Learning Outcomes

Risk Management

Core & Specialized Credentials

International Certification Alliance

Version 1.0 — August 2026

LICENSING INFORMATION

The work in this document was facilitated by the International Certification Alliance (ICA) and done through the contributions of various experts and practitioners. These learning objectives are intended to help the growing Tomorrow-Ready™ community worldwide.

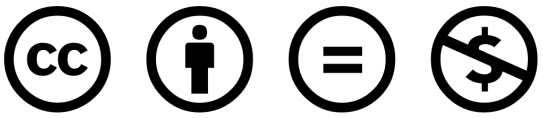

TABLE OF CONTENTS

HOW TO READ THIS DOCUMENT

This document outlines the learning outcomes that accredited member organizations must address to offer ICA's Risk Management certification. To achieve a certification, a learner must complete the core credential plus at least two specialized credentials.

Each learning outcome (LO) follows a particular pattern, described below.

0.0 Learning Outcome Name

Additional Context, describing why this Learning Outcome is important or what it is intended to impart.

The learning outcome's purpose further describes what is expected to be imparted to the learner (e.g., a key point, framework, model, approach, technique, or skill).

CORE CREDENTIAL LEARNING OUTCOMES

Risk Management Core

Risk Management is an 8-hour Core Credential for professionals who want to develop a shared understanding of how organizations identify, evaluate, and act on risk in conditions of speed, complexity, and interconnection. Traditional risk management was built for a world of stable categories and annual review cycles. In environments shaped by rapid technology change, interconnected global systems, and emerging risk types such as AI-enabled decision-making, those approaches leave organizations exposed to risks they cannot see coming and slow to respond to the ones they do.

1. What Risk Management Is and Why It Matters

1.1 Compliance-Oriented and Strategic Risk Management

Risk management can operate as a compliance activity or as an integrated part of strategy and daily decisions. The difference affects speed, opportunity-taking, resilience, and organizational confidence.

Build learners' understanding of why risk management must evolve beyond periodic compliance in complex environments. Explain the difference and impact on organizations of strategically integrated risk management.

1.2 Emerging and Traditional Risk

Emerging risks such as AI-enabled decisions, geopolitical instability, and interconnected digital systems can move faster, cross boundaries more easily, and remain less visible than traditional risks.

Build learners' ability to recognize the distinguishing characteristics of emerging risk (such as speed, interconnection, or visibility), so they can adapt identification and monitoring practices rather than forcing new risk types into frameworks built for a different risk landscape.

2. Risk Appetite, Culture, and Ownership

2.1 Risk Appetite and Decision Guidance

Risk appetite only adds value when it translates into guidance people can use in real decisions. Broad policy language without thresholds or decision rules provides little practical direction.

Build learners' understanding of risk appetite as a practical decision guide of both what the organization will refuse as well as what it is willing to take on for any specific course of action.

2.2 Risk Ownership and Culture

Risk ownership works when it is clear who does the work, who monitors it, and who provides independent assurance. When those roles blur or sit unassigned, information does not reach the person with authority to act.

Develop learners' ability to establish who owns, monitors, and assures a risk, and to recognize where unclear ownership or a culture that penalizes early warning would delay a response. Cover the factors that cause risk information to not reach someone with authority to act such as ambiguous ownership, layers of reporting, blocked information flow, or cultural reluctance to share bad news.

3. Identifying, Assessing, and Prioritizing Risk

3.1 Risk Identification and Assessment Methods

Static checklists and annual reviews can miss risks that emerge between cycles or fall outside existing categories. Effective identification combines structured methods with ongoing input from people close to the work.

Build learners' understanding that risk identification isn't one-size-fits-all and different methods surface different types of risk depending on the context. Develop understanding of common risk identification and assessment methods, the types of risks they surface, and where each is most useful.

3.2 Risk Assessment Gaps and Interconnections

Risk assessments can appear complete while missing interconnected risks, outdated likelihood assumptions, or gaps in coverage. These weaknesses can create false confidence in the risk picture.

Develop learners' ability to identify what a risk assessment is missing as well as what it contains. Cover how to critique risk assessments for factors such as coverage, outdated reasoning, or unaccounted interconnections.

