**YAKAMICHI** INTELLIGENCE CENTRE

PLAYBOOK 03

# Executive Protection & Counter-Surveillance

A risk-led operating playbook for protecting executives, sensitive environments, information and strategic activity.

| ASSESS | PREVENT | PROTECT | DETECT | RESPOND |
|---|---|---|---|---|
| **Threat & exposure** | Reduce vulnerability | People & places | Anomalies & compromise | Escalate safely |

**EXECUTIVE PURPOSE**

Integrate executive protection, travel security, information protection and lawful counter-surveillance into one governance model focused on consequence, discretion and continuity.

YAKAMICHI PERSPECTIVE

**Protection is strongest when intelligence, physical security, cyber hygiene and executive behavior reinforce one another.**

# Contents & Operating Principles



### SCOPE & SAFETY

This playbook is defensive. Counter-surveillance activities should be lawful, authorized, proportionate and conducted by qualified professionals. It does not provide instructions for covert interception, evading law enforcement or defeating legitimate security controls.

# Executive Protection Governance & Risk

Executive protection is an enterprise risk discipline, not simply close protection. It protects people whose compromise, injury, coercion, disappearance or information exposure could create disproportionate consequences for the organization.

| ROLE | ACCOUNTABILITY |
|---|---|
| **Board / Executive Sponsor** | Risk appetite, material threats and program oversight |
| **Security Leader** | Protection strategy, standards, escalation and coordination |
| **Executive / Principal** | Compliance with agreed protective measures and reporting |
| **Protective Intelligence** | Threat monitoring, assessment and warning |
| **Cyber / IT** | Digital identity, device and account protection |
| **Facilities / Travel** | Physical environments, transport and logistics |
| **Legal / HR** | Authority, privacy, employment and incident considerations |

- Define who qualifies for enhanced protection and why.
- Use risk-based measures rather than status-based convenience.
- Protect executive privacy while preserving necessary security visibility.
- Coordinate physical, cyber, travel and information controls.
- Review protection after material changes in role, threat or exposure.

**GOVERNANCE RULE**

The goal is proportionate protection. Excessive measures can impair business and privacy; inadequate measures can leave predictable vulnerabilities.

# Threat, Vulnerability & Exposure Assessment

Protection begins with a structured assessment of credible threats, vulnerabilities, exposure and consequence. Assessments should distinguish evidence from assumption and be refreshed when conditions change.

| DIMENSION | EXAMPLES |
|---|---|
| **Threat** | Targeted harassment, crime, hostile interest, protest, insider concern, stalking |
| **Vulnerability** | Predictable routines, weak access control, exposed personal data, insecure travel |
| **Exposure** | Public profile, transactions, disputes, sensitive negotiations, geopolitical activity |
| **Consequence** | Safety, coercion, confidential information, continuity, reputation |
| **Controls** | Protective staffing, access, cyber controls, travel measures, monitoring |

## Risk Triggers

- New executive appointment or increased public profile.
- Major transaction, restructuring, litigation or contentious decision.
- Travel to a materially higher-risk location.
- Credible threatening communication or suspicious approach.
- Personal information leak, account compromise or doxxing.
- Repeated unexplained anomalies around residence, office or travel.

**ASSESSMENT PRINCIPLE**

Avoid converting unusual behavior into certainty. Record observations, corroborate facts and escalate according to risk rather than speculation.

# Protective Intelligence & Early Warning

Protective intelligence helps leadership recognize relevant changes early. It combines lawful information gathering, internal reporting and structured assessment to identify credible risks to protected people and activities.

| INPUT | PURPOSE |
|---|---|
| **Open-source information** | Identify public threats, exposure and contextual change |
| **Internal reporting** | Capture concerning contacts, anomalies and incidents |
| **Travel / geopolitical intelligence** | Understand location-specific risk |
| **Cyber telemetry** | Detect account compromise and identity exposure |
| **Security observations** | Identify repeated access or environmental concerns |
| **Executive reporting** | Capture direct approaches, harassment or unusual contact |

## Assessment Output

- What happened and what is verified?
- Why might it matter to the protected person or organization?
- What alternative explanations remain plausible?
- What is the assessed level of concern and confidence?
- What protective action, if any, is proportionate now?
- Which indicators would justify escalation or de-escalation?

