

Data Security, Privacy and Ownership Assessment



Data is one of the primary assets for any association or organization. Data regarding attendees or members and their interactions with the organization's systems constitute significant value. This data can be used to understand the interests of the users, create personalized experiences, make meaningful business connections, and help drive business growth.

The increase in value of these digital assets is also accompanied with increased risk to the organization via cyber security breaches, privacy law failures, and data ownership confusion between the organization and their technology vendors.

The cost of cyber insurance is skyrocketing as cyber security incidents increase. Additionally, when organizations fail to implement proper security and privacy controls, they risk losing insurance coverage after security incidents have occurred. These risks

Assessment Benefits

1. Provide risk insights to leadership
2. Identify areas to focus resources and investment
3. Minimize audit failure risks
4. Ensure complete data ownership

can damage an organization's brand and can create devastating expense scenarios.

Organizations must have a clear understanding of their risk position regarding Cyber Security, Data Privacy, and Data Ownership. ClearTone Consulting offers an assessment service addressing all three areas and resulting in an executive assessment report that identifies the weaknesses and strengths of your organizations risk position.

The **Data Security Assessment** scores an organization's position within these twelve NIST 800-53 categories:

1. Information Security Policy and Governance
2. Organization of Information Security
3. Asset Management
4. Access Control
5. Communication Security and Network Management
6. Physical and Environmental Security
7. Human Resources and Awareness
8. Security Incident Management
9. Business Continuity and Disaster Recovery
10. Application Security and Vulnerability Management
11. Compliance and Data Privacy
12. Cloud Security (if used)

Data Privacy Assessment scores an organization's adherence to privacy law and best practices within these ten GDPR categories:

1. Accountability governance
2. Breach management
3. Consent and notices
4. Data protection impact assessment
5. Data subject rights
6. Data transfers
7. Privacy by design and default
8. Processing principles
9. Processors
10. Records of processing

Data Ownership Assessment includes a review of vendor, supplier, and processor agreements regarding ownership of data, data aggregations, and metadata.