



# Information Resources Deployment Review 2024 Instructions

## Guidance for Texas State Agencies and Institutions of Higher Education

### Table of Contents

Introduction.....	4
Information Resources Deployment Review Requirements.....	4
IRDR Data .....	4
SPECTRIM .....	4
How to Use These Instructions .....	5
Reporting Requirements and Deadlines .....	5
State Agencies .....	5
Health and Human Services Agencies.....	5
Institutions of Higher Education.....	5
IRDR Overview.....	6
Part 1: Agency Environment.....	6
Part 2: Compliance with State Standards .....	6
Information Resources Corrective Action Plan .....	6
Part 3: Alignment with State Technology Goals .....	6
Part 4: IT Inventory.....	7
Support .....	7
General Inquiries.....	7
SPECTRIM Help.....	7
2024 IRDR Questions.....	8
Part 1: Agency Environment.....	8
Section 1.01 – Information Resources Management .....	8
Section 1.02 – Information Security.....	10
Section 1.03 – Digital Accessibility .....	17
Section 1.04 – Continuity of Operations.....	21
Section 1.05 – Electronic Records Management.....	22
Section 1.06 – Contracting .....	26
Section 1.07 – Hardware and Software Environment.....	29
Section 1.08 – E-Learning .....	32
Section 1.09 – Advanced Technologies and Methods.....	33
Section 1.10 – Transformation and Modernization.....	39
Section 1.11 – Project Delivery .....	42

Section 1.12 – Shared Networks.....	44
Section 1.13 – Data Management and Privacy Practices.....	45
Section 1.14 – Training and Planning.....	48
Section 1.15 – Optional Comments on Agency IT Environment.....	49
Part 2: Compliance with State Standards .....	50
Section 2.01 – Security.....	50
Section 2.02 – State Websites.....	52
Section 2.03 – Electronic and Information Resources Accessibility.....	54
Section 2.04 – Geographic Information Systems.....	55
Section 2.05 – Electronic Records Management.....	56
Section 2.06 – Additional Standards.....	57
Part 3: State Strategic Plan for Information Resources Management.....	60
Section 3.01 – Alignment with 2024-2028 State Strategic Plan Technology Objectives.....	60
Section 3.02 – Progress Toward 2022-2026 State Strategic Plan Technology Objectives.....	61
Part 4: IT Inventory.....	62
Overview.....	62
Sensitive Inventory Data.....	62
Guidance for Completing the Inventory .....	62
Inventory Attestation and IRDR Submission .....	63
Acronym List .....	64
Glossary.....	66



## Introduction

### Information Resources Deployment Review Requirements

The Information Resources Manager (IRM) of each state agency and institution of higher education (IHE) is required<sup>1</sup> to conduct an [Information Resources Deployment Review \(IRDR\)](#) each even-numbered year. State agencies must follow instructions provided by the Texas Department of Information Resources (DIR) and submit the IRDR to the [Quality Assurance Team \(QAT\)](#) for analysis.<sup>2</sup> This document provides instructions for submitting the IRDR.

The IRDR assesses how your agency's information resources (IR) support your agency's mission, goals, and objectives. It also demonstrates how your agency's IR deployment aligns with the state's technology direction, outlined in the [State Strategic Plan \(SSP\) for Information Resources Management](#). Lastly, the IRDR confirms your agency's compliance with the state's IR-related statutes, rules, and standards.

### IRDR Data

The collection of IRDR data serves as both an internal review of your agency's information technology (IT) environment and the source for DIR's analysis of the state's aggregate IT environment. DIR uses the IRDR to produce several legislatively mandated reports including the [Biennial Performance Report](#) and [Cybersecurity Report](#).

DIR complies with the Texas Public Information Act<sup>3</sup> for all public information requests. Due to the inherently sensitive nature of system-level cybersecurity information, DIR treats the information collected through the IRDR as confidential and will request a decision from the Office of the Attorney General for all public information requests that DIR receives seeking IRDR information.

### SPECTRIM

IRMs must submit their IRDR by **March 31, 2024**, through the [Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management \(SPECTRIM\)](#). In addition to the IRDR, SPECTRIM supports security and other IT-related reporting from state agencies. Online submission of the IRDR through SPECTRIM constitutes complete submission to the QAT. You are not required to provide a signature or submit a hard copy.

DIR opens SPECTRIM for 2024 IRDR data entry in **January 2024**. You may [log in to SPECTRIM](#) at any time to view your agency's past IRDR responses. For help with SPECTRIM, email [grc@dir.texas.gov](mailto:grc@dir.texas.gov).

---

<sup>1</sup> See Government Code Section [2054.0965](#).

<sup>2</sup> See Government Code Section [2054.097](#).

<sup>3</sup> See Government Code Chapter [552](#).

## How to Use These Instructions

DIR provides these instructions to assist you in complying with statutory requirements. These instructions contain:

- **Guidance statements** that provide background information, statutory references, roles involved, and suggested resources;
- **Links to statutory references and other resources** that may assist you in answering IRDR questions;
- An **acronym list and glossary** with definitions of technical terms used in this document; and
- A **navigable table of contents** that allows you to navigate to a specific section of the IRDR questions.

Unless otherwise indicated, you should select only one answer to each question; in addition, you should answer questions based on fiscal year (FY) 2023.

You may want to distribute these instructions to other employees within your agency to gather answers before SPECTRIM is open for data input.

## Reporting Requirements and Deadlines

### State Agencies

State agencies must complete and submit their IRDR (including IT inventory of application assessment) to the QAT through SPECTRIM by **March 31, 2024**. If applicable, state agencies must also submit their Information Resource Corrective Action Plans (IRCAP) by **May 31, 2024**.

### Health and Human Services Agencies

Health and Human Services agencies must receive approval<sup>4</sup> of their IRDR from the Health and Human Services Commission prior to submitting their completed IRDR to the QAT through SPECTRIM by **March 31, 2024**, and if applicable, their IRCAPs by **May 31, 2024**.

