COPENHAGEN COMPLIANCE | INFORMATION SECURITY INSTITUTE

Certified Risk Manager Program

Probability, predictive modeling and quantitative risk for executives who have to put a number on uncertainty..

WHY THIS PROGRAM

Risk registers stall in one meeting, when someone asks how much the worst year could cost, how likely it is, and which control is worth paying for.

In two days you build the answers with risk officers, finance leaders, auditors and architects in the room. You leave with models, worksheets and a method you can use on Monday.

COPENHAGEN COMPLIANCE

2 days	Data first	Modeling	5+ years
Progressive, modular program	Python and Power BI shown, not required	No actuarial background required	Relevant experience for admission

Request program dates or apply: jeanette@e-compliance.academy

Job Market Needs

THE SHIFT	Boards have stopped asking for another heat map. CFOs, auditors and regulators want to know what a risk costs, how often it is likely to hit and what a control buys back. A 1 to 5 score cannot answer that, because it multiplies labels that were never numbers. Organizations need risk professionals who can turn an opinion into a probability distribution and a distribution into a decision.
THE MODELING WORK	Quantitative risk managers start from the business objective and ask what could stop it. They split each scenario into how often it happens and how much it costs when it does, pick a distribution that fits the mechanism, and simulate the result. When data is thin they calibrate expert judgment and say openly how wide the uncertainty is. The output is a loss exceedance curve a CFO can read.
THE OPERATING RISK	AI has added a second job. Predictive models drift, generative tools give wrong answers with confidence, and agents can take actions nobody approved. These failures have a frequency and a cost like any other loss, so they can be modeled the same way. Risk teams need oversight tiers, circuit breakers and monitoring thresholds in place on the first day of deployment, and they need to price those controls against the exposure they remove.
THE SKILLS REQUIRED	The work needs executive-level probability and statistics: Poisson, log-normal and beta-PERT distributions, Monte Carlo simulation, Value-at-Risk and Expected Shortfall. It needs judgment about uncertainty, including expert calibration, bias and scenario design. It needs financial fluency in risk appetite, capacity and risk-adjusted ROI, plus enough AI literacy to follow how models fail. The reference standards are ISO 31000, ISO/IEC 23894, FAIR and the NIST AI Risk Management Framework.

Program Overview

This two-day program prepares executives, risk leaders, finance leaders, compliance officers, auditors and architects to measure exposure instead of classifying risks. Day 1 covers quantitative risk management, from the business objective to scenario modeling, simulation and financial reserves. Day 2 applies the same discipline to predictive, generative and agentic AI.

The program uses a progressive, modular format. Every 45-minute module combines an executive explanation, a method, a live demonstration and a short exercise, so that each participant leaves with a technique or a management artifact they can reuse the next day. Excel is the common entry point. Python and Jupyter show how the same calculations scale, and Power BI shows how to report them. No programming background is needed.

Both days are connected on purpose. Day 1 teaches you to measure uncertainty and financial exposure. Day 2 uses that same measurement to decide whether an AI system is worth deploying, which controls it needs and when the organization must step in.

Target Audience and Value Delivered

The program gives each role a specific piece of the quantitative toolkit:

Chief Risk Officers	Replace heatmap reporting with exposure ranges, loss exceedance curves and limits the board can defend.
Chief Financial Officers	Tie risk to capital, reserves and liquidity, and compare investments on a risk-adjusted basis.
Chief AI Officers	Quantify AI failure scenarios and show, in money, what each governance control protects.
CISOs and Security Leaders	Express cyber scenarios as frequency and severity, and size the losses with FAIR.
C-suite Executives	Read a loss distribution, ask sharper questions of the risk function and decide with numbers.
Compliance Leaders	Move from checklist reporting to evidence of how much exposure each control removes.
Internal Auditors	Test the assumptions behind a risk model, check expert calibration and backtest predictions.
Enterprise Architects	See how model drift, shared dependencies and agent permissions turn into correlated losses.
Senior Risk Professionals	Build reusable Monte Carlo models and calibration worksheets in Excel and Python.

