Information Security Due Diligence Questionnaire

This questionnaire can be used as the basis for an internal due diligence review of your existing information security management system. Conducting regular review will help elevate your security posture through identifying security gaps, as well as ensure you are acting with an acceptable standard of care.

Information Security Management

1. Identify the individual within senior management that is responsible for developing, implementing and enforcing information security and data protection requirements (e.g., CISO/CSO/CTO).
2. Identify the size and skills composition of the dedicated information security team.
3. Identify the security-related certifications held by members of the information security team (e.g., CISSP, CISA/CISM, CEH, GIAC).
4. Describe written information security policies and procedures maintained by the company
5. Describe any information security training provided to employees (include details of any security awareness training, as well as training for security personnel)
6. Identify any third-party vendors and the specific functions they provide which augment the services of the internal information security team.
7. Describe any security certifications, compliance activities, and/or due diligence efforts performed by third-party vendors.

Data Protection

1. Describe the policies, procedures, and technologies implemented to protect data entrusted into the companies care. (e.g., physical/logical segmentation, user access controls, encryption, separation of duties)
2. If encryption is used to protect data, describe the cryptographic solutions implemented (include name of commercial products/solutions, encryption key size/strength, and algorithms)
3. Describe the Identity and Access Management solution implemented (include details surrounding account provisioning/termination and role-based assignments).

Network and System Management

1. Describe the process for provisioning new devices and systems (include details of system hardening standards followed, procedures for implementation, and configuration management solutions).
2. Describe any antivirus solutions that are implemented (include details of scan and update schedules, name of commercial products).
3. Describe the patch management policies, procedures, and solutions that are implemented.
4. Describe any intrusion detection/prevention systems (IDS/IPS) implemented.

5. Describe any data loss prevention, security information event management (SIEM), and/or file integrity management (FIM) solutions implemented.
6. Describe the change management policies, procedures, and solutions that are implemented.

Wireless and Remote Access

1. Describe any wireless technologies that are utilized in the transmitting of sensitive data (include details of documented policies, configuration standards, and security controls established)
2. Describe the remote access technologies utilized by employees to access company resources and sensitive data (include authentication requirements, and access controls established).
3. Describe any remote access policies implemented, including any requirements for multifactor authentication for all remote access to sensitive data and systems.

Incident Response

1. Describe the nature and extend of the companies incident response plan (include details of the personnel/teams involved in carrying out the reporting, escalation and remediation associated with an information security incident.
2. Describe any notification timelines and requirements established by the incident response plan
3. Describe any system and network monitoring and logging that is configured (include details on the type of events that are logged and any notification capabilities).
4. Describe any central log management solutions that are implemented (include details of review processes, and notification policies/procedures).
5. Describe the capabilities (either internally or through a third-party) of readily conducting a forensics investigation.
6. Describe any implemented breach notification policies and procedures used in notifying clients in the event of unauthorized access and/or data breach.
7. Describe any signification information security incidents that have occurred in the past two years.

Business Continuity and Disaster Recovery

1. Describe any business continuity and/or disaster recovery plans that have been implemented (include details of documented policy/procedures as well as business and technical solutions implemented)
2. Identify any capabilities that have been implemented to provide high-availability service (include such details as back-ups, redundancy, and HOT/WARM/COLD sites).
3. Describe any regular disaster recovery plan testing that is performed.
4. Describe any established backup policies and procedures (include details of schedules, storage, and testing of restores).

Cyber Insurance Policy Protection

1. Describe the extent to which cyber liability insurance policy coverage is maintained.