### Institutions of Higher Education

IHEs are required<sup>5</sup> to complete an electronic and information resources (EIR) agency accessibility survey. They meet this requirement by submitting IRDR Sections 1.03, 2.02, and 2.03 through SPECTRIM by **March 31, 2024**. These are the only sections that IHEs are required to submit to DIR.

---

<sup>4</sup> See Government Code Section [531.027\(a\)\(3\)](#).

<sup>5</sup> See Government Code Section [2054.463](#) and Texas Administrative Code Section [213.40](#).



### IRDR Overview

#### Part 1: Agency Environment

Part 1: Agency Environment asks questions about the agency's IR environment. IRMs may need to consult with other employees to answer questions related to information security, digital accessibility, continuity of operations, project management, data management, and privacy practices.

**IHEs must complete Section 1.03.**

#### Part 2: Compliance with State Standards

Part 2: Compliance with State Standards asks IRMs to report the status of their agency's compliance with key IR-related statutes, rules, and standards. State agencies reporting that they are out of compliance in one or more areas must develop an IRCAP<sup>6</sup> describing how they will address any deficiencies.

**IHEs must complete Sections 2.02 and 2.03.**

IRMs should review technology-related statutes and rules referenced in Part 2: Compliance with State Standards and consult with their legal counsel as needed to determine the status of their compliance with each requirement.

#### Information Resources Corrective Action Plan

IRCAPs will be available in SPECTRIM once a state agency completes their IRDR. Please note that each area of non-compliance requires an IRCAP, so you may have multiple IRCAPs to complete. State agencies must submit IRCAPs by **May 31, 2024**.

DIR must report the status of agency IRCAPs to the State Auditor's Office and the Legislative Budget Board.<sup>7</sup> DIR may report to the governor and the presiding officer of each house of the Legislature that an agency's IR deployment decision is not in compliance with the state strategic plan, IR-related statute, or department rules.

#### Part 3: Alignment with State Technology Goals

Part 3: Alignment with State Technology Goals asks IRMs to report how their agency's IR deployment initiatives align with the statewide technology goals and objectives outlined in the [2024-2028 State Strategic Plan for Information Resources Management](#). In addition, IRMs identify the progress their agencies have made on the statewide technology priorities described in the [2022-2026 State Strategic Plan for Information Resources Management](#).

**Part 3 does not apply to IHEs.**

<sup>6</sup> See Government Code [2054.097 \(a\)](#).

<sup>7</sup> See Government Code [2054.097 \(a-1\)](#).

## Part 4: IT Inventory

Part 4: IT Inventory asks IRMs to provide an inventory of their agency's IR assets as required by Government Code Sections 2054.068 and 2054.0965. DIR uses the information from this inventory to complete legislatively mandated reports that provide a statewide perspective of information technology infrastructure and associated business applications used by state agencies.

**Part 4 does not  
apply to IHEs.**

## Support

DIR staff are committed to supporting you during the IRDR reporting period and will strive to answer all inquiries within one business day.

Please submit inquiries whenever you need help understanding a question or are uncertain how to respond.

### General Inquiries

For general inquiries about IRDR content (e.g., question clarification, process questions), please email [IRDR@dir.texas.gov](mailto:IRDR@dir.texas.gov).

Additional information on the IRDR (including frequently asked questions) is available on the [IRDR webpage of DIR's website](#).

Please ensure that your IRM designation is current, as IRDR reminders and updates are shared with IRMs via the TX-IRM list.

### SPECTRIM Help

For help with SPECTRIM (such as resetting your password or obtaining your credentials), email [grc@dir.texas.gov](mailto:grc@dir.texas.gov).



### 2024 IRDR Questions

#### Part 1: Agency Environment

Part 1: Agency Environment provides a review of the operational aspects of your agency's IR deployment in support of your agency's mission, goals, and objectives.

Many of this year's questions are from previous IRDRs and your agency's answers to those questions will be prepopulated in SPECTRIM. Questions that have not been used in previous IRDRs are labeled as "New". As a reminder, you can [log in](#) to SPECTRIM to view your past answers at any time.

#### Section 1.01 – Information Resources Management

- 1.01.01 Does your agency's Information Resources Manager play a significant role in the following? (Select all that apply.)
- Agency Strategic Plan
  - Biennial Operating Plan for Information Resources
  - Legislative Appropriations Request
  - Agency Security Plan
  - None of the above
- 1.01.02 Does your agency develop a technology roadmap/tactical plan?
- Yes
  - In planning
  - No
- 1.01.03 Does your agency stream governmental open meetings on the internet?
- Yes, video and audio
  - Yes, audio only
  - No, but plan to stream open meetings in the future
  - No, and no plans to stream open meetings in the future
- 1.01.04 Does your agency plan to allow governmental body members to virtually participate in board meetings during the next biennium?
- Yes, video and audio
  - Yes, audio only
  - No, but plan to allow virtual participation in the future
  - No, and no plans to allow virtual participation in the future
  - The agency does not have a governmental body
- 1.01.05 For which of the following categories does your agency evaluate maturity levels? (Select all that apply.)
- Information Security



- Data Management
- Accessibility
- Contracting and Procurement
- Enterprise Architecture
- Application Development
- Project Management
- Quality Management
- Strategic Planning
- Governance
- Cloud
- Continuity of Operations or Disaster Recovery
- Mobility
- Identity and Access Management
- Digital Transformation
- Other, write in <enter text>

1.01.06 Please list all vendors your agency leverages to manage the agency's IT infrastructure and briefly describe their role. <enter text>

New

1.01.07 Which of the following workforce initiatives does your agency leverage to address staffing resources? (Select all that apply.)

- Skills-based hiring
- Apprenticeships
- Internships
- Remote or hybrid work
- Targeted recruitment of people with specialized skills
- Targeted recruitment of people returning to the workforce after a break in service
- Retention bonuses for hard-to-fill positions
- Other, write in <enter text>
- None of the above

New

1.01.08 What are the top IT skills your organization will need to fulfill your agency's mission in the future? (Select five.)

