

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

ISO 24029 — Assessment of Robustness of Neural Networks

ISO Certification Programme



LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference IIT-AII-24029 • ISO IT & Related Technologies

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IIT-AII-24029
AWARD	Certificate
ASSESSMENT	430 marks — 258 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1

Assessment Techniques for AI Systems

5 chapters · 30 classes105 marks

• 1 Foundations of AI System Assessment Techniques — 6 classes

› 1.1 Identify Key Components of AI System Assessment

› 1.2 Analyze Assessment Techniques for AI Robustness

› 1.3 Compare Qualitative and Quantitative Assessment Methods

› 1.4 Design a Framework for Evaluating AI Systems

› 1.5 Implement Assessment Metrics for Neural Network Robustness

› 1.6 Reflect on the Impact of Assessment Techniques on AI Development

• 2 Evaluating Neural Network Architectures — 6 classes

› 2.1 Understand Key Characteristics of Neural Network Architectures

› 2.2 Explore Common Neural Network Models and Their Applications

› 2.3 Assess Performance Metrics for Neural Networks

› 2.4 Analyze Strengths and Weaknesses of Various Architectures

› 2.5 Apply Evaluation Techniques to Compare Neural Network Designs

› 2.6 Develop a Framework for Robustness Assessment in Neural Networks

• 3 Robustness Metrics and Measurement Methods — 6 classes

› 3.1 Identify Key Robustness Metrics for Neural Networks

› 3.2 Analyze Measurement Methods for Evaluating Robustness

› 3.3 Explore Statistical Techniques for Robustness Assessment

› 3.4 Compare Different Robustness Metrics in Real-world Scenarios

› 3.5 Apply Robustness Measurement Methods to Sample AI Systems

› 3.6 Review Best Practices for Reporting Robustness Results

• 4 Testing Strategies for AI System Resilience — 6 classes

› 4.1 Identify Key Concepts in AI Resilience Assessment

› 4.2 Explore Various Testing Strategies for Neural Networks

› 4.3 Analyze Effectiveness of Stress Testing Techniques

› 4.4 Implement Adversarial Testing to Evaluate Robustness

› 4.5 Develop a Framework for Continuous Testing in AI Systems

› 4.6 Create a Comprehensive Report on AI System Resilience Findings

• 5 Future Trends in AI Robustness Assessment — 6 classes

› 5.1 Explore Emerging Frameworks for AI Robustness Assessment

› 5.2 Analyze Current Trends Influencing AI System Security

› 5.3 Identify Key Metrics for Evaluating Neural Network Resilience

› 5.4 Examine Case Studies on Robustness Failures in AI

› 5.5 Develop Strategies for Implementing Robustness Assessments

› 5.6 Reflect on Future Challenges and Opportunities in AI Robustness

• 1 Fundamentals of Data Analysis in Neural Networks — 6 classes

- › 1.1 Define Key Concepts of Data Analysis in Neural Networks
- › 1.2 Identify Different Data Types Used in Neural Networks
- › 1.3 Explore Data Preprocessing Techniques for Machine Learning
- › 1.4 Analyze the Role of Training Data in Neural Network Performance
- › 1.5 Evaluate Model Performance Metrics for Neural Network Assessment
- › 1.6 Apply Data Visualization Techniques to Interpret Neural Network Results

• 2 Statistical Methods for Data Interpretation — 6 classes

- › 2.1 Define Key Statistical Concepts for Data Interpretation
- › 2.2 Apply Descriptive Statistics to Summarize Data Sets
- › 2.3 Utilize Probability Distributions in Data Analysis
- › 2.4 Conduct Hypothesis Testing for Statistical Inference
- › 2.5 Analyze Correlation and Regression Techniques
- › 2.6 Implement Statistical Methods for Real-World Data Interpretation

• 3 Validation Techniques for Robustness Assessment — 6 classes

- › 3.1 Identify Key Validation Techniques for Neural Networks
- › 3.2 Analyze Metrics for Evaluating Model Robustness
- › 3.3 Compare Cross-Validation Methods for Robust Assessment
- › 3.4 Implement Data Augmentation for Enhanced Validation
- › 3.5 Examine the Impact of Adversarial Testing on Robustness
- › 3.6 Apply Robustness Assessment Techniques in Real-World Scenarios