3.3 Risk Prioritization

Organizations cannot address every risk at once. A defensible prioritization approach uses explicit criteria rather than urgency, recency, or influence alone.

Develop learners' ability to prioritize risks using consistent, explicit criteria or a decision rubric, then challenge them to think systemically. Teach that risk prioritization often happens in isolation (risk A scores highest, risk B second) but when risks are considered together, the picture changes. One risk might amplify another, or addressing risk A first prevents risk B from materializing, or two lower-priority risks together create a bigger problem than any single risk.

4. Responding to Risk and Integrating It into Decisions

4.1 Risk Monitoring and Treatment

Risk management requires both continued monitoring and a deliberate treatment choice. Monitoring without response, or response without monitoring, leaves the organization exposed as conditions change.

Develop learners' ability to combine monitoring indicators, triggers, and treatment into a practical risk response approach for speed and coverage.

4.2 Integrating Risk in Strategic Decisions

Strategic decisions often involve incomplete information, competing priorities, and risks that have no precedent. Risk analysis arriving after the choice is made can only confirm it, object to it, or add friction. And by then, the moment it could have changed the decision has passed.

Build learners' ability to apply risk thinking to actual strategic decisions, not just identify risks in isolation. Help learners understand that the same risks look different depending on how much risk the organization can or will tolerate. Reinforce the importance of making risk appetite visible and using it to evaluate strategic decisions while it can still change the outcome.

SPECIALIZED CREDENTIAL LEARNING OUTCOMES

Risk Appetite and Tolerance Design

Risk Appetite and Tolerance Design is a 2-4 hour Specialized Credential for professionals who want to develop their ability to define risk appetite in terms specific enough to actually guide decisions, rather than producing a statement that sits in a policy document unused. Most organizations have a risk appetite statement. Few can explain what it means for the decision in front of them right now. This course focuses on closing that gap: translating appetite from a general statement of risk tolerance into thresholds, examples, and decision rules that people can actually apply.

1.1 Usable Risk Appetite Statements

Risk appetite statements often remain too broad to guide real decisions. Usable statements provide enough specificity to shape choices when trade-offs and exposure must be judged.

Build learners' understanding of what makes risk appetite decision-usable rather than merely descriptive. Cover who sets and owns the risk appetite statements.

2.1 Stated and Actual Risk Appetite

An organization's real tolerance is often revealed more clearly by past decisions than by policy language. Comparing stated appetite with actual choices can expose meaningful gaps.

Develop learners' ability to compare stated risk appetite with actual decision patterns. Teach that stated risk appetite ("We're innovative and willing to take calculated risks") often doesn't match actual decision-making patterns ("We rejected that initiative because it was too risky").

3.1 Designing Usable Risk Appetite Statements

A practical risk appetite statement translates general posture into thresholds and decision rules. These rules reduce ambiguity about what teams may accept and what requires escalation.

Build learners' ability to translate abstract risk appetite into concrete, decision-usable statements that actually guide behavior. Teach them that vague appetite statements ("We're willing to take reasonable risks") don't help decision-makers. They need thresholds—specific boundaries about what the organization will refuse and what it will accept. Introduce types of risk, such as financial, reputational, technology, or operational, and cover how the type of risk impacts the risk appetite in different organizations.

4.1 Practical Use of Risk Appetite

A risk appetite statement provides little governance value if people do not refer to it when making decisions. Evaluation therefore needs observable evidence of actual use or non-use.

Build learners' ability to recognize whether risk appetite statements are actually being used to guide decisions or just sitting in policy documents. Teach them what evidence looks like. Cover evidence of use such as decision documents reference the appetite statement, people explain decisions in terms of thresholds, conversations about risk align with stated appetite, or decisions that would violate appetite don't happen. Cover evidence of non-use such as decisions contradict stated appetite, people are unaware the statement exists, risk conversations ignore appetite, or decisions get justified after the fact rather than checked against it.

Risk Escalation and Reporting Design

Risk Escalation and Reporting Design is a 2-4 hour Specialized Credential for professionals who want to develop their ability to design how risk information moves from where it is first noticed to the governance body responsible for acting on it. Risk oversight fails less often because no one saw a risk coming, and more often because someone saw it and the information never reached anyone with the authority or the urgency to act. This course focuses on the practical design of escalation paths, reporting cadence, and decision triggers that get risk information to the right people in time to matter.