- Artificial intelligence
- Cloud environment
- Critical thinking
- Cybersecurity
- Data analysis
- Data science
- Database management
- Digital literacy



# Information Resources Deployment Review 2024 Instructions

- Edge computing
- Machine learning
- Network engineering
- Network management
- Network security
- Relationship management
- Robotics
- Robotics process automation
- Security architecture
- Strategic thinking
- Unstructured data
- Other, write in <enter text>

New

1.01.09 How many dedicated (100% of time or full-time) IT professionals, excluding contractors, does your agency currently employ? <enter number>

New

1.01.10 Approximately, what is the average number of contracted IT professionals your agency employed in the previous biennium? <enter number>

## Section 1.02 – Information Security

### Security Management

1.02.01 Does the Information Security Officer have additional job titles/responsibilities beyond information security?

- Yes
- No

1.02.02 To whom does the Information Security Officer report in your agency?

- Information Resources Manager or Chief Information Officer
- Executive Director (or equivalent)
- Other executive-level position
- Other, write in <enter text>

1.02.03 How often does the Executive Director (or equivalent) sign off on high impact information resources security risks?

- Always
- Sometimes
- Occasionally
- Rarely
- Never

---

**Coordinate with your agency's Information Security Officer (ISO) when completing Section 1.02.**

**For security standards, training requirements, and more, see DIR's [Information Security webpage](#).**

---



# Information Resources Deployment Review

## 2024 Instructions

- 1.02.04 How many dedicated (100% of time or full-time) security professionals, excluding contractors, does your agency currently employ? <enter a number>
- 1.02.05 How many dedicated (100% of time or full-time) security contractor positions does your agency plan to have over the next biennium? <enter a number>
- 1.02.06 Is your combined agency information security staffing level sufficient for addressing your security needs?
  - Yes
  - No
- 1.02.06a How many dedicated (100% of time or full-time) security professionals, excluding contractors, would your agency require to adequately fulfill security program needs?
  - <Enter a number>

### Security Budget

- 1.02.07 Does your agency's budget include line items for information security?
  - Yes
  - No
- 1.02.08 What is your agency's information security funding as a percentage of its overall IT budget?
  - <Enter a percentage>
- 1.02.09 What is the biennial trend for your security budget?
  - Decrease of 11% or more
  - Decrease of 6-10%
  - Decrease of 1-5%
  - Security budget has remained the same
  - Increase of 1-5%
  - Increase of 6-10%
  - Increase of 11% or more
  - Not applicable/do not know
- 1.02.10 Does your agency budget adequate resources and funds to address the operational and financial impacts of a cybersecurity event/incident?
  - Yes
  - In planning
  - No



### Security Practices

1.02.11 What are your agency's top five security initiatives for the current biennium?  
(Select five.)

- Developing a security strategy
- Security governance
- Aligning security initiatives with agency goals
- Security risk assessments
- Data protection or data loss prevention
- Security staffing
- Security training and awareness
- Security regulatory and legislative compliance
- Security infrastructure improvement
- Zero Trust
- Application security
- Identity and access management
- Security compliance (e.g., internal) remediation
- Managing or outsourcing of security services
- Disaster recovery/Business continuity
- Network mapping
- Other, write in <enter text>

1.02.12 What are the greatest barriers your agency faces in addressing security?  
(Select three.)

- Lack of executive or management support
- Lack of support from business stakeholders
- Lack of clarity on mandates, roles, and responsibilities
- Conflicting federal/state rules and requirements
- Lack of sufficient funding
- Lack of procurement oversight and control
- Lack of visibility and influence within the agency
- Lack of a security strategy (e.g., shifting priorities)
- Inadequate availability of security professionals
- Inadequate competency of security professionals
- Lack of documented processes
- Lack of legislative support
- Increasing sophistication of threats
- Emerging technologies
- Inadequate functionality or interoperability of security products
- Other, write in <enter text>



### Multifactor Authentication

- 1.02.13 Which of the following best describes your agency's multifactor authentication (MFA) implementation?
- MFA has not been implemented on any agency systems
  - MFA has been implemented on critical agency systems
  - MFA has been implemented on most agency systems
  - MFA has been implemented on all agency systems
- 1.02.14 What percentage of agency users are covered by MFA?  
<enter a percentage>
- 1.02.14a Is your agency interested in learning about free MFA available through DIR?
- Yes
  - No

### Endpoint Detection and Response

- 1.02.15 Which of the following best describes your agency's Endpoint Detection and Response (EDR) capabilities?
- EDR has been enabled through O365
  - DIR's Statewide EDR product has been implemented
  - Another EDR product has been implemented
  - Plan to use DIR's statewide EDR
  - Plan to implement EDR using another product
  - EDR has not been implemented on any agency systems
- 1.02.15a On what types of devices has EDR been implemented? (Select all that apply.)
- Desktop/laptop systems
  - Servers
  - Tablets
  - Phones
  - None of the above
- 1.02.15b Is your agency interested in learning about free EDR available through DIR?
- Yes
  - No

### Zero Trust

- 1.02.16 Which of the following best describes your agency's Zero Trust capabilities?
- Zero Trust implementation is planned
  - Zero Trust implementation is in progress
  - Zero Trust has been implemented
  - Zero Trust has not been implemented and no plans are in place

### Identity and Access Management

New

- 1.02.16a Which of the following best describes your agency's identity and access management implementation on internal- and external-facing agency devices and applications?
- Identity and access management has not been implemented on any agency device or application
  - Identity and access management has been implemented on critical agency devices and applications
  - Identity and access management has been implemented on most agency devices and applications
  - Identity and access management has been implemented on all agency devices and applications

### Incident Response

- 1.02.17 How often does your agency review and, if necessary, revise its security incident response plan and procedures?
- Every six months or less
  - Annually
  - Every other year
  - No formal revision schedule exists
  - Agency does not have an incident response plan
- 1.02.17a How often does your agency exercise its security incident response plan and procedures?
- Every 6 months or less
  - Annually
  - Every other year
  - No formal exercise schedule exists
  - Agency does not have an incident response plan

### Cybersecurity Insurance

- 1.02.18 Does your agency have any form of cybersecurity insurance? (If no, proceed to question 1.02.19.)
- Yes

