2022 Biennial Performance Report
Consolidated Assessment of Agency IT Infrastructure

This report addresses Section 2054.068 of the Government Code requiring the Texas Department of Information Resources (DIR) to collect information on the status and condition of each state agency's information technology (IT) infrastructure and report to state leadership on the information collected.[1]

Background

DIR assesses each state agency's IT infrastructure security and operational risk using multiple data sources, as explained in the *Methodology* section. DIR uses this information to:

- produce an overall assessment of state agency security and operational risks,
- provide an analysis of state agencies found to be at higher security and operational risks, and
- present an overview of agencies' proposed efforts to address those risks.[2]

Findings

DIR identified and contacted agencies at higher operational and security risk relative to other state agencies. All high-risk agencies completed remediation plans to address the identified deficiencies and submitted their plans to DIR.

Methodology

DIR analyzes state agencies' levels of risk and calculates a score for each agency, based on a 100-point scale with 100 being the lowest risk and 0 being the highest risk. The following provides the breakdown of the risk score and an overview of the calculations for each contributing factor.

Information Resources Deployment Review (IRDR) – 30 points

Section 2054.0965 of the Government Code requires state agencies to complete a review of the operational aspects of the agency's information resources deployment and report the results to DIR. Designed by DIR and conducted biennially, the Information Resources Deployment Review (IRDR) survey asks agencies standardized questions about information security, continuity of operations, disaster recovery, digital storage, agency hardware and software, and legacy applications. For this analysis, DIR selected 16 IRDR questions and assigned varying points to each response option.

Agency Security Plans – 30 points

Section 2054.133 of the Government Code mandates that state agencies develop and periodically update an information security plan referred to as the Agency Security Plan. The 2022 methodology for Agency Security Plans requires agencies to assess their maturity on a scale of 0 (non-existent) to 5 (optimized) for

[1] *See* Government Code Section 2054.068(g), which excludes from this analysis a university system or institution of higher education as defined by Education Code Section 61.003.

[2] Pursuant to Section 2054.068(d), DIR submits this analysis to the governor, chair of the House Appropriations Committee, chair of the Senate Finance Committee, speaker of the House of Representatives, lieutenant governor, and staff of the Legislative Budget Board.

40 security objectives. For this section, the average maturity of all security objectives determined the agency’s score.

Security Services – 20 points

DIR assigned values of 0 through 10 to state agencies based on how recently they obtained a DIR-provided Texas Cybersecurity Framework Security Assessment and an external network penetration test. If an agency had not obtained these services, DIR gave the agency a score of 0 for that category. The overall security services score is the combined assessment and penetration test scores.

Monthly Security Incident Reporting – 10 points

1 Texas Administrative Code Sections 202.23 and 202.73 require state agencies and institutions of higher education to submit monthly security incident reports to DIR no later than nine calendar days after the end of the month. These security reports include a summary of security-related events and incidents. To determine the score for this section, DIR reviewed the period from September 2020 to August 2022 and assigned a value based on the number of reports submitted on time.

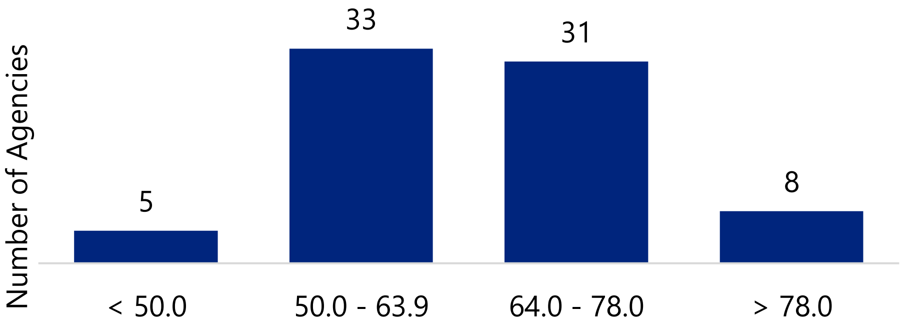
IT Inventory – 10 points

Sections 2054.068(b) and 2054.0965(a) of the Government Code require state agencies to complete an IT inventory[3] as part of the IRDR. The inventory prompts agencies to rate the criticality or impact and failure probability of each server instance on a scale of 1 (low) to 5 (high). DIR multiplies the average probability and impact rating to determine a general risk score for each agency based on the inventory.

Agency Risk Score Distribution

DIR's analysis provides the distribution of agency scores as represented below. The 77 agencies that DIR assessed had an average score of 63.8 and a median score of 64.3.

2022 Agency Risk Score Distribution



[3] *See* Government Code Section 2054.068(b), which requires a state agency to complete an inventory of its servers, mainframes, cloud services, and other information technology equipment, and Government Code Section 2054.0965(a) and (b), which requires a state agency to complete a review of the operational aspects of the agency’s information resources deployment including major information systems, other operational or logistical components, major databases, and applications.