<table>
<thead>
<tr>
<th>Bill Sec.</th>
<th>Data Management Advisory Committee</th>
<th>Data Officer</th>
<th>CISO</th>
<th>CPO</th>
<th>CTO</th>
<th>TSLAC</th>
<th>Records Mgmt.</th>
<th>Risk</th>
<th>DIR Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>RA</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>3</td>
<td>Regional Cybersecurity Working Groups (by Dec. 1, 2021)</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Designated Data Management Officer</td>
<td>RA</td>
<td>R</td>
<td></td>
<td>RC</td>
<td></td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Security Controls for State Agency Data</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td></td>
<td></td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Data Classification, Security, and Retention Requirements (all IT projects initiated on or after Jun. 14, 2021)</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td>C</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>6</td>
<td>Texas Volunteer Incident Response Team (by Dec. 1, 2021)</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Agency Information Security Assessment and Report</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Use of Next Generation Technology</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Regional Network Security Centers</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Restrictions on State Agency Use of Certain Individual-Identifying Information</td>
<td>C</td>
<td>C</td>
<td>RA</td>
<td></td>
<td></td>
<td>C</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Submit report related to Texas Volunteer Incident Response Team (not later than Oct. 15, 2022)</td>
<td>RA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Section 11 contains effective dates
Section 13 qualifies that the added Govt. Code applies only to information acquired, retained, or disseminated on or after effective data of the Act
Red = OCDO Primary Accountabilities
* All entities are likely “I” for Informed, too
Shared Strategic Asset Responsibilities

1. Interprets and applies regulatory requirements
2. Develops policies, standards, and training protocols
3. Analyzes existing and drafts new bills for legislative consideration
4. Enterprise information governance / management
5. Monitors, analyzes, and reviews legislation
6. Evaluates third-party contracts & makes practice / controls recommendations
7. Consults with other program areas for assessment of threats to information privacy
8. Provides guidance in strategic operations
9. Performs information security risk analysis and audits
10. Reviews and monitors confidential/sensitive data controls
11. Performs data analysis / architecture work
12. Develops security and business continuance standards and plans
13. Plans security architecture
Data Management Advisory Committee
Senate Bill 475 Data Accountabilities Framework & Deliverables

(SB 475 Sections 1, 4 and 5)

The DMAC represents a community of Data Management Officers (DMOs), designated (per SB 475) by their respective organizations to lead the development of their data management programs.

The DMAC community:

- Are required to provide input to the DIR CDO in developing and maturing the state’s overall data management program.
- Are responsible for addressing both strategic and tactical elements of their own enterprise data management programs.
- Collaborate and share best practices, as well as develop governance policies and guiding frameworks/principles for each organization to adopt.
- Fosters relationships to better enable information sharing and other data-related initiatives to support the fulfillment of their organization’s core mission.
Pillar 1: Standards and Best Practices

**Goals & Strategies**

1. Establish an agency data governance program to identify the agency’s data assets, exercise authority and management over the data assets, and establish related processes and procedures to oversee the data assets.
2. Coordinate with the agency’s ISO, the agency’s records management officer, and TSLAC to ensure the agency’s records management programs apply to all types of data storage media + increase awareness of and outreach for the agency’s records management programs within the agency.
3. Coordinate with the agency’s ISO, the agency’s records management officer, and TSLAC to conduct a data maturity assessment of the agency’s data governance program.
4. Reduce duplicative information collection.
5. On initiation of an information resources technology project, classify the data produced from or used in the project and determine appropriate data security and applicable retention requirements.

**Performance Measures**

- % of (SB 475-eligible) agencies with an enterprise data governance policy in place
- Data owners identified versus # of domains
- # Published data definitions
- Confirmed adherence to data management standards and policies (certification process)
- % of agencies that have completed the maturity assessment

Pillar 2: Data Security and Controls

**Goals & Strategies**

1. Improve the control and security of information collected by state agencies.
2. Improve information management and analysis to increase information security, uncover fraud and waste, reduce agency costs, improve agency operations, and verify compliance with applicable laws.
3. Each state agency entering into or renewing a contract with a vendor authorized to access, transmit, use, or store data shall include a provision in the contract requiring the vendor to meet the security controls the agency determines are proportionate with the agency’s risk under the contract based on the sensitivity of the agency’s data.
4. Coordinate with the agency’s ISO, the agency’s records management officer, and TSLAC to implement best practices for managing and securing data in accordance with state privacy laws and data privacy classifications.

**Performance Measures**

- % of agencies with approved standards and asserted compliance
- % of agencies with completed annual risk assessments
- % of identified risks audited (internal)
- # of requests received for ad hoc risk advisory services (external)
- % employees completed security training

Pillar 3: Interagency Coordination

**Goals & Strategies**

1. Promote between agencies the sharing of information, including customer information.
2. Improve information management and analysis to increase information security, uncover fraud and waste, reduce agency costs, improve agency operations, and verify compliance with applicable laws.
3. Assist the department in the development and management of a data portal for use by agencies.
4. Encourage agencies to collect and post on the agencies’ websites or the Open Data Portal information related to an agency’s functions or other data maintained by the agency that is in an open file format and is machine-readable, exportable, and easily accessible by the public.
5. Encourage the evaluation of open document formats for storing data and documents generated by agencies.
6. Post on the Open Data Portal at least three high-value data sets.

**Performance Measures**

- % of agencies sharing information
- # of agencies leveraging the CDP for data sharing
- % of agencies & IHEs with >=3 published HV datasets
- % of publishing agencies with Exec. Dashboards
- % of publishing agencies participating in ODUG
- # of TSDEC briefings/engagements
- # of TSDEC adoptees/users

Encourage agencies to leverage the DIR Closed Data Portal.
DMAC & Data Leadership Structure

DMAC Components
- The DIR Board
- Data Management Officers
- DMAC Workgroups

DIR Data Leadership Team
- Core (voting) Members: Data Officer (chair), Chief Data Officer (co-chair), Chief of Staff, Chief Risk Officer, Director of Program Development
- Contributing (non-voting) members: Information Security Officer, PMO Director, IRM, General Counsel