- No, but actively seeking
  - No
- 1.02.18a Has your agency filed any claims with your cybersecurity insurance provider?
- Yes
  - No
- 1.02.18b Which of the following does or will the insurance policy cover? (Select all that apply.)
- Breach notification
  - Business interruption
  - Credit monitoring
  - Incident response services
  - Media liability
  - Professional liability
  - Ransomware/Extortion
  - Regulatory fines
  - Not applicable
  - Other, write in <enter text>
- 1.02.18c Have you seen an increase in cybersecurity insurance premiums or deductibles, or a reduction in coverage since the last biennium?
- Yes
  - No
  - N/A

### Third-party Security

- 1.02.19 Does your agency integrate security requirements into third-party service contract agreements?
- Yes, for all third-party contracts
  - Yes, for contracts involving confidential or regulated data
  - No
- 1.02.19a How often does your agency conduct security assessments on third-party partners and other service providers with access to information assets?
- Prior to entering into a contract
  - Annually
  - As needed
  - The agency does not conduct third-party security assessments.



### Risk Management

New

1.02.20 What are your agency's top five Texas Cybersecurity Framework priorities for the next biennium? (Select five.)

#### IDENTIFY

- Privacy and Confidentiality
- Data Classification
- Critical Information Asset Inventory
- Enterprise Security Policy, Standards, and Guidelines
- Control Oversight and Safeguard Assurance
- Information Security Risk Management
- Security Oversight and Governance
- Security Compliance and Regulatory Requirements Management
- Cloud Usage and Security
- Security Assessment and Authorization/Technology Risk Assessments
- External Vendors and Third-Party Providers

#### PROTECT

- Enterprise Architecture, Roadmap and Emerging Technology
- Secure System Services, Acquisition and Development
- Security Awareness and Training
- Privacy Awareness and Training
- Cryptography
- Secure Configuration Management
- Change Management
- Contingency Planning
- Media
- Physical and Environmental Protection
- Personnel Security
- Third-Party Personnel Security
- System Configuration Hardening and Patch Management
- Access Control
- Account Management
- Security Systems Management
- Network Access and Perimeter Controls
- Internet Content Filtering
- Data Loss Prevention
- Identification and Authentication
- Spam Filtering
- Portable and Remote Computing
- System Communications Protection



- Information Systems Currency

DETECT

- Vulnerability Assessment
- Malware Protection
- Security Monitoring and Event Analysis
- Audit Logging and Accountability

RESPOND

- Cybersecurity Incident Response
- Privacy Incident Response

RECOVER

- Disaster Recovery Procedures

### Section 1.03 – Digital Accessibility

- 1.03.01 Is your agency participating in the state's free website accessibility scanning program?
- Yes (If selected, skip 1.03.01a and 1.03.01b as they are not applicable.)
  - No, but plan to
  - No

---

Coordinate with your agency's EIR Accessibility Coordinator (EIRAC) when completing Section 1.03.

For accessibility requirement standards, training requirements, and more, see DIR's [EIR Accessibility webpage](#).

IHEs must complete Section 1.03.

---

- 1.03.01a If the answer to 1.03.01 is no, which of the following best describes why?
- Lack of resources to analyze, report, and distribute findings
  - Lack of technical skills to remediate errors
  - Security concerns
  - Not aware of program
  - Agency uses an alternate scanning program or service (If selected, answer 1.03.01b.)
  - Other, write in <enter text>

**New**

- 1.03.01b If using an alternate scanning program or service, please select one from the following:
- Deque Axe tools (e.g., Axe Auditor/Axe Monitor)
  - Google Lighthouse
  - Level Access AMP
  - Pa11y
  - Siteimprove (standalone contract)
  - WebAIM WAVE



# Information Resources Deployment Review

## 2024 Instructions

- Other, write in <enter text>
  
- 1.03.02 Does your agency perform accessibility compliance testing during web development or updates?
  - Yes - all pages and designs
  - A subset of pages and designs
  - No (If selected, skip 1.03.02a-1.03.02b as the questions are not applicable.)
  - Not applicable (If selected, skip 1.03.02a-1.03.02b as the questions are not applicable.)
  
- 1.03.02a How does your agency perform accessibility compliance testing during web development or updates? (Select all that apply.)
  - Automated testing
  - Manual
  - Functional or quality assurance testing
  - Testing using assistive technology
  - Usability testing with a person who has a disability
  
- 1.03.02b What percentage of your agency's publicly facing web pages are in full compliance with the state accessibility requirements in 1 Texas Administrative Code (TAC) Chapters 206 and 213?
  - <Enter a percentage:>
  
- New
  
- 1.03.02c When does your agency perform accessibility compliance testing during web development or updates? (Select all that apply.)
  - During the website development lifecycle
  - At the end of the website development lifecycle before deployment
  - During scheduled review cycles
  - Only when a problem is identified
  
- 1.03.03 Does your agency perform accessibility compliance testing on agency web-based, native, and hybrid applications?
  - Yes
  - No (If selected, skip questions 1.03.03a-1.03.03b as they are not applicable.)
  - Not applicable (If selected, skip questions 1.03.03a-1.03.03b as they are not applicable.)
  
- 1.03.03a How does your agency perform accessibility compliance testing on agency web-based, native, and hybrid applications? (Select all that apply.)
  - Automated testing
  - Manual testing

- Functional or quality assurance testing
- Testing using assistive technology
- Usability testing with a person who has a disability

New

1.03.03b When does your agency perform accessibility compliance testing on internal application development projects? (Select all that apply.)

- During the development lifecycle
- At the end of the development lifecycle before deployment
- During scheduled review cycles
- Only when a problem is identified

1.03.04 Does your agency document results of accessibility compliance testing?

- Yes, always
- Sometimes
- No
- The agency does not perform accessibility compliance testing (If selected, skip 1.03.04a as the question is not applicable.)

1.03.04a Does your agency take corrective action based on the results of accessibility compliance testing?

- Yes, always
- Sometimes
- No

1.03.05 What types of challenges has your agency faced when attempting to achieve compliance with state accessibility requirements? (Select all that apply.)

