

100-Mark Total Scale		1. Statutory Year-Work Grade Distribution & Final Assessment System (Term 1)	
Assessment Component	Weight (%)	Marks Allocated	Regulatory Guidelines, Evidence & Classroom Execution
Weekly Continuous Quizzes	15 %	15 Marks	Parallel Tri-Model quizzes (A, B, C) assessing AI mechanics, cybersecurity, and web engineering.
Homework Assignments	15 %	15 Marks	Textbook exercises, research papers, LMS platform tasks, and weekly problem sets.
Class Participation & Discipline	5 %	5 Marks	Active lab engagement, note-taking in notebook, safety compliance, and positive behavior.
Practical Performance Tasks	10 %	10 Marks	Two dedicated lab tasks: 1) DMZ & RSA Cryptography, 2) Interactive Accessible Web App.
October Standardized Exam	5 %	5 Marks	School-level unified written/practical exam covering Chapter 1 (IT & AI Foundations).
November Standardized Exam	5 %	5 Marks	School-level unified written/practical exam covering Chapters 2 & 3 (Cybersecurity & Web Apps).
Total Coursework / Year-Work Subtotal		50 Marks	Recorded periodically and submitted to the School Examination Control Committee.
Term 1 Summative Final Examination	50 %	50 Marks	Unified final exam: 20 Marks Practical Lab Exam + 30 Marks Written Theoretical Paper.
Overall Term 1 Grand Total	100 %	100 Marks	Official semester score determining academic standing and promotion criteria.

Pedagogical Standards	2. Parallel Tri-Model Assessment Strategy (Models A, B, C) & Differentiation
Academic Integrity & Anti-Copying: Distribute Models A, B, and C alternately across adjacent student seating rows to ensure authentic individual diagnostic responses. Equi-Difficulty Calibration: Each model targets the identical Depth of Knowledge (DOK) and core learning outcome while modifying parameter values, code snippets, or architectural topologies. Immediate Formative Feedback: Administer during the opening 7–10 minutes of the weekly session, followed by rapid targeted remediation to eliminate conceptual bottlenecks. Theory-to-Code Integration: Questions balance architectural comprehension (e.g. 3-Tier, DMZ) with technical precision (DOM manipulation, cryptographic math, CSS Grid).	

Performance Rubric	3. Laboratory Competency Descriptors & Mastery Criteria	
Proficiency Band	Score Range	Demonstrated Technical Competencies & Behavioral Indicators
Exceeds Standards (Advanced)	85% - 100%	Flawlessly articulates AI neural mechanisms, configures secure network DMZ policies, writes clean semantic HTML5/CSS Grid/JS code, and adheres strictly to WCAG accessibility guidelines.
Meets Standards (Proficient)	75% - 84%	Demonstrates sound technical grasp of 3-Tier architecture and REST APIs; constructs functional web pages and explains encryption protocols with minor syntactic or formatting flaws.
Developing (Approaching)	65% - 74%	Requires structured teacher prompts to trace DOM tree modifications or distinguish between symmetric and asymmetric ciphers; benefits from guided lab worksheets.
Needs Remediation (Novice)	Below 65%	Struggles to connect algorithmic principles to lab implementations; enrolled in the weekly remedial intervention program and assigned foundational platform drills.

Week 1: IT Development, Moore's Law & Edge Computing

Chapter 1: Unit 1-1

Model A

State Moore's Law. How has exponential transistor scaling driven the emergence of modern generative AI?

Model B

Compare Cloud Computing and Edge Computing in terms of transmission latency and bandwidth efficiency.

Model C

Provide two real-world application scenarios where edge computing is indispensable due to real-time response needs.

Homework: Solve textbook exercises on page 14 regarding edge hardware deployment in industrial automation.

Week 2: AI Mechanics, Learning Paradigms & Neural Networks

Chapter 1: Unit 1-2

Model A

Precisely differentiate between Supervised Learning, Unsupervised Learning, and Reinforcement Learning.

