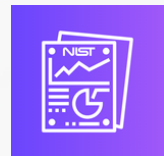




# **AKYLADE** **AI Security Foundation™** **(A/AISF™) Exam Objectives**






## **Exam Code: AIF-001**



## EXAM DETAILS

EXAM NAME	AKYLADE AI Security Foundation™ (A/AISF™)
EXAM CODE	AIF-001
QUESTION ITEMS	50 multiple-choice questions
DURATION	60 minutes
PASSING SCORE	700 points on a scale of 100 to 900 points

## EXAM DOMAINS

	DOMAIN	EXAM COVERAGE
	1.0 Artificial Intelligence Concepts	23%
	2.0 AI Risk Management	19%
	3.0 AI Risks and Trustworthiness	22%
	4.0 NIST AI RMF Core	21%
	5.0 NIST AI RMF Profiles	15%

## IMPORTANT NOTE:

AKYLADE continuously reviews and updates exam content to ensure that exams remain current, relevant, and secure. When necessary, AKYLADE may publish updated exams based on the existing exam objectives, but all related exam preparation materials will remain valid during a given exam's lifecycle. Under each objective, a list of bulleted examples has been provided to aid candidates during their studies. These lists are not exhaustive and serve as examples of technologies, processes, regulations, or tasks related to the relevant objective. Other examples may appear on the exam, even if they are not listed directly under the objective in this document.



## DOMAIN 1: Artificial Intelligence Concepts (23%)

### 1.1 Explain the basic principles and key terms associated with AI and machine learning.

- Artificial intelligence (AI)
- Machine learning (ML)
- Deep learning (DL)
- Natural language processing (NLP)
- Computer vision
- Types of machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning
  - Semi-supervised learning
  - Self-supervised learning
  - Transfer learning
- Machine learning algorithms
  - Regression
  - Classification
  - Clustering
- Reasons for data preprocessing
  - Improving data quality
  - Enhancing model performance
  - Increasing training efficiency
  - Reducing bias
  - Facilitating feature extraction
- Methods of data preprocessing
  - Data augmentation
  - Data cleaning
  - Data normalization
  - Data reduction
  - Data scaling
  - Data transformation
  - Feature engineering

### 1.2 Explain how deep learning functions and how neural networks are structured to support deep learning.

- Structure and components of neural networks
  - Nodes
    - Input neurons
    - Hidden neurons
    - Output neurons
  - Layers
    - Dense (fully connected) layers
    - Convolutional layers
    - Recurrent layers
  - Weights
- Bias
- Activation functions
  - Rectified linear unit (ReLU)
  - Sigmoid
  - Hyperbolic tangent (Tanh)
  - Softmax
- Training process
  - Forward propagation
  - Loss function
  - Backward propagation
  - Optimization algorithms
- Neural network architectures
  - Convolutional neural network (CNN)
  - Recurrent neural networks (RNN)
- Applications of deep learning
  - Image recognition
  - Video recognition
  - Speech recognition
  - Fraud detection
  - Algorithmic trading

### 1.3 Summarize the AI lifecycle and the steps required to develop an AI model.

- AI lifecycle
  - Plan and design
  - Collect and process data
  - Build and use model
  - Verify and validate
  - Deploy and use
  - Operate and monitor
  - Use or impacted by
- AI system key dimensions
  - Application context
  - Data and input
  - AI model
  - Task and output
- AI model development
  - Defining objectives
  - Data preprocessing
  - Model training
  - Evaluation
  - Tuning
  - Deployment

### 1.4 Summarize the various AI actors and their associated tasks that have an active role in the AI system lifecycle.

- AI actor tasks
  - AI design
  - AI development
  - AI deployment
  - Operation and monitoring
  - Test, evaluation, verification, and validation (TEVV)
  - Human factors
  - Domain expert
  - AI impact assessment
  - Procurement
  - Governance and oversight
- Additional AI actors
  - Third-party entities
  - End users
  - Affected individuals/communities
  - General public
- Other AI actors
  - Trade associations
  - Standards-developing organizations
  - Advocacy groups
  - Researchers
  - Environmental groups
  - Civil society organizations