FOR ANYONE WHO OWNS A RISK REGISTER

The method also works for managers who own risks without running a formal risk function. You get a practical way to size a single risk, to challenge a score someone handed you, and to explain the result on one page.

Curriculum Highlights

The program is built around measurement, simulation and decisions. You will practice these techniques on realistic cases:

- **Measure exposure.** Translate business objectives into risk exposures with ISO 31000, and set appetite, capacity and tolerance in financial terms.
- **Model frequency and severity.** Use Poisson, log-normal, beta-PERT and generalized Pareto distributions, and choose each one from the mechanism behind the event.
- **Simulate.** Run Monte Carlo models with 100,000 or more iterations and read the results as Loss Exceedance Curves, Value-at-Risk and Expected Shortfall.
- **Calibrate judgment.** Use seed questions, equivalent bets and absurdity tests so that thin data does not stop the analysis.
- **Quantify AI failure.** Put numbers on model drift, adversarial attacks and agentic failures, and price the controls that reduce them.

- **Decide.** Turn exposure into risk-adjusted ROI for the board, then connect prediction to monitoring and controlled automated responses.

Learning is hands-on. Case studies, guided exercises, decision simulations and group discussion carry most of the two days.

Career Outcomes

When you finish, you will be able to replace subjective scoring with quantified exposure and defend your numbers in front of a CFO, an auditor or a regulator. Key outcomes:

- Build an objective-based risk assessment and a financial risk appetite statement with measurable limits and escalation triggers.
- Challenge a conventional risk matrix and rebuild its top scenarios with probabilities and loss ranges.
- Construct frequency-severity models and run Monte Carlo simulations in Excel and Python.
- Read and present Loss Exceedance Curves, VaR and Expected Shortfall, and set reserves for a stated confidence level.
- Calibrate expert estimates and document them so that an auditor can follow every assumption.
- Assess an AI investment with risk-adjusted ROI, and design the oversight, thresholds and circuit breakers that go with it.

The approach is practical and tool-neutral. You work with facilitators who have built and audited risk models in real organizations, and you take away templates and worksheets, not slide decks. The material draws on ISO 31000, ISO/IEC 23894, FAIR, Cooke's Classical Model, the NIST AI Risk Management Framework and NIST AI 600-1.

Learning Experience

Each module follows the same rhythm: a management problem, a method, a worked example and a decision. Participants get decision frameworks, worked examples with realistic financial assumptions and reusable Excel and Python tools. Pre-reading gives the group shared terminology and a few reflection questions before the first session. Facilitators with enterprise experience guide the discussion on modeling choices, assumptions and what the results mean for a budget, a reserve or a go or no-go decision.

Real-World, Impact-Driven Learning

Every technique is tied to a real enterprise decision. We look at how risk models behave, and fail, in practice. The LTCM case shows what happens when a model underestimates extreme conditions. A credit approval failure shows how a small error rate becomes a tail loss. An autonomous agent shows how a control can be priced against the exposure it removes. Through these cases, participants learn to estimate losses, challenge assumptions, price controls and make investment decisions with evidence a board can inspect.

Program Description

Day 1: Quantitative risk management, from risk identification to financial exposure

DAY 1 LEARNING OBJECTIVE

Give participants the concepts, methods and tools to measure business exposure instead of classifying risks. The emphasis is on understanding uncertainty, modeling potential losses and allocating resources better. The day runs from 09:00 to 16:00: eight 45-minute modules, 6 hours of instruction and 1 hour of breaks.

09:00 - 09:45
45 minutes

Module 1. Risk management as decision support: ISO 31000 in practice

Module and focus area: Objectives, uncertainty and exposure.

Curriculum topics:

- Risk as the effect of uncertainty on objectives, and what that means in a budget meeting.
- Start from the objective at risk. A generic inventory of threats tells you little about what matters.
- Map risk sources, vulnerabilities, threat vectors, events, probabilities and consequences.
- Apply the ISO 31000 principles to strategic planning, operational decisions and financial performance.

Critical tools and methods: ISO 31000 framework, objective-based risk assessment, source-event-consequence mapping, pre-mortem analysis, reference class forecasting.