Model B

Outline the structural layers of an Artificial Neural Network (Input layer, Hidden layers, Output layer).

Model C

Contrast classical Machine Learning with Deep Learning regarding automated feature extraction from raw data.

Homework: Draw a conceptual diagram showing how weights and biases propagate signals through perceptron nodes.

Week 3: AI in Daily Life, Industry & Recommender Systems

Chapter 1: Unit 1-3

Model A

Explain how Collaborative Filtering generates product recommendations based on peer user behavior patterns.

Model B

Compare Content-Based Filtering with Collaborative Filtering, citing a practical example for each method.

Model C

Detail the role of Computer Vision and Natural Language Processing (NLP) in autonomous vehicles and voice agents.

Homework: Analyze an e-commerce platform and document the algorithmic recommendation techniques used.

Week 4: AI Ethics, Algorithmic Bias & Explainable AI (XAI)

Chapter 1: Unit 1-4

Model A

Define the "Black Box" dilemma in deep neural models and explain why Explainable AI (XAI) is critical.

Model B

Explain how Algorithmic Bias enters trained models and discuss its societal and legal consequences.

Model C

Analyze the ethical and copyright challenges posed by generative Deepfakes and synthetic media.

Homework: Write a concise critique (5 lines) addressing moral dilemma algorithms in autonomous navigation.

Week 5: AI Model Evaluation Workshop & October Review

October Review

Model A

Calculate model Accuracy if a classifier processes 100 test samples and correctly predicts 85 of them.

Model B

Distinguish between Precision and Recall metrics, explaining which is prioritized in critical medical diagnoses.

Model C

Justify why overall Accuracy is misleading when evaluating classifiers trained on highly imbalanced datasets.

Homework: Complete the October mock examination paper in the student workbook covering Chapter 1.

Week 6: Cryptographic Technologies, Hashes & Digital Signatures

Chapter 2: Unit 2-1

Model A

Compare Symmetric encryption (e.g. AES) and Asymmetric encryption (e.g. RSA) regarding key distribution.

Model B

State the core properties of cryptographic hash functions (e.g. SHA-256). Why is collision resistance essential?

Model C

Explain how Digital Signatures guarantee sender authentication, message integrity, and non-repudiation.

Homework: Create an encryption flow chart illustrating the role of Public and Private keys in an RSA session.

Week 7: Network Security Design, Firewalls & DMZ Architecture

Chapter 2: Unit 2-2

Model A

Define a Demilitarized Zone (DMZ) in network topology and name two public servers placed inside it.

Model B

Explain the Zero Trust Architecture philosophy and its foundational mantra: "Never trust, always verify."

Model C

How does a Packet Filtering Firewall inspect incoming traffic using IP headers and TCP/UDP port numbers?

Homework: Draw an enterprise network diagram showing LAN, DMZ, perimeter firewalls, and the public internet.

Week 8: Incident Response, CSIRT Framework & Business Continuity (BCP)

Chapter 2: Unit 2-3

Model A

Order the phases of incident handling in the CSIRT framework: Detection, Containment, Eradication, Recovery, Lessons.

Model B

What is the primary objective of a Business Continuity Plan (BCP) following a severe cyber breach?

Model C

List three immediate containment procedures to execute upon discovering a ransomware infection on a corporate host.

Homework: Summarize digital forensics protocols for collecting chain-of-custody volatile memory artifacts.

Week 9: Cybersecurity Defense Simulation & Attack Mitigation Lab

Chapter 2: Practical Lab

Model A

Analyze a deceptive phishing email and identify three technical red flags in URL syntax and sender domain headers.

Model B

How are Distributed Denial of Service (DDoS) attacks detected, and what traffic filtering mitigates the load?

Model C

Explain the cryptographic mechanism of Password Salting and Hashing to prevent rainbow table lookup attacks.