## 1.5 Given a scenario, assess AI maturity and develop strategies for AI implementation.

- Evaluate AI maturity level
  - Utilize AI maturity models
    - Gartner AI maturity model
    - Cisco AI readiness index
  - Assess current AI capabilities and resources
  - Analyze organizational context
    - AI utilization
    - Intended outcomes
  - Conduct stakeholder interviews and surveys
  - Identify capability gaps
    - People
    - Processes
    - Technology
- Align AI strategies with business goals
  - Define AI vision and mission statements
  - Align AI initiatives with strategic objectives
  - Establish AI governance and leadership
  - Develop a business case for AI projects
- Develop a roadmap
  - Prioritize gaps
    - Based on impact
    - Based on feasibility
  - Create phased roadmap for adoption
  - Set short-term goals
  - Set long-term goals
- Facilitate cross-functional collaboration to design AI models
  - Roles and responsibilities
    - Enterprise architects
    - Security
    - DevOps
    - Business representatives
  - Develop a strong culture
    - Collaborative
    - Innovative
- Develop and implement AI strategies
  - AI centers of excellence (CoE)
  - AI ethics and governance frameworks
  - Training and development programs
  - AI solution iterative implementation
- Monitor and evaluate AI initiatives
  - AI performance metrics and KPIs
  - Periodic reviews and updates of strategies
  - Adapt based on feedback and results
  - Continuously improve and scale initiatives



## 1.6 Summarize the common AI technologies, tools, and use cases utilized across various industries.

- AI frameworks and libraries
  - Apache MXNet
  - Apache Spark
  - Caffe
  - XGBoost
  - Deeplearning4j (DL4J)
  - WatsonX
  - Keras
  - LangChain
  - Microsoft Cognitive Toolkit (CNTK)
  - OpenAI
  - OpenNN
  - PyBrain
  - PyTorch
  - Scikit-learn
  - TensorFlow
- AI platforms and services
  - OpenAI
    - ChatGPT
    - Dall-E
    - Sora
- AWS
  - Amazon Bedrock
  - Amazon Q
  - AWS SageMaker
- Google AI Platform
  - Gemini
  - Vertex AI
- Microsoft
  - Azure AI
  - Copilot
- SAP Hana Cloud
- WatsonX
- Use cases
  - Finance
  - Algorithmic trading
  - Fraud detection
  - Risk management
  - Credit scoring
- Healthcare
  - Diagnostics
  - Imaging
  - Personalized medicine
  - Predictive patient outcomes
- Manufacturing
  - Predictive maintenance
  - Quality control
  - Supply chain optimization
- Retail
  - Automated self-checkout
  - Customer sentiment analysis
  - Customer support
  - Inventory management
  - Recommendation systems

## 1.7 Explain the ethical considerations, the role of data, and the deployment challenges that can occur while developing AI solutions.

- Ethical considerations
  - Fairness
  - Transparency
  - Accountability
  - Privacy
- Deployment challenges
  - Scalability
  - Integration
  - Regulatory compliance
  - Bias mitigation
- Role of data
  - Quality
  - Collection methods
  - Privacy
  - Security considerations
- Difference between AI and traditional systems



## DOMAIN 2: AI Risk Management (19%)

### 2.1 Explain the basic principles and key terms associated with AI risk management.

- Risk
- Threats
- Vulnerabilities
- Harm
  - To people
  - To organizations
  - To ecosystems
- Impacts
- Risk management
- Risk tolerance
- Risk appetite
- Types of risk
  - Inherent risk
  - Residual risk
  - Control risk
- Risk treatment
  - Risk acceptance
  - Risk avoidance
  - Risk mitigation
  - Risk transference

### 2.2 Given a scenario, explain how to conduct risk measurement for an AI system.

- Purpose of risk measurement
- Risk measurement challenges
  - Third-party software
  - Third-party hardware
  - Third-party data
  - Tracking emergent risks
  - Availability of reliable metrics
  - Risks at different AI lifecycle stages
  - Risk in real-world settings
  - Inscrutability
  - Human baseline
- Tools for measuring risk
  - Risk assessment frameworks
    - NIST AI risk management framework (AI RMF)
    - ISO/IEC 27005 and 31000
  - Risk analysis tools
    - OCTAVE
    - FAIR
  - Vulnerability assessment tools
  - Threat modeling tools
  - Penetration testing tools
  - AI-specific risk assessment tools
    - IBM AI Fairness 360
    - Google's What-If tool
- Determining risk tolerance
  - Legal or regulatory requirements
  - Policies and norms
  - Key stakeholders
    - Executives
    - Policy makers
    - System owners
    - Industries

