**Text

Description automatically generated**

**Checklist for preparing and deploying an information privacy program**

*By Paul Kirvan, FBCI, CISA*

Use the following checklist to develop an information privacy program.

|  | **Activity** | **Details** | **Comments** |
| --- | --- | --- | --- |
|  | 1. Business plan preparation | Justify the preparation, management and costs of a privacy program. |  |
|  | 1. Management approval and funding | This activity uses the business plan. |  |
|  | 1. Create an internal privacy team | Include representation from IT, legal, risk management, business unit leaders and others as appropriate. |  |
|  | 1. External advisors | Identify and involve advisors who have expertise in creating privacy programs. |  |
|  | 1. Project plan | Ensure the plan has objectives and target dates with identified roles and responsibilities. |  |
|  | 1. Current privacy activities | Examine how privacy is currently handled. Perform a gap analysis, and review previous audit reports. |  |
|  | 1. Identify what needs to be protected | This includes business identifiable information, personally identifiable information (PII) and other data. Ask questions about the data: Where is it located? Who uses it? Who has custody of it? How is it kept secure while being transmitted and used? How do authorized users access the data? |  |
|  | 1. Standards and regulations | Review and select relevant standards and regulations on information privacy as guidance. This is also important from an audit perspective. |  |
|  | 1. Privacy policy | Privacy policies set the ground rules for information privacy and how an organization plans to maintain compliance. |  |
|  | 1. Privacy risk management | Develop a privacy risk management process to manage privacy risks, threats and vulnerabilities. |  |
|  | 1. Operations and management | Identify staff who will implement and manage the program following deployment. |  |
|  | 1. Define privacy controls | Identify information privacy controls (e.g., regulatory compliance, records management, privacy breach assessments and dealing with contractors and third parties) and technology controls (e.g., access controls and user authentication). |  |
|  | 1. Define privacy management controls | Outline daily privacy activities, such as separating business and personal information and collecting, handling, and transmitting business identifiable information and PII. |  |
|  | 1. Breach management | Decide how to deal with breaches, for example, incident response and breach management, including preparing an after-action report. |  |
|  | 1. Awareness and training | Launch an employee awareness and training program. Include new hire training, refresher training for existing employees and ongoing reminders to all employees and third parties. |  |
|  | 1. Reporting process | Document the processes needed to provide privacy activity reports to regulatory and other government agencies. |  |
|  | 1. Program review and testing | Evaluate the program's effectiveness, and identify areas for corrective action. |  |
|  | 1. Rollout schedule | Keep those involved in program rollout informed, and keep senior management updated on the plan's progress. |  |
|  | 1. Post-rollout evaluation | One to two months after rollout, survey employees on the plan. |  |
|  | 1. Annual review | Align an annual review with the schedule of information security activities. Evaluate the program's progress, and gather evidence for an audit review. |  |