**INTELLIGENCE DISCIPLINE**

Protective intelligence should reduce uncertainty, not amplify fear. Separate facts, judgments, confidence and information gaps.

# Residence, Office & Venue Security

Protective environments should reduce unauthorized access, preserve privacy, support emergency response and avoid creating unnecessary friction.

| LAYER | CONTROL OBJECTIVE |
|---|---|
| **Perimeter / approach** | Detect and manage unauthorized approach where appropriate |
| **Entry** | Credential visitors, deliveries and service personnel |
| **Interior** | Protect private work, conversations, records and devices |
| **Life safety** | Emergency communications, evacuation and medical response |
| **Information** | Control displays, documents, conferencing and sensitive discussions |
| **Vendors** | Authorize, escort or supervise access according to risk |

## Pre-Event / Venue Review

- Confirm access points, private areas and emergency exits.
- Identify who controls guest, vendor and staff access.
- Protect confidential meeting spaces and executive holding areas.
- Coordinate medical, fire and emergency procedures.
- Establish communication and escalation contacts.
- Review changes on the day rather than relying solely on an earlier plan.

**ENVIRONMENT PRINCIPLE**

Good protective design creates layers. No single receptionist, camera, lock or guard should carry the entire burden.

# Travel, Movement & Event Protection

Travel changes exposure. The appropriate level of support should reflect destination risk, executive profile, purpose of travel, local conditions and ability to obtain reliable assistance.

| PHASE | CONTROL |
|---|---|
| **Pre-travel** | Risk assessment, itinerary governance, contacts, medical and communications |
| **Transport** | Vetted arrangements appropriate to local risk and business need |
| **Accommodation** | Location, access, privacy and emergency considerations |
| **Meetings** | Venue, attendee, information and transport coordination |
| **Movement** | Avoid unnecessary public disclosure of live itinerary |
| **Contingency** | Alternate transport, communications and emergency assistance |

## Travel Escalation Indicators

- Rapid deterioration in local security or civil conditions.
- Credible threat connected to traveler, employer or event.
- Loss of communications, documentation or critical device.
- Unexpected itinerary exposure or unauthorized disclosure.
- Medical emergency, detention, major transport disruption or natural hazard.

**TRAVEL PRINCIPLE**

Security should preserve business flexibility. Plans need alternatives, not brittle schedules that fail when one assumption changes.

# Executive Digital & Information Exposure

Physical protection and digital exposure increasingly converge. Public records, social media, compromised accounts and device data can reveal relationships, routines, travel and sensitive organizational activity.

| AREA | PROTECTIVE MEASURE |
|---|---|
| **Accounts** | Strong authentication, recovery protection and compromise monitoring |
| **Devices** | Managed security, encryption, updates and remote-loss procedures |
| **Personal data** | Reduce unnecessary public exposure and data-broker footprint where lawful |
| **Social media** | Avoid real-time disclosure of sensitive movement or private locations |
| **Communications** | Use approved channels for sensitive business information |
| **Family / staff** | Provide proportionate awareness where their exposure affects executive risk |

## Executive Hygiene

- Use separate business and personal identities where appropriate.
- Treat unexpected credential, payment and urgent-contact requests as verification events.
- Report lost devices and suspicious account activity immediately.
- Avoid posting sensitive travel or location details in real time.
- Review who can access calendars, travel plans and contact data.

**CONVERGENCE PRINCIPLE**

An executive's digital footprint can become a map of physical routines. Information protection is therefore part of personal protection.

# TSCM Governance & Technical Security Inspections

Technical Surveillance Counter-Measures (TSCM) is a specialized defensive discipline used to assess sensitive environments for unauthorized surveillance risks. Engagements should be authorized, legally reviewed where necessary and performed by qualified personnel.

| STAGE | GOVERNANCE REQUIREMENT |
|---|---|
| **Authorization** | Written scope, responsible client authority and lawful access |
| **Risk definition** | Why the inspection is required and what areas/assets are in scope |
| **Provider assurance** | Competence, confidentiality, equipment governance and conflicts |
| **Site control** | Coordinate access without unnecessarily advertising sensitive details |
| **Findings** | Document observations, confidence, limitations and remediation |
| **Evidence** | Preserve potential evidence and escalate suspected unlawful devices appropriately |
| **Follow-up** | Remediate vulnerabilities and define conditions for reassessment |

## When to Consider a Professional TSCM Review

- Before or after highly sensitive meetings or transactions where risk justifies it.
- Following credible evidence of unauthorized surveillance or unexplained technical anomalies.
- After uncontrolled construction, renovation or third-party access to sensitive areas.
- When an executive office, boardroom or other sensitive environment changes materially.
- As part of a proportionate assurance program for exceptionally sensitive facilities.

