

Organization Name: _____
 Date and Time: _____ Initial Verification: ☐ Follow-Up Verification: ☐
 Evaluated Geographic Area: _____
 Responsible Analyst: _____

Instructions: Review each item below and check the corresponding box if the situation applies. If it does not apply to your case, mark "N/A." Provide additional observations in the corresponding fields if necessary.

Once all items have been reviewed, total the number of "Yes," "No," and "N/A" responses. Place the sum for each category at the end of the section.

DEFICIENCIES IN THE SECURITY OPERATIONS MANAGEMENT SYSTEM (SOMS)

Security Operations Management System" (SOMS)

LEADERSHIP AND STRATEGY		YES NO N/A	Observations
1. The management has clearly defined in writing what its EPRM policy is and acts consistently with it on a daily basis ...			
1	Defines the general principles, intent, and overall objectives of EPRM.	☐ ☐ ☐	_____
2	The management assumes its responsibility in EPRM, understanding it as part of business continuity and emphasizing its importance in the organization's operations.	☐ ☐ ☐	_____
2. The CRIIRM policy			
3	Is appropriate for the context, needs, and resources of the organization.	☐ ☐ ☐	_____
4	Includes strict compliance with relevant legislation, standards, commitments, and codes of conduct.	☐ ☐ ☐	_____
5	Contains a commitment to continuous improvement.	☐ ☐ ☐	_____
6	Establishes principles for the risk assessment process for CRI, taking into consideration (or establishing) risk criteria for CRI in the organization.	☐ ☐ ☐	_____

7	It is fully aligned with the organization's policies on quality, risk management, business continuity, safety and health, travel management, sustainability, etc.	☐ ☐ ☐	
8	It establishes levels of responsibility within the organization for specific activities or with third parties, when relevant.	☐ ☐ ☐	
3. The roles, functions, responsibilities, competencies, relationships, and accountability of all relevant parties involved in EPRM have been defined and assigned. In practice ...			
9	No interference or overlap (operational or administrative responsibilities) has been detected.	☐ ☐ ☐	
10	Each individual is provided with adequate and sufficient means (including training) to perform within the system.	☐ ☐ ☐	
TOTAL			

WORK ORGANIZATION	YES NO N/A	Observations
-------------------	----------------	--------------

1. In the company, there is strategic-level planning that ...

11	Establishes plans to achieve strategic objectives and indicators to measure their compliance.	☐ ☐ ☐	
12	Is carried out with the participation of management, senior personnel most closely involved in the reviewed aspects, and relevant stakeholders.	☐ ☐ ☐	

2. The EPRM strategic planning is periodically reviewed and controlled. This review ...

13	Is conducted with the participation of management, senior personnel with the most relevant expertise, and those working on the planning,	☐ ☐ ☐	
----	--	--	--

alongside relevant stakeholders.

14 Is complemented by an effective system of notifications, control, verification, etc. ☐ | ☐ | ☐ _____

3. Regarding EPRM processes ...

15 ... are represented on a process map, identifying key processes, and assigning a responsible party to each. ☐ | ☐ | ☐ _____

16 ... work teams are structured based on processes rather than a purely functional division by departments, areas, etc. ☐ | ☐ | ☐ _____

17 ... a role analysis has been conducted, considering each individual's contributions to the final results of the process, including job mobility. ☐ | ☐ | ☐ _____

4. The standard operational procedures ...

18 ... are consistent with the threat level, the methods used, and the capabilities of the personnel involved in protection. ☐ | ☐ | ☐ _____

19 ... are approved, reviewed periodically, and made available. ☐ | ☐ | ☐ _____

20 ... undergo a trial period before being standardized. They are coordinated with the necessary training and oral instructions. ☐ | ☐ | ☐ _____

TOTAL

| |

RELIABILITY	YES NO N/A	Observations
-------------	----------------	--------------

1. Reliability in personnel is ensured through ...

21 Conducting background checks and verifying employment references for all employees before hiring. ☐ | ☐ | ☐ _____

22 Adjusting the scope and depth of verification based on the level of ☐ | ☐ | ☐

access, with critical positions being those with access to protectees, valuable property, or sensitive information.

- 23 Implementing a reliability program for critical roles that includes periodic checks to prevent drug abuse, technical reliability tests (e.g., polygraph or voice stress analysis), lifestyle verification to identify illegal activities (theft, fraud) or personal issues, and regular training updates on confidentiality and identifying indicators of suspicion.

☐ | ☐ | ☐

- 24 Mandatory annual updates for critical roles generally include background checks, home visits, drug screening, and other technical reliability tests.

☐ | ☐ | ☐

2. Sensitive information control is primarily achieved through ...

- 25 Assigning custodians and access levels with the corresponding permissions.

☐ | ☐ | ☐

- 26 Requiring the signing of non-disclosure and non-compete agreements.

☐ | ☐ | ☐

- 27 ... through the use of a secure IT network (encrypted email, encrypted telephony, etc.).

☐ | ☐ | ☐

- 28 ... avoiding the use of personal devices or unsecured networks.