- Lack of executive support or prioritization for accessibility initiatives
- Lack of staff with required knowledge/skill sets
- Lack of available training to improve accessibility compliance
- Insufficient budget for staff, training, testing tools, or technology modernization
- Lack of trained staff for testing
- Testing is cost prohibitive
- Lack of awareness that testing should be performed during development
- Vendor developer did not build testing into the project
- Accessibility not integrated into agency IT development lifecycle
- Accessibility not integrated into agency procurement processes
- Accessibility not integrated into agency project management lifecycle
- Limitations in available accessible commercial products or services
- None
- Other, write in <enter text>

1.03.06 What is the current agency status for each of the following accessibility metrics?

Select from:

- Currently measuring
- Planning to measure
- Not measured or planned

General Accessibility Awareness and Overview training <status>

MS Office Accessibility training <status>

PDF Accessibility training <status>

Developer training (WCAG standards) <status>

Project Manager training <status>

Procurement Staff training <status>

Percentage of compliant web pages <status>

Percentage of compliant web documents <status>

Percentage of web videos captioned <status>

Percentage of accessible digital offerings procured <status>

Percentage of accessible applications developed <status>

Total number of accessibility exceptions <status>

Other, write in <enter text> <status>

New

1.03.07 Which [WCAG](#) standard has your agency adopted for accessibility compliance?

- [WCAG 2.0 AA](#)
- [WCAG 2.1 AA](#)
- [WCAG 2.2 AA](#)
- None

1.03.08 How much of your agency's Accessibility Coordinator's time is dedicated to accessibility weekly?

- 40 hours or more
- 30-39 hours
- 20-29 hours
- 10-19 hours
- less than 10 hours

1.03.09 Does your agency have staff registered for courses in DIR's free digital accessibility learning management system, Access Academy?

- Yes
- No



- 1.03.10 How valuable and effective is Access Academy, DIR's free digital accessibility learning management system, to your agency in achieving accessibility compliance with 1 TAC Chapters 213 and 206?
- Very valuable
  - Somewhat valuable
  - Neither valuable nor not valuable
  - Not very valuable
  - Not valuable

### Section 1.04 – Continuity of Operations

- 1.04.01 Has your agency implemented ongoing or daily remote working solutions to support alternative workplace arrangements?
- Implemented
  - In progress
  - In planning
  - No
- 1.04.02 Does your agency incorporate work-from-home or alternative workplace arrangements in its continuity of operations or business continuity plans, related to potential scenarios which could limit the use of central facilities?
- Yes, plan includes working from home in such scenarios
  - Yes, plan includes alternative workplaces in such scenarios
  - Yes, plan includes both work-from-home and alternative workplace options
  - No
- 1.04.03 Does your agency maintain a written disaster recovery plan for information resources in support of its Continuity of Operations Plan (COOP)?
- Yes, implemented
  - Yes, as part of the DCS disaster recovery plan
  - No, in progress (If selected, skip questions 1.04.03a-1.04.03b as they are not applicable.)
  - No (If selected, skip 1.04.03a-1.04.03b as they are not applicable.)
- 1.04.03a Has your agency's COOP been revised or updated in the last 12 months?
- Yes
  - No
- 1.04.03b Has your agency's COOP been tested in the last 12 months other than the pandemic response?
- Yes
  - No



- 1.04.04 Does your agency utilize cloud services or disaster recovery-as-a-service (DRaaS) in COOP?
- Yes
  - Considering
  - No
- 1.04.04a Has your agency successfully tested the disaster recovery-related application(s) for compatibility with cloud services?
- Yes
  - In progress
  - No

New

- 1.04.05 Does your agency include contingency plans for addressing disruptions in or increase demand for connectivity (network/broadband/cellular) in its COOP?
- Yes
  - No

### Section 1.05 – Electronic Records Management

- 1.05.01 For which of the following areas does your agency have a policy or policy provision relating to digital data and records management practices? (Select all that apply.)
- Data classification (e.g., public, sensitive, etc.)
  - Records disposition based on retention schedules
  - Local/desktop storage
  - Hierarchical storage
  - Email
  - Duplicate file management
  - Mobile storage and backup
  - Social media
  - Employee separation
  - Data retention schedule separate from state required records retention schedule
  - Other, write in <enter text>
- 1.05.02 Does your agency use any automated tools to enforce the records retention policy?
- Yes

---

Coordinate with your agency's Data Management Officers (DMOs) and Records Management Officers (RMOs) when completing Section 1.05.

For data management information, see DIR's [Office of the Chief Data Officer webpage](#) and the Texas State Library and Archive Commission's [Records Management webpage](#).

---

- In planning
  - No
- 1.05.03 Which digital preservation techniques does your agency use? (Select all that apply.)
- Technology preservation (retain hardware and software used to create and access content)
  - Technology emulation (current technology used to replicate and preserve functionality of older technology using metadata descriptions)
  - Content migration (move content from old storage platform, media, and format technology to new)
  - Analog conversion (convert digital content to microfilm or microfiche)
  - Print to paper
  - Transfer archival records to the Texas Digital Archive at the Texas State Library and Archives Commission
  - Cloud storage
  - Application of checksum/hash
  - Other, write in <enter text>
- 1.05.04 How much does your agency anticipate its digital storage spending to increase compared to the previous biennium?
- 0-5%
  - 5-10%
  - 10-20%
  - 20-50%
  - Over 50%
  - Unknown
- 1.05.05 What are the greatest barriers your agency faces regarding the management of electronic records and digital data storage? (Select three.)
- Cost
  - Unclear understanding of data
  - Underdeveloped data management practices
  - Difficulty applying retention schedules
  - Lack of policy and enforcement
  - Lack of executive engagement
  - Competing priorities/initiatives
  - Staff training
  - Business process
  - Format of records
  - Other, write in <enter text>