**TSCM PRINCIPLE**

A technical inspection is not a substitute for access control, cyber security or information discipline. It is one layer in a broader protective system.

# Insider, Vendor & Sensitive Meeting Risk

Sensitive activity often depends on employees, contractors, advisers, cleaners, maintenance personnel, event staff and technology providers. Access should be proportionate to need and consequence.

| RISK | CONTROL |
|---|---|
| **Unnecessary access** | Least privilege and role-based physical/information access |
| **Vendor presence** | Pre-authorization, identity verification and appropriate supervision |
| **Sensitive meetings** | Attendee control, approved conferencing and document handling |
| **Temporary staff** | Defined access duration and return/revocation procedures |
| **Departures** | Prompt credential, device and access revocation |
| **Concerns** | Clear reporting and fair investigation procedures |

## Sensitive Meeting Protocol

- Define the sensitivity of the discussion before choosing controls.
- Limit attendees and distribution to genuine need-to-know.
- Use approved rooms, devices and conferencing services.
- Control unattended documents, whiteboards and displays.
- Confirm guest/vendor access and room servicing arrangements.
- Record actions and decisions without creating unnecessary sensitive copies.

**INSIDER-RISK PRINCIPLE**

Protective controls should focus on access and behavior, not stereotypes or unsupported suspicion.

# Incident Response, Crisis Coordination & Evidence

Protection incidents can cross physical security, cyber, privacy, legal, HR and law-enforcement boundaries. Escalation should be clear before pressure arrives.

| INCIDENT | IMMEDIATE PRIORITY |
|---|---|
| **Threat / harassment** | Safety, preservation of communications and assessment |
| **Unauthorized access** | Protect people, control area and preserve relevant records |
| **Lost / stolen device** | Personal safety, account/device containment and reporting |
| **Suspected surveillance device** | Do not unnecessarily disturb; secure area and escalate to qualified authority |
| **Travel crisis** | Account for traveler, establish communications and coordinate assistance |
| **Information compromise** | Contain exposure, preserve evidence and assess affected activity |

## Response Principles

- Protect life and immediate safety first.
- Use established emergency services and law enforcement when appropriate.
- Preserve evidence without encouraging unqualified handling.
- Maintain confidentiality and need-to-know.
- Record material decisions, times and accountable owners.
- Review protective measures after the incident and close systemic gaps.

**EVIDENCE PRINCIPLE**

When suspected criminal or unlawful surveillance activity is involved, preserve the scene and engage appropriate qualified professionals or authorities rather than improvising technical handling.

# 180-Day Executive Protection Program

| WINDOW | PRIORITY | DELIVERABLES |
|---|---|---|
| **0–30 Days** | Governance & baseline | Sponsor, protected-person criteria, threat/exposure baseline, escalation contacts |
| **31–60 Days** | Environment & digital exposure | Office/residence reviews, account/device hardening, information exposure reduction |
| **61–90 Days** | Travel & sensitive activity | Travel standards, venue protocol, sensitive-meeting controls |
| **91–120 Days** | TSCM & vendor assurance | Authorized provider model, inspection governance, vendor access review |
| **121–150 Days** | Exercise response | Threat/travel/information incident tabletop with executives and support teams |
| **151–180 Days** | Institutionalize | Metrics, periodic reassessment, remediation tracking and executive reporting |

## Program Outcomes

- Risk-based protection criteria are documented.
- Executives understand reporting and protective expectations.
- Travel and sensitive meeting protocols are usable.
- Digital and physical exposure are assessed together.
- TSCM is governed as a qualified defensive service.
- Incidents have clear escalation and evidence procedures.
- Material findings are tracked to closure.