Practical exercise: Pick a business objective and build an objective-at-risk map. Show the events that could block it and what each one would cost.

You leave with: An objective-based risk map that links targets, uncertainty, exposure and consequences.

09:45 - 10:30
45 minutes

Module 2. Risk appetite, capacity and tolerance: setting financial boundaries

Module and focus area: Limits, thresholds and escalation.

Curriculum topics:

- Tell appetite, capacity and tolerance apart, and see who owns each one.
- Set strategic exposure limits and operational guardrails.
- Work with absolute financial boundaries, insolvency thresholds and liquidity constraints.
- Turn an appetite statement into indicators and escalation thresholds you can monitor.
- Compare inherent and residual exposure.

Critical tools and methods: Risk appetite framework, financial capacity and liquidity analysis, tolerance thresholds, Key Risk Indicators, limit and escalation matrices.

Practical exercise: Evaluate a hypothetical investment with uncertain cash flows. Set the maximum acceptable loss and the escalation thresholds from the organization's financial capacity.

You leave with: A financial risk appetite statement with measurable limits, tolerances and escalation triggers.

10:30 - 10:45 *Morning break*

10:45 - 11:30
45 minutes

Module 3. Beyond the risk matrix: why qualitative scores fail financial decisions

Module and focus area: Measurement and its limits.

Curriculum topics:

- Why 1 to 5 scales, high-medium-low ratings and traffic lights cannot carry arithmetic.
- Why multiplying a likelihood score by an impact score does not give a financial exposure.
- Measurement inversion: teams rank what is easy to score and miss what matters economically.
- Where qualitative screening still helps, and where probabilistic analysis becomes necessary.
- Inherent and residual risk beyond static control-effectiveness ratings.

Critical tools and methods: Ordinal versus cardinal measurement, quantitative exposure models, scenario comparison, control effectiveness assessment, expected loss with uncertainty ranges.

Practical exercise: Take a conventional 5x5 risk register and challenge its rankings. Rebuild three scenarios with probability estimates and financial loss ranges.

You leave with: A redesigned assessment that replaces unsupported scores with exposure estimates a manager can act on.

11:30 - 12:15
45 minutes

Module 4. Scenario engineering: turning business threats into model-ready inputs

Module and focus area: From brainstorm to evidence-based scenarios.

Curriculum topics:

- Build scenarios from actors, triggers, vulnerabilities and consequences.
- Separate causes, initiating events and loss outcomes.
- Count direct and indirect impacts, including liquidity, operational and reputational effects.
- Follow dependencies and cascading failures through the business.

Critical tools and methods: FAIR (Factor Analysis of Information Risk), bow-tie analysis, FMEA, structured red teaming, Analysis of Competing Hypotheses, scenario-based loss estimation.

Practical exercise: Model a supplier disruption or a cyber incident. Identify the initiating event, the vulnerabilities, the loss pathways, the financial consequences and the controls that could interrupt them.

You leave with: A structured scenario model, ready for quantitative parameters.

12:15 - 12:45 *Lunch break*

12:45 - 13:30
45 minutes

Module 5. Modeling frequency and severity: the statistical foundations of loss

Module and focus area: Distributions that fit the event mechanism.

Curriculum topics:

- Why exposure needs probability distributions and not single-point estimates.
- Model how often an event happens separately from how much it costs.
- Expected loss versus maximum potential loss.
- Rare events and high-impact consequences, and how extreme loss behaves.
- Choose a distribution from the mechanism behind the event.

Critical tools and methods: Poisson distribution for event frequency, log-normal for right-skewed loss severity, beta-PERT for bounded expert estimates, generalized Pareto for extreme tails, compound Poisson-lognormal for aggregate frequency and severity.

Practical exercise: Build a frequency and severity model for an operational failure. Use a Poisson distribution for annual incidents and a log-normal distribution for individual losses.

You leave with: A frequency-severity model with documented assumptions and parameter estimates.

13:30 - 14:15
45 minutes

Module 6. Expert judgment calibration: measuring what historical data cannot tell you

Module and focus area: Defensible estimates from limited evidence.

