imaa
Institute for Mergers, Acquisitions & Alliances

M&A Due Diligence

Cybersecurity Checklist

1. IDENTIFY CYBERSECURITY OBJECTIVES:

- Define the specific objectives for the cybersecurity due diligence process.
- Determine the level of integration required for the target organization's cybersecurity systems.

2. ASSEMBLE A DUE DILIGENCE TEAM:

- Build a dedicated team of experts with knowledge in cybersecurity, IT infrastructure, legal, and compliance.
- Assign specific responsibilities to each team member.

3. ACQUIRE RELEVANT DOCUMENTATION:

- Request and review all cybersecurity policies, procedures, and standards of the target organization.
- Review incident response plans, disaster recovery plans, and business continuity plans.
- Obtain documentation related to previous security audits, penetration testing, and vulnerability assessments.

4. ASSESS CYBERSECURITY GOVERNANCE:

- Evaluate the target organization's cybersecurity governance structure, including roles and responsibilities.
- Review the reporting lines and communication channels for cybersecurity matters.
- Assess the effectiveness of cybersecurity awareness programs and training.

5. EVALUATE INFORMATION SECURITY MANAGEMENT:

- Review the target organization's information security management framework and policies.
- Assess the effectiveness of risk management processes, including detection, assessment, and mitigation.
- Evaluate the implementation of security controls and their alignment with industry best practices and regulatory obligations.

6. REVIEW TECHNICAL INFRASTRUCTURE:

- Assess the target organization's network architecture, including firewalls, routers, switches, and wireless networks.
- Review the inventory of hardware and software systems, including operating systems, databases, and applications.
- Evaluate the configuration management processes and change management controls.

7. EVALUATE ACCESS CONTROLS AND IDENTITY MANAGEMENT:

- Review user access management processes, including account provisioning, termination, and privilege management.
- Assess the implementation of multi-factor authentication, password policies, and access control mechanisms.
- Evaluate the effectiveness of identity and access management systems.

8. ASSESS SECURITY INCIDENT MANAGEMENT:

- Evaluate the target organization's incident response capabilities, including the process for detecting, analyzing, and responding to security incidents.
- Review previous security incidents and the organization's response to them.
- Assess the existence of a formalized security incident management team.

9. REVIEW DATA PROTECTION AND PRIVACY:

- Evaluate the target organization's data protection policies, including data classification, encryption, and data loss prevention measures.
- Assess compliance with relevant privacy regulations, such as GDPR or CCPA.
- Review contracts and agreements related to data sharing, data processing, and third-party vendors.

10. EVALUATE VENDOR AND THIRD-PARTY RISK MANAGEMENT:

- Review the target organization's processes for assessing and managing vendor and third-party risks.
- Assess the due diligence process followed for selecting and engaging third-party vendors.
- Evaluate the security controls and oversight mechanisms for third-party relationships.

11. ASSESS COMPLIANCE AND LEGAL REQUIREMENTS:

- Review the target organization's compliance with applicable industry standards and regulations.
- Evaluate the existence of necessary licenses, certifications, and accreditations.
- Identify any legal or regulatory risks associated with the target organization's cybersecurity posture.

12. PERFORM SECURITY TESTING AND ASSESSMENTS:

- Conduct vulnerability assessments and penetration testing on critical systems and applications.
- Perform security code reviews for custom-developed applications.
- Assess the maturity of security monitoring and logging capabilities.

13. EVALUATE BUSINESS CONTINUITY AND DISASTER RECOVERY:

- [ ] Review the target organization's business continuity and disaster recovery plans.
- [ ] Assess the adequacy of backup and recovery processes for critical systems and data.
- [ ] Evaluate the testing and maintenance of business continuity and disaster recovery plans.

14. REVIEW INSURANCE COVERAGE:

- [ ] Evaluate the target organization's cybersecurity insurance coverage, including policy terms and exclusions.
- [ ] Assess the adequacy of coverage based on the identified risks and potential impact.

15. CONDUCT COMPLIANCE AND LEGAL REVIEWS:

- [ ] Engage legal experts to review contracts, agreements, and intellectual property rights.
- [ ] Assess any legal or regulatory issues related to the target organization's cybersecurity practices.
- [ ] Identify any potential liabilities or legal risks associated with past security incidents.

16. DEVELOP A REMEDIATION PLAN:

- [ ] Based on the findings from the due diligence process, develop a detailed plan to address identified gaps and vulnerabilities.
- [ ] Prioritize remediation activities based on the level of risk and potential impact on the business.