**PROGRAM PRINCIPLE**

Executive protection should feel calm, discreet and prepared. The program earns trust by reducing uncertainty without turning ordinary business into permanent crisis mode.

APPENDIX A

# Executive Protection Risk Assessment

| FIELD | RECORD |
|---|---|
| **Protected person / role** | _____ |
| **Business consequence** | Why enhanced protection may be justified |
| **Threat indicators** | Verified concerns and sources |
| **Exposure** | Public profile, travel, transactions, disputes |
| **Vulnerabilities** | Physical, digital, procedural and dependency gaps |
| **Current controls** | Existing protective measures |
| **Risk judgment** | Low / Moderate / High / Critical + confidence |
| **Actions** | Owner, due date and escalation threshold |

APPENDIX B

# Executive Travel Security Checklist

- ☐ Destination and itinerary risk reviewed
- ☐ Emergency and medical contacts confirmed
- ☐ Transport and accommodation arrangements verified
- ☐ Sensitive itinerary distribution minimized
- ☐ Devices/accounts prepared for travel risk
- ☐ Alternate communications available
- ☐ Meeting/venue considerations reviewed
- ☐ Traveler knows escalation contacts
- ☐ Material local changes monitored
- ☐ Post-travel incidents/anomalies reported

APPENDIX C

# Sensitive Meeting Checklist

- ☐ Sensitivity level defined
- ☐ Attendees limited to need-to-know
- ☐ Room/access arrangements appropriate
- ☐ Approved conferencing and devices used
- ☐ Visitor/vendor access understood
- ☐ Documents/displays controlled
- ☐ Whiteboards/materials cleared after meeting
- ☐ Actions and records distributed appropriately
- ☐ Unusual technical/physical concerns reported

APPENDIX D

# TSCM Engagement Governance Record

| FIELD | RECORD |
|---|---|
| **Authorized requester** | Name / role / authority |
| **Reason** | Risk basis for professional inspection |
| **Scope** | Authorized rooms, assets and dates |
| **Provider** | Qualified provider and confidentiality terms |
| **Legal/privacy review** | Required? completed? |
| **Findings classification** | Observation / concern / confirmed issue |
| **Evidence handling** | Responsible authority / professional |
| **Remediation** | Actions, owners and due dates |
| **Reassessment** | Trigger / date |

**IMPORTANT**

This record governs a professional defensive engagement. Technical inspection methods and equipment operation should remain with appropriately trained and authorized specialists.

APPENDIX E

# Incident & Anomaly Reporting Record

| FIELD | DETAIL |
|---|---|
| **Date / time** | _____ |
| **Location / context** | _____ |
| **Reporter** | _____ |
| **Observation** | Facts only: what was seen, heard or received |
| **Immediate action** | Safety / access / account / area measures |
| **Evidence** | Messages, access records, CCTV or other lawful records preserved |
| **Assessment** | Concern level, confidence and alternatives |
| **Escalation** | Security / legal / HR / authorities as appropriate |
| **Follow-up** | Owner and review date |

# Executive Protection Maturity Model & Checklist

| LEVEL | CHARACTERISTICS | EXECUTIVE MEANING |
|---|---|---|
| **1 — Reactive** | Incident-led, fragmented physical/digital protection | Unpredictable response |
| **2 — Developing** | Basic assessments, travel and executive controls | Some coverage, inconsistent integration |
| **3 — Managed** | Risk-led program, intelligence, TSCM governance and exercises | Repeatable protection |
| **4 — Adaptive** | Continuous assessment, integrated intelligence and lessons learned | Protection evolves with exposure |

## Executive Checklist

- ☐ Executive protection governance and sponsor defined
- ☐ Threat/vulnerability assessments refreshed when risk changes
- ☐ Protective intelligence reporting established
- ☐ Office/residence/venue security reviewed proportionately
- ☐ Travel security protocol operating
- ☐ Executive digital exposure addressed
- ☐ TSCM engagements governed and professionally delivered
- ☐ Sensitive meeting and vendor controls established
- ☐ Incident escalation and evidence procedures documented
- ☐ Program exercised and material findings tracked

# Yakamichi Perspective

**Executive protection is not a wall around a person. It is a disciplined system that reduces avoidable exposure, detects meaningful change and gives leaders room to operate with confidence.**

## REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA
Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence