THE COMPANION SERIES

The Compliance Companion

TURNING COMPLIANCE OBLIGATIONS INTO DECISIONS THAT FIT THE ORGANISATION

Adriaan Bosch

Physical Security Strategist · adriaanbosch.net

Contents

Purpose and Use

This playbook is written to support decision-making in complex security environments. It is intended to help practitioners and leaders navigate situations where compliance, operational reality, and accountability intersect. It does not attempt to prescribe outcomes or replace professional judgement. The guidance is deliberately concise and practical. It is designed to be read quickly and applied thoughtfully.

How This Playbook Should Be Used

This document should be used as decision support, not instruction.

It is not:

- a checklist,
- a framework to be applied mechanically,
- or a substitute for leadership judgement.

The value of this playbook lies in how it is interpreted and applied within context, not in strict adherence to its content.

Contextual Assumptions

This playbook cannot determine what is appropriate. It assumes that organisational context, leadership intent, and operational reality have been considered first. Without these, no guidance (regardless of quality) can produce effective or defensible outcomes. Readers are expected to apply judgement and remain accountable for decisions made using this material.

On Compliance and Standards

Compliance is not rejected in this playbook. It is treated as a constraint that must be navigated, not as a proxy for decision-making. Where standards, guidance, or regulatory requirements are referenced, they are intended to inform decisions, not replace them. Where compliance and operational reality conflict, that tension should be addressed explicitly rather than concealed behind process.

Distribution and Use

Final Note

Indecision doesn't stop outcomes, it only changes who shapes them.

This playbook exists to keep decisions deliberate, explainable, and grounded in reality.

Section 1: Intent

Compliance in protective security is hard. The landscape shifts constantly as new standards appear, old guidance is updated, and sector regulators refine expectations. Organisations are expected to keep pace with all of it, even when the rules overlap, conflict, or fail to match the realities of day-to-day operations.

Compliance also sits at the heart of corporate governance. Boards use it to judge whether security is performing. Executives rely on it to defend funding decisions. Audit teams use it to test assurance. Because of this, compliance often determines how much resource is allocated to security and how the wider strategy is shaped.

Yet compliance is rarely straightforward. Most organisations operate across multiple layers of obligation:

- National standards and codes
- Sector-specific requirements
- Internal corporate rules
- Local policies and legacy practices
- Regional or international variations

These layers rarely align neatly. A standard might demand a control that clashes with operational flow. A corporate rule may assume technology the site does not have. A sector guideline could require staff behaviours that local culture makes difficult. In short, compliance rarely fits “as written”.

This raises a simple question: how is compliance applied in real operational contexts without breaking strategy, culture, or feasibility?

This playbook is designed to answer that question. It provides a structured way to:

- interpret what a compliance requirement actually means,
- test whether it will work within the organisation, and
- adjust it without losing the intent of the original rule.

Examples show why this matters:

- A standard may call for biometric access, but PPE prevents fingerprint use.
- Guidance may require camera coverage, but heritage laws block visible installations.
- Corporate policy may require strict perimeter control, but emergency response needs open flow.

In each case, compliance is not rejected, it is translated into a workable, defensible solution.

The intent of this playbook is therefore clear:

to help organisations meet compliance obligations in a way that is practical, context-aware, and operationally sustainable.

It aims to give practitioners confidence. It aims to support decision-making. And it aims to create a consistent method for aligning compliance requirements with the realities of the environments they must protect.

Purpose

The purpose of this playbook is to give organisations a clear, practical way to apply security compliance requirements in real operational environments. Most guidance documents explain what must be achieved, but they offer limited help on how to make those requirements work within the constraints of staffing, culture, workflows, budgets, and technology.

This playbook closes that gap. It offers a repeatable method to interpret each requirement, test it against organisational context, and shape it into a control that remains both compliant and workable. The intent is not to replace formal standards or regulatory codes. Instead, it strengthens them by helping practitioners convert written rules into operational outcomes that make sense on the ground.

The playbook also provides a shared language for security teams, compliance officers, operational managers, designers, and auditors. It helps everyone understand the reasoning behind decisions and gives leadership clearer assurance that compliance is being applied intelligently rather than rigidly.

Who This Playbook Is For

This playbook is written for the people responsible for turning protective-security requirements into everyday practice. It applies across industries and organisational sizes. The typical users include:

- Protective security practitioners who must interpret guidance and convert it into controls.
- Operational and site managers who understand how work actually happens and what is possible.
- Security designers and engineers integrating requirements into layouts, systems, and specifications.
- Compliance, risk, and audit teams who need clarity behind decisions and assurance evidence.
- Governance boards and senior leaders who allocate resources and set expectations.
- Global security leads managing portfolios across countries with different regulatory demands.

The playbook is written in plain, accessible language so it can move easily between strategic discussions and operational conversations.

What This Playbook Covers

The playbook covers the full journey from reading a compliance requirement to implementing a solution that works. It provides:

1. A method to interpret and understand compliance obligations

Different frameworks use different terminology, structures, and assumptions. The playbook explains how to break a requirement down, identify its intent, and understand how it fits within wider governance expectations.

2. A structured context-assessment model

Compliance only works when it matches the organisation’s reality. The playbook helps map this reality using three layers:

- Institutional Drivers, strategy, governance, familiar systems, and corporate expectations.
- Operational Domains, movement, human factors, culture, priorities, and resources.
- Structural Enablers, technology, stakeholders, and external influences.

This gives users a clear, evidence-based view of what will help or hinder compliance.

3. A Fit-Testing process

This checks whether each compliance requirement can operate effectively inside the organisation. It highlights conflicts, constraints, or impractical assumptions before they become problems.

4. A method for refining and documenting controls

Where a requirement clashes with context, the playbook shows how to adjust it without losing the original compliance intent. It also provides the documentation structure to justify decisions and satisfy audit needs.

5. Integration into design, procurement, operations, and assurance

The playbook explains how validated requirements feed into design briefs, tender documents, operational procedures, and assurance cycles.

6. Tools, templates, and examples

Clear templates such as Fit Matrices, Context Profiles, Decision Logs, and Learning Logs support repeatable, defensible work.