- 1.05.06 Which of the following maturity levels best describes your agency's information security data classification policies and processes?
- Initial: Data classification policies exist but classifications are inconsistent, unreliable, and inaccurate. At least some parts of the organization have adopted in practice a sensitive/non-sensitive data classification.
  - Repeatable: Data classification policies and processes are defined and repeatable. Across the organization, there is a common understanding of what is the organization's most important and sensitive information. Data owners have been identified for most information.
  - Defined: The organization's data-classification policies are aligned with applicable regulations and the organization's own risk assessments. The organization takes enforcement actions (such as spot checks, audits, process controls, awareness communications, and data-leak prevention controls) that reinforce these classifications.
  - Controlled: Data is managed by technology that requires classification as new data is created. Automated policies ensure data is consistently classified across the organization. Data classification monitoring is continuous, proactive, and preventative, involving appropriate metrics.
  - Optimized: Data is managed based on classification levels that align to business need and mission criticality.
  - None of the above: Data classification policies and procedures do not exist.
- 1.05.07 How often does your agency assess digital data for compliance with established retention requirements?
- Monthly
  - Quarterly
  - Annually
  - Biennially
  - Intermittently, as needed
  - The agency does not assess for compliance with retention requirements
  - Other, write in <enter text>
- 1.05.08 What percentage of data stored beyond its required retention schedule is unnecessary as of September 1, 2023?
- <Enter a percentage>
- 1.05.08a What are the primary reasons for storing digital data and records beyond the established retention requirements? (Select three.)
- Administrative, audit, or legal holds
  - Competing priorities
  - Organizational practices/culture
  - Limited data visibility/metadata



- Potential for reuse/reference/research
- Technology/system makes deletion/purging difficult
- Not applicable, as the agency does not exceed retention requirements
- Other, write in <enter text>

1.05.09 What is the approximate volume (in gigabytes) of digital records dispositioned in FY 23?

- write in <enter a number>

New

1.05.09a What is the approximate number of digital records dispositioned in FY 23?

- write in <enter a number>

1.05.10 Do the storage solutions utilized allow your agency to meet the security requirements of the data?

- Yes, for all data
- Yes, for most data
- No
- Unsure

1.05.11 For data stored in the cloud, which of the following security controls does your agency implement? (Select all that apply. If the agency does not utilize cloud storage, please select "Not Applicable.")

- Virtual Data Center connectivity
- Anti-virus software
- Operating system patching
- Security Information and Event Management
- Continental US-only operations
- Appropriate vendor certifications (e.g. HIPAA, FERPA, CJIS compliance)
- Background-checked employees
- Virtual Local Area Network
- Encryption at rest and in transit
- Host Intrusion Protection Services
- Host Intrusion Detection Services
- Web Application Firewall services (public facing)
- Network Intrusion Prevention Services
- Data Loss Prevention software
- Not Applicable (Agency does not store data in the cloud)
- Other, write in <enter text>



# Information Resources Deployment Review

## 2024 Instructions

- 1.05.12 For data stored in locally hosted, agency-managed servers and storage devices (excluding workstations), which of the following security controls has your agency implemented? (Select all that apply.)
- Virtual Data Center connectivity
  - Anti-virus software
  - Operating system patching
  - Security Information and Event Management
  - Continental US-only operations
  - Appropriate vendor certifications (e.g. HIPAA, FERPA, CJIS compliance)
  - Background-checked employees
  - Virtual Local Area Network
  - Encryption at rest and in transit
  - Host Intrusion Protection Services
  - Host Intrusion Detection Services
  - Web Application Firewall services (public facing)
  - Network Intrusion Prevention Services
  - Data Loss Prevention software
  - Other, write in <enter text>

### Section 1.06 – Contracting

- 1.06.01 Does your agency attempt to negotiate a lower price when procuring technology goods and services through the DIR Cooperative Contracts Program?
- Yes, frequently
  - Yes, sometimes
  - No, (If selected, skip question 1.06.01a.)

- 1.06.01a How frequently is your agency able to negotiate a lower price when procuring technology goods and services through the DIR Cooperative Contracts Program?
- Almost always
  - Most of the time
  - Frequently
  - Infrequently
  - Rarely

---

State agencies are required to purchase hardware, software, and technical services through DIR by [Government Code Section 2157.068](#).

State agency employees directly involved in IT contract negotiations must complete DIR's procurement training as required by [Government Code Section 656.050\(b\)](#).

For information on procuring IT products and services, see DIR's [Buying Through DIR webpage](#).

---

- 1.06.02 How many Automated Information System (AIS) procurements as defined by [Government Code Section 2157.001](#), that will exceed \$10 million during the entire contract term, including optional renewals and extensions, does your agency plan to make in the next biennium?
- Less than 5
  - 5-10
  - 11-15
  - Over 15
- 1.06.03 What additional products or services would you like to see made available through DIR's Cooperative Contracts Program?
- <enter text>
- 1.06.04 How many Statements of Work (SOW) does your agency anticipate submitting to DIR in the next biennium?
- 0-5
  - 6-10
  - 11-20
  - 21-30
  - 31-50
  - 51-100
  - More than 100
- 1.06.05 How many [Cooperative Contracts exemptions](#) does your agency anticipate submitting to DIR in the next biennium?
- <Enter a number>
- 1.06.05a For what types of products/services is your agency most often submitting exemptions?
- <enter text>
- 1.06.05b What type of blanket exemptions, if any, should DIR consider adding in the future?
- <enter text>
- 1.06.06 Approximately how many DIR IT Staff Augmentation solicitations does your agency intend to leverage in the next biennium?
- 0-5
  - 6-10
  - 11-20
  - Over 20
  - Other, write in <enter number>

- 1.06.07 Which of the following types of software, hardware, or technology would interest your agency for a bulk purchase initiative? (Select all that apply.)
- Adobe software
  - Antivirus software
  - Business Intelligence/analytics software (e.g., Tableau, Power BI)
  - Desktops/laptops
  - EIR Accessibility tools
  - Endpoint detection and response
  - Enterprise content management systems
  - Facilities management software
  - Fleet management software
  - Geographic Information Systems (GIS) software
  - Integrated risk management software
  - Learning management systems
  - Multifactor authentication software
  - Productivity software (e.g., digital signature software, collaboration software)
  - Surveillance software and products
  - Videoconferencing equipment
  - Other, write in <enter text>
- 1.06.08 Approximately how many agency staff are involved with IT contract negotiations?
- <Enter a number>
- 1.06.08a Of the number above, approximately, how many agency staff have taken the statutorily-required DIR IT negotiations training?
- <Enter a number>
- 1.06.08b Of the number remaining to be trained, how many agency staff plan to attend training in the next biennium?
- <Enter a number>
- 1.06.09 Has your procurement division implemented agile contracting?
- Yes
  - In planning
  - No

## Section 1.07 – Hardware and Software Environment

### Client Hardware Environment

For each category of end-user computing device, what is the approximate number of devices used in your agency? Enter a number.

