YAKAMICHI INTELLIGENCE CENTRE

EXECUTIVE BRIEFING 11

Technical Surveillance Counter-Measures (TSCM)

An Executive Guide to protecting sensitive conversations, spaces and information from covert technical surveillance.

ASSESS	INSPECT	PROTECT	ASSURE
Understand exposure	Examine environment	Reduce opportunity	Reassess over time

EXECUTIVE PREMISE

The most valuable information in an organization is often spoken before it is written. Strategy meetings, negotiations, investigations, board deliberations and executive conversations can therefore become attractive targets for covert collection. TSCM provides a disciplined way to assess and reduce that exposure.

Executive Summary

Technical Surveillance Counter-Measures is the professional discipline used to identify indicators of unauthorized technical surveillance and to strengthen environments against covert collection. It sits at the intersection of physical security, information protection, technical security and counterintelligence.

Modern exposure is broader than the traditional image of a hidden microphone. Sensitive spaces contain wireless devices, conferencing systems, smart displays, building technologies, mobile phones, networked equipment and third-party infrastructure. Any of these can create unintended collection pathways when poorly governed, compromised or deliberately manipulated.

For executives, TSCM should be risk-led. Not every room requires the same level of assurance. Priority should follow the sensitivity of information, threat profile, travel or event context, recent changes to a space and the consequences of compromise.

When TSCM Becomes Material

- Board meetings, mergers and acquisitions, major negotiations or strategic planning.
- Executive offices and conference rooms where highly sensitive matters are routinely discussed.
- Locations used for investigations, legal strategy, crisis management or regulated information.
- High-risk travel, temporary meeting venues and unfamiliar third-party facilities.
- Following suspicious access, unexplained equipment changes, insider concerns or other credible indicators.

Executive Takeaways

1. Protect conversations	Information security extends beyond digital files and networks.
2. Prioritize by risk	Use threat, sensitivity and consequence to determine assurance level.
3. Control the environment	Access, devices and room governance matter before technical inspection begins.
4. Use qualified specialists	TSCM requires disciplined methodology, appropriate equipment and professional judgment.
5. Treat assurance as recurring	A secure room today is not automatically secure after people, equipment or circumstances change.

The Yakamichi TSCM Assurance Framework

1. Threat & Information Assessment Identify what information requires protection, plausible collection threats and the consequences of compromise.

2. Environmental Baseline Understand the room, adjoining spaces, infrastructure, authorized devices, access history and recent changes.

3. Technical Inspection Conduct a structured professional examination using methods appropriate to the environment and assessed risk.

4. Physical & Procedural Review Examine access control, room use, device practices, housekeeping, contractor activity and other conditions that may create exposure.

5. Findings & Remediation Document anomalies and vulnerabilities, validate findings, prioritize corrective action and preserve confidentiality.

6. Continuing Assurance Reassess after renovations, equipment changes, suspicious events, sensitive milestones or according to an established risk cycle.

Risk-Based Assurance Levels

Level	Typical Context	Executive Approach
1 — Routine	Ordinary internal meetings	Baseline room and device hygiene
2 — Sensitive	Executive, legal or commercial discussions	Periodic professional assurance
3 — High	Transactions, investigations, major negotiations	Enhanced inspection and tighter access controls
4 — Critical	Credible threat or exceptional consequence	Specialist-led, event-specific protective program

What TSCM Is Not

TSCM is not a theatrical 'bug hunt,' a consumer gadget scan or a guarantee that surveillance is impossible. A professional program combines technical examination with environmental knowledge, threat context and procedural controls, then reports findings with appropriate confidence and limitations.

Board and Executive Responsibilities

- Which conversations or locations would create material harm if covertly collected?
- Who decides when a TSCM assessment is required?
- Are executive offices, boardrooms and sensitive meeting spaces governed differently from ordinary rooms?
- How are contractors, cleaners, maintenance personnel and temporary access managed in sensitive spaces?
- What happens to room assurance after renovations, new conferencing equipment or unexplained technical changes?
- Are high-risk travel and off-site meetings included in protective planning?
- Who receives and controls sensitive TSCM findings?

Common Protection Gaps

One-time inspection	Assurance degrades as spaces, equipment and access change.
Device ambiguity	No authoritative baseline of what equipment belongs in a sensitive room.
Access overexposure	Too many staff, contractors or visitors can enter sensitive environments without scrutiny.
Meeting complacency	Phones, wearables, conferencing devices and remote participants are not governed according to information sensitivity.
Poor finding control	Sensitive assessment reports are distributed too broadly, creating a new information risk.

Executive Metrics

Useful measures include percentage of designated sensitive spaces with current assurance, overdue remediation, unauthorized or unexplained equipment changes, sensitive-room access exceptions, high-risk events supported, post-renovation reassessments completed and time taken to resolve material findings.

180-Day Executive Action Plan

0–30 DAYS | Identify sensitive environments

Classify boardrooms, executive offices, negotiation rooms and other locations according to information sensitivity and consequence.

31–60 DAYS | Establish governance

Define TSCM triggers, responsible executives, report handling, access expectations and approved specialist support.

61–90 DAYS | Baseline priority spaces

Document authorized equipment, physical conditions, access patterns and technical infrastructure in the highest-risk locations.

91–120 DAYS | Conduct professional assurance

Perform risk-appropriate TSCM assessments and remediate material vulnerabilities or unexplained anomalies.

121–180 DAYS | Institutionalize protection

Establish recurring assurance cycles, change triggers, high-risk meeting procedures and executive reporting.

Executive Checklist

- ☐ Sensitive spaces identified and classified
- ☐ TSCM governance owner assigned
- ☐ Risk-based inspection triggers documented
- ☐ Authorized room equipment baselined
- ☐ Sensitive-space access controls reviewed
- ☐ High-risk meeting device rules established
- ☐ Qualified TSCM support identified
- ☐ Material findings remediated and tracked
- ☐ Renovation and equipment-change triggers defined
- ☐ TSCM reports restricted to authorized recipients

Yakamichi Perspective

Counter-surveillance begins with a simple recognition: some information is valuable enough that others may try to obtain it before you intend to disclose it.

A mature TSCM program combines professional technical assurance with disciplined access, device and meeting practices. Its purpose is not paranoia. It is proportionate protection of consequential information.

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