



12-MONTH PROFESSIONAL PROGRAMME

AI Agents for Business

Month 10: Agent Safety and Security

Design, test and govern business agents that use tools, knowledge and human approval to complete bounded work.

MONTH	LESSONS	QUIZZES	ACTIVITIES
10 / 12	30	30	60

PROGRAMME DATA CHART



Module purpose

Develop professional capability in agent safety and security through strategic analysis, applied labs, quality assurance, risk controls and a portfolio deliverable.

Professional outcomes

- Connect the module to measurable business value and responsible ownership.
- Complete 30 guided lessons and 30 formative knowledge checks.
- Produce practical portfolio evidence using fictional, public or properly authorised information.
- Apply privacy, security, fairness, validation and human-review controls.

Copyright and use

This guide is supplied for the registered learner's personal educational use. The logo, design, curriculum structure and original course text remain the intellectual property of Global Educational Consultants. The visible logo and page watermark identify the source; they cannot technically prevent all unauthorised copying.

30-lesson professional study plan

Month 10 develops agent safety and security from strategy through applied practice, assurance and an actionable module plan.

01	Strategic Context	Connect the topic to a measurable professional outcome
02	Core Concepts	Explain the essential concepts and their practical limits
03	Professional Terminology	Use the vocabulary accurately with stakeholders
04	Capability Map	Distinguish people, process, data and technology capabilities
05	Use-Case Discovery	Identify a valuable and appropriately bounded use case
06	Stakeholder Needs	Analyse users, owners and people affected by the work
07	Workflow Mapping	Map the current process before introducing a
08	Data Readiness	Assess quality, access, provenance and permitted use of data
09	Privacy and Security	Apply proportionate privacy and security controls
10	Prompt and Instruction Design	Create clear instructions, context and output requirements
11	Tool Configuration	Configure a scalable tool without relying on unsafe defaults
12	Structured Outputs	Produce consistent outputs that people and systems can validate
13	Guided Skills Lab	Complete a controlled hands-on exercise
14	Comparative Tool Lab	Compare approaches using consistent success criteria
15	Professional Case Study	Apply the method to a realistic business scenario
16	Quality Rubric	Define accuracy, relevance, clarity and acceptance criteria
17	Validation and Fact-Checking	Verify important claims against dependable evidence
18	Bias and Inclusion Review	Identify unfair outcomes and improve accessibility
19	Failure-Mode Analysis	Test ambiguity, edge cases and predictable breakdowns
20	Risk and Control Design	Match controls to impact, likelihood and reversibility
21	Human Review and Approval	Assign accountable review and escalation decisions
22	Team Collaboration	Coordinate roles, handoffs and shared standards
23	Performance Metrics	Measure quality, time, cost, adoption and outcomes
24	Value and ROI	Build a realistic value case with explicit assumptions
25	Integration Blueprint	Connect the work safely to existing business systems
26	Scenario Simulation	Rehearse normal, difficult and failure scenarios
27	Troubleshooting Clinic	Diagnose weak outputs and improve the underlying design
28	Portfolio Deliverable	Create evidence of professional capability
29	Professional Review	Present the work for structured peer or manager feedback
30	Module Action Plan	Define next steps, ownership and measures for improvement

30 interactive knowledge checks

Choose the most professional answer. An answer key and application guidance follow the questions.

01. What is the strongest professional approach to strategic context in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply strategic context to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

02. What is the strongest professional approach to core concepts in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply core concepts to authorised information, test the result and document accountable human review.

03. What is the strongest professional approach to professional terminology in Agent Safety and Security?

- A. Define the outcome, apply professional terminology to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

04. What is the strongest professional approach to capability map in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply capability map to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

05. What is the strongest professional approach to use-case discovery in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply use-case discovery to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

06. What is the strongest professional approach to stakeholder needs in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply stakeholder needs to authorised information, test the result and document accountable human review.

07. What is the strongest professional approach to workflow mapping in Agent Safety and Security?

- A. Define the outcome, apply workflow mapping to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

08. What is the strongest professional approach to data readiness in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply data readiness to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

09. What is the strongest professional approach to privacy and security in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply privacy and security to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

10. What is the strongest professional approach to prompt and instruction design in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply prompt and instruction design to authorised information, test the result and document accountable human review.