7. Alignment with multiple frameworks

The playbook is compatible with:

- NPSA OR1 and OR2
- ISO 31000 and ISO 27005
- NIST Cybersecurity Framework
- National regulatory codes
- Sector-specific requirements
- Internal corporate security standards
- International business-unit guidance

8. Human Factors, Sustainability, and Culture

Compliance only holds if people can reliably use the controls put in place. This playbook explains how behaviour, usability, culture, and long-term maintenance shape the success of compliance decisions. It examines:

- Human Factors: how PPE, task load, ergonomics, and staff experience affect interaction with controls.
- Culture and Values: how openness, risk tolerance, authority dynamics, and service expectations influence acceptance of security measures.
- Sustainability: how staffing levels, maintenance capacity, lifecycle budgets, and training continuity determine whether controls stay compliant over time.

These elements help practitioners avoid technically correct solutions that fail when exposed to real-world operational behaviour.

9. Future-Ready Integration with AI and Digital Assurance

The playbook prepares organisations for emerging digital tools by showing how structured context data supports accurate, controlled automation. It outlines:

- How AI uses structured context such as Fit Matrices, Context Profiles, and Decision Logs to support early reasoning and cross-checks.
- Where AI can assist, identifying common conflicts, checking designs for inconsistencies, and highlighting recurring compliance issues across projects.

- Where AI cannot replace humans, it does not certify compliance, make final decisions, or understand risk intent without oversight.
- How digital twins can simulate flow, bottlenecks, and sensor coverage to inform compliance decisions.
- How adaptive governance works by linking maintenance, staffing, and operational data to automated prompts for re-validation.

This provides a realistic, credible approach to digital assurance that supports human judgement without overstating technological capability.

2. Foundations of Compliance in Protective Security

Compliance in protective security sits within a complex system of overlapping rules, expectations, and operational constraints. Practitioners rarely deal with a single standard. Instead, they face a mixture of laws, sector guidance, voluntary frameworks, and internal requirements, each carrying different authority and purpose. Understanding how these layers fit together, and how they influence real operational environments, is essential before attempting to apply any specific security requirement.

This section establishes that foundation. It introduces the compliance hierarchy, explains why compliance is difficult in practice, and shows why interpretation is a critical part of delivering protective security.

2.1 Compliance as a Multi-Layered System

Protective security does not operate under one set of rules. It sits within a hierarchy of obligations, each layer influencing how controls must be designed and implemented. Conflicts between layers are normal, which makes understanding precedence vital.

Compliance Hierarchy: From Highest to Lowest Authority

- Statutory / Legal Requirements
- Regulatory / Licensing Obligations
- Health & Safety and Fire Codes
- Sector-Specific Mandatory Standards
- Internal Corporate Security Requirements
- Voluntary Standards and Best Practice Frameworks (ISO, NIST, ASIS)
- Local Constraints, Culture, and Legacy Practice

This hierarchy shows practitioners what takes priority when rules clash. It prevents teams from unintentionally choosing a “best practice” measure that violates law, safety requirements, or licensing conditions.

Examples illustrate the point clearly:

- Fire safety always overrides a corporate access-control requirement.
- GDPR restrictions on biometrics override voluntary sector guidance.
- Licensing conditions override internal design preferences.

Understanding this structure helps practitioners make decisions that are compliant, defensible, and aligned with the legal environment.

Why Compliance Has Layers

Compliance is built from multiple sources:

- Statutory & Legal Obligations define what an organisation must do.
- Regulators & Licensing Bodies set specific conditions for certain operations.
- Health & Safety & Fire Codes protect life and frame what security may or may not do.

- Sector Guidance provides additional expectations tailored to risk.
- Voluntary Frameworks (ISO, NIST, ASIS) shape governance but require interpretation.
- Corporate Requirements drive consistency across an organisation.
- Local Context shapes what is practically achievable.

Security is affected strongly by rules outside its domain, privacy law, workforce regulations, accessibility standards, and safety codes often influence feasibility more than security-specific guidance.

2.2 Why Compliance Is Difficult in Practice

Compliance appears simple on paper but becomes challenging within real operational environments. Several predictable issues make direct application of guidance impossible.

1. Standards assume ideal conditions

Most frameworks describe what “good” looks like, but assume consistent staffing, modern infrastructure, stable budgets, and predictable behaviour. Real sites rarely match these assumptions.

2. Frameworks originate from different viewpoints

ISO, NIST, NPSA, and sector guidance are written for different industries and use different terminology. They may contradict each other or require translation before they can be applied.

3. Regional and legal variations create complexity

A control acceptable in one country may be prohibited in another. Privacy, surveillance, biometrics, and emergency-egress regulations differ significantly across regions.

4. Existing conditions shape feasibility

Legacy systems, heritage buildings, space constraints, maintenance limitations, and shared or leased facilities all influence how compliance can be delivered.

5. Compliance changes over time

Standards update. Regulations evolve. Corporate strategy shifts. Technology ages. Compliance is dynamic; controls must adapt.

These challenges create a significant gap between guidance and what an organisation can actually deliver.

2.3 The Gap Between Guidance and Operational Reality

Compliance guidance describes what should be achieved, but not always how to achieve it within real organisational constraints. This gap is where most implementation failures occur.

Common examples include:

- Biometric systems failing due to PPE in laboratories, cleanrooms, or industrial sites.
- Surveillance expectations conflicting with GDPR or local privacy law.
- Barrier controls contradicting fire-egress rules requiring free movement during emergencies.
- Visible security measures clashing with cultural expectations in schools, universities, or public buildings.
- Procedural controls breaking down due to staffing shortages or inconsistent shift patterns.

These situations do not mean compliance is impossible. They mean compliance must be interpreted and adapted so the intent is preserved while operational reality is respected.

2.4 Compliance as a Governance Driver

Compliance strongly influences corporate governance. Boards, executives, and auditors rely on compliance performance to judge whether security is working. It affects:

- budget allocation,
- investment decisions,
- organisational risk appetite,
- internal reporting,
- audit readiness,
- and accountability after incidents.

Because of this, practitioners need a method that not only delivers compliance but proves why a chosen control is appropriate for the context. Transparent reasoning and clear documentation are essential for governance confidence.

2.5 The Role of Interpretation

Interpretation is unavoidable in protective security. Every requirement contains assumptions, about staffing, culture, technology, and workflow, that must be unpacked before implementation.

Effective interpretation means understanding:

- the intent of the requirement,
- the assumptions behind it,
- the constraints of the environment,
- the impact on people and operations,
- and the precedence of conflicting obligations.

This playbook provides a structured, repeatable method for interpreting requirements consistently across different sites, teams, and regions. It reduces ambiguity, strengthens assurance, and supports defensible decision-making.

