORD / Operational Plan are new terms, you're not running physical penetration tests. Stop here. Get training.

Prior to the Engagement

Much of the below should form part of your initial scoping and be checked before any contracts / proposals are signed.

Lawful authority to proceed is **not** being granted at this stage, but rather approval-in-principle sought. You'll also want to understand what the customer wants to achieve through a penetration test, ensure it's the right service and whether you are the right company to provide.

I tend to nudge those wanting to "find our security vulnerabilities" away from a full physical pen test as it represents poor value. Mostly, physical pen testing is contractual compliance, insurance or regulatory driven.

You'll want a written scope defining intended test areas and intended methods (required for permissions and provider capability) – this will form part of the draft Statement of Work (SOW). This will evolve, but it is a starting point for what follows.

Approvals In-Principle

I suggest doing no prep work until the below are confirmed. The legal review is just to ensure there are no hard-blocks on a pen test.

- An email or similar from building owner or similar (as needed).
- Internal legal review of a draft testing outline / scope (customer must be able to provide legal / compliance review if regulated industry, e.g. finance, healthcare, nuclear).
- Approval from senior leadership at an appropriate level in the organisation.

Ideally, check the customer has the above to hand before even booking a scoping call.

The prospective customer should be aware they'll need stakeholder permissions / notifications which may include:

- Building owner / Landlord consent.
- Facilities management approval (may be an external supplier).
- Property management company authorisation.
- Associated / nearby sensitive businesses which may suffer collateral intrusion / alert police.

- Companies / individuals who are intended to be impersonated or who may be otherwise suffer reputational impact (e.g. contractors, partner organisations or individuals).
- Deepfake releases for any subjects with use terms, data protection obligations and dataset deletion schedules.
- Owners / administrators of any PACS system to be evaluated, especially if card cloning or credential analysis is requested.
- Any Responsible Persons for fire, health and safety, etc.
- Owners of leased hardware or equipment which may be involved with the test.

Most of the above are gateways to provision / performance / utility of a physical penetration test. Without these a test can not proceed. Make sure your contract / SOW states the customer is responsible for obtaining and demonstrating these permissions with cancellation penalties being applied if they fail to do so. When considering if a stakeholder needs to give initial consent, the prospective customer needs to consider second and third order effects on stakeholders.

A contract should not be entered into until the customer company have approached and received agreement-in-principle from any of the above who have a veto power on the test. These stakeholders may wish to see a draft scope and authorised TTPs, but should not expect full RA and final plans as yet.

But Why Define Scope Now?

This is an initial “can Styx do this and will stakeholders let us?” scope, not a final document. Realistically, you can build this from the initial scoping call notes in 30 minutes using templates. The customer can then run this past the right people.

Defining scope at this stage is essential to customers obtaining permissions and for ensuring you, as the provider, are capable of providing services. For example, presence of radiation controlled environments in a hospital will dictate the insurance, training and experience required by the contractors to be engaged. Port authority buildings may be fine, but an insurance driven inability to go waterside might make a company unsuited to replicating real-world threats.

A customer’s internal legal review will identify regulatory / contractual issues which may make a penetration test, which fulfils the desired strategic objectives, impossible. It will also help identify potential

industry specific criminal / civil offences requiring specific permissions from stakeholders or preventative actions, such as the removal of compartmentalised data for the duration of the test or compliance training. This will also answer questions about insurance coverage which should be part of your standard due diligence.

There may be some elements where permissions won't make or break go-forward authority. It's reasonable to note these permissions must be sought but not delay engagement awaiting them.

Styx Security has declined work / objectives in industrial or regulated environments where the company is not equipped to fulfil obligations safely or effectively. Whilst there is an expectation that you will have to do learning, training and other prep, if you're not happy working in a specific industrial environment, for example, you should just turn down the work and refer onwards.

Your Expectations of the Prospective Customer

Some customers will never have requested a physical pen test before and will need proactively guiding. If this is the case, the below aren't really red flags – you're being engaged as a competent and knowledgeable consultant to fill these knowledge gaps.