Curriculum topics:

- Thin historical data does not stop quantitative analysis.
- Use subject-matter experts for probabilities and loss ranges.
- Spot overconfidence, anchoring and extreme-value bias.
- Aleatory uncertainty (inherent randomness) versus epistemic uncertainty (limited knowledge).
- Calibrate minimum, most likely and maximum estimates, and check how credible and consistent the experts are.

Critical tools and methods: Cooke's Classical Model, seed questions and calibration scoring, equivalent bet test, absurdity test, beta-PERT distribution, expert elicitation protocols.

Practical exercise: Estimate the financial impact of an emerging risk with three-point expert estimates. Challenge the numbers with equivalent bets and absurdity tests, then choose a distribution.

You leave with: A calibrated expert-judgment worksheet with documented probability and impact assumptions.

14:15 - 14:30 *Coffee break*

14:30 - 15:15
45 minutes

Module 7. Monte Carlo simulation: calculating aggregate risk exposure

Module and focus area: From point estimates to simulated outcomes.

Curriculum topics:

- Move from deterministic estimates to stochastic simulation.
- Random sampling and probability distributions in practice.
- Combine frequency and severity into an aggregate annual loss, using convolution and compound loss models.
- Run 100,000 or more iterations and read expected loss, median, variance and extreme outcomes.
- Model several interacting variables, and know where correlation assumptions break down.

Critical tools and methods: Monte Carlo simulation, compound Poisson-lognormal models, distribution convolution, Excel-based stochastic modeling, a Python simulation engine, sensitivity and scenario analysis.

Practical exercise: Build or run a simulation that combines annual event frequency with financial severity. Compare the simulated distribution with a deterministic expected-loss estimate.

You leave with: A simulated annual loss distribution with expected loss, percentile outcomes and documented assumptions.

15:15 - 16:00
45 minutes

Module 8. Loss exceedance curves, Value-at-Risk and the LTCM lessons

Module and focus area: Tail risk, reserves and the limits of models.

Curriculum topics:

- Read and interpret Loss Exceedance Curves, and percentile estimates from P10 to P99.
- Value-at-Risk compared with Expected Shortfall.
- Set financial reserves and contingency funding, and turn simulated outcomes into capital allocation decisions.
- The Long-Term Capital Management case: leverage, liquidity, correlation assumptions, and a model that underestimated extreme market conditions.
- Why stress testing and reverse stress testing belong beside probabilistic modeling.

Critical tools and methods: Loss Exceedance Curves, Value-at-Risk, Expected Shortfall, stress and reverse stress testing, backtesting and exceedance analysis, liquidity and capital adequacy thresholds.

Practical exercise: Interpret a simulated LEC and set a reserve for a stated confidence level. Then see what happens when the assumptions about correlation, liquidity and tail behavior get worse.

You leave with: An executive risk exposure report that turns probability distributions into reserves, limits and management decisions.

DAY 1 EXPECTED RESULT

Participants finish the first day with a practical quantitative risk assessment, built from a business objective and a scenario through probabilistic modeling, simulation and a measured financial exposure.

Day 2: AI risk management, from probabilistic modeling to governance

DAY 2 LEARNING OBJECTIVE

Apply quantitative risk management to predictive, generative and agentic AI. Participants learn to turn AI failure scenarios into measurable financial exposure and to set up governance mechanisms that support operating decisions. The day follows the same 09:00 to 16:00 timetable.

09:00 - 09:45
45 minutes

Module 1. Beyond AI governance paperwork: managing risk that touches business objectives

Module and focus area: AI as a source of opportunity and of exposure.

Curriculum topics:

- Why inventories and static checklists do not support operational risk decisions.
- How predictive, generative and agentic systems differ, and why that changes the risk.
- Apply ISO 31000 and ISO/IEC 23894 to AI-related business objectives.
- Map each AI system to the processes, decisions and stakeholders it affects.
- Separate model risk, data risk, operational risk and third-party dependency, and give each an owner in the business, in technology and in risk.

Critical tools and methods: ISO 31000, ISO/IEC 23894, AI risk classification, AI system inventory and model register, model cards and system documentation, trust-boundary mapping, human rights impact assessments.