1.1 Risk Escalation Failure Patterns

Risk information can be delayed, softened, or lost as it moves through organizational layers. Unclear ownership and reluctance to surface bad news often worsen the problem.

Build learners' understanding of why risk escalation breaks down in practice. Introduce challenges such as filtering, translation loss, competing priorities, unclear ownership, or delays in reporting.

2.1 Risk Reporting and Escalation Paths

Managing risk isn't just about identifying it. It's about getting information to people who can act, without it getting delayed, distorted, or deprioritized along the way.

Develop learners' ability to trace and diagnose where existing escalation paths break down. Cover the journey from when the risk is first noticed to when it is acted on and what happened at each step of the way.

3.1 Risk Escalation Structures

Escalation structures only work if they're specific, clear about who does what, and actually tested. Vague structures leave critical risks stranded.

Develop learners' ability to create escalation structures that function clearly under real operating conditions. Cover the specific of effective escalation structures such as triggers, ownership, destination, and expected governance response before pressure is high. This reduces reliance on ad hoc judgment.

4.1 Timeliness of Risk Escalation

A risk identified but escalated too late is almost as useless as a risk not identified at all.

Develop learners' ability to assess whether an escalation structure produces governance action within an appropriate, defined timeframe. Timeliness needs a clear standard tied to the risk and context.

Portfolio and Investment Governance

Portfolio and Investment Governance is a 2-4 hour Specialized Credential for professionals who want to develop their ability to govern how organizations make, review, and adjust decisions about where to invest time, money, and capability. At the portfolio level, governance determines which work gets started, how resources are allocated across competing priorities, and when to persevere, pivot, or stop. Without deliberate portfolio governance, organizations default to whoever advocates loudest, perpetuating work that no longer serves strategy and leaving high-value opportunities unfunded.

1.1 Portfolio Governance and Strategic Value

Portfolio governance is more than project approval or budget control. It allocates finite organizational capacity toward work expected to create strategic value.

Build learners' understanding of portfolio governance as a strategic allocation mechanism rather than a gatekeeping process.

2.1 Portfolio Investment Decisions

Portfolio decisions involve competing priorities, limited capacity, incomplete information, political pressure, and time sensitivity. Without a structured approach, influence can outweigh strategic value.

Build learners' ability to approach portfolio investment decisions as a structured, evidence-based activity that accounts for strategic alignment, feasibility, capacity, and the cost of delay. Cover the risks of not having a structured approach to portfolio investment decisions.

3.1 Adaptive Portfolio Review

Annual portfolio reviews can be too slow for fast-changing environments. More frequent review allows organizations to continue, adjust, or stop work as strategic conditions change.

Develop learners' ability to create a portfolio review process that supports ongoing adjustment rather than periodic re-approval. Introduce the components of portfolio review processes such as cadence, criteria, and escalation paths.

4.1 Portfolio Governance Effectiveness

Organizations often measure project delivery without assessing whether portfolio governance allocated resources to the highest-value work. This allows weak prioritization systems to persist.

Develop learners' ability to assess whether portfolio governance connects investment decisions with strategic value. Introduce assessment criteria such as strategic alignment, prioritization bias, and resource allocation effectiveness. Discuss the discipline needed to stop funding portfolios that are no longer the highest priority.

AI-Augmented Cybersecurity Awareness

AI-Augmented Cybersecurity Awareness is a 2-4 hour Specialized Credential for professionals who want to build the practical judgment needed to recognize, evaluate, and respond to the cyber and information-security risks that AI tools introduce into everyday work, both threats coming in and confidential data going out. AI has made social engineering more convincing, security tooling more automated, and the line between a genuine signal and a fabricated one harder to see at a glance. At the same time, the most common daily incident is not a sophisticated attack but an employee pasting client or company data into a public AI tool without realizing the risk. Professionals who treat AI-generated security alerts, communications, or media as automatically trustworthy, or automatically suspect, and who are not alert to their own outbound data risk, are poorly equipped to protect themselves, their teams, and their organizations.

1.1 AI-Enabled Cyber Threats

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

Help learners update their assumptions about common cyber threats in an AI-augmented environment. For example, AI makes convincing phishing, voice cloning, deepfakes, and automated attack activities.