If the company has experience with penetration testing, you should expect to hear about:

- Insurance – PLI / PI / cyber and values. They should be telling you what amounts they expect from you.
- Experience / mandatory training – Styx has experience in some quite niche areas but little experience in others.
- Licensing – We have declined work because our telecoms license (OFCOM) didn't cover the requirements of the job.
- What TTPs you can employ, the risks and the relation to the threats facing the customer organisation – lock damage, marks, impact on fire controls, etc.
- Data controls for anything exfiltrated, including photographic and video evidence.

Not asking all of these isn't a big deal. If insurance isn't queried at some point prior to signing, you should have concerns. If this is a niche industry, you should ask about mandatory training requirements if the information is not offered.

Post-Signing, Prior to Go-Forward Authority

Nearly everything you do beyond this point is billable. You're now contracted and performing duties in the service of that contract.
The SOW in a physical engagement is a living document and should have reached version 1.0 at this stage for a contract to be signed. This is still expected to evolve substantially with TTPs being approved or declined as passive / hostile reconnaissance is performed and the picture of the target evolves. The strategic objectives and out of scope areas are usually set at this point.

You must have an agreed process for versioning the SOW, operational plan, etc and ensuring everyone is on the same versions as they evolve.

Required Documentation

Prior to go-forward authority, the following is required:

- Final SOW / ROE (Rules of Engagement):
  - Clear scope boundaries (areas, TTPs, etc)
  - Explicit out of bounds areas / systems / items
  - Testing hours and time windows (may be *very* narrow)
  - Social engineering permissions and limits (if applicable)
  - Emergency abort procedures
  - Impersonation permissions and boundaries
  - Abort parameters
  - When to present letters of authority (and the impact on the test – being caught probably shouldn't stop the test).
  - Have you a plan for discovery of actual criminality? *
- A final operational plan, for which the elements affecting authority and consent are now agreed, approved and unlikely to be subject to material change. You may wish to highlight elements which are fixed (due to permissions) and fluid (can be changed).
- A risk assessment based upon this operational plan with controls and sign off from the POC and team leader / contract manager.
- Written permission, based on this operational plan (redacted if needed), RA, ROE, etc from the stakeholders, building owners and other individuals / organisations identified.
- Point of Contact (POC – usually x2-x3) identified and to be available during the operational element of the engagement using approved communications methods. These people will need to

have authority to agree changes to the SOW / ROE / scope and decide if a test should proceed if a contractor is compromised. They will need to be prepared to validate the lawful presence of the contractor on site.**

- A plan for updating the SOW retrospectively from logs, etc. Often this is done using Signal or similar messaging applications to update with mid-op decisions.
- Signed letters of authority signed by appropriate stakeholders ***
- Post-test clean up plan must be in place:
  - Compromised security systems remediated and restored to full operational capability.
  - Feedback to any employees subject to aggressive social engineering techniques.
  - Sensitive information breaches contained / exfiltrated sensitive data logged, secured and redacted promptly.
  - Cloned / “breached” credentials inactivated and notes placed on security logs detailing inaccuracies in PACS records (especially where used for life safety processes).
- A clear plan must be in place for if the test is terminated for safety or compliance reasons during the operational element.****
- Customer internal communication plan
  - Key personnel notified (only as required, may include some security team members, management, facilities management)
  - Third-party security vendors informed (SOC, security guards, monitoring services)
  - Plan to prevent false alarm calls to police (without exposure to real offenders)
- Internal Legal & Compliance Review (customer and contractor)
  - Data Protection Act compliance check
  - Review of local / industry specific regulations
  - Insurance verification
  - Specialist compliance or regulatory considerations, e.g. radiation controlled zones, financial regulations, etc.

* A plan for stumbling upon real criminality is worthwhile. If you find a cannabis grow in a building the customer thinks is unused, this may or may not be considered an immediate risk. Whether the test is terminated at this point is a question you should have considered in advance. The client may not be happy if you terminate a test worth many thousands of pounds, at their cost, without prior arrangement.