Homework: Design a comprehensive cybersecurity auditing checklist for multi-factor online banking security.

Week 10: 3-Tier Web Application Architecture & RESTful APIs

Chapter 3: Unit 3-1

Model A

Explain the specific role of each tier in a 3-Tier Architecture: Presentation Tier, Application Tier, and Database Tier.

Model B

Define a REST API and compare JSON versus XML as standard formats for asynchronous client-server data transfer.

Model C

Map the four fundamental database CRUD operations to standard HTTP request methods: GET, POST, PUT, DELETE.

Homework: Construct a syntactically valid JSON object representing a student profile with nested skills arrays.

Week 11: HTTP/HTTPS Protocols, Status Codes & WebSockets

Chapter 3: Unit 3-2

Model A

Explain the exact meaning of HTTP status codes: 200 OK, 301 Moved, 403 Forbidden, 404 Not Found, 500 Internal Error.

Model B

Identify the critical cryptographic difference between standard HTTP and TLS-encrypted HTTPS transport.

Model C

Contrast stateless HTTP requests with persistent, full-duplex WebSockets for low-latency live applications.

Homework: Inspect network request headers via browser Developer Tools (F12) and record status code diagnostics.

Week 12: Frontend HTML5 Semantics, CSS3 Grid & JavaScript DOM

Chapter 3: Unit 3-3

Model A

List three HTML5 semantic elements and explain their significance for SEO indexing and screen reader accessibility.

Model B

Write a CSS rule establishing a responsive 3-column layout using 'grid-template-columns: repeat(3, 1fr)'.

Model C

Write JavaScript code targeting element '#submit-btn' that toggles a class on user click using 'addEventListener'.

Homework: Construct a semantic HTML5 webpage featuring a structured navigation bar and responsive CSS Grid cards.

Week 13: Interactive Web Application Lab & November Review

November Review

Model A

Trace JavaScript code that captures user input from a form and dynamically appends an '' node into a '' tree.

Model B

Demonstrate how 'fetch()' asynchronously sends a GET request to an API endpoint and parses response JSON.

Model C

Diagnose the standard error 'Uncaught TypeError: Cannot read property of null' in DOM element selection.

Homework: Complete Chapter 3 self-assessment questions and prepare code files for the interactive lab showcase.

Week 14: Media Formats, Vector (SVG) vs Raster & Compression

Chapter 4: Unit 4-1

Model A

Contrast Raster images (JPEG/PNG) with Vector graphics (SVG/Bézier) regarding resolution scalability and file size.

Model B

Distinguish Lossy compression (e.g. JPEG, MP3) from Lossless compression (e.g. PNG, FLAC) in quality retention.

Model C

Calculate audio bitrate for uncompressed stereo sound recorded at a 44.1 kHz sampling rate and 16-bit depth.

Homework: Convert an icon into raw SVG format and analyze its underlying vector coordinate ' markup.

Week 15: Information Design, UI/UX Principles & WCAG Accessibility

Chapter 4: Unit 4-2

Model A

Differentiate between User Interface (UI) design and User Experience (UX) architecture in software engineering.

Model B

Explain the 60-30-10 color rule and how it ensures visual balance and user focal hierarchy in page layouts.

Model C

Cite two essential WCAG 2.2 AA accessibility guidelines designed to support visually impaired screen reader users.

Homework: Sketch a low-fidelity wireframe for an educational portal prioritizing accessible navigation flows.

Week 16: Website Heuristic Evaluation, Web Vitals (LCP) & PDCA

Chapter 4: Units 4-3 & 4-4

Model A

Explain two of Jakob Nielsen's 10 Usability Heuristics (e.g. Visibility of system status, Error prevention).

Model B

Define Largest Contentful Paint (LCP) as a Core Web Vital. What is the target threshold for good user experience?

Model C

Outline the iterative Design Thinking cycle: Empathize, Define, Ideate, Prototype, and Test.

