



## Covert Weapons Concealment Assessment

Purpose: To evaluate whether frontline screening personnel (e.g., X-ray operators, access control teams, rovers) can detect hidden weapons or deter social-engineering attempts of bypassing screening, and whether proper escalation procedures are followed.

### 1. PREPARATION

Test Focus (select one):

- Knife in bag (flat, visible profile)
- Knife concealed in a book, pouch or interior pocket of property
- Non-metallic weapon (carbon fiber, plastic)
- Weapon taped under common facility rolling equipment. (janitorial cart, dolly, rolling bag, re-stocking cart)
- Social engineering: actor claims “I already cleared security”, “was already in once today”, “I just ran to my car” while bypassing screening.

Assigned Roles:

Red Team (Concealment role): \_\_\_\_\_

Observer: \_\_\_\_\_

Escalation Contact (if detected): \_\_\_\_\_

Screening Location: \_\_\_\_\_

Test Date/Time: \_\_\_\_\_

Equipment Type (X-ray, HHMD, Visual Search, Cursory Search): \_\_\_\_\_

### 2. SCREENING ASSESSMENT LOG

Criteria	Notes
Was the threat object detected?	
How long did it take to detect?	
What raised suspicion (if any)?	
Was the correct escalation triggered?	
Was the property re-screened?	
Was law enforcement or management contacted?	



### 3. POST-ASSESSMENT DEBRIEF

Score	Rating	Interpretation	Recommended Action
5	<b>Exceptional</b>	Response was timely, consistent, and aligned with SOPs. Staff showed high vigilance without prompting.	Use as a model for other teams. Consider peer training or advanced scenario drills.
4	<b>Strong</b>	Minor gaps in timing or communication, but threat was identified and handled effectively.	Reinforce with quarterly refreshers and no-notice testing.
3	<b>Adequate</b>	Threat was detected eventually, but only after missed cues or unclear handoffs.	Conduct targeted retraining and reinforce escalation roles.
2	<b>At Risk</b>	Threat was not identified or was allowed access for a period of time. SOPs were unclear or ignored.	Revisit SOPs, retrain staff, and repeat test within 30 days. Consider Averitas evaluation.
1	<b>Critical Gap</b>	No detection or response. Breach occurred with full access. Personnel unaware or untrained.	Immediate remediation needed. Engage Averitas and initiate full readiness audit.

Category	Score (1-5)	Comments
Threat detection effectiveness		
Escalation timing		
SOP adherence		
Screening consistency		

*Add all lines together and notate score in Section 4.*

Additional Notes:

---



---



---



Recommended Actions:

- Retrain on screening protocol
- Conduct additional covert weapon awareness drills
- Stand down with all guard staff
- Engage Averitas for professional covert testing drills
- Engage Averitas for SOP review and gap analysis
- Engage Averitas for professional covert testing plan

**4. FOLLOW-UP**

Incident logged in internal system? [Yes] / [No]

Feedback loop closed with involved staff? [Yes] / [No]

Next planned covert test date: \_\_\_\_\_

Prepared by: \_\_\_\_\_

Total Score: \_\_\_\_\_

**5. Averitas Readiness Index**

<b>Total Score</b>	<b>Status</b>	<b>Interpretation</b>	<b>Action Recommendation</b>
<b>17–20</b>	<b>Operationally Ready</b>	Systems are performing well under stress. Minor adjustments may improve further.	Continue testing monthly. Use this team as a model.
<b>13–16</b>	<b>Moderate Risk</b>	Gaps exist under real-world conditions. Response may be delayed or inconsistent.	Reinforce weak points. Schedule next covert test in 14 days.
<b>9–12</b>	<b>High Risk</b>	Teams are struggling with execution, awareness, or consistency.	Immediate retraining and SOP reinforcement recommended. Highly encouraged to consult Averitas.
<b>4–8</b>	<b>Critical Breakdown</b>	Threats go undetected. No trust in current response posture.	Engage Averitas immediately for full readiness audit.