Practical exercise: Assess an AI-enabled business process. Map its objectives, the decisions it influences, the stakeholders it affects, its failure modes and who is accountable.

You leave with: An AI system risk profile that links technology, objectives, stakeholders and accountability.

09:45 - 10:30
45 minutes

Module 2. AI failure engineering: how models and agents cause losses

Module and focus area: Failure mechanisms and how they spread.

Curriculum topics:

- Start from specific failure mechanisms and skip the generic risk categories.
- Data quality, data drift and distribution shift. Overfitting and prediction errors.
- Hallucinations and unreliable generated output. Adversarial inputs and manipulated model behavior.
- Reward misspecification and unintended optimization.
- Unauthorized tool use and excessive permissions in agentic systems.
- Trace how a failure spreads across processes and to outside stakeholders.

Critical tools and methods: AI failure-mode analysis, FMEA adapted to AI, bow-tie analysis, adversarial red teaming, threat modeling, data and model drift analysis, attack trees, trust-boundary mapping.

Practical exercise: Analyze a hypothetical agent that reviews contracts, retrieves information and starts business workflows. Trace the failure paths and estimate direct and cascading consequences.

You leave with: An AI failure-mode register with threat vectors, vulnerabilities, consequences and measurable risk parameters.

10:30 - 10:45 *Morning break*

10:45 - 11:30
45 minutes

Module 3. Quantifying AI failures: from technical vulnerability to financial loss

Module and focus area: Frequency, severity and residual exposure for AI.

Curriculum topics:

- Turn failure mechanisms into probability-based loss scenarios.
- Estimate failure frequency and impact severity separately.
- Cost of wrong predictions and wrong generated output. Operational losses from unauthorized agent actions.
- Cascading effects across processes, customers and suppliers.
- Put human oversight and control effectiveness into residual exposure.
- Why historical incident data ages quickly when AI systems keep changing.

Critical tools and methods: FAIR applied to AI losses, frequency-severity modeling, Poisson distributions for event counts, log-normal distributions for loss severity, scenario-based probability estimates, compound loss distributions, control-adjusted residual risk analysis.

Practical exercise: Quantify a failure in an AI-assisted credit approval process. Estimate error frequency, average impact and tail losses, then the residual exposure after human approval and extra validation.

You leave with: A quantitative AI failure model showing baseline exposure, control-adjusted exposure and financial consequences.

11:30 - 12:15
45 minutes

Module 4. Distribution engineering for AI risk: uncertainty and extreme outcomes

Module and focus area: Modeling with scarce incident data.

Curriculum topics:

- Pick a probability distribution for each failure mechanism.
- Model uncertainty when incident data is scarce, using beta-PERT for expert estimates of probability and impact.
- Combine Poisson frequency and log-normal severity into compound loss distributions.
- Rare but costly AI failures, and dependence between AI components that creates correlated failure paths.
- Keep uncertainty ranges and stop treating assumptions as facts. Stress-test the parameters and the tail.

Critical tools and methods: Beta-PERT for sparse expert estimates, Poisson for incident frequency, log-normal for financial severity, compound Poisson-lognormal for aggregate AI losses, generalized Pareto for extreme tails, Monte Carlo for combined exposure.

Practical exercise: Build a probability model for an AI system with a short operating history. Use beta-PERT for an uncertain failure path, log-normal severity and Poisson frequency to produce an aggregate exposure profile.

You leave with: An AI risk distribution model with documented parameters, uncertainty ranges and assumptions.

12:15 - 12:45 *Lunch break*

12:45 - 13:30
45 minutes

Module 5. Expert judgment and AI risk calibration: making estimates defensible

Module and focus area: Calibration for auditability.

Curriculum topics:

- Why AI risk models lean on expert judgment and not on complete datasets.
- Tell an informed estimate from an unsupported opinion, and calibrate technical, operational and business experts.
- Seed questions test how accurate expert probabilities are.
- Equivalent bets expose the gap between a stated probability and real confidence. Absurdity tests catch implausible extremes.
- Combine expert estimates with empirical evidence, and document the assumptions for audit and later updates.