Homework: Audit an educational web page using Lighthouse DevTools; record LCP metrics and usability feedback.

Performance Task 1: Network Security DMZ Topology & RSA Public-Key Cryptosystem

Weeks 6 - 8 | Weight: 10 Marks

Problem Scenario & Objective: An enterprise hospital requests a secure network redesign to protect confidential electronic patient records while maintaining a public-facing appointment booking portal. **Required Laboratory Implementation:**

- Draft a comprehensive network security topology illustrating: Internal Secure LAN, Demilitarized Zone (DMZ) hosting Web & Mail servers, Perimeter Firewalls, and Public Internet.
- Formulate an Access Control List (Firewall Packet Filtering Rules) permitting inbound HTTPS/HTTP (Ports 443/80) to the DMZ while enforcing a strict "Deny-All" default rule to the internal database.
- Simulate the RSA asymmetric cryptographic handshake: demonstrate public/private key pairing, confidential payload encryption, and digital signature authentication.

Evaluation Criterion	Exemplary (Full Mark: 2.5)	Proficient (1.5 to 2.0)	Developing / Needs Guidance (< 1.5)
DMZ Network Topology	Flawless segmentation, precise DMZ boundary isolation, and accurate host placement.	Correct topology with minor labeling or subnet masking omissions.	Flawed isolation; internal hosts exposed directly to public traffic.
Firewall Policy Rules	Rigorous port binding (443, 80), explicit state inspection, and default deny-all.	Functional rules but omits logging policies or transport protocol specifications.	Overly permissive rules creating clear security vulnerabilities.
RSA Cryptographic Simulation	Accurate demonstration of public-key encryption, private-key signing, and non-repudiation.	Correct key usage with minor conceptual confusion regarding signature hashing.	Confuses symmetric shared secret with asymmetric public-key mechanics.
Oral Defense & Timeliness	Punctual submission, confident articulation of defense decisions, and lab discipline.	Completed on time with slightly hesitant technical defense responses.	Late submission with significant difficulty explaining system design choices.

Performance Task 2: Accessible Interactive Web Application Prototype (HTML5 / CSS Grid / JS DOM)

Weeks 13 - 15 | Weight: 10 Marks

Problem Scenario & Objective: Engineer a fully functional educational client application displaying digital safety advisories and AI literacy cards that conforms strictly to international accessibility standards. **Required Laboratory Implementation:**

- Author a clean semantic HTML5 layout employing: ``<header>``, ``<nav>``, ``<main>``, ``<article>``, ``<aside>``, and ``<footer>`` with descriptive ``alt`` tags and ARIA labels.
- Construct a responsive CSS Grid layout utilizing ``repeat(auto-fit, minmax(250px, 1fr))`` styled in accordance with the 60-30-10 balanced color rule.
- Embed an event-driven JavaScript DOM engine: enable interactive category card filtering, real-time input search, and dynamic Dark/Light theme switching.

Evaluation Criterion	Exemplary (Full Mark: 2.5)	Proficient (1.5 to 2.0)	Developing / Needs Guidance (< 1.5)
Semantic HTML5 & Accessibility	Exemplary semantic structure conforming to WCAG 2.2 AA standards with full ARIA support.	Sound semantic tagging with minor omissions in accessibility metadata.	Non-semantic markup over-relying on generic unstructured ` <code><div></code> ` elements.
Responsive CSS Grid Design	Fluid responsive layout across screen viewports applying the 60-30-10 color principle.	Functional CSS Grid with minor alignment flaws during narrow viewport scaling.	Broken layout constraints, overlapping elements, or insufficient contrast.
JavaScript DOM Reactivity	Robust event handling (<code>addEventListener</code>), zero console warnings, and smooth UI updates.	Interactive features operate as intended with minor state caching defects.	Syntax errors halt script execution or fail to bind DOM elements.
Code Hygiene & Optimization	Modular code structure, meaningful identifiers, clear comments, and rapid LCP rendering.	Readable code with acceptable runtime responsiveness and standard formatting.	Disorganized scripts lacking inline documentation or optimization.

