Project Design Phase:

1. System Architecture Design

Network Security Architecture:

- Firewalls, IDS/IPS, and VPN configurations.
- Segmented network topology to isolate critical systems.

Application Security Design:

- Secure coding standards and encryption mechanisms.
- Multi-layer authentication and authorization methods.

Security Monitoring & Incident Response Design:

- Deployment of **SIEM tools** (IBM QRadar, Splunk).
- Automated **threat detection and response mechanisms**.

---

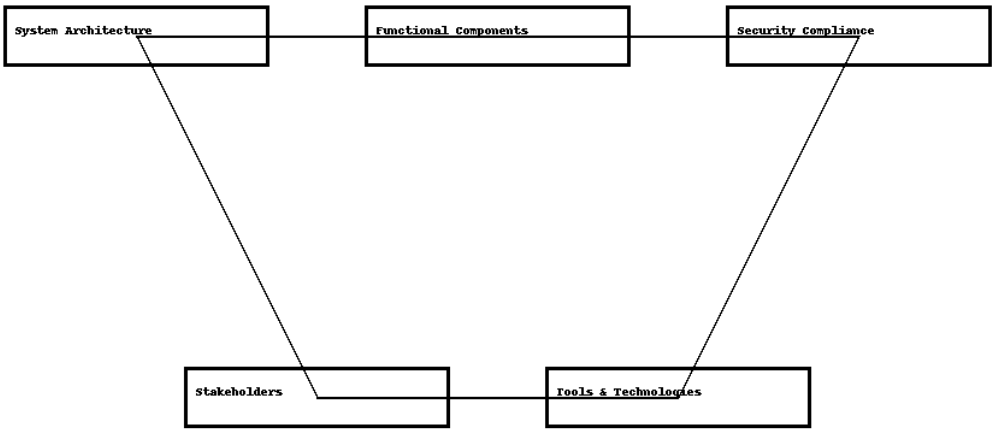
2. Functional Components

🔹 **Security Assessment & Testing Module** – Conducts vulnerability assessments using Nessus, Burp Suite, OWASP ZAP.
🔹 **Real-time Monitoring & Log Analysis** – Uses SIEM for correlation of security events.
🔹 **Access Control & Authentication System** – Implements MFA, Role-Based Access Control (RBAC).
🔹 **Incident Response & Remediation** – Automated alerting, forensic analysis, and recovery plans.

---

3. Tools & Technologies Used

Vulnerability Scanning: Nessus, OpenVAS, Nikto
Web Security Testing: Burp Suite, OWASP ZAP, Acunetix
Network Security: Nmap, Wireshark, Snort
Security Monitoring: IBM QRadar, Splunk, ELK Stack
Compliance & Reporting: CIS Benchmarks, SCAP, Tenable



4. Security Compliance & Best Practices

Compliance Frameworks: ISO 27001, PCI-DSS, GDPR, NIST
Secure Development Lifecycle (SDLC): Integrating security into every development stage.
Regular Patch Management: Automated updates for OS, applications, and security tools.
Encryption Standards: TLS 1.2+, AES-256 for data at rest and in transit.