Critical tools and methods: Cooke's Classical Model, expert elicitation, seed questions, equivalent bet and absurdity tests, beta-PERT parameterization, calibration scoring and Brier score.

Practical exercise: Estimate the probability and cost of an AI agent executing an unauthorized transaction. Challenge the estimates with calibration questions and revise the distribution.

You leave with: A defensible AI risk parameterization worksheet with expert assumptions and calibration evidence.

13:30 - 14:15
45 minutes

Module 6. Monte Carlo simulation for AI risk: from single failures to enterprise exposure

Module and focus area: Aggregation, dependency and residual risk.

Curriculum topics:

- Aggregate several AI failure scenarios into one enterprise loss distribution.
- Simulate interacting risks across data, models, infrastructure, human oversight and autonomous agents.
- Combine frequency and severity distributions in simulations of 100,000 or more iterations.
- Correlation and dependency between AI failure events.
- Inherent and residual exposure after controls, with percentile estimates and Loss Exceedance Curves for AI losses.

Critical tools and methods: Monte Carlo simulation, compound Poisson-lognormal modeling, distribution convolution, correlation and dependency analysis, Loss Exceedance Curves, VaR and Expected Shortfall, sensitivity analysis and stress testing.

Practical exercise: Simulate the annual financial exposure of an enterprise AI portfolio that holds predictive models, generative applications and autonomous agents. Compare the results before and after governance controls.

You leave with: An enterprise AI exposure distribution showing expected losses, tail-risk estimates and residual exposure after mitigation.

14:15 - 14:30 *Coffee break*

14:30 - 15:15
45 minutes

Module 7. Translating AI risk into boardroom metrics: financial exposure, VaR and risk-adjusted ROI

Module and focus area: Decisions for the CFO, the CRO and the board.

Curriculum topics:

- Why AI governance needs financial and operational evidence.
- Turn technical failure scenarios into currency loss estimates, with expected annual loss and extreme losses side by side.
- Calculate AI-related Value-at-Risk and Expected Shortfall.
- Weigh the benefits of AI adoption against implementation cost, monitoring expense and human oversight.
- Measure risk-adjusted return on investment and compare automation benefits with the added exposure.

Critical tools and methods: FAIR financial risk modeling, Expected Annual Loss, VaR and Expected Shortfall, Loss Exceedance Curves, total cost of ownership, risk-adjusted ROI, expected value of information, cost-benefit and sensitivity analysis.

Practical exercise: Compare two options: an autonomous AI workflow and a human-operated process. Set operational savings against implementation cost, residual loss exposure and the control spend each needs.

You leave with: An AI investment decision model with risk-adjusted ROI, expected loss, financial exposure and recommended control investment.

15:15 - 16:00
45 minutes

Module 8. From predictive risk to autonomous controls: governing agents and continuous monitoring

Module and focus area: Oversight, circuit breakers and backtesting.

Curriculum topics:

- Connect risk prediction to operational decisions and automated responses. Separate the prediction, policy and execution layers.
- Set human oversight, authorization boundaries, escalation thresholds and control activation rules.
- Govern agents that have access to enterprise tools, data and workflows. Test in shadow mode before production.
- Design algorithmic circuit breakers and kill switches.
- Monitor continuously: drift detection, event-driven reassessment, and backtesting that checks predictions against outcomes.
- Draft an executive roadmap for quantitative AI governance.

Critical tools and methods: AI control plane and agent governance, Markov Decision Processes, reward function design, human-in-the-loop and human-on-the-loop controls, shadow-mode deployment, circuit breakers, model performance monitoring, Brier score and backtesting, Population Stability Index, living risk registers.

Practical exercise: Design a governed response architecture for an agent that detects a high-risk transaction and can start a control response. Define the authorization boundaries, escalation conditions, human intervention points and emergency shutdown.

You leave with: An AI risk control blueprint with monitoring indicators, decision thresholds, oversight tiers and an implementation roadmap.

DAY 2 EXPECTED RESULT

Participants finish with an AI risk assessment and a financial exposure model, backed by calibrated assumptions, simulation outputs and a governance architecture that connects AI predictions to controlled business actions.

