1. Strategic Alignment and Initial Scoping

Objective: Establish a high-level understanding of the target organization's technology landscape and cyber posture before deep due diligence begins.

Key Activities:

- **Technology Fit Assessment:**
  - Evaluate compatibility with acquirer's tech stack, platforms, and enterprise architecture.
  - Identify overlaps (e.g., CRM, ERP, cloud, DevOps tools).
- **Security Culture & Governance:**
  - Review policies, frameworks (ISO 27001, NIST CSF), and governance maturity.
  - Assess incident management and business continuity frameworks.
- **Initial Red Flags:**
  - Historical breaches, regulatory investigations, or data violations.

Deliverables:

- Preliminary technology and security alignment report
- Deal "go/no-go" input from CIO & CISO

2. Technical Due Diligence

Objective: Deep-dive into the target's IT infrastructure, data assets, and cybersecurity risk profile.

Key Areas of Assessment:

A. IT Infrastructure and Architecture

- Inventory of systems, applications, and integrations.
- Legacy systems and technical debt identification.
- Scalability, cloud strategy, and modernization level.

B. Data and Information Assets

- Data classification, lineage, and protection mechanisms.
- Data privacy compliance (GDPR, DPDP Act, etc.).
- Shadow IT and data residency issues.

C. Cybersecurity Posture

- **Controls Assessment:** Endpoint, identity, network, and application security.
- **Vulnerability Exposure:** Pen test results, open CVEs, patch management.
- **Incident History:** Past breaches, response effectiveness, and lessons learned.
- **Third-party Risk:** Vendor security governance and SaaS dependencies.

D. Compliance & Regulatory

- Sector-specific requirements (HIPAA, PCI-DSS, RBI, etc.).
- Audit trails, certifications, and pending compliance gaps.

Deliverables:

- Technology and Security Due Diligence Report
- Risk Register with quantifiable impact
- Integration readiness score

3. Risk Quantification and Valuation Impact

Objective: Translate technology and security findings into measurable business and financial risk.

Key Activities:

- Map vulnerabilities and weaknesses to potential valuation adjustments.
- Model potential breach cost exposure and remediation cost post-acquisition.
- Identify "deal breakers", unpatchable legacy systems, ongoing data lawsuits.

Deliverables:

- Technology Risk Valuation Report
- Cost of Security Remediation Estimate

4. Integration Planning and Transition Strategy

Objective: Prepare for Day-1 readiness and long-term technology integration.

Key Activities:

- **Integration Architecture Design:** Define interoperability, migration timelines.
- **Security Harmonization Plan:**
  - Unified identity and access management (IAM).
  - Centralized logging and SOC integration.
  - Standardize endpoint protection and cloud controls.
- **Data Migration & Retention:** Secure, compliant data transition planning.
- **Change Management & Communication Plan:** Policy, and culture alignment.

Deliverables:

- Technology Integration Blueprint
- Cybersecurity Harmonization Roadmap
- Day-1 Transition Plan

5. Pre-Close Security Validation

Objective: Verify no last-minute technology or security concerns remain before deal closure.

Key Activities:

- Conduct targeted vulnerability scans and threat intel review.
- Verify access control and privilege clean-up (especially for shared systems).
- Ensure data room and M&A communications are securely managed.

Deliverables:

- Pre-Close Cyber Validation Report
- Executive Summary for the M&A Steering Committee

6. Executive Decision Support

Output to Board and M&A Team:

- Cyber Risk Rating (Low / Moderate / High)
- Tech Debt & Integration Complexity Score
- Estimated Time and Cost to Securely Integrate
- Residual Risk Appetite Fit
