

# Privacy Manager Certification

## Examination Blueprint for the Certified Information Privacy Manager (CIPM)



### What the blueprint tells you:

The examination blueprint indicates the range, or minimum and maximum number, of items that are included on the CIPM examination from the major domains and topics of the Body of Knowledge.

### How to use the blueprint to guide your exam preparation:

Questions may be asked from any of the listed topics under each domain. Use the minimum and maximum ranges to help you determine which domains and topics will be represented to a lesser or greater degree on the exam.

### Why don't all the numbers add up?

The number of questions listed for each topic represents a range. Within a domain, a minimum number of items may be chosen from one topic, while a maximum number of items may be chosen from another topic. Regardless, the total number of questions within each domain will not fall below the minimum or exceed the maximum amount.

<b>I. Developing a Privacy Program</b>	<b>13</b>	<b>17</b>
A. Create a company vision	1	3
B. Establish a Data Governance model	1	3
C. Establish a privacy program	3	5
D. Structure the privacy team	1	3
E. Communicate	4	6
<b>II. Privacy Program Framework</b>	<b>9</b>	<b>11</b>
A. Develop the Privacy Program Framework	3	5
B. Implement the Privacy Program Framework	2	4
C. Develop Appropriate Metrics	2	4
<b>III. Privacy Operational Lifecycle: Assess</b>	<b>13</b>	<b>17</b>
A. Document current baseline of your privacy program	1	3
B. Processors and third-party vendor assessment	3	5
C. Physical Assessments	1	3
D. Mergers, acquisitions, and divestitures	1	3
E. Privacy Impact Assessments and Data Protection Impact Assessments	4	6

<b>IV. Privacy Operational Lifecycle: Protect</b>	<b>12</b>	<b>16</b>
A. Information security practices	4	6
B. Privacy by Design	2	4
C. Integrate privacy requirements and representation into functional areas across the organization	2	4
D. Other Organizational Measures	2	4
<b>V. Privacy Operational Lifecycle: Sustain</b>	<b>5</b>	<b>7</b>
A. Monitor	2	4
B. Audit	2	4
<b>VI. Privacy Operational Lifecycle: Respond</b>	<b>9</b>	<b>11</b>
A. Data-subject information requests and privacy rights	5	7
B. Privacy incident response	3	5