☐ | ☐ | ☐

3. For conflicts involving current personnel within the organization ...

- 29 The company has an anonymous method for reporting unethical/illegal behavior and a procedure for investigating such cases.

☐ | ☐ | ☐

- 30 When it is necessary to terminate an employee, there is a standardized operating procedure for proper termination (e.g., collection of corporate belongings, security interview, signing of a confidentiality agreement, etc.).

☐ | ☐ | ☐

TOTAL

| |

COMPETENCY DEVELOPMENT		YES NO N/A	Observations
1. Security Induction			
31	New employees and contractors receive a security briefing during the induction program.	☐ ☐ ☐	_____
32	Everyone in the organization periodically attends security training sessions (quarterly, annually, or at other intervals).	☐ ☐ ☐	_____
2. Security Training			
33	The training program is organized and implemented according to the risk profile of each position.	☐ ☐ ☐	_____
34	Security policy and procedure training primarily includes practical components.	☐ ☐ ☐	_____
3. In your company, executive trust is fostered because ...			
35	Risks are transparently communicated according to the risk profile of each position.	☐ ☐ ☐	_____
36	Executives directly involved are always consulted regarding their expectations and perceptions of security.	☐ ☐ ☐	_____
4. It can be assured that your organization enjoys ...			
37	... smooth communication about indicators of suspicion, threats, and risks, exemplified by directors and middle management, and expressed through written reports or frequent personal meetings.	☐ ☐ ☐	_____
38	... information systems that facilitate the storage of protective intelligence in databases, including communication with external partners, etc.	☐ ☐ ☐	_____
5. Security information shared through reports, notice boards, and messages in your organization includes, among other topics ...			
39	... foreseeable risk events, self-protection measures, and risks affecting different job profiles.	☐ ☐ ☐	_____

40	... plans, policies, and procedures classified as internal knowledge for all in the organization.	☐ ☐ ☐	
TOTAL			

SELF-PROTECTION CULTURE	YES NO N/A	Observations
-------------------------	----------------	--------------

1. Regarding the positive reinforcement of safe actions ...

41	It is based on written standards aligned with the level of risk.	☐ ☐ ☐	
42	Standards have been initially communicated and updated, including situational reports and procedures.	☐ ☐ ☐	
43	Mediante supervisión del cumplimiento, refuerzo positivo	☐ ☐ ☐	
44	... employees are supported by providing communication channels for their suggestions.	☐ ☐ ☐	
45	... compensations (not only financial) are awarded to recognize positive results and attitudes.	☐ ☐ ☐	

2. Communication of indicators of suspicion and potential threats ...

46	... is included in one or more procedures and protocols.	☐ ☐ ☐	
47	... is encouraged. There is no fear of retaliation and can be positively reinforced when it leads to significant improvements.	☐ ☐ ☐	
48	... is transformed into useful knowledge and/or real actions and is followed up on.	☐ ☐ ☐	

3. Regarding the communication mentioned in the previous requirement, it is true that ...

49	... it is shared and improved by all stakeholders.	☐ ☐ ☐	
50	... it is constantly updated.	☐ ☐ ☐	
TOTAL			

DEFICIENCIES IN THE EXECUTIVE PROTECTION PROGRAM (RPATO)

"Executive Protection Program (EPP)"

RISK MANAGEMENT		YES NO N/A	Observations
1. Understanding the Context and Requirements			
51	Risk management is specific to the company's operational context.	☐ ☐ ☐	_____
52	Risk management considers corporate policies, as well as applicable laws, standards, agreements, and organizational commitments.	☐ ☐ ☐	_____
53	The organization has access to regularly updated situational reports to understand the operational context.	☐ ☐ ☐	_____
2. Risk Assessment			
54	Follows a standardized, replicable, and traceable model, such as the EPRM model.	☐ ☐ ☐	_____
55	Systematic risk assessment is conducted, starting with the context and operations, followed by the evaluation of specific threats and identification of operational vulnerabilities.	☐ ☐ ☐	_____
56	Risk profiles for executives are established according to the probability and impact of assessed risks.	☐ ☐ ☐	_____
57	Risk assessment is updated periodically and whenever there are changes in the context.	☐ ☐ ☐	_____
3. Regarding the actions planned at the tactical level ...			
58	... are based on actual and current risk assessments, aligning with the entity-level planning and risk assessments.	☐ ☐ ☐	_____
59	... clearly define the actions to be taken, specify who is responsible, and establish deadlines for action completion.	☐ ☐ ☐	_____

60 ... the team has participated in its design, incorporating their suggestions and improvement initiatives.

☐ | ☐ | ☐

TOTAL

| |

PROTECTION PROCEDURES

YES | NO |
N/A

Observations

1. Standardized protection procedures exist for operations specific to the following scenarios ...

61 Residence, workplace, travel and transportation, personal activities, and transition areas.

☐ | ☐ | ☐

Compliance with standardized procedures is evaluated through ...