• 4 Data Visualization and Reporting Results — 6 classes

- › 4.1 Identify Key Elements of Effective Data Visualizations
- › 4.2 Explore Different Types of Data Visualizations and Their Uses
- › 4.3 Analyze the Impact of Color and Design on Data Interpretation
- › 4.4 Develop Interactive Dashboards for Dynamic Data Presentation
- › 4.5 Construct Comprehensive Reports that Communicate Findings Clearly
- › 4.6 Present Data Insights to Stakeholders Using Visual Tools

• 5 Advanced Analytical Techniques for Neural Network Optimization
— 6 classes

- › 5.1 Analyze Neural Network Performance Metrics
- › 5.2 Evaluate Data Preprocessing Techniques for Optimization
- › 5.3 Implement Regularization Methods to Prevent Overfitting
- › 5.4 Explore Hyperparameter Tuning Strategies
- › 5.5 Apply Advanced Optimization Algorithms
- › 5.6 Assess Model Robustness through Validation Techniques

• 1 Understanding Neural Network Architectures and Components —
6 classes

- › 1.1 Explore Key Components of Neural Networks
- › 1.2 Identify Types of Neural Network Architectures
- › 1.3 Analyze the Role of Activation Functions
- › 1.4 Examine the Importance of Layers in Neural Networks
- › 1.5 Evaluate Different Training Techniques for Resilience
- › 1.6 Design a Simple Neural Network Architecture

• 2 Principles of Robustness in Neural Networks — 6 classes

- › 2.1 Define Robustness in Neural Networks
- › 2.2 Identify Challenges to Neural Network Robustness
- › 2.3 Explore Techniques for Enhancing Robustness
- › 2.4 Evaluate Robustness through Testing Methods
- › 2.5 Analyze Case Studies of Robust Neural Networks
- › 2.6 Implement Best Practices for Resilience in Design

• 3 Techniques for Enhancing Neural Network Robustness — 6 classes

- › 3.1 Identify Key Vulnerabilities in Neural Networks
- › 3.2 Explore Regularization Techniques for Enhanced Generalization
- › 3.3 Implement Data Augmentation Strategies for Robust Training
- › 3.4 Analyze Adversarial Training Methods to Improve Resilience
- › 3.5 Evaluate Ensemble Techniques for Enhanced Network Performance
- › 3.6 Apply Robustness Metrics to Assess Neural Network Strength

• 4 Testing and Evaluating Neural Network Robustness — 6 classes

- › 4.1 Identify Key Metrics for Neural Network Robustness
- › 4.2 Explore Common Testing Techniques for Neural Networks
- › 4.3 Implement Adversarial Testing Scenarios
- › 4.4 Analyze Performance Under Varying Conditions
- › 4.5 Conduct Comparative Evaluations of Robustness Strategies
- › 4.6 Develop a Comprehensive Robustness Assessment Report

• 5 Real-World Applications and Case Studies of Resilient Neural Networks — 6 classes

- › 5.1 Analyze the Importance of Resilient Neural Networks in Industry
- › 5.2 Explore Case Studies of Neural Networks in Healthcare Applications
- › 5.3 Examine the Role of Resilience in Autonomous Vehicles
- › 5.4 Investigate Financial Sector Applications of Robust Neural Networks
- › 5.5 Assess the Impact of Neural Networks in Natural Disaster Management
- › 5.6 Develop Proposals for Future Applications of Resilient Neural Networks

• 1 Understanding Neural Networks: Fundamentals and Architecture

— 6 classes

- › 1.1 Define Neural Networks: Key Concepts and Terminology
- › 1.2 Explore Neural Network Architecture: Layers and Nodes
- › 1.3 Analyze Activation Functions: Types and Their Impact
- › 1.4 Examine Learning Algorithms: Training Neural Networks
- › 1.5 Investigate Common Architectures: CNNs and RNNs
- › 1.6 Apply Concepts: Designing a Simple Neural Network

• 2 Identifying Vulnerabilities: Common Weaknesses in Neural Networks — 6 classes

