APPENDIX B - SELF-ASSESSMENT WORKSHEET

ASSESSMENT & SCORING GUIDANCE

For each question, select the value that best represents your organization's current practice.

Score	Description
1 – Emerging	Practices are ad hoc or inconsistently applied. Activities are primarily reactive or compliance-driven.
2 – Developing	Practices are defined and repeatable but not yet strategic. Processes exist, though integration and sustainment vary across teams or systems.
3 – Established	Practices are formalized, sustained, and measured. Outcomes are consistently used to drive improvement and inform tactical, operational, and management decisions.

After completing all questions:

1. Sum the five scores in each section and divide by 5 to find your Section Average.
2. Add all section averages and divide by 4 to find your Overall Average.
3. Use the Overall Average to identify your corresponding ARMOR Level

SELF-ASSESSMENT SCORE

Section	***Worksheet Results***	
Governance & Strategy		
Testing Cadence & Scope		
Remediation & Sustainment		
Integration & Collaboration		
Overall Score (SUM ÷ 4)	*SUM:*	*AVG:*

Resulting ARMOR Level *(circle one)*

Level 1	Level 2	Level 3	Level 4	Level 5
Ad-Hoc	Repeatable	Managed	Optimized	Resilient
(1.0 – 1.4)	(1.5 – 2.0)	(2.1 – 2.4)	(2.5 – 2.8)	(2.9 – 3.0)

SECTION 1 – GOVERNANCE & STRATEGY

#	QUESTION	1	2	3
1	Does the organization have a documented risk-aligned offensive security strategy?	☐	☐	☐
2	Are roles and responsibilities for offensive security clearly defined across the organization?	☐	☐	☐
3	Is leadership regularly briefed on offensive security outcomes and risk implications?	☐	☐	☐
4	Are offensive security results used to inform policy, investment, or strategic decisions?	☐	☐	☐
5	Are threat intelligence and risk context incorporated into planning and prioritization?	☐	☐	☐

Section 1 Total: ____ **Section 1 Average (÷5):** ____

SECTION 2 – TESTING CADENCE & SCOPE

#	QUESTION	1	2	3
6	How consistently are penetration tests or security assessments performed?	☐	☐	☐
7	Does testing include cloud, SaaS, and third-party, and on-prem assets?	☐	☐	☐
8	Are red/purple team exercises conducted to measure detection and response capability?	☐	☐	☐
9	Are test scopes threat-informed (based on adversary behaviors or emerging risks)?	☐	☐	☐
10	Are tabletop exercises or crisis simulations conducted for critical systems and processes?	☐	☐	☐

Section 2 Total: ____ **Section 2 Average (÷5):** ____

SECTION 3 – REMEDIATION & SUSTAINMENT

#	QUESTION	1	2	3
11	Are findings triaged, prioritized, and tracked to resolution within defined SLAs?	☐	☐	☐
12	Is remediation validated through retesting or continuous validation processes?	☐	☐	☐
13	Are recurring or systemic findings analyzed for root causes and process improvement?	☐	☐	☐
14	Are sustainment metrics (e.g., remediation rate, mean time to validate) reviewed regularly?	☐	☐	☐
15	Are remediation and validation processes documented and reviewed for effectiveness?	☐	☐	☐

Section 3 Total: ____ **Section 3 Average (÷5):** ____

SECTION 4 – INTEGRATION & COLLABORATION

#	QUESTION	1	2	3
16	Are offensive security results communicated to defensive and operations teams?	☐	☐	☐
17	Are red/purple team insights used to improve detection and response capabilities?	☐	☐	☐
18	Do business units understand and act on relevant offensive security outcomes?	☐	☐	☐
19	Are results integrated with enterprise risk management reporting and dashboards?	☐	☐	☐
20	Are cross-functional reviews or after-action reports conducted following exercises?	☐	☐	☐

Section 4 Total: ____ **Section 4 Average (÷5):** ____