Knowledge checks 11-20

11. What is the strongest professional approach to tool configuration in Agent Safety and Security?

- A. Define the outcome, apply tool configuration to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

12. What is the strongest professional approach to structured outputs in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply structured outputs to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

13. What is the strongest professional approach to guided skills lab in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply guided skills lab to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

14. What is the strongest professional approach to comparative tool lab in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply comparative tool lab to authorised information, test the result and document accountable human review.

15. What is the strongest professional approach to professional case study in Agent Safety and Security?

- A. Define the outcome, apply professional case study to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

16. What is the strongest professional approach to quality rubric in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply quality rubric to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

17. What is the strongest professional approach to validation and fact-checking in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply validation and fact-checking to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

18. What is the strongest professional approach to bias and inclusion review in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply bias and inclusion review to authorised information, test the result and document accountable human review.

19. What is the strongest professional approach to failure-mode analysis in Agent Safety and Security?

- A. Define the outcome, apply failure-mode analysis to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

20. What is the strongest professional approach to risk and control design in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply risk and control design to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

Knowledge checks 21-30

21. What is the strongest professional approach to human review and approval in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply human review and approval to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

22. What is the strongest professional approach to team collaboration in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply team collaboration to authorised information, test the result and document accountable human review.

23. What is the strongest professional approach to performance metrics in Agent Safety and Security?

- A. Define the outcome, apply performance metrics to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

24. What is the strongest professional approach to value and roi in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply value and roi to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

25. What is the strongest professional approach to integration blueprint in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply integration blueprint to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

26. What is the strongest professional approach to scenario simulation in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply scenario simulation to authorised information, test the result and document accountable human review.

27. What is the strongest professional approach to troubleshooting clinic in Agent Safety and Security?

- A. Define the outcome, apply troubleshooting clinic to authorised information, test the result and document accountable human review.
- B. Enter confidential information into any public tool to improve detail.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

28. What is the strongest professional approach to portfolio deliverable in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Define the outcome, apply portfolio deliverable to authorised information, test the result and document accountable human review.
- C. Accept the most fluent AI response without checking evidence or risk.
- D. Remove human approval immediately so the process is faster.

29. What is the strongest professional approach to professional review in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Define the outcome, apply professional review to authorised information, test the result and document accountable human review.
- D. Remove human approval immediately so the process is faster.

30. What is the strongest professional approach to module action plan in Agent Safety and Security?

- A. Enter confidential information into any public tool to improve detail.
- B. Accept the most fluent AI response without checking evidence or risk.
- C. Remove human approval immediately so the process is faster.
- D. Define the outcome, apply module action plan to authorised information, test the result and document accountable human review.

GLOBAL EDUCATIONAL CONSULTANTS

 **GLOBAL
EDUCATIONAL**
CONSULTANTS LIMITED

Answer key and application guidance

Every correct answer applies the same professional standard: a clear outcome, authorised information, proportionate safeguards, validation and accountable human review.

01 - C	02 - D	03 - A	04 - B	05 - C	06 - D
07 - A	08 - B	09 - C	10 - D	11 - A	12 - B
13 - C	14 - D	15 - A	16 - B	17 - C	18 - D
19 - A	20 - B	21 - C	22 - D	23 - A	24 - B
25 - C	26 - D	27 - A	28 - B	29 - C	30 - D

Module portfolio project

Create a professional Agent Safety and Security implementation pack containing: a one-page business objective; stakeholder and workflow map; authorised data checklist; prompt or process design; normal, ambiguous and failure tests; quality and risk rubric; measured results; and a 30-day improvement plan with a named owner.

Q1 DISCOVER	Q2 BUILD	Q3 INTEGRATE	Q4 LEAD
-------------	----------	--------------	---------

Responsible-use and trademark notice

AI tools and product features change frequently. Check current provider terms, organisational policies and applicable law before live use. Third-party product names and trademarks belong to their respective owners. Educational references do not imply endorsement, partnership or vendor certification.