## 2.3 Given a scenario, explain how an AI risk assessment is conducted.

- Risk identification
  - Define objective
  - Define scope
  - Identify risks
  - Conduct threat modeling
- Risk analysis
  - Analyze risk scenarios
  - Assess vulnerabilities
    - AI model
    - Data
    - Infrastructure
- Risk evaluation
  - Prioritize risks
  - Compare against risk tolerance
  - Validate risks with penetration testing
- Risk mitigation
  - Develop mitigation strategies
  - Deploy measures
  - Implement security controls
- Documentation and reporting
  - Prepare risk assessment report
  - Communicate results of report
- Monitor and review
  - Monitor risk environment
  - Consider emerging risks
  - Review and update assessment

## 2.4 Summarize how governance is used to integrate AI risk management policies, practices, and processes across the organization.

- AI risk management integration and documentation in organizational governance
  - Frameworks
  - Policies
  - Practices
  - Processes
  - Development guidelines
    - Risk by design
    - Impact on AI system development
- Emerging guidance and standards
  - ISO 27090
  - ISO 27091
  - ISO 31000
  - ISO 42001
  - Industry best practices
  - Regulatory requirements
  - AI Act (Regulation EU 2024/1689)
- Governance roles and responsibilities
  - Board of directors
  - Chief executive officer (CEO)
  - Chief risk officer (CRO)
  - Chief information security officer (CISO)
  - Chief data officer (CDO)
  - Chief legal officer
  - AI governance committee
  - AI ethics officer
  - AI risk management team
  - Legal and compliance team
  - Internal audit team
  - Project managers
  - Business unit leaders





## DOMAIN 3: AI Risks and Trustworthiness (22%)



### 3.1 Summarize the different characteristics of trustworthy AI systems.

- Valid and reliable
  - Accuracy
  - Robustness
  - Generalizability
- Safe
  - Secure and resilient
  - Accountable and transparent
- Explainable and interpretable
  - Privacy-enhanced
  - Fair with harmful bias managed

### 3.2 Given a scenario, balance the different characteristics of trustworthy AI systems based on the AI system's context of use to reduce negative AI risks.

- Valid and reliable
- Safe
- Secure and resilient
- Accountable and transparent
- Explainable and interpretable
- Privacy-enhanced
- Fair with harmful bias managed

### 3.3 Given a scenario, identify, document, and mitigate risks associated with AI systems.

- Risk identification
  - Identify potential security risks
    - Vulnerabilities in AI models, data, and infrastructure
  - Identify ethical and social risks
    - Bias and fairness issues
    - Privacy and data protection issues
  - Identify operational risks
    - System performance
    - Reliability
    - System integrations
    - Deployments
- Risk mitigation
  - Implement security controls
    - Encryption
    - Access controls
    - Secure development
    - Periodic security assessments
    - Security training
  - Address bias and fairness
    - Bias detection
    - Bias mitigation
    - Diverse training data
    - Representative training data
- Enhance transparency and explainability
  - Use interpretable models
  - Explainability of AI decisions
  - Transparency in development
- Strengthen privacy protections
  - Data anonymization
  - Pseudonymization
  - Data protection regulatory compliance

- Ensure robustness and reliability
  - Rigorous testing
  - Validation of AI models
  - Redundancy implementation
  - Failover mechanism utilization
- Develop risk management plans
  - Use of frameworks and policies
  - AI risk monitoring and response
- Conduct continuous monitoring and improvement
  - AI system performance monitoring
  - Review and update of strategies and practices

### 3.4 Given a scenario, identify different AI threat actors based on their characteristics or motivations.

- External threat actors
  - Hackers
  - Cybercriminals
  - Nation-state actors
  - Industrial spies
- Internal threat actors
  - Malicious insider threats
- Negligent insider threats
  - Disgruntled employees
- Supply chain threat actors
  - Third-party vendors
  - Open-source contributors
- Threat actor motivations
  - Financial gain
  - Political or ideological beliefs
  - Corporate advantage
  - Revenge or retaliation

