AI training

GLOBAL AI SOLUTIONS

information security institute

Proposal for your tailored corporate AI compliance awareness program

Partnered with

COPENHAGEN COMPLIANCE

information security institute

Proposed training approach

Structure

Our AI Governance Training Program is designed to empower managers and employees with practical tools, frameworks, and actionable insights to navigate the complexities of AI adoption responsibly.

Delivery

To maximize the program's impact, we can align the training content with your organization's specific needs and challenges.

We will work with your team to customize scenarios and case studies for relevance.

COPENHAGEN
COMPLIANCE

Proposed training approach

Expected impacts

Managers

Gain actionable knowledge to procure, develop, and oversee AI systems, ensuring alignment with organizational goals and regulatory standards.

quip leaders with the confidence and knowledge to make informed decisions about AI investments, ensuring alignment with organizational priorities and ethical standards.

Employees

Cultivate awareness and confidence to contribute to a culture of responsible AI use.

Empower your team to identify and address AI-related risks early, reducing potential liabilities and enhancing trust in AI-driven processes.

COPENHAGEN COMPLIANCE

Organizational benefits

- Streamlined AI procurement and development processes.
- Enhanced risk management and regulatory compliance.
- Improved alignment of AI systems with organizational objectives and ethical standards.

Duration

- Managers: 7 hours (can be split into two sessions).
- Employees: 2 hours (single session).

Format

- Interactive lectures, case studies, and hands-on exercises.
- Pre-reading materials provided to maximize session productivity.

COPENHAGEN COMPLIANCE

Resources

- Facilitators, including checklists, models, standard templates, and sample contractual clauses.
- Customized policies and guidelines tailored to your organization's needs.

Facilitators

- AI project checklist
- AI risk taxonomy
- AI impact assessment template
- Quantification model
- ISO 42001 control matrix
- EU AI Act compliance checklist
- Implantation roadmap
- AI service level agreement
- AI standard clauses
- Responsible AI policy template
- AI governance policy template

COPENHAGEN
COMPLIANCE

Modular approach

Manager Training (7 Hours)

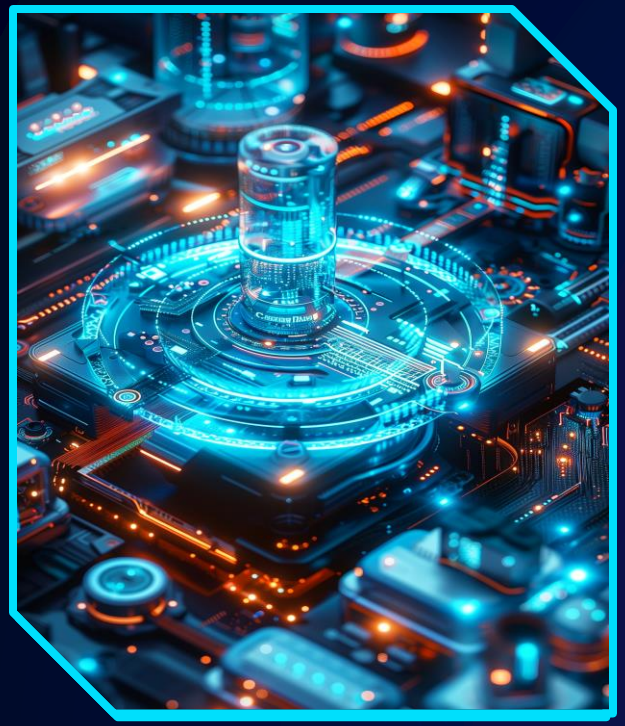
- Focused on strategic decision-making, compliance, and operationalizing AI governance.
- Includes in-depth discussions, real-world case studies, and interactive workshops.

General Employee Training (2 Hours)

- Provides foundational understanding and awareness of AI concepts, risks, and responsibilities.
- Simplifies technical and compliance topics to ensure broad accessibility.