- |         |                                  |          |
|---------|----------------------------------|----------|
| 1.07.01 | Desktops, owned                  | <number> |
| 1.07.02 | Desktops, leased or seat managed | <number> |
| 1.07.03 | Laptops, owned                   | <number> |
| 1.07.04 | Laptops, leased or seat managed  | <number> |
| 1.07.05 | Tablet computers                 | <number> |
| 1.07.06 | Smartphones/cell phones          | <number> |
| 1.07.07 | Printers, network and dedicated  | <number> |

For each category of end-user computing device, what is the planned refresh cycle?

- |         |                                  |                   |
|---------|----------------------------------|-------------------|
| 1.07.08 | Desktops, owned                  | <number of years> |
| 1.07.09 | Desktops, leased or seat managed | <number of years> |
| 1.07.10 | Laptops, owned                   | <number of years> |
| 1.07.11 | Laptops, leased or seat managed  | <number of years> |
| 1.07.12 | Tablet computers                 | <number of years> |
| 1.07.13 | Smartphones/cell phones          | <number of years> |
| 1.07.14 | Printers, network and dedicated  | <number of years> |

- 1.07.15 What is the approximate average age of desktops and laptops currently in use by your agency?
- 1 year    2 years    3 years    4 years    5 years    6+ years
- 1.07.16 What is the approximate age of the oldest desktops or laptops currently in use by your agency?
- 1 year    2 years    3 years    4 years    5 years  
 6 years    7 years    8 years    9 years    10+ years

### Client Software Environment

- 1.07.17 What is your agency's current primary client operating system?
- Microsoft Windows 10
  - Microsoft Windows 11
  - Apple Macintosh OS X, 11, Big Sur
  - Apple Macintosh OS X, 12, Monterey
  - Apple Macintosh OS X, 13, Ventura
  - Apple Macintosh OS X, 14, Sonoma
  - Other, write in <enter text>

- 1.07.18 If your agency is planning or considering migration to a newer primary client operating system in the next biennium, which will it be?
- No migration is currently planned
  - Microsoft Windows 10
  - Microsoft Windows 11
  - Apple Macintosh OS X, 11, Big Sur
  - Apple Macintosh OS X, 12, Monterey
  - Apple Macintosh OS X, 13, Ventura
  - Apple Macintosh OS X, 14, Sonoma
  - Other, write in <enter text>
- 1.07.19 What is your agency's current primary client office productivity suite?
- Microsoft 365 (O365)
  - Microsoft Office 2016
  - Microsoft Office 2019
  - Microsoft Office 2021
  - Apple iWork
  - Microsoft Office 2016 for Macintosh
  - Microsoft Office 2019 for Macintosh
  - Google Workspace
  - Other, write in <enter text>
- 1.07.20 If your agency is planning or considering an upgrade to a newer office productivity suite in the next biennium, which will it be?
- No upgrade is currently planned
  - Microsoft Office 2021
  - Apple iWork
  - Microsoft Office 2021 for Macintosh
  - Google Workspace
  - Other, write in <enter text>

### Server Environment

- 1.07.21 How many physical hardware hosts exist in your agency's virtualized server environment, excluding those managed by DIR's Shared Technology Services (Data Center Services) contracts?
- <Enter a number>
- 1.07.22 How many virtual server instances exist in your agency's virtualized server environment, excluding those managed by DIR's Shared Technology Services (Data Center Services) contracts?
- <Enter a number>

- 1.07.23 How many physical server instances exist in your agency's non-virtualized server environment, excluding those managed by DIR's Shared Technology Services (Data Center Services) contracts?
- <Enter a number>
- 1.07.24 What is the refresh cycle for physical servers managed by your agency?
- 3 years
  - 4 years
  - 5 years
  - 6 or more years
- 1.07.25 What is the approximate average age of servers currently managed by your agency?
- 1 year
  - 2 years
  - 3 years
  - 4 years
  - 5 years
  - 6+ years
- 1.07.26 What is the approximate age of the oldest servers currently managed by your agency?
- 1 year
  - 2 years
  - 3 years
  - 4 years
  - 5 years
  - 6 years
  - 7 years
  - 8 years
  - 9 years
  - 10+ years

### Network Environment

- 1.07.27 What is the status of agency support for IPv6?
- Complete
  - In progress
  - In planning
  - Not planned
- 1.07.28 Does your agency employ separate staff to manage its Local Area Network and Wide Area Network?



- Yes
- No
- The agency uses managed network services
- Other, write in <enter text>

### Microservices

- 1.07.29 What is the status of deployment of Microservices in your agency?
- Currently using
  - Planning to use
  - Do not use and not planning to use

### Section 1.08 – E-Learning

- 1.08.01 Which of the following types of technology are used in training programs provided by your agency? (Select all that apply.)
- Technology-based training available through the agency
  - Recording available on agency's website
  - Recording available on YouTube
  - Recording available via podcasting
  - Live broadcast via webinar
  - Live teleconference
  - Online training Software-as-a-Service (SaaS) solution
  - None of the above
  - Other, write in <enter text>
- 1.08.02 Does your agency have a Learning Management System (LMS)?
- Yes; name of primary LMS: <enter text>
  - In progress; name of primary LMS: <enter text>
  - No, but considering
  - No
- 1.08.03 Which of the following does your agency use for training employees? (Select all that apply.)
- Online training, developed by the agency
  - Online training, third-party
  - Tracking systems for personnel training/certifications
  - Software for curriculum development and content management
  - None of the above
  - Other, write in <enter text>
- 1.08.04 What percentage of training provided by your agency is internet-based (e.g., online self-paced, online-instructor led, webinars)?
- <Enter a percentage>