- › 2.1 Analyze Common Weaknesses in Neural Networks
- › 2.2 Explore Key Factors Affecting Neural Network Performance
- › 2.3 Identify Sources of Vulnerability in Dataset Preparation
- › 2.4 Investigate Architectural Flaws in Neural Network Design
- › 2.5 Assess the Impact of Adversarial Attacks on Neural Networks
- › 2.6 Develop Strategies to Mitigate Identified Vulnerabilities

• 3 Testing for Robustness: Methodologies and Tools — 6 classes

- › 3.1 Identify Key Concepts in Neural Network Robustness
- › 3.2 Explore Different Testing Methodologies for Robustness
- › 3.3 Analyze Tools for Evaluating Neural Network Performance
- › 3.4 Implement Unit Testing Strategies for Neural Networks
- › 3.5 Conduct Stress Testing on Neural Network Models
- › 3.6 Develop a Robustness Assessment Framework for Practical Application

• 4 Mitigation Strategies: Enhancing Neural Network Resilience — 6 classes

- › 4.1 Identify Vulnerabilities in Neural Networks
- › 4.2 Analyze Common Threats to Neural Network Integrity
- › 4.3 Explore Data Augmentation Techniques for Robustness
- › 4.4 Implement Adversarial Training to Enhance Resilience
- › 4.5 Evaluate the Effectiveness of Regularization Methods
- › 4.6 Design a Comprehensive Robustness Assessment Plan

• 5 Assessment Compliance: Aligning with ISO 24029 Standards — 6 classes

- › 5.1 Understand ISO 24029 Standards for Neural Network Assessment
- › 5.2 Identify Key Components of Robustness in Neural Networks
- › 5.3 Evaluate Current Assessment Methods Against ISO 24029
- › 5.4 Develop Assessment Criteria for Neural Network Compliance
- › 5.5 Implement Best Practices for Aligning Neural Networks with ISO Standards
- › 5.6 Analyze Case Studies of Neural Network Compliance Assessments

• 1 Understanding ISO Standards in Artificial Intelligence — 6 classes

- › 1.1 Define Key ISO Standards in Artificial Intelligence
- › 1.2 Explore the Importance of Compliance in AI Systems
- › 1.3 Identify the Components of ISO 24029 Certification
- › 1.4 Assess the Role of Neural Networks in Achieving Standards
- › 1.5 Examine Case Studies on ISO Compliance in AI
- › 1.6 Develop an Action Plan for Implementing ISO Standards

• 2 Overview of ISO 24029 and Its Objectives — 6 classes

- › 2.1 Define ISO 24029 and Its Key Components
- › 2.2 Explore the Objectives of ISO 24029
- › 2.3 Identify Stakeholders in the Assessment Process
- › 2.4 Assess the Importance of Neural Network Robustness
- › 2.5 Analyze Compliance Requirements under ISO 24029
- › 2.6 Develop an Action Plan for Implementing ISO 24029

• 3 Framework for Assessing Neural Network Robustness — 6 classes

- › 3.1 Define Neural Network Robustness and Its Importance
- › 3.2 Explore ISO 24029 Standards for Neural Networks
- › 3.3 Identify Key Criteria for Assessing Robustness
- › 3.4 Analyze Common Assessment Methods for Neural Networks
- › 3.5 Evaluate Real-World Case Studies of Neural Network Failures
- › 3.6 Develop a Robustness Assessment Plan for a Neural Network

• 4 Compliance Requirements and Implementation Strategies — 6 classes

- › 4.1 Overview Compliance Requirements for ISO 24029
- › 4.2 Identify Key Stakeholders in Compliance Implementation
- › 4.3 Analyze Current Practices Against ISO 24029 Standards
- › 4.4 Develop Effective Compliance Strategies for Neural Networks
- › 4.5 Create an Action Plan for Implementing Compliance Procedures
- › 4.6 Evaluate and Monitor Compliance Effectiveness Post-Implementation

• 5 Case Studies and Future Trends in ISO Compliance — 6 classes

- › 5.1 Analyze Key Case Studies in ISO 24029 Compliance
- › 5.2 Identify Common Challenges in Implementing ISO Standards
- › 5.3 Evaluate Trends in Neural Network Robustness Assessments
- › 5.4 Discuss Future Directions for ISO Compliance in AI
- › 5.5 Develop Strategies for Enhancing ISO Certification Processes
- › 5.6 Create a Compliance Action Plan Based on Case Study Insights