3. The Compliance Companion Model

The Compliance Companion Model gives practitioners a structured way to interpret, validate, and implement compliance requirements in real organisational environments. It acts as a navigation system, helping teams move from the written rule to a workable solution that fits the terrain they operate in.

Its purpose is simple: ensure that every protective-security control not only aligns with the requirement but genuinely works in practice. The model brings together the intent of the requirement, the context of the organisation, and the feasibility of delivery into a single, achievable objective.

Compliance cannot be treated as a mechanical exercise. Standards describe destinations, but they rarely reflect the complex, shifting terrain that practitioners must traverse. The Companion Model fills that gap. It guides practitioners through a consistent reasoning process helping practitioners understand the intent of the requirement, how it interacts with their environment, and which adjustments ensure the organisation reaches the intended protective outcome without getting lost along the way.

3.1 Why a Model Is Needed

Compliance frameworks often assume conditions that do not fully exist, ideal infrastructure, predictable human behaviour, seamless technology, stable budgets, and consistent governance. Organisations do not operate in those ideal conditions. They function with shifting priorities, aging assets, varying skill levels, and cultural influences that shape behaviour every day.

In this environment, interpreting a standard “as written” can lead to solutions that are technically correct but operationally unworkable. A requirement might expect a certain type of control, but the workforce, the building, or the legal environment may not support it. This tension is the core reason a structured model is needed.

The Compliance Companion Model formalises the reasoning that good practitioners already use intuitively. It captures the thinking process, makes it repeatable, and replaces guesswork with defendable logic. This is crucial for governance, audit, and consistency across teams.

3.2 Way-Finding: Turning Rules into Routes

Compliance requirements function like maps. They set out destinations and describe the broad landscape of protective-security expectations. A map is essential, but it does not tell a traveller which route to take, how to adapt to conditions, or when to adjust course.

To move from map to movement, practitioners need way-finders. These are the cues and decision aids that help organisations interpret direction, judge options, and choose routes that fit their terrain. Way-finders make static guidance usable in real environments where priorities shift, constraints emerge, and people behave in unpredictable ways.

Effective way-finding relies on three groups of aids.

Decision Markers show direction.

They bring together the organisation’s strategic intent, risk appetite, compliance outcomes, and professional heuristics. These markers act like a compass reading, ensuring decisions remain aligned with

long-term direction and defensible when requirements conflict.

Behaviour Guides show what is workable.

They include operational protocols, frontline insights, routine habits, and workflow patterns. These guides reveal how people actually move and decide under pressure. They ensure the chosen route reflects the lived reality of the organisation, not an idealised version of it.

Terrain Indicators show what the environment can support.

They describe the limits and opportunities shaped by technology, infrastructure, layout, system dependencies, and environmental cues. These indicators highlight where routes are feasible, where adjustments are needed, and where certain paths are blocked entirely.

Together, these way-finders help practitioners turn written rules into routes that are practical, repeatable, and grounded in reality. They also set the stage for the structured approach that follows. Each way-finder group mirrors a specific type of organisational terrain. Decision Markers align with strategic and governance influences. Behaviour Guides reflect day-to-day operations. Terrain Indicators capture the physical and technical foundations that enable or restrict delivery.

3.3 The Three-Layer Context Model

The Companion Model is built around a simple central idea:

A compliance control succeeds only when it fits the organisations context or in other words terrain it must operate in.

To understand that terrain, the model breaks context into three layers each acting like a different part of a landscape that shapes the available routes.

Institutional Layer: Strategic Terrain

This layer describes the organisational landscape: strategic direction, governance style, legal obligations, risk appetite, and familiar systems. It reveals which routes are possible and which directions are incompatible with the organisation’s broader journey.

It answers the fundamental question:

Is the requirement aligned with the organisation’s identity and long-term direction of travel?

If not, the route will face resistance, delays, or diversion.

Operational Layer: Day-to-Day Pathways

This layer describes how people actually move and behave: workflow rhythms, staffing patterns, culture, expectations, pressures, and mission priorities. It shows how the “travellers” in the system interact with controls, where bottlenecks appear, and which paths are naturally followed or bypassed.

Compliance succeeds only when people can reliably follow the route it sets.

Structural Layer: Physical and Technical Infrastructure

This layer describes the physical and technical structures that either support or block a chosen route. It includes technology architecture, interoperability, facility constraints, stakeholder relationships, and external influences such as landlords, partners, and regulators.

Even the best-intended pathway fails if the structural layer cannot support it, just as a map may indicate a road that no longer exists.

3.4 How the Model Works

The Companion Model acts like a route-planning engine, applying the three context layers through a clear, repeatable sequence of steps:

- Understand the requirement's intent, identify what it is trying to protect and why. This is the map's destination marker.
- Assess the context layers ; understand the organisation's terrain: strategic, operational, and structural.
- Fit-test the requirement, check where the planned route aligns with the terrain, and where it collides with real-world constraints.
- Refine the requirement, adjust the route where needed while keeping the destination intact.
- Document the reasoning, record the chosen path so governance teams understand how and why the final route was taken.

This cycle turns compliance from a rigid instruction into a navigable journey , structured, deliberate, and adaptable as conditions change.

3.4 Principles That Hold the Model Together

The Companion Model is held together by principles that act like consistent way-finding rules, ensuring the route remains clear and defensible:

- Intent over literal wording: The destination matters more than the exact phrasing of the signpost.
- Context as a decision driver: Routes must match the terrain. A theoretically perfect path may be unusable on the ground.
- Proportionality: Controls should be strong, but not so burdensome that people look for shortcuts.
- Documentation as assurance: Recording decisions creates a navigable trail for auditors and leaders.
- Repeatability: Teams should be able to use the same method and reach similar conclusions across sites.

Together, these principles make the model stable, flexible, and suitable for any compliance landscape.

3.5 A Model That Works Across Frameworks

The Companion Model is intentionally framework-agnostic. It does not replace national standards or regulatory codes. Instead, it provides the consistent way-finding method that allows practitioners to navigate across them.

Whether a requirement comes from NPSA OR1/OR2, ISO 31000, ISO 27005, NIST CSF, a regulatory authority, or an internal policy, the same structured route is used. This avoids misinterpretation, reduces inconsistency, and ensures requirements are applied in a way that respects both the letter and the intent of the rule.

.

4. The Compliance Conversion Workflow

The Compliance Conversion Workflow turns the Compliance Companion Model into a practical, repeatable sequence of actions. It converts written requirements into solutions that preserve compliance intent while fitting the organisation's operational, cultural, and structural realities.