Final Executive Case Study

One integrated case ties both days together. **Should an enterprise automate a critical business process with agentic AI?** Participants receive a hypothetical multinational that is considering an autonomous AI solution for contract review, compliance screening and transaction processing. They must:

1. Identify the business objectives and the potential benefits.
2. Identify the AI failure scenarios and threat vectors.
3. Estimate event frequency and loss severity.
4. Calibrate the uncertain parameters with expert judgment.
5. Simulate aggregate exposure with Monte Carlo.
6. Calculate VaR, Expected Shortfall and residual risk.
7. Compare expected automation savings with implementation cost and risk-adjusted ROI.
8. Define the controls, human oversight and escalation thresholds that deployment requires.
9. Present a recommendation to a simulated executive committee.

> **FINAL ASSESSMENT**
> The executive decision: approve, reject, postpone or conditionally approve the AI investment, with quantitative evidence and a defensible control strategy.

Participant Deliverables

By the end of the program, each participant has built the following materials:

DAY 1: QUANTITATIVE RISK MANAGEMENT

- Objective-based risk assessment
- Risk appetite and financial tolerance framework
- Quantitative scenario assessment
- Frequency and severity distribution model
- Expert judgment calibration worksheet
- Monte Carlo simulation results
- Loss Exceedance Curve and financial reserve assessment

DAY 2: AI RISK MANAGEMENT

- AI system risk and failure-mode register
- Probabilistic AI failure model
- Calibrated AI risk assumptions
- Simulated enterprise AI exposure
- AI risk-adjusted ROI assessment
- AI governance and control architecture
- Executive implementation roadmap

Master Toolkit: Software, Frameworks and Methodologies

The program runs on practical tools. This table consolidates what participants use across the two days.

Category	Critical tools and methodologies
Risk standards	ISO 31000, ISO/IEC 23894
Risk quantification	FAIR, frequency-severity analysis
Scenario engineering	Bow-tie, FMEA, red teaming
Expert judgment	Cooke's Classical Model, seed questions, equivalent bets
Statistical modeling	Poisson, log-normal, beta-PERT, generalized Pareto
Simulation	Monte Carlo, distribution convolution
Financial exposure	VaR, Expected Shortfall, Loss Exceedance Curves, Expected Annual Loss
Risk decisions	Risk appetite, capacity, tolerance, risk-adjusted ROI
Predictive analytics	Random Forest, Gradient Boosting, model validation
Explainable AI	SHAP, LIME
Model monitoring	ROC-AUC, precision, recall, F1, PSI, Brier score
Agentic governance	MDPs, reward functions, oversight tiers, circuit breakers
Operational governance	Model inventories, control registers, continuous monitoring

Practical software environment

Tool	How participants use it
Microsoft Excel	Probability calculations, distribution parameters, risk registers, exposure models, sensitivity analysis and executive reporting. Excel is the entry point for everyone.
Python	Monte Carlo simulation, statistical distributions, predictive analytics and automated risk calculations.
Jupyter Notebook	Live demonstrations of stochastic simulation and reproducible exercises, with charts of the distributions.
Microsoft Power BI	Executive dashboards, exposure visualization, risk indicators and management reports.

Excel is the accessible entry point for all participants. Python and Jupyter show how the same calculations can be scaled, automated and reproduced.

How each module is taught

Activity in each 45-minute module	Time	Purpose
Executive concept and business context	10 min	Frame the management problem
Methodology and critical tools	10 min	Show the analytical approach
Practical demonstration	10 min	Apply the tools to a realistic case
Participant exercise	10 min	Make an assessment or a decision
Conclusions and management implications	5 min	Turn findings into action

Enhancing Your Executive Profile and Networks

Completing the Certified Risk Manager program shows that you can measure uncertainty, model loss and tie risk to a financial decision. That is the skill set behind roles such as Chief Risk Officer, head of enterprise risk, quantitative risk lead, AI risk manager and risk advisor to the board. You gain the confidence to defend a reserve, a limit or an AI investment in front of a CFO, an audit committee or a regulator.