62 Inspections of conditions and observation of individual actions.

☐ | ☐ | ☐

63 Drills and penetration tests (e.g., red teaming exercises).

☐ | ☐ | ☐

3. Plans exist for ...

64 Emergencies associated with each identified risk.

☐ | ☐ | ☐

65 Contingencies for potential escalation of foreseeable events and for unforeseeable events.

☐ | ☐ | ☐

66 All plans are tested periodically through tabletop exercises and coordinated drills.

☐ | ☐ | ☐

4. Investigations are conducted for ...

67 Every qualified threat, with records maintained until it is fully resolved.

☐ | ☐ | ☐

68 Every disruptive event, until causes are identified along with immediate corrective measures and preventive actions.

☐ | ☐ | ☐

5. Reports and documentation include ...

69 ... communication of results and measurement using operational indicators.

☐ | ☐ | ☐

70 ... a short-term improvement plan, as well as a long-term plan that considers outcomes, technical contributions, and best practices from the sector and highly successful organizations.

☐ | ☐ | ☐

TOTAL

| |

PROTECTION TEAM AND EQUIPMENT		YES NO N/A	Observations
1. The selection of protection equipment ...			
71	... is based on standardized competency profiles aligned with international standards or recommendations.	☐ ☐ ☐	
72	... identifies team leaders and members based on reliability tests, knowledge exams, standardized skills assessments, physical fitness evaluations, and proven experience.	☐ ☐ ☐	
73	... ensures each protection team is independent and equipped with sufficient human and material resources for regular, emergent, and contingent operations according to the risk profile of each position.	☐ ☐ ☐	
2. Daily verifications include ...			
74	... the operational readiness of vehicles, communications, and other technology used by the team.	☐ ☐ ☐	
75	... the physical and psychological fitness of personnel through in-person communication with their team leader.	☐ ☐ ☐	
76	... the functionality of data encryption systems and electronic counter-surveillance measures (TSCM).	☐ ☐ ☐	
77	... operational training and communication through daily refreshers of Standard Operating Procedures.	☐ ☐ ☐	
3. In performance evaluations ...			
78	... every new team member is assessed upon joining, and their onboarding includes successfully completing a mentoring and on-the-job training program.	☐ ☐ ☐	

79	... performance evaluations are conducted every six months, with updates to reliability tests, knowledge exams, standardized skills assessments, and physical fitness evaluations.	☐ ☐ ☐	
80	... the evaluation results generate an improvement plan (knowledge, skills, and physical fitness). A second opportunity to pass is provided based on performance and reliability levels close to the expected results.	☐ ☐ ☐	
TOTAL			

TECHNICAL TRAINING OF THE TEAM	YES NO N/A	Observations
1. The technical protection training plan ...		
81	... considers the specific characteristics, context, and risks of the organization.	☐ ☐ ☐
82	... is related to and builds upon previous training processes.	☐ ☐ ☐
2. It can be assured that the training received by the protection team ...		
83	... is periodic, theoretical and practical, timely, and sufficient. It also has the necessary means and resources.	☐ ☐ ☐
84	... includes monitoring of training needs and the effectiveness/impact of previously provided training on knowledge, skills, and attitudes.	☐ ☐ ☐
3. Regarding the incorporation of new protection technologies, the team ...		
85	... receives the necessary theoretical and practical training.	☐ ☐ ☐
86	... demonstrates adaptability in using information to support decision-making within the organization.	☐ ☐ ☐
4. There is no doubt that in your organization ...		
87	... equal treatment and opportunities are provided to all workers.	☐ ☐ ☐

88	... mutual trust fosters collaboration among individuals.	☐ ☐ ☐	
89	... people are considered key to the organization's long-term survival, with an emphasis on their development beyond short-term objectives.	☐ ☐ ☐	
5. In your organization, improvement and learning...			
90	... are practiced at the individual, team, and organizational levels. Senior management is involved in the programs and guides based on opportunities for improvement and innovation, rather than on problems or dissatisfaction to be corrected.	☐ ☐ ☐	
TOTAL			

OPERATIONAL TASKS	YES NO N/A	Observations	
1. Regarding role orders and work instructions, the following is ensured...			
91	... team leaders develop them based on the current risk level and the needs of the protectees.	☐ ☐ ☐	
92	... they are documented and updated whenever necessary.	☐ ☐ ☐	
93	... their drafting is used as a learning opportunity: those involved participate, and others with lesser involvement are informed.	☐ ☐ ☐	
94	... individuals most familiar with the practice of the process in question—operatives themselves—are encouraged to participate in their development.	☐ ☐ ☐	
95	... a procedure exists for the daily communication and updating of orders at each position.	☐ ☐ ☐	
2. Control of operational tasks is based on ...			
96	... a unified command, supervision, and support from the team leader.	☐ ☐ ☐	

97

... constant communication between the operations center and protection team members.

☐

|

☐

|

☐

98

... updates on changes, protective intelligence, and disruptive events, communicated by the leader to each team member and executives.

☐

|

☐

|

☐

99

... systematically documenting both failures and successes to improve future operations.

☐

|

☐

|

☐

100

... el aprendizaje en equipo, sensibilización del peligro, conciencia de riesgos y compromiso de los controles en los que sus funciones se enmarcan.

☐

|

☐

|

☐

TOTAL

|

|