This workflow is not a checklist. It is a disciplined thinking process. It guides practitioners from first reading a requirement to the point where it becomes a validated, documented, and defensible protective-security control. By following this workflow, organisations avoid costly redesigns, operational friction, and compliance drift, all common problems when standards are interpreted informally or inconsistently.

The workflow has five stages. Each stage builds on the previous one, gradually shaping the requirement into something the organisation can use confidently. When followed consistently, it becomes the backbone of compliance assurance.

4.1 Stage One: Understanding the Requirement (Input Collection)

The workflow begins with clarity. Before any analysis can happen, practitioners must understand what the requirement is asking for and why it exists. This first stage involves more than simply lifting text from a standard; it involves reading the requirement with intention.

Every requirement contains an implicit goal, assumptions about the environment, and an expected protective outcome. For example, a requirement for "controlled access" assumes that the environment can support authentication technology, trained staff, and reliable flow management. A requirement for "appropriate surveillance coverage" assumes that camera placement is unrestricted by privacy regulations or structural limitations.

Stage One requires practitioners to gather all relevant inputs: the exact text of the requirement, the framework it comes from, any associated guidance, the broader organisational objectives, and any related documents, such as internal policies or existing risk assessments. The purpose is not to judge feasibility yet. It is simply to understand what must be achieved and the logic behind it.

This stage ensures that the team has a common reference point before moving into interpretation and testing.

4.2 Stage Two: Understanding the Organisation (Context Assessment)

Once the requirement is understood, the next step is to examine the environment it must fit into. This is where the three-layer context model becomes operational. The aim is to build a clear picture of the organisation's reality, not the idealised environment assumed by many standards.

The context assessment looks at institutional drivers, operational behaviours, and structural enablers. It explores how decisions are made, what constraints exist, how people actually work, and what systems, infrastructure, and partnerships underpin the environment. This is the moment where theoretical compliance meets human behaviour and practical limitations.

This assessment captures the subtle but important details that determine whether implementation is possible: the presence of PPE, the pace of operations, the availability of maintenance, the interoperability

of technology, and the culture that defines how people respond to controls.

The goal of this stage is not to find reasons to reject the requirement. Instead, it is to understand the environment well enough to predict where friction will appear later. Good practitioners know that compliance fails not because a requirement is incorrect, but because it was applied without considering how the organisation truly works.

The output of Stage Two is a clear and structured understanding of context, the foundation for decision-making in later stages.

4.3 Stage Three: Fit Testing (Testing the Requirement Against Reality)

Stage Three is where theory meets practice. Fit Testing is the structured examination of how well the requirement aligns with the organisation's context. It is the thinking engine of the entire workflow.

Fit Testing asks a single question:

Can this requirement function effectively within this organisation as it exists today?

To answer this, practitioners examine the requirement through the lens of all three context layers. They look for areas of alignment, misalignment, friction, or full conflict. This process reveals predictable issues: controls that burden users, technologies that cannot integrate, governance paths that complicate approval, or expectations that contradict safety or privacy law.

Understanding fit is not about passing or failing a requirement. It is about understanding the degree to which the organisation supports the intent behind it. Some requirements align naturally. Others need refinement. A few require significant adaptation to avoid operational breakdown or non-compliance with higher-authority obligations.

The output of Stage Three is a clear view of the requirement's fit across the organisation, the evidence needed for the next stage.

4.4 Stage Four: Refinement and Resolution

Stage Four is where compliance becomes practical. Using the results from Fit Testing, practitioners refine the requirement so it achieves its protective purpose in a way the organisation can sustain.

Refinement does not weaken compliance. Instead, it strengthens it by ensuring that the control is operationally workable. The refinement process identifies what needs to change, whether that is the technology, the process, the user interaction, or the conditions under which the control is applied. It may involve proposing alternatives that achieve the same intent, modifying the method of implementation, or documenting conditions that must be in place for success.

Crucially, refinement is accompanied by reasoning. Every change is captured with a clear explanation of why it was required, what constraint influenced it, and how the revised solution still meets the compliance objective. This makes decisions transparent and protects the organisation from accusations of diluting requirements.

The product of this stage is the Validated Requirement, a version of the original requirement adapted to the organisation's real-world needs while retaining its protective purpose.

4.5 Stage Five: Integration and Assurance

The final stage takes the validated requirement and embeds it into the organisation's systems, workflows, and assurance structures. Compliance does not end with refinement; it becomes real only when implemented, maintained, and reviewed.

Integration ensures that the validated requirement is reflected in:

- design briefs,
- procurement specifications,
- operational procedures,
- training materials,
- and assurance plans.

This stage also embeds the requirement into governance routines. Decision logs, context assessments, and validation records become part of the audit trail. They give the organisation a defensible narrative explaining why a particular approach was chosen and how it aligns with both compliance intent and operational feasibility.

Where possible, organisations can also use these outputs to support digital assurance, future audits, and continuous improvement cycles, helping security mature over time and respond to changes in risk, technology, or regulation.

Stage Five closes the loop but also starts the next cycle. As contexts shift, requirements may need to be re-validated. The workflow supports this adaptability, ensuring compliance remains active, not static.

5. Context Domains & Drivers

Context is the anchor of the Compliance Companion Model. It ensures that compliance requirements are tested against how the organisation actually functions, not how a standard imagines it. Many compliance failures occur not because the requirement is incorrect, but because it was applied without understanding the environment that must sustain it. Section 5 unpacks that environment.

To make context usable, the playbook divides it into three layers, institutional, operational, and structural. Each layer captures a different part of the organisation's reality. Together, they form a complete picture of the forces that shape whether a protective-security control will succeed, fail, or require adaptation.

Context does not exist to make compliance easier. It exists to make compliance accurate. It reveals why some measures work on some sites and fail on others. It highlights constraints early, before designs are locked in. And it gives practitioners the confidence to adjust a requirement while preserving its intent.

This section explains each layer in depth, showing what it represents, why it matters, and how it influences compliance decisions.

5.1 Institutional Drivers: Understanding the Organisation's Direction of Travel

The institutional layer explains the deeper forces that shape how an organisation thinks, chooses, and prioritises. These forces do not appear on drawings or flowcharts, yet they influence every decision that follows. They set the tone for what is acceptable, what is discouraged, and what is strategically important.