COPENHAGEN COMPLIANCE

Training content for managers



- Foundations of AI: Introduction to machine learning, deep learning, neural networks, and key AI concepts.
- Practical AI Applications: Differentiate types of machine learning algorithms and apply them to real-world business scenarios.
- Business Integration: Identify AI opportunities tailored to your organization, including customer journey optimization.
- Data Governance for AI: Implement best practices for data quality, compliance, and governance in AI initiatives.
- Risk and Compliance Management: Assess and mitigate risks, impacts, and controls across the AI lifecycle. Comply with frameworks like ISO 42001, the EU AI Act, and responsible AI principles. Ensure proper vetting and integration of third-party AI systems and software.
- Strategic Planning: Plan business cases, allocate resources, and define actionable steps for AI adoption.

COPENHAGEN
COMPLIANCE

Training content for employees

- Understanding AI Basics: An introduction to what AI is, including its history, applications, and types.
- Ethical AI Practices: Guidelines for fairness, transparency, and accountability when using AI tools.
- Risk Awareness: Recognize potential risks and compliance considerations in using AI systems.
- Organizational Role: Understand the role of employees in supporting AI governance and ethical AI use..
- AI Essentials: Develop a foundational understanding of AI concepts and technologies and their impact on day-to-day operations.
- Hands-On AI Tools Training: Practical sessions to familiarise employees with AI tools relevant to their job roles.

