# ****Deliverable 1: Project Proposal & Conceptual Design****

## ****Objective****

*The objective of this project is to design and implement a* ***Cyber Risk Scoring System*** *using core concepts of* ***Data Structures and Algorithms (DSA)****.  
The system will take cyber security parameters as input, analyze their risk contribution, and generate a numerical cyber-risk score to evaluate the overall security posture.  
This project bridges theoretical DSA knowledge with practical cyber security applications, serving as a foundation for automated risk-analysis systems used in real-world environments.*

## ****1. Problem Description and Project Aim****

*With the rapid rise of cyber threats in today’s digital landscape, organizations face increasing challenges in evaluating their cybersecurity posture effectively.  
Traditional, manual risk-assessment methods are often slow, inconsistent, and prone to human error.*

*To address this issue, our project introduces an automated* ***Cyber Risk Scorer****, designed to evaluate system security based on multiple key parameters, including:*

*• Password strength  
• Number of open ports  
• Encryption status  
• Malware detection  
• Network vulnerabilities*

*The system intelligently assigns a* ***weighted score*** *to each factor, calculates an* ***overall risk index****, and categorizes the results into three distinct levels —* ***Low****,* ***Medium****, or* ***High Risk*** *— providing a clear and efficient way to assess cyber security readiness.*

## ****2. Key Data Structures****

*The following data structures will form the foundation of our Cyber Risk Scorer:*

*•* ***Arrays*** *– To store predefined risk factors and their individual scores.  
•* ***Structures*** *– To represent each system’s risk attributes collectively.  
•* ***Linked Lists*** *– To maintain dynamic records of systems and their scores.  
•* ***Priority Queue / Heap*** *– To rank systems in order of risk severity.  
•* ***Hash Maps*** *– To quickly associate risk factors with their corresponding weights.  
•* ***Graphs (Optional Extension)*** *– To represent network nodes and vulnerabilities among interconnected systems.*

## ****3. Main Algorithms****

*The project will employ several algorithms to efficiently process and evaluate data:*

*•* ***Weighted Risk Calculation Algorithm*** *– Computes the overall cyber-risk score using weighted averages.  
•* ***Sorting Algorithms (Quick Sort / Heap Sort)*** *– Ranks systems by risk score.  
•* ***Searching Algorithms (Binary Search)*** *– Quickly locates specific systems or risk factors.  
•* ***Graph Traversal (DFS / BFS)*** *– Analyzes vulnerability connections in network-based extensions.*

## ****4. Data Flow: Input, Processing, and Output****

### ****Input:****

*The system will initially receive data from the user (admin) regarding system configurations such as:*

*– Number of open ports  
– Password policy strength  
– Firewall status  
– Detected vulnerabilities*

*For the initial version, this data will be* ***hardcoded*** *for simplicity, ensuring focus on algorithmic design. Later, it may be extended to accept* ***live or file-based input****.*

### ****Processing:****

*The system will assign weights to each factor, compute the total risk score, and categorize the results using the designed algorithms.*

### ****Output:****

*The system will display each system’s computed* ***risk score****, its* ***classification (Low / Medium / High)****, and a* ***ranked list*** *of all systems according to their risk level.*

## ****5. Integration of DSA Concepts****

*This project integrates several DSA concepts learned in class, including:*

*–* ***Arrays*** *for storing factors  
–* ***Linked Lists*** *for managing records dynamically  
–* ***Stacks and Queues*** *for intermediate processing and ranking  
–* ***Sorting and Searching Algorithms*** *for efficient analysis  
–* ***Graphs (Optional)*** *for visualizing network vulnerabilities*

*These structures collectively demonstrate how theoretical DSA knowledge can be applied to practical cyber security challenges.*

## ****Conclusion****

*The* ***Cyber Risk Scorer*** *project serves as a practical example of how* ***Data Structures and Algorithms*** *can be integrated into cyber security applications.  
By automating the process of evaluating and ranking system vulnerabilities, it provides both educational value and real-world relevance.  
This project highlights the power of algorithmic thinking in solving modern cyber security problems.*