The program also builds an active network of risk, finance, audit, compliance and technology leaders. In case discussions and group exercises you test your assumptions against peers from finance, healthcare, legal and logistics. You compare how they calibrate experts, handle thin data and present tail risk, and you leave with lasting professional connections and access to an executive alumni network.

World-Class Instructors

Experts with deep industry and academic experience lead the program. Participants learn from recognized leaders in AI, risk management, compliance and corporate governance.



PROGRAM DIRECTOR

Prof. Kersi F. Porbunderwalla

Prof. Porbunderwalla has spent decades in governance, risk and compliance (GRC), in both corporate and academic settings. He is a former professor at IE Law School and Copenhagen Business School, and has lectured at Georgetown University, Cass Business School and Fordham University.

He is President and CEO of Copenhagen Compliance, The Information Security Institute, The Corporate Governance Institute, The EUGDPR and The E-Compliance Academy. His work has produced GRC networks that offer certifications and training across four continents, with a focus on AI-driven solutions, GRC applications and frameworks for cybersecurity and data privacy.



LEAD TRAINER

Prof. Hernan Huwyler

Prof. Hernan Huwyler, MBA, CPA, CAIO, CCAR-P, teaches quantitative risk management and AI risk governance. He has managed AI governance and risk control inside global AI developers and technology and consulting firms, and he builds his sessions around what happens when models meet tight budgets, strict regulators and real customer data.

He is an Academic Director at IE Business School and IE Law School, has taught executive education at IE since 2013, and is lead instructor for the Chief AI Officer certification at Copenhagen Compliance. He has trained more than 1,500 compliance, privacy, AI and risk professionals. Auditors want evidence, CFOs want numbers they can defend, and engineers want clear specifications. He designs each module to give all three.

Industry Recognition

Copenhagen Compliance has certified more than 5,000 professionals in privacy, data governance, risk and controls, and the Certified Risk Manager program builds on that record. The syllabus draws on ISO 31000,

ISO/IEC 23894, FAIR, Cooke's Classical Model, Monte Carlo methods, the NIST AI Risk Management Framework and NIST AI 600-1, and the specific editions and regulatory requirements are checked again when the teaching materials are prepared.

About the Institutions

Copenhagen Compliance, a leader in governance, risk and compliance (GRC) implementation and training, offers this certification. It has been a prominent GRC management agency since 2014 and understands the regulatory challenges multinational organizations face. We believe that layering on more compliance is not the answer. We equip professionals with solutions to the real problems organizations have in governance, risk management and compliance.

Copenhagen Compliance provides GRC tools, software and services that streamline these processes. Its global GRC platform includes standardized frameworks and guidance that help organizations run efficient, automated GRC operations. Resources cover risk assessment, policy management, incident tracking, internal controls and audit functions.

Copenhagen Compliance works with the **Information Security Institute**, which adds a network of events, educational resources and industry insight on AI, IT and cybersecurity. The Institute supports safe technology adoption in global institutions, and its modules address regulations and frameworks including AI, GDPR, cybersecurity and technology standards, ISO 42001, ISO 27001, SOX and NIST, as well as corporate social responsibility and ESG requirements.

Together, the two institutions give certification holders foundational knowledge and current insight into AI governance, risk and compliance.

Admission Requirements

This certification is designed for senior risk professionals, executives, finance and audit leaders, compliance officers and architects. Admission requires at least 5 years of experience in a relevant field, such as risk management, finance, audit, compliance, technology or general management. No coding background is needed, because the program focuses on the managerial and strategic use of quantitative risk methods.

Admission Process

To secure your place, reach out or submit your application. You can request more information, including upcoming program dates, from the team at eCompliance Academy. Email **jeanette@e-compliance.academy** for personal guidance from a program advisor.

When we receive your application, our program coordinator will email you to confirm receipt and walk you through the next steps. You will get an overview of upcoming dates and details on how to access your preparatory study materials. Payment details arrive at the same time, so you can secure your spot.

Program fees must be paid before the course begins and before you receive your pre-reading and study materials. Payment confirms your participation and gives you access to the materials that set the foundation for your learning.

A risk assessment earns its keep when it changes a business decision. We look forward to helping you move your risk function from scores to decisions.