COPENHAGEN
COMPLIANCE

Copenhagen Compliance reach

IN ROOM

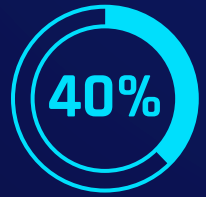
> 400 training sessions

ONLINE

5,000

Recognized trained professionals wordwide since 2014

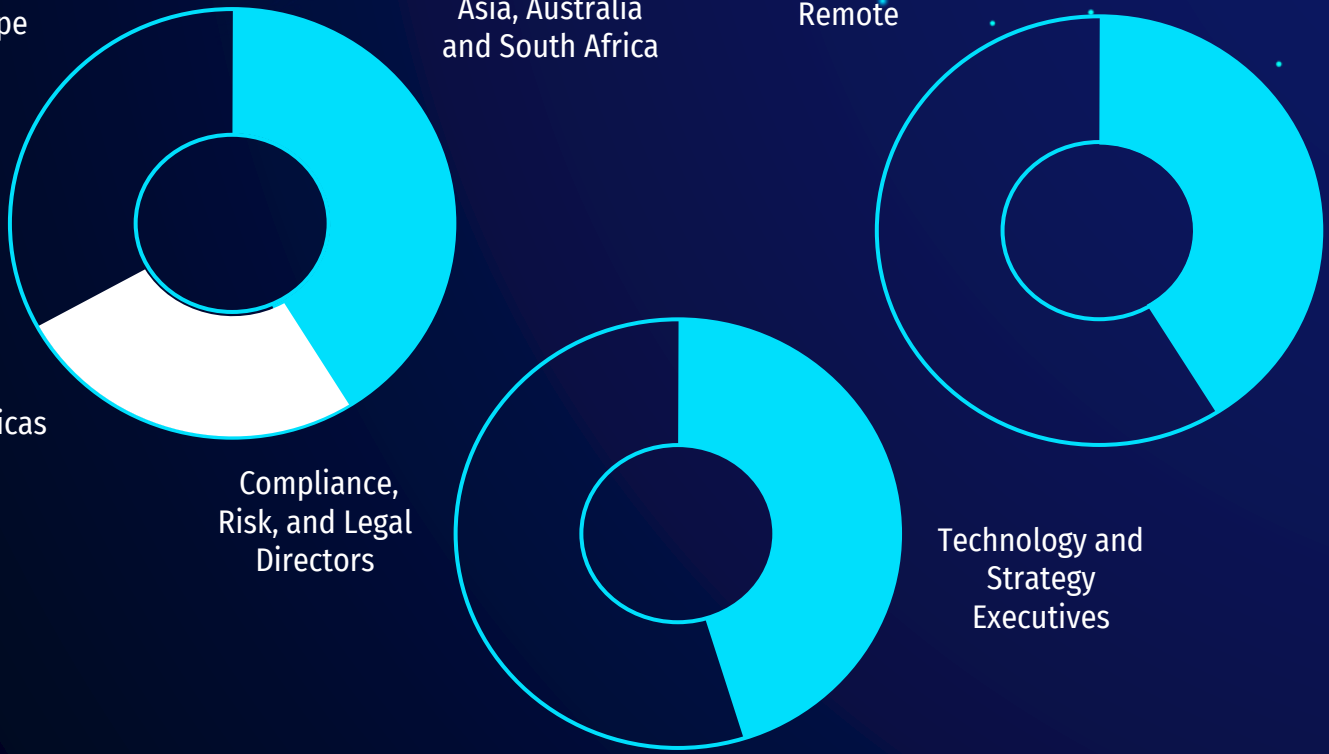
IT and cyber



Compliance

Business

Profile of certified AI professionals



COPENHAGEN COMPLIANCE

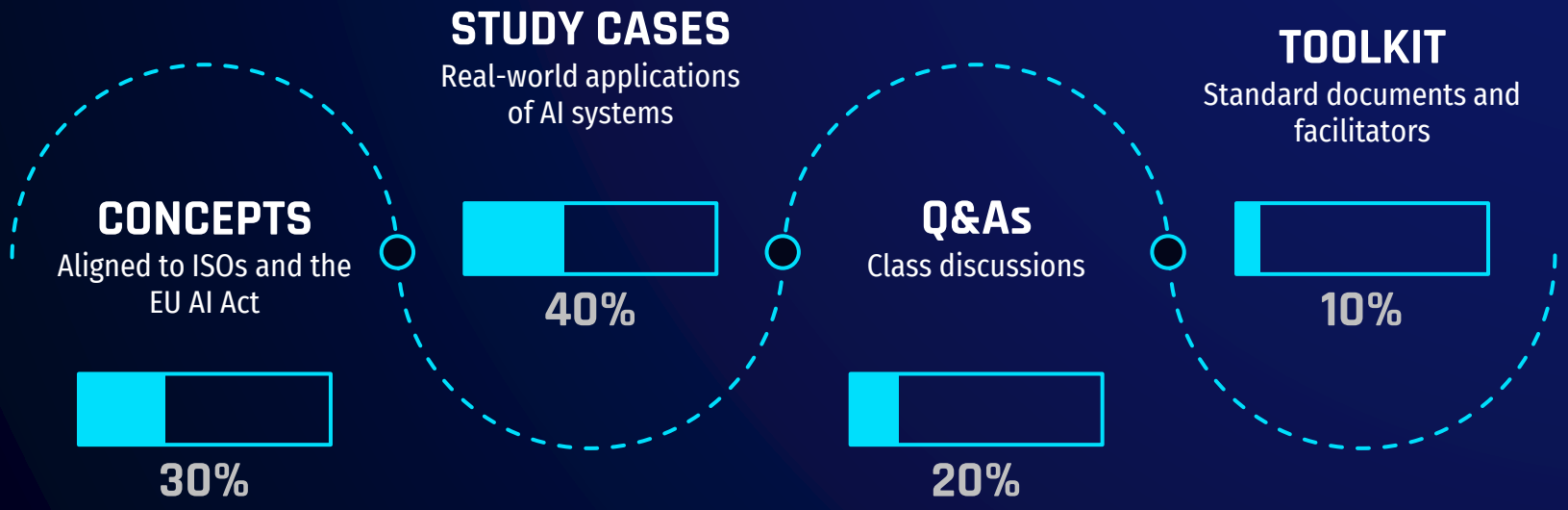
Profile of certified AI professionals

Ensure your organisation meets the AI Act requirements by training management and employees with the Artificial Intelligence Compliance Trained Professional (AICT) program. This flexible distance-learning or onsite course is specifically designed to equip participants with the knowledge and skills necessary to navigate AI compliance and execution effectively across corporate frameworks.