Strategic Intent and Long-Term Direction

Every organisation has a trajectory, digital transformation, expansion, consolidation, public-service mission, or cost efficiency. These strategic choices influence the type of controls that make sense. A company moving aggressively toward automation may favour solutions that minimise human intervention. A public-sector body with transparency commitments may avoid controls perceived as overly intrusive.

Understanding this direction is essential because compliance must support strategy, not work against it. A control that contradicts strategy may never gain momentum, even if technically compliant.

Governance Style and Risk Appetite

Governance varies dramatically: highly centralised organisations demand consistency and documentation, while decentralised ones prioritise autonomy and flexibility. Risk appetite also differs, some teams will tolerate bold, visible measures; others avoid anything that might disrupt operations or reputation.

These cultural governance patterns influence how compliance is interpreted. They determine how strict or flexible implementation must be, how much evidence is required, and how decisions are escalated.

Familiar Systems and Organisational Habits

Organisations rarely start from scratch. They carry existing systems, workflows, platforms, and habits. People naturally trust what they already know. If a control builds on familiar technology or practice, adoption is easier. If it introduces entirely new behaviour, resistance grows.

The institutional layer therefore answers the question:

Does this requirement align with who the organisation is and where it is going?

Understanding this layer prevents solutions that are technically strong but strategically misaligned.

5.2 Operational Context: Understanding How Work Actually Happens

The operational layer addresses the lived reality of the organisation. This is where compliance meets human behaviour, workflow pressures, culture, and day-to-day constraints. No matter what a requirement says, it will ultimately succeed or fail at the point of use.

Movement, Flow, and Activity Patterns

Organisations have characteristic rhythms, peak entry times, shift changes, visitor surges, or continuous 24/7 operations. These patterns define how people move, how quickly they must pass through control points, and how much friction they can tolerate.

Implementing a requirement without understanding flow often leads to bottlenecks, workarounds, and procedural bypasses.

Human Factors and Behaviour

People interact with controls under real conditions: PPE, fatigue, noise, tight schedules, and competing priorities. These conditions shape error rates and compliance reliability. If a measure expects perfect behaviour, it is likely to fail.

Understanding human factors helps practitioners deliver controls that people can realistically follow, not controls that require ideal performance.

Culture, Values, and Perception

Culture profoundly influences how security is received. Some environments embrace visible control measures. Others see them as barriers to openness, trust, or customer experience. Culture affects whether users challenge, comply, or quietly avoid controls.

This layer acknowledges that compliance is not purely technical; it is social.

Mission Priorities and Non-Negotiables

Every organisation has activities that must never be hindered, emergency care, teaching, manufacturing, logistics, guest experience. Security must support these priorities, not impede them.

Compliance must therefore adapt to preserve mission-critical functions.

Resource and Sustainability Constraints

A control may be fully compliant on installation day but collapse after six months if the organisation cannot maintain it. Staffing shortages, limited technical support, or constrained budgets all affect sustainability.

The operational layer answers the question:

Can this requirement be executed reliably by the people who must use it every day?

5.3 Structural Enablers: Understanding What Makes Implementation Possible

The structural layer captures the physical, technical, organisational, and external conditions that constrain or enable implementation. It is where architecture, systems, and stakeholders meet.

Technology Architecture and Interoperability

Compliance often assumes smooth integration, but real organisations host a mix of legacy systems, proprietary platforms, cloud infrastructure, and differing vendor ecosystems. A requirement that depends on integration may fail if the architecture cannot support it.

Understanding these technical realities avoids designing controls that cannot be delivered.

Infrastructure, Estate, and Physical Constraints

Older buildings, heritage restrictions, limited cabling routes, lighting challenges, or shared tenancy arrangements create physical limits that compliance must respect.

Architecture shapes feasibility long before procurement.

Governance, Stakeholder Networks, and Organisational Interfaces

Many security measures require cooperation: IT, Facilities, HR, Legal, union groups, shared tenants, landlords, regulators, or community bodies. Each carries its own priorities and constraints.

Implementation succeeds when these stakeholders are understood early, not discovered late.

Community, Social, and External Environment

Security measures interact with the outside world, public expectations, media sensitivity, cultural norms, political climate, and local sentiment. These external forces influence viability, particularly for visible or intrusive measures.

The structural layer answers the question:

Is the organisation structurally capable of supporting this requirement in a reliable and compliant way?

5.4 How the Three Layers Work Together

The three layers are not independent; they interact continuously. A requirement may be aligned with strategy (institutional) but fail operationally due to human factors, or be operationally sound but blocked by infrastructure or legal constraints.

The layers provide a complete map of influences:

- The institutional layer explains why decisions make sense.
- The operational layer explains how work really happens.
- The structural layer explains what is technically and physically possible.

When a requirement is examined across all three layers, its feasibility can be understood with clarity, and refinements can be justified transparently.

This interplay is what makes the Compliance Companion approach rigorous and defensible.

5.5 Why Context Must Be Documented

Documenting context is not an administrative burden, it is a core assurance activity. It provides:

- transparency in decision-making,
- evidence for audits and governance boards,
- protection when incidents occur,
- consistency across regions and teams,
- and a reusable knowledge base for future designs.

Context captures the reasoning that frameworks leave unsaid. It makes compliance decisions human, grounded, and realistic.

6. Tools, Templates & Checklists

The Compliance Companion relies on a small set of tools to support each stage of the workflow. These tools ensure that compliance decisions are structured, transparent, and repeatable across different sites and teams. They provide a common method for capturing context, testing requirements, refining solutions, and recording decisions in a way that can withstand governance and audit scrutiny.

To keep the main body of this playbook focused on methodology, the tools themselves are presented in full in the Annexures. Section 6 describes the purpose and intended use of each tool so practitioners understand how they fit into the overall process before applying them.

6.1 Context Profile

The Context Profile is the starting point for all compliance interpretation. It captures the strategic, operational, and structural conditions that shape whether a requirement can be implemented successfully. The profile brings together the facts that matter most: organisational priorities, user behaviour, movement patterns, cultural expectations, technical limitations, and site-specific constraints.

Its purpose is simple:

To provide a clear, shared understanding of the environment so compliance requirements can be interpreted accurately.

The full, practitioner-ready template is provided in Annexure A.

6.2 Fit Testing Matrix

The Fit Testing Matrix provides a structured way to evaluate whether a compliance requirement aligns with the conditions captured in the Context Profile. It highlights where a requirement fits well, where it partially fits, and where it conflicts with operational, institutional, or structural realities.