### 3.5 Given a scenario, explain the relationship between AI risks and societal impacts.

- Ethical guidelines
- Fairness and equality
- Bias and discrimination
- Transparency and explainability
  - Model transparency
  - Thorough documentation
- Accountability and responsibility
  - Clear roles and responsibilities
  - Monitoring and reporting
  - Continuous oversight and governance
  - Protocols for ethical violations
- Data privacy
  - Collection
  - Storage
  - Use
- Cybersecurity threats
- Job displacement
- Economic inequality
- Human-AI interactions
- Cultural change
- Regulations and governance
- Public awareness and education
- Stakeholder involvement



## DOMAIN 4: NIST AI RMF Core (21%)

### 4.1 Summarize the key aspects of the NIST Artificial Intelligence (AI) Risk Management Framework (RMF) Core.

- AI RMF Core
  - Purpose
  - Benefits
  - Effectiveness
  - Usage
  - Relationship with organizational policies
- Components of the AI RMF Core
  - Govern
  - Map
  - Measure
  - Manage
- Implementation challenges
- Alignment with business objectives
- Best practices

### 4.2 Given a scenario, utilize the Govern function's categories and subcategories to conduct AI risk management.

- GOVERN 1 - Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively
- GOVERN 2 - Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks
- GOVERN 3 - Workforce diversity, equity, inclusion, and accessibility are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle
- GOVERN 4 - Organizational teams are committed to a culture that considers and communicates AI risks
- GOVERN 5 - Processes are in place for robust engagement with relevant AI actors
- GOVERN 6 - Policies and procedures are in place to address AI risks and benefits arising from third-party software and data, and other supply chain issues

### **4.3 Given a scenario, utilize the Map function's categories and subcategories to conduct AI risk management.**

- MAP 1 - Context is established and understood
- MAP 2 - Categorization of AI systems is performed
- MAP 3 - AI capabilities, targeted usage, goals, and expected benefits and costs with appropriate benchmarks are understood
- MAP 4 - Risks and benefits are mapped for all components of the AI systems, including third-party software and data
- MAP 5 - Impacts on individuals, groups, communities, organizations, and society are characterized

### **4.4 Given a scenario, utilize the Measure function's categories and subcategories to conduct AI risk management.**

- MEASURE 1 - Appropriate methods and metrics are identified and applied
- MEASURE 2 - AI systems are evaluated for trustworthy characteristics
- MEASURE 3 - Mechanisms for tracking identified AI risks over time are in place
- MEASURE 4 - Feedback about efficacy of measurement is gathered and assessed

### **4.5 Given a scenario, utilize the Manage function's categories and subcategories to conduct AI risk management.**

- MANAGE 1 - AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed
- MANAGE 2 - Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors
- MANAGE 3 - AI risks and benefits from third-party entities are managed
- MANAGE 4 - Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks, are documented and monitored regularly to ensure effectiveness and continual improvement





## DOMAIN 5: NIST AI RMF Profiles (15%)

### 5.1 Summarize the key aspects of the NIST Artificial Intelligence (AI) Risk Management Framework (RMF) Profiles.

- AI RMF Profiles
  - Purpose
  - Benefits
  - Effectiveness
  - Usage
- Components of an AI RMF Profile
  - Executive summary
  - Background
    - Objective of profile
    - Scope of profile
    - Type of profile
      - Current
      - Target
    - Definitions (optional)
  - Intended audience
- AI System management and schedule
  - Roles and responsibilities
  - Decision-making authority
  - Lifecycle stages
    - Decision points at each stage
    - Decision authority for each stage
    - Resources for each stage
    - Documentation of each decision point
- Prioritization methods of subcategories
  - Audiences
  - AI lifecycle stages
  - Mission objectives
  - Risk tolerances
  - Domains
  - Business drivers
  - Manufacturer priorities
  - Security environments
- Profile use cases

### 5.2 Given a scenario, manage AI risks within an organization by utilizing an AI RMF Profile.

- Creation of a profile
- Implementation of a profile
  - Processes
  - Steps
- Updating a profile
- Tailoring a profile
- Challenges associated with profiles

### 5.3 Given a scenario, utilize best practices and tools for managing a NIST Artificial Intelligence (AI) Risk Management Framework (RMF) Profile.

- Best practices
  - Implement risk management strategies
  - Support organizational goals
  - Develop AI systems
  - Meet regulatory compliance
- Tools
  - AI governance platforms
  - Compliance management tools
  - Risk management tools
- AI RMF Profiles
- Risk management strategies
- Metrics and analytic tools
- Collaboration tools