Participants who pass the online exam will receive a *Certificate of Completion*, offering verifiable proof of their expertise in AI compliance. This certification demonstrates your organization's commitment to ethical and regulatory AI practices, providing evidence of readiness to meet legislative standards and build trust with stakeholders.

COPENHAGEN
COMPLIANCE

Learning approach

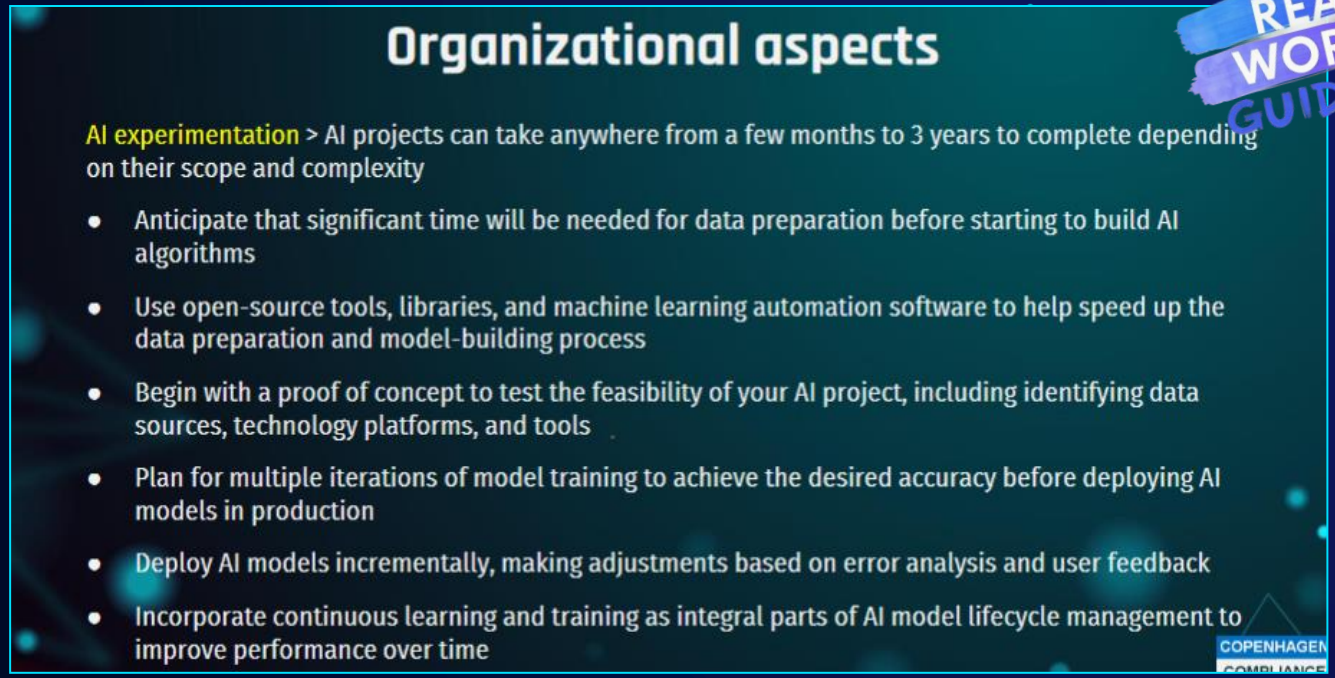


Practical Advise In Classes

Recommendations

- To ensure AI projects address real problems and deliver value, identify
  - how current processes function, where inefficiencies or bottlenecks exist, and how they can potentially be automated, improved, or optimized, and
  - expectations from the business stakeholders on business and objectives requirements, and financial
- Define clear objectives by setting measurable success criteria and aligning them with user needs, ensuring that the AI project has well-defined goals from the start
- Assemble a cross-functional AI Ops Team with representation from data science, IT, and business functions to promote collaboration and prevent siloed efforts
- Conduct a technical feasibility assessment early in the project to understand AI's capabilities and limitations, preventing unrealistic expectations and scope overreach
- Vet AI vendors and solutions by thoroughly evaluating their technical offerings and ensuring they align with the project's requirements and constraints