The intent of the matrix is to make alignment, or misalignment, visible. It avoids ambiguity by recording the reasoning behind each assessment and setting out the implications of leaving a requirement unchanged. This tool ensures that feasibility is tested systematically rather than informally.

The full matrix is available in Annexure B.

6.3 Requirement Refinement Log

Where the Fit Testing Matrix identifies misalignment, the Requirement Refinement Log records how the requirement is adapted to maintain its protective purpose while ensuring the organisation can deliver it in practice.

The purpose of the log is to document the refinement process clearly and consistently. It captures the original requirement, the issue encountered, the adapted requirement, and the rationale behind the change. It also notes any dependencies, such as training, system upgrades, or governance conditions, required for the refined measure to succeed.

The template is provided in Annexure C.

6.4 Decision Log

Adapted requirements must be approved formally. The Decision Log records this governance step. It provides a simple, consistent format for noting who approved the refinement, when the decision was made, and any associated risk acceptance or conditions.

The intent of the Decision Log is to ensure compliance adaptations remain accountable. It provides a traceable record for governance boards, auditors, and regulators, demonstrating that changes were deliberate and aligned with the organisation's authority structure.

The full Decision Log is included in Annexure D.

6.5 Learning Log

The Learning Log supports continuous improvement. It captures insights from each project, highlighting recurring friction points, successful adaptations, or systemic issues observed across different sites.

Its purpose is to build a long-term understanding of how compliance performs in practice. This allows future designs and governance decisions to benefit from accumulated evidence rather than relying on isolated experience.

The Learning Log template is provided in Annexure E.

6.6 How the Tools Connect

Each tool supports a specific stage of the workflow, but their value is highest when used together.

- The Context Profile defines the environment.
- The Fit Testing Matrix checks each requirement against that environment.
- The Requirement Refinement Log records adjustments that preserve compliance intent.
- The Decision Log provides governance approval.
- The Learning Log feeds insights into future decisions and organisational improvement.

This system creates a consistent chain from interpretation to assurance. It gives practitioners a clear pathway for turning compliance obligations into practical, defensible controls.

7. Embedding the Compliance Companion

Embedding the Compliance Companion means turning the method from a standalone workflow into a core organisational practice. When embedded well, the Companion strengthens governance, improves assurance, builds capability, and helps the organisation mature in how it understands and applies compliance. This section explains how these elements connect and how they support long-term, sustainable use of the model.

Embedding is not a one-time action. It is a gradual process where the method first proves its value on individual projects and then becomes the accepted way of interpreting and applying compliance across the organisation. The purpose of this section is to show how this transition happens and what conditions support it.

7.1 Adoption: Moving From Local Use to Organisational Practice

Adoption usually begins in small steps. Teams apply the workflow to a single project, review, or site assessment and quickly see the benefits: clearer reasoning, better fit between compliance and reality, and reduced friction during design or audit. This early success creates the internal confidence needed to use the method more widely.

As projects build momentum, the Companion becomes part of programmes, initiatives, and risk processes. Teams begin to treat the Context Profile, Fit Testing, and refinement activities as standard practice rather than optional steps. Over time, these activities become familiar, expected, and increasingly normalised.

The final stage of adoption occurs when the organisation incorporates the method into policy, design standards, assurance frameworks, or governance documentation. At this point, the Companion becomes part of “how the organisation works” rather than something applied by individuals.

7.2 Governance: Establishing Authority and Clarity

For the Companion to function consistently, the organisation needs clear governance structures. This ensures that decisions made during refinement are authorised correctly and that responsibilities are well understood.

Governance provides clarity in three areas.

First, it establishes ownership. Security or risk teams typically lead the workflow, but approval for refined requirements often rests with operational leaders or governance boards. This distinction ensures that decisions remain aligned with business priorities.

Second, governance clarifies accountability. Refining a requirement affects compliance exposure and operational outcomes. Decision-makers must understand and accept these implications.

Third, governance integrates the Companion into organisational decision pathways. When governance bodies routinely review refined requirements and decision records, the method becomes part of formal oversight and not an informal or isolated process.

Strong governance gives the Companion legitimacy. It ensures that refinements are not merely practical but defensible and aligned with organisational authority.

7.3 Assurance: Making Compliance Transparent and Verifiable

Embedding the Companion into assurance processes ensures that compliance is visible, traceable, and supported by evidence. It also strengthens the organisation's ability to defend decisions during audits, inspections, or regulatory engagement.

Design assurance benefits from the Companion by verifying that feasibility has been tested before systems are procured or constructed. Fit Testing and refinement outputs show that compliance has been considered at the right time with the right information. Operational assurance benefits because auditors can assess controls against validated requirements instead of assumptions, leading to fairer, more accurate evaluations.

The method also supports procurement and vendor assurance. Validated requirements help suppliers understand what is needed and why, reducing mismatches between proposals and operational needs. When changes occur, whether through incidents, staffing shifts, or technology upgrades, the Companion provides a structured way to re-validate assumptions, ensuring controls remain aligned with reality over time.

Assurance makes the Companion transparent. It shows that compliance decisions were deliberate, structured, and grounded in documented reasoning.

7.4 Capability: Building the Skills That Sustain the Method

Embedding the Companion requires more than tools and processes; it requires people who understand how to use them. Capability must be developed across leadership, practitioners, designers, and operational managers.

Strategic leaders need to understand why structured compliance interpretation strengthens governance and reduces risk. Their support gives the Companion authority and ensures it receives attention at senior levels. Practitioners require deeper knowledge: how to assess context, test fit, refine requirements, and document decisions to a high standard. Their competence ensures the method is applied consistently and effectively.

Design and engineering teams must understand how validated requirements shape technical choices, system integration, and physical layouts. Operational managers contribute essential context insight and must understand how their environment affects compliance feasibility.

Building capability across these groups ensures the Companion does not rely on a single champion or specialist. Instead, it becomes a shared organisational method.

7.5 Maturity: Developing a Stable, Repeatable Organisational Approach

Maturity occurs when the Companion becomes part of the organisation's DNA. This is not achieved through enforcement alone but through repeated use, shared learning, and alignment with governance and assurance.

Maturity becomes visible when teams instinctively use the Context Profile and Fit Testing steps at the start of projects. It grows when insights from Learning Logs influence policy updates, design improvements, or procurement choices. It becomes stronger when decision-makers expect to see refinement logic and

justification as part of governance packs.