** Note that mid-op changes to the SOW, etc are not unilateral and must be agreed by both contractor and customer organisation. “I’ve

found this, it's almost certainly vulnerable, it's out of scope but likely an important finding – do you want us to attempt to open it?" is a common question and the POC needs to be able to say "yes", "no" or "leave for now". Default is to leave it. The contractor also has no obligation to accept ad-hoc changes or additions (e.g. "whilst you're here, could you check…") which may affect billing, safety, equipment or have adverse operational impact. We actually say we can decline such requests without justification as mid-op is often not the time or place for such discussion. "Sorry, unable." is a reasonable response.

*** Wet ink or formal electronic signatures (e.g. DocuSign) are strongly preferred. Where emailed authority is used (last resort), the full email chain must be preserved and reference the current SOW. Emails should only contain non-sensitive authority details (location, time, date). Sensitive operational information must not be included. **A typed name in a PDF editor is not sufficient and should never be accepted.**

**** Styx Security's contract states by default that if all POCs aren't available at the start time, the test can be terminated at the customer's cost (we're unlikely to do that if 2/3 are available but it's a statement of how seriously this is taken). Should no POC be contactable whilst on-site (outside of a no-comms condition), the operatives are to withdraw by the safest and most expedient method available. They may decide to do this covertly or overtly depending on which is safer, less disruptive and may consider, at their discretion, impact on repeat testing.

Final Go-Forward Authority

The team leader / contract manager checks all the documentation has been completed and signed by the appropriate people, referencing the same version of any documents.

The risk assessment is signed off by the customer representatives and team leader / contract manager.

The overall objectives must be clear with strategic outcomes and tactical objectives. This prevents interpretation leading to scope-creep and unauthorised activities.

The above distilled into Operational Orders (OPORD) which are provided to team members. These may be part of the planning or only contracted for the operational days. Regardless, the OPORD and letters of authority should contain the information they need to complete the assignment and satisfy themselves that the assignment has been competently planned with full permissions and compliance. Additional information, such as complete RA, operational plan, email trails demonstrating permissions and such should be available, within a reasonable time frame, to any independent contractors. They have due diligence obligations and will wish to satisfy themselves of lawful authority, duty of care and adequate risk assessment alongside their insurance requirements, skills and competence.

If a sub-contractor can not fully satisfy themselves of lawful authority and have the OPORD pass their due diligence and competency checks, they are legally and morally obliged to withdraw. You will need enough time to fix the issues or replace the sub-contractor.

Permissions must be based on a clear operational plan with contingency planning and abort criteria. Consideration must be given to collateral intrusion to other businesses, shared areas, individuals caught up in surveillance and so on.

Points of contact must be available via the approved communications methods and authorised to dictate adjustments to scope as the operational element evolves. It’s useful to have everyone in a Signal or similar messaging app group at this stage. Make sure you have backup comms methods and a no-comms plan as well.

Abbreviations

CMA – Computer Misuse Act

DPA – Data Protection Act

MOE – Method of entry. Ways of breaking into things. Often covert method of entry is used, prefixed with a “c” – cMoE.

OPORD – Operational Order – document given to contractors to outline the engagement, risks, role, expectations, TTPs, plan, etc. This is intentionally a slightly different terminology to the “Operations Order” used by the military, as it has a similar goal (to fully inform all those involved in executing an operation) whilst having a different process and use case.

PACS – Physical Access Control System – usually some form of key card and associated electronic locking / computer systems.

POC – Point of Contact – in this context, usually the main contact within the client organisation who is authorised to agree changes to scope / ROE / SOW and confirm the contractors are lawfully on the premises. Usually two or three of these are required to be contactable prior to operational elements being given final go-forward authority.

RA – Risk assessment.

ROE – Rules of Engagement – what TTPs can be used, where is in scope, out of scope, out of bounds entirely and so on.

SOW – Statement of Work – part of the contract which defines what is to be done and how, amongst other things. In a physical test, this is a living document which is often extensively revised as the project progresses.

SOC – Security Operations Centre

TTP – Tactics, techniques and procedures – there are various TTPs which can be used to achieve the goals set out. Destructive / damaging TTPs are usually authorised on a case by case basis. Sometimes even minor covert MOE techniques which may cause scratches to door frames are excluded. Social engineering only engagements often require aggressive techniques to be authorised explicitly and consideration given to the mental state / robustness of targets.