Practical Advise In Classes



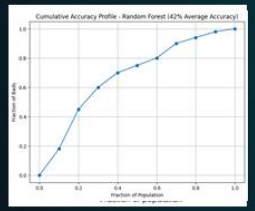
Practical Advise In Classes

REAL WORLD GUIDANCE

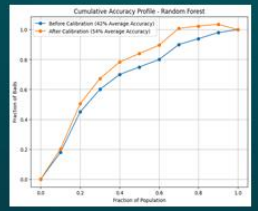
Model calibration

Accuracy

Random forest before calibration



Random forest after calibration



Step 1 Calibration > adjusting a model's output to make sure the predicted probabilities accurate

Step 2 Validation > assessing how well a model performs on unseen data to determine if the model generalizes well beyond the training data, focused on accuracy, precision, and recall metrics and mean absolute errors

Step 3 Fine-tuning > adjusting the model's hyperparameters (learning rates, batch sizes, regularization strength (L1 or L2), iterations) or retraining it on specific data to improve performance

COPENHAGEN COMPLIANCE

Tools with Examples

RESOURCES

Example Use case analysis form

Use case title	Objective	Business need (problem)
Automating due diligence questionnaire reporting with AI	To automate the generation of due diligence questionnaire reports by leveraging an AI agent, reducing manual effort, and ensuring consistency and accuracy	We frequently receive due diligence questionnaires from clients, requiring detailed responses on security controls, policies, and procedures. The

Expected user roles	Expected reach	Expected needed data
• Security Analysts: Review and finalize AI-generated reports • Compliance Officers: Ensure responses align with regulatory requirements • IT Managers: Oversee the integration of the AI agent	• Internal teams: 7 employees in the security, compliance, and IT departments • External stakeholders: 240 clients receiving our due diligence confirmations per year	• IT control matrix: list of 154 security controls and corresponding narratives • Internal policies: 12 documents of the organization's security policies

Guidelines with Demonstrations

WALKTHROUGH

Basic elements of AI model cards

Model basics

- **Model type**: define a standardized taxonomy for model types and include a separate field for a brief description
- **Licenses and citations**: documenting the intellectual property and referencing original works related to the model
- **Date and version:** tracking version history and release dates for model iterations
- **Glossary**: definitions of technical terms used References: list of sources, tools, and methodologies

Intended uses

- **Purpose and scope**: clarification of the model's intended applications and limitations
- **Compliance and legal considerations**: addressing context-specific laws, norms, and expectations relevant to the model's deployment settings

Training and evaluation

- **Data sources and preparation**: details on the datasets used, including preprocessing steps.
- **Testing and validation**: describing test sets, metrics, and tools used during the model's evaluation phase.
- **Performance limitations**: known limitations in the model's performance under various conditions.
- **Metrics justification**: explaining the choice of performance metrics and any trade-offs considered during model development.

Discussion Cases

LEARN
OTHERS

Business case 1 ChatGPT ban

Intro

Apple has banned employees from using ChatGPT and other AI tools, citing concerns over data security, privacy, and potential exposure of proprietary information.

Facts

- The ban on AI tools like ChatGPT stems from fears that data shared with these platforms owned or backed by Apple's rival Microsoft could compromise sensitive company information
- Similar bans have been implemented by other companies due to incidents of accidental data leaks and concerns about compliance

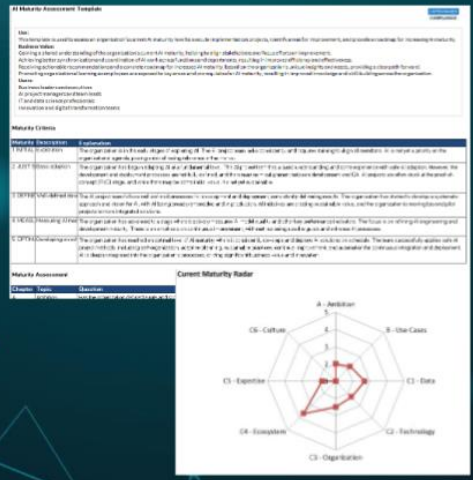
Discussion

How should companies balance the efficiency gains from AI tools with the potential risks to proprietary data and operations in the responsible AI policy?