A mature organisation also re-validates compliance when conditions change. This prevents outdated assumptions from weakening controls. Maturity is therefore the point where compliance interpretation becomes continuous rather than periodic, adaptive rather than fixed.

When these characteristics are present, the Companion functions not as a project tool but as an organisational capability, a repeatable, reliable approach that strengthens decision-making and improves outcomes.

8. Future Integration & Digital Assurance

Protective security is entering a period of rapid technological change. Organisations are moving towards environments where data, automation, and simulation play a larger role in both risk management and compliance. The Compliance Companion is designed to support this shift. By structuring context, documenting reasoning, and capturing lessons over time, the Companion creates the foundation needed for future digital assurance tools and AI-supported decision-making.

This section explains how the method aligns with technological developments, how structured context enables automation, and how organisations can prepare for an assurance landscape that is increasingly data-driven. The goal is not to predict technology, but to ensure that the organisation is positioned to adopt it safely, responsibly, and effectively.

8.1 Structured Context as the Foundation for Automation

Digital assurance depends on structured information. AI systems, automated design checks, and simulation tools require consistent, well-formed data to produce meaningful results. Much of the data needed for automation does not exist in most organisations, or it exists only in narrative form. The Compliance Companion directly addresses this gap.

By using tools such as the Context Profile, Fit Testing Matrix, and Refinement Log, organisations create structured datasets describing operational behaviours, constraints, technology environments, and historical lessons. This structured context can later be integrated into digital systems that support:

- automated compliance validation
- design-stage simulations
- predictive maintenance and incident forecasting
- digital twin modelling
- AI-supported risk assessment

Structured context is the bridge between today's compliance practice and tomorrow's digital assurance capability.

8.2 AI-Supported Interpretation: Augmenting, Not Replacing, Human Judgement

AI has the potential to support compliance interpretation, but only if the organisation understands its limitations. AI can recognise patterns, compare past cases, highlight inconsistencies, and suggest alternative approaches. It cannot understand intent, apply legal precedence, or replace risk judgement.

When paired with the Companion's structured outputs, AI can support practitioners by:

- flagging recurring context-requirement conflicts
- identifying past refinements that resolved similar issues
- checking requirements for internal consistency
- reviewing design documents for obvious compliance mismatches
- providing early warnings where context changes affect compliance

This assistance improves consistency and reduces the cognitive load on practitioners. However, final decisions must remain in human hands. AI acts as a guide, not a substitute for informed professional judgement.

8.3 Digital Twins: Testing Compliance Before Implementation

Digital twins allow organisations to model movement, behaviour, and system performance in virtual space. While still developing, they already offer significant potential for compliance.

Digital twins can help testers:

- simulate user flow and identify bottlenecks
- test how controls perform during peak traffic
- visualise sightlines for surveillance planning
- assess the impact of new layouts on access control
- experiment with different control combinations before deployment

The Compliance Companion strengthens the usefulness of digital twins by providing the contextual detail needed to make simulations realistic. Without context, simulations become abstract. With context, simulations become decision-support tools that improve accuracy, reduce rework, and validate feasibility early.

8.4 Automated Compliance Checking: Strengthening Design Assurance

As organisations digitise drawings, asset registers, and design documents, automated compliance checking becomes more practical. AI and rule-based systems can compare design elements against validated requirements, identifying:

- missing controls
- incorrect placements
- overlooked constraints
- conflicts between compliance expectations and technical design
- deviations from approved refined requirements

This capability does not remove the need for human review, but it significantly improves design assurance by catching predictable issues early. Automated checks work best when the organisation already uses validated, refined requirements something the Companion delivers by default.

8.5 Predictive Compliance: Anticipating Challenges Before They Develop

Predictive models use historical patterns to forecast where compliance is likely to fail. When informed by Learning Logs and context data, predictive compliance tools can:

- warn when staffing changes increase the risk of procedural breakdowns
- identify environments where specific controls repeatedly struggle
- forecast maintenance demand for certain technologies

- highlight early signals of cultural resistance
- suggest alternative control strategies for high-risk contexts

These insights help practitioners act before issues emerge rather than reacting after controls fail or audits identify deficiencies.

Predictive compliance is only possible when the organisation has structured historical data, another output the Companion naturally produces.

8.6 Preparing the Organisation for Digital Assurance

Future integration requires more than technology. It requires the organisation to adopt practices that support trustworthy automation. This includes:

Clear Data Ownership

Teams must know who maintains the context data, how it is updated, and how changes are authorised.

Governance for Automation

Digital assurance tools must be subject to oversight to ensure they remain aligned with legal, ethical, and operational expectations.

Technical Integration

Digital tools must integrate with existing system architecture rather than operate in isolation.

Training and Capability

Staff must understand how to interpret outputs from AI or simulations and how to question them appropriately.

By preparing these foundational elements, organisations avoid common pitfalls, such as unverified automation, overreliance on AI outputs, or fragmentation between digital and operational practices.

8.7 The Ethical Dimension: Transparency, Fairness, and Trust

As organisations adopt automated and AI-supported tools, new ethical considerations arise. The Companion supports responsible use by promoting transparency, structured reasoning, and documented decision-making.

These principles ensure that:

- AI does not make decisions without human oversight
- automated insights are reviewed through the lens of operational reality
- privacy and data-protection obligations are respected
- compliance remains aligned with legal and human expectations
- users understand how decisions were made

Ethical clarity strengthens trust between practitioners, governance bodies, and the people affected by security measures.

9. Terminology & Glossary

A compliance playbook relies on consistent language. Different standards, industries, and organisations often use the same terms differently, creating confusion or inconsistent interpretation. This glossary provides clear definitions for the key terms used throughout the Compliance Companion. Each term is defined in plain English and linked to how it is used within this document.

