



AI-Augmented Cybersecurity Awareness

Practical judgement for AI-related security risks in Banking and Finance

ICAGILE-ACCREDITED SPECIALIZED CREDENTIAL · IC-AICA

AI changes what a convincing cyber threat can look and sound like. It also changes the everyday risk of sensitive client, commercial, and internal information leaving the bank through unsafe AI use. This practical course builds the judgment to recognise signals, verify before acting, and protect information before prompting.



THE COURSE PROMISE

Help Banking and Finance professionals make better security decisions when AI can both defend and be weaponised.

DURATION

3 hours 15 minutes, including breaks

FORMAT

Live in-person or remote delivery

AUDIENCE

Cross-functional professionals and people managers

PRIOR KNOWLEDGE

No technical or cybersecurity background required

1

Recognise

See how AI changes the scale, speed, and believability of common cyber threats.

2

Verify

Treat security signals as inputs that need independent verification before action.

3

Protect

Build practical routines for safe AI use and team readiness.



THE EXPERIENCE

A practical security decision workshop

Built for Banking and Finance organisations, this fast-moving, scenario-led session keeps the focus on what people need to do at the moment a decision matters. Participants work through a fictional bank case involving a spoofed IT-security alert, a deepfake urgent request, and the unsafe copying of work information into a public AI tool.

Who this is for

Professionals, managers, and teams across banking and financial services who work with communications, client information, operational data, approvals, or AI-enabled tools.

What participants leave with

A usable verification routine, clearer data boundaries for unapproved AI tools, and one practical readiness improvement in each risk direction.

FOUR CONNECTED LEARNING MOVES

1

Update assumptions

Explore how AI can make phishing, impersonation, deepfakes, and automated attack or defence activity more scalable, rapid, or believable.

2

Triage the signal

Examine suspicious communications and alerts without falling into automatic trust or automatic suspicion.

3

Verify independently

Choose and practise a pre-established route to confirm identity, requests, or content before acting.

4

Improve readiness

Review inbound threat preparedness and outbound data exposure, then identify one improvement for each.

CORE MESSAGE

**In an AI-augmented environment, the safest default is neither trust nor distrust.
It is a proportionate, independent verification step.**



WHAT PARTICIPANTS WILL DEVELOP

Learning outcomes

The course is designed around the following ICA Specialized Credential learning outcomes.

1

1.1 AI-Enabled Cyber Threats

Explain at least three ways AI changes the scale, speed, or believability of common cyber threats or the defences against them, with a practical implication for each.

2

2.1 AI-Generated Security Signals

Analyse at least two AI-generated security alerts or suspicious communications for indicators of legitimacy or fabrication, and state the appropriate verification step for each.

3

3.1 Verification Practices in an AI-Augmented Environment

Apply a verification practice to one real or simulated scenario, with documented scope, verification method, and responsibility; state one category of information that would not go into an unapproved tool.

4

4.1 Readiness for AI-Related Security Risks

Evaluate a team's or organisation's AI-related security readiness across inbound threats and outbound data exposure, with one practical improvement for each.

A FOUNDATION FOR THE COURSE

The course builds on the concepts introduced in the AI & Technology Literacy Core Certification. Learners who have not completed that certification are encouraged to do so first to get the most from this course.



MODULES 1 & 2

Course outline

1

1.1 AI-Enabled Cyber Threats

40 MINUTES

SOURCE FOCUS

AI makes convincing cyber threats easier and faster to produce, changing what suspicious activity can look and sound like.

IN THE ROOM

Participants explore how AI affects phishing, impersonation, deepfakes, and automated attack or defence activity. They identify the practical impact of scale, speed, and believability in a bank setting.

PRACTICAL APPLICATION

Create a short threat-change map that connects three AI-enabled shifts to a decision a Banking and Finance professional might need to make.

2

2.1 AI-Generated Security Signals

35 MINUTES

SOURCE FOCUS

AI increasingly generates legitimate security alerts while also helping attackers create convincing imitations. Neither automatic trust nor automatic suspicion is a safe default.

IN THE ROOM

Participants triage simulated alerts and suspicious communications, looking for indicators of legitimacy or fabrication. They decide what can be checked and who should be involved before action.

PRACTICAL APPLICATION

Analyse two scenario signals, including a spoofed IT-security alert or deepfake urgent request, and state the appropriate independent verification step for each.

BREAK PATTERN

In person: one 15-minute break after Module 2. Remote: the first of two 10-minute breaks follows Module 1; the second follows Module 3.



MODULES 3 & 4

Course outline

3

3.1 Verification Practices in an AI-Augmented Environment

40 MINUTES

SOURCE FOCUS

Many AI-enabled attacks succeed because no verification step exists at the moment it matters. A simple practice established in advance can reduce that risk.

IN THE ROOM

Participants develop a practical verification routine for identity, requests, or content. They also identify information categories that must not be entered into an unapproved AI tool.

PRACTICAL APPLICATION

Apply a verification practice to the bank case, documenting scope, independent verification method, and responsibility before choosing an action.

4

4.1 Readiness for AI-Related Security Risks

35 MINUTES

SOURCE FOCUS

AI-related security risk includes both attacks coming into the organisation and sensitive information leaving through unsafe AI use. Effective readiness must address both.

IN THE ROOM

Participants assess team or organisational readiness across inbound threats and outbound data exposure. The session brings the case together through a focused debrief and outcome-aligned application check.

PRACTICAL APPLICATION

Complete a concise readiness review and define one practical improvement for inbound AI-enabled threat readiness and one for outbound data protection.

LEARNING APPROACH

Scenario-led, discussion-based, and applied. Participants practise judgment rather than memorising rules, using a Banking and Finance case that makes the consequences of fast, unverified action visible.

PRACTICAL TAKEAWAY

A proportionate verification habit, a clearer boundary for sensitive data, and a concrete next step to strengthen AI-related security readiness.