2.1 AI-Generated Security Signals

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

Build learners' ability to treat AI-generated security signals as inputs that require verification before action. For example, this might include an AI-generated phishing email impersonating IT support or a deepfake voice request for an urgent wire transfer.

3.1 Verification Practices in an AI-Augmented Environment

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.

Develop learners' ability to use a practical verification routine for identity, requests, or content before acting. For example, a verification practice might be confirming an urgent payment request through a separate, pre-established phone call rather than replying to the email or message that made the request.

4.1 Readiness for AI-Related Security Risks

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

Help learners assess organizational readiness across inbound threats and outbound data exposure rather than focusing on attack awareness alone.

Growth Strategy

Growth Strategy is a 2-4 hour Specialized Credential for professionals who want to develop their ability to evaluate and choose among the different paths an organization can pursue to grow, and to design a growth approach that fits its capabilities and risk tolerance. Growth is often treated as an unqualified goal rather than a strategic choice with real trade-offs between the risk, capability, and time each path requires.

1.1 Growth Paths and Trade-offs

Organizations often choose growth paths based on opportunity size without understanding the timeline.

Build learners' understanding of the trade-offs among common growth paths. Introduce common ways growth paths differ such as risk, capability requirements, and time to results. Cover common factors for timelines differences such as market maturity, capability overlap, execution complexity, capital requirements, and competitive urgency.

2.1 Growth Path Fit

A growth path that fits one organization may overwhelm another. Growth path fit is about whether this organization can execute it given who they are, what they have, and what they can tolerate.

Develop learners' ability to assess whether a growth path fits the organization's capabilities and risk tolerance. Teach categories of growth path fit such as capital, capabilities, market position, and risk tolerance.

3.1 Designing a Growth Approach

Growth that happens in stages succeeds more often than growth that tries to scale before proving fundamentals.

Build learners' understanding that staged growth reduces risk by proving assumptions and building capabilities before committing major resources. Teach that a two-stage approach isn't just "do something small, then scale". Each stage has specific objectives that build toward the next.

4.1 Growth Returns and Strategic Commitment

Growth initiatives can continue because stopping feels like failure even when returns no longer justify the original risk and resource commitment. Evaluation needs to compare current results with that starting point.

Develop learners' ability to assess whether a growth path still justifies the resources and risk originally committed. Teach how to distinguish between paths that are working but need adjustment, paths that need restructuring or timeline extension, and paths that should be exited.

Decision-Making Under Uncertainty

Decision-Making Under Uncertainty is a 2-4 hour Specialized Credential for professionals who want to develop their ability to make sound decisions when information is incomplete, conditions are changing, and outcomes cannot be predicted with confidence.

1.1 Decision-Making Under Uncertainty

In some decisions uncertainty is deep enough that no amount of analysis will resolve it — the only way forward is to choose a path, act, learn from what happens, and be ready to change course. This goes beyond the Core's treatment of uncertainty as one factor among many.

Build learners' understanding of decision-making under deep uncertainty as an ongoing cycle of committing, testing, learning, and adjusting.

2.1 Critical Assumptions and Weak Signals

When evidence is incomplete, teams need to know which assumptions matter most and which signals would show that conditions are changing.

Develop learners' ability to focus attention on assumptions and signals that could materially change a decision.

3.1 Adaptive Decision Approaches

Uncertain decisions may benefit from staged commitments, experiments, checkpoints, or triggers that preserve future choice. A single irreversible commitment may be too rigid for changing conditions.

Develop learners' ability to design decision approaches that enable action while preserving learning and adaptability.

4.1 Persist, Pivot, or Stop Decisions

Uncertainty continues after a decision is made. The hardest part is often not spotting that a change is needed, but having the willingness and commitment to act on it — persisting, pivoting, or stopping — despite sunk cost, ego, or pressure to stay the course.

Develop learners' ability and resolve to change a decision when the evidence calls for it, not only to recognize that it should change.

SPECIAL THANKS

ICA would like to give special thanks to the contributors:

Kerri Sutey · Paulo Dias · Christina Hartikainen · Tricia Broderick · Samantha Davis · Evan Leybourn