Official October Standardized Exam (Chapter 1: IT & AI Foundations + Unit 2-1
Cryptography)

Total Score: 15 Marks | Duration: 45
Minutes

Question 1: Multiple Choice Questions (5 Marks — 1 Mark per item)

- Moore's Law postulates that the number of transistors on an integrated circuit doubles approximately every two years while: [Cost falls by half — Price doubles — Chip dimensions expand — Scaling ceases].
- A computing paradigm that processes telemetry data at local network nodes rather than routing to remote cloud hubs is: [Cloud Warehousing — Edge Computing — Mainframe Hosting — Dial-up Access].
- The machine learning paradigm wherein an agent learns an optimal behavioral policy through numerical reward signals is: [Supervised — Unsupervised — Reinforcement Learning — Manual Rule-based].
- Under the RSA asymmetric cryptosystem, a confidential ciphertext payload sent to Bob is encrypted using: [Bob's Public Key — Alice's Private Key — Symmetric Passphrase — Cryptographic Hash].
- A fundamental defining property of cryptographic hash functions (such as SHA-256) is that they are: [Two-way reversible — One-way non-invertible — Key-dependent — Data-expanding].

Question 2: True / False Conceptual Verification (5 Marks)

- Collaborative Filtering generates recommendations based on historical user similarity patterns rather than item attributes. ()
- Explainable AI (XAI) refers to complex neural architectures whose internal logic cannot be audited or inspected by humans. ()
- A Digital Signature guarantees sender identity validation, message integrity verification, and non-repudiation. ()
- Deep Learning systems require continuous manual human intervention to extract features from complex unstructured datasets. ()
- Multi-Factor Authentication (MFA) mandates combining two or more distinct categories: knowledge, possession, or biometrics. ()

Question 3: Technical Problem Solving & Comparative Analysis (5 Marks)

- An AI clinical diagnostics model evaluated 200 patient records. It successfully generated 180 accurate predictions and misclassified 20 cases. **Calculate the model's Accuracy percentage**, stating the underlying formula. (2.5 Marks)
- Construct a comparative matrix** contrasting Symmetric and Asymmetric encryption across: Key quantity, Computational velocity, and Primary security use case. (2.5 Marks)

Official November Standardized Exam (Network Security, Incident Response, Web Apps & DOM)

Total Score: 15 Marks | Duration: 45
Minutes

Question 1: Scientific & Technical Terminology (5 Marks — 1 Mark per item)

- A dedicated perimeter subnet isolating trusted internal local networks from untrusted public Internet connections. (.....)
- A specialized organizational response team tasked with monitoring, forensic investigation, and containment of cyber incidents. (.....)
- A transport protocol establishing persistent, full-duplex, bi-directional communication channels over a single TCP connection. (.....)
- An HTTP response status code designating that the requested server resource does not exist. (.....)
- A programming interface representing an HTML document as a structured tree of object nodes traversable by scripting engines. (.....)

Question 2: Script Analysis & DOM Manipulation (5 Marks)

Examine the following JavaScript code snippet:

```
const card = document.getElementById("info-card");
card.addEventListener("click", function() {
    this.classList.toggle("highlight");
});
```

- Explain the runtime visual effect produced when a user triggers a mouse click event on the `#info-card` element. (2.5 Marks)
- Justify why `classList.toggle()` is architecturally superior to inline `style.backgroundColor = 'yellow'` regarding separation of concerns. (2.5 Marks)

Question 3: Architectural Principles & UX Engineering (5 Marks)

- In a 3-Tier Enterprise Architecture, **justify why** the presentation client tier must never communicate directly with the backend database. (2.5 Marks)
- State the 60-30-10 color design rule and illustrate how applying it enhances cognitive visual hierarchy and user accessibility on a portal. (2.5 Marks)