Ready-to-Use Facilitators

HANDS-ON

Tool 7 Maturity assessment template



- This document helps you to evaluate their AI capabilities, identify gaps, and define a strategic roadmap for growth

Tool 1 AI project charter and plan

AI Project Charter and Plan Template

I. Project Overview

Field	Response
Project Name:	[Insert project name]
Project Description:	[Provide a concise summary of the project's purpose, scope, and expected outcomes]
Business Objectives:	
• Primary Objective:	[Describe the main goal of the AI project, e.g., increasing operational efficiency, developing a new product]
• Secondary Objectives:	[List other objectives that support the primary goal, such as improving customer satisfaction, enhancing data analysis capabilities]
Alignment with Organizational Strategy:	[Explain how the project supports the organization's strategic goals and priorities, including expected business benefits and strategic alignment]

II. Governance Framework

Field	Response
Project Sponsor:	[Name and title of the person sponsoring the project, responsible for high-level support and funding]
Project Manager:	[Name and title of the person managing the project, responsible for day-to-day operations and project execution]
AI Development Team:	[List names and titles of key team members, include roles such as data scientists, AI engineers, project analysts]
Governance Structure:	[Describe the structure for decision-making, oversight, and project management, including any steering committees or review boards]
Accountability:	[Define who is accountable for specific aspects of the project, including development, deployment, and maintenance]

III. Risk Assessment

Field	Response
Risk Categories:	[Identify categories of potential risks, such as technical failures, ethical concerns, legal issues, and societal impacts]
Risk Prioritization:	[Assess and rank risks based on their likelihood and potential impact on the project]
Mitigation Strategies:	[Detail strategies to address each identified risk, including contingency plans, risk reduction techniques, and monitoring procedures]

IV. Data Governance

- This document it used to establish roles, manage resources, and communicate progress to stakeholders
- It defines the project's scope, governance, and risk management. It guides the project from initiation through execution, ensuring alignment with organizational goals and compliance with regulations
- Regular updates and reviews keep the project on track and responsive to changes

Kersi Porbunderwalla > Program lead

- Professor at the IE Law School, the Copenhagen Business School from 1984-1993 and lecturer at Georgetown University, Cass Business School, and Fordham University
- President and CEO at Copenhagen Compliance, The Information Security Institute, The Corporate Governance Institute, The EUGDPR and The E-Compliance Academy
- Established global GRC networks to provide certifications and training and has trained professionals on four continents
- Lead organization in the development and implementation of AI-driven solutions, GRC applications,, and frameworks, including specialized cybersecurity and privacy products

COPENHAGEN
COMPLIANCE

Hernan Huwyler › Instructor

- Executive Education Director at IE Law School, driving innovation in risk management, audit, AI, and control through professorships and lectures at top-tier universities and law schools
- Results-driven executive leading technology, risk, privacy, and compliance programs in Forbes 500 organizations and Big Four firms
- Expert risk assessor and data analyst, utilizing predictive models in Python and R to inform business decisions and optimize risk, impact, control, and compliance assessments for clients and organizations.
- Researcher and influencer in AI, compliance, and IT audit

COPENHAGEN
COMPLIANCE


CERTIFICATION ★ EXERCISES ★ RESEARCH ★ TRAINING
IMPROVE ★ ORGANIZATION ★ NEEDS
IN CONTROL ★ FACILITATION
INSTRUCTION ★ COURSES ★ AUTHORITY ★ TRACKING
COPENHAGEN
COMPLIANCE
Global GRC Solutions
The Talent & Consultancy Exchange Pool