Term	Definition
10.1 Core Compliance Terms	10.1 Core Compliance Terms
Requirement	A statement within a law, standard, framework, or internal policy that sets out what must be achieved. In this playbook, requirements express protective intent, not fixed technical solutions.
Compliance	The act of meeting, sustaining, and demonstrating alignment with a requirement. Compliance is both an outcome (meeting the requirement) and a process (ensuring ongoing alignment).
Intent	The protective purpose behind a requirement, what it is trying to achieve rather than how it is worded. Intent guides refinement and prevents rigid interpretation.
Adaptation / Refinement	Any change made to a requirement's mechanism of delivery to ensure it fits organisational reality while preserving compliance intent.
Fit Testing	The structured process of evaluating how well a requirement aligns with the organisation's strategic, operational, and structural context.
Validation	The point at which a requirement has been assessed, refined if necessary, and accepted as workable and compliant within the environment.
10.2 Context Terms	10.2 Context Terms
Institutional Context	The strategic direction, governance expectations, priorities, and organisational habits that shape decision-making.
Operational Context	The behaviours, workflows, culture, staffing patterns, human factors, and activity rhythms that determine how people interact with controls.
Structural Context	The systems, infrastructure, technology, facility constraints, and stakeholder arrangements that enable or limit implementation.
Context Profile	A structured summary of the environmental factors that influence compliance feasibility.
10.3 Governance and Assurance Terms	10.3 Governance and Assurance Terms
Governance	The organisational structures, decision pathways, and authority levels that guide how compliance decisions are made, approved, and monitored.
Assurance	The processes that verify compliance has been applied correctly, including design reviews, audits, and operational assessments.
Risk Owner	The role or function responsible for accepting the risk associated with a compliance decision or refinement.
Approval (Governance Approval)	Formal acceptance of a refined requirement, documented within the Decision Log.
Oversight	Monitoring conducted by governance bodies to ensure compliance decisions remain aligned with organisational expectations.
10.4 Tools and Workflow Terms	10.4 Tools and Workflow Terms
Context Profile (Tool)	The foundational tool used to capture the strategic, operational, and structural factors relevant to a site or system.
Fit Testing Matrix (Tool)	The tool used to assess the alignment between a requirement and the context profile.
Requirement Refinement Log (Tool)	The tool used to record modifications to a requirement while maintaining intent.
Decision Log (Tool)	The tool used to record governance approval for refinements or adaptations.
Learning Log (Tool)	The tool used to capture insights and recurring issues observable across multiple projects or assessments.

Term	Definition
Compliance Workflow	The five-stage process used throughout the Companion to turn written requirements into validated, workable controls.
10.5 Digital and Future-Focused Terms	10.5 Digital and Future-Focused Terms
Digital Assurance	The use of data-driven tools, automation, simulation, or AI to support design reviews, audits, and compliance monitoring.
AI-Supported Interpretation	The use of machine intelligence to highlight patterns, identify conflicts, or assist with compliance reasoning, without replacing human judgement.
Predictive Compliance	Forecasting compliance challenges based on historical patterns and structured context data.
Digital Twin	A digital or virtual model of a site, system, or environment used to simulate user behaviour, system performance, or control interactions in a controlled space.
10.6 Cross-Domain Terms	10.6 Cross-Domain Terms
Health & Safety Requirements	Obligations derived from safety legislation, emergency planning, or duty-of-care frameworks that often limit or shape security controls.
Privacy / Data Protection	Rules governing the capture, storage, and use of personal data, including surveillance and biometric data.
Licensing Conditions	Mandatory requirements placed on certain types of premises or operations by regulators or authorities.
Accessibility Requirements	Standards or regulations ensuring all users, including those with disabilities, can safely use facilities and systems.

Annexure A: Context Profile Template

Instructions:

Complete this profile before Fit Testing. Capture only the information relevant to the compliance requirements being examined. Use evidence where possible.

Context Layer	Domain	Key Information (Short Statements)	Evidence Source	Relevance (H/M/L)	Notes for Fit Testing
Institutional	Strategy & Direction				
Institutional	Governance & Risk Appetite				
Institutional	Organisational Habits & Familiar Systems				
Operational	Movement & Workflow Patterns				
Operational	Human Factors (PPE, task load, user needs)				
Operational	Culture & Values				
Structural	Technology Architecture & Integration Limits				
Structural	Facilities & Physical Constraints				
Structural	Stakeholder Complexity (internal/external)				

Example Row

Operational → Human Factors → “PPE worn at all times in clean zone” → SOP 4.7 → High → “Biometrics likely to fail.”

Annexure B: Fit Testing Matrix

Instructions:

Use one row per requirement. Base all assessments on evidence captured in the Context Profile.

Fit Rating Key

Fit Good fit

Partial Partial fit (minor adaptation needed)

Unfit Poor fit (will not work without refinement)

Requirement ID	Requirement Text	Context Domain	Fit Rating (Fit / Partial / Unfit)	Reason (Context Evidence)	Impact if Unchanged	Suggested Adaptation

Example Row

R-03 → “Fingerprint access must be used for Lab A” → Human Factors → Unfit → “Glove use blocks sensors” → “Frequent override required” → “Contactless dual-factor access.”

Annexure C: Requirement Refinement Log

Instructions:

Record each refinement clearly. Aim for factual, concise entries. Document dependencies (training, technology, agreements).

Requirement ID	Original Requirement	Issue Identified	Revised Requirement	Justification (Intent Preserved)	Dependencies / Notes

Example Row

R-03 → “Fingerprint access for labs” → “PPE blocks biometrics” → “Card + PIN” → “Maintains authentication intent; reliable with PPE” → “Upgrade cards to smart type.”

Annexure D: Decision Log

Instructions:

Use to record governance approval for all refined requirements. Log only the approved decision, not discussion.

Decision ID	Linked Requirement	Decision Summary	Approved By	Date	Notes / Risk Acceptance

Example Row

D-05 → R-03 → “Approve dual-factor alternative for Labs” → Risk Owner (Operations) → 12/04/2025 → “Residual risk negligible.”

Annexure E: Learning Log

Instructions:

Capture insights after each project or review. Focus on recurring issues, effective adaptations, and systemic patterns.

Lesson ID	Issue Identified	Context Trigger	Outcome Observed	Recommendation	Recorded By	Date

Example Row

L-02 → “Biometrics fail in PPE environments” → “Three PPE sites” → “High bypassing rate” → “Use contactless authentication for PPE areas” → Site Manager → 18/06/2025.

Contact and Continuation

This playbook is part of a broader effort to make good security decision-making more accessible. It is intentionally shared freely to encourage discussion, challenge established practice, and support practitioners who operate under real-world constraints.

If this material has been useful, or if it has prompted disagreement or questions, further conversation is welcomed.

Related Work

Additional playbooks and material will be released periodically, each addressing a specific aspect of security decision-making. The writing behind this playbook lives at adriaanbosch.net.

Licence

Author

Adriaan Bosch

Physical Security Strategist

Contact

https://adriaanbosch.net

https://www.linkedin.com/in/adriaanbosch/