### Section 1.09 – Advanced Technologies and Methods

#### Geographic Information Systems

- 1.09.01 Does any part of your agency develop, maintain, or use geographic information/data? (Select all that apply.)
- Develop
  - Maintain
  - Utilize
  - None of the above (If selected, skip 1.09.02-1.09.04 as they are not applicable.)
- 1.09.02 Is the geographic information/data your agency develops or maintains required by state law to fulfill agency duties?
- Yes
  - No (If selected, skip 1.09.02a as it is not applicable.)
- 1.09.02a Provide the names, a short description, and all statutory references that relate to the geographic data.  
<enter text>
- 1.09.03 Does your agency provide public access to the geospatial datasets it develops or enhances? (Select all that apply.)
- Yes, datasets can be downloaded from a public website
  - Yes, datasets are published via a web service
  - Yes, datasets are provided upon request
  - No, explain: <enter text>
- 1.09.04 Does your agency deploy one or more GIS web map services?
- Yes
  - In planning
  - No, but would like to in the future
  - No
- 1.09.05 Does your agency share or obtain GIS services or data through another governmental entity or institution of higher education?
- Yes; identify agencies: <enter text>
  - No

---

Coordinate with your agency’s Chief Technology Officer and Project Management Office, or their equivalents, when completing Section 1.09.

For information on advanced technologies and methods, see DIR’s and [Digital Project Services webpage](#).

---



### Cloud

- 1.09.06 In which of the following categories does your agency leverage public cloud services? (Select all that apply.)
- Active Directory
  - Office productivity software - Collaboration and planning tools
  - Email
  - Enterprise Content Management – Human Resources
  - Enterprise Content Management – Financial
  - Enterprise Content Management
  - Geographic Information System
  - Storage
  - Digital storage/electronic records
  - Disaster recovery
  - Program/business applications (e.g. licensing)
  - Citizen/customer relationship management
  - Imaging
  - Infrastructure-as-a-Service (IaaS)
  - Platform-as-a-Service (PaaS)
  - Software-as-a-Service (SaaS)
  - Mainframe
  - Telecommunications
  - Security
  - None
  - Other, write in <enter text>
- 1.09.07 What are the greatest barriers to public cloud adoption for your agency? (Select five.)
- Application incompatibility
  - Application currency
  - Organizational practices/culture changes
  - Competing priorities
  - Migration costs
  - Network connectivity between cloud and local servers
  - Cybersecurity considerations
  - Complexity/Technical skills
  - Cost management and control
  - Regulatory compliance considerations
  - Bandwidth issues
  - Procurement or contracting rules and processes
  - Workforce skills
  - Legal constraint
  - Budget constraint



# Information Resources Deployment Review

## 2024 Instructions

- Other, write in <enter text>

### New

1.09.08 Which cloud characteristics matter the most to your agency? (Select three.)

- Scalability
- Metered financial models
- Security
- Packaged business capabilities
- Speed of response
- Speed to solution
- Other, write in <enter text>

### New

1.09.09 How would you characterize your agency's approach to cloud services?

- We have fully implemented our cloud strategy or road map
- We have completed a cloud strategy or roadmap
- We are developing a cloud strategy or roadmap
- We are planning a cloud strategy or roadmap but have not started
- We are not pursuing cloud services at this time

### New

1.09.10 Over the last two years, how has the pace of your cloud adoption changed?

- Accelerated cloud adoption plans in all functional areas
- Accelerated cloud adoption plans in some functional areas
- No change in cloud adoption plans
- Decelerated cloud adoption plans in some functional areas
- Decelerated cloud adoption plans in all functional areas

## Artificial Intelligence

1.09.11 How does your agency currently use AI solutions? (Select all that apply.)

- Chatbots
- Data analysis
- Data management
- Services to customers/clients/constituents
- Human resources management
- Process improvement
- Process automation or workflow
- Customer relationship management
- Inventory control
- Cybersecurity
- Workforce productivity
- Digital accessibility
- None of the above, we do not use AI (If selected, go to question 1.09.17.)
- Other, write in <enter text>

- 1.09.12 Define your agency's maturity in implementing AI solutions. (Select one.)
- Initial
  - Repeatable
  - Defined
  - Controlled
  - Optimized
- 1.09.13 What are your agency's top productivity priorities for using AI solutions? (Select three.)
- Increase work output and efficiency
  - Free up staff work hours from repeatable assignments
  - Identify previously unknown trends
  - Increase resiliency
  - Improve the end user/customer experience
  - Provide greater digital accessibility
  - Other, write in <enter text>
- 1.09.14 What are the greatest challenges for using AI solutions in your agency? (Select all that apply.)
- Lack of dedicated personnel
  - Lack of executive engagement
  - Lack of qualified staff
  - Competing priorities
  - Copyright infringement
  - Lack of perceived interest
  - Budgetary restrictions
  - Unclear or lack of acceptable use policies
  - Limited available public-sector use cases
  - Security concerns
  - Privacy concerns
  - Potential for fraud and misuse
  - Poor data quality
  - Other, write in <enter text>
- New**
- 1.09. 15 How is your agency currently using or preparing to use **generative AI** solutions? (Select all that apply.)
- Chatbots
  - Data analysis
  - Data management
  - Digital accessibility testing

- Services to customers/clients/constituents
- Human resources management
- Process improvement
- Process automation or workflow
- Customer relationship management
- Inventory control
- Automated decisions
- Code development
- Cybersecurity
- Workforce productivity
- None, my agency is not currently using generative AI
- None, but my agency is preparing to use generative AI
- Other, write in <enter text>

**New**

- 1.09.16 How does your agency currently address the risk of using AI? (Select all that apply.)
- Acceptable use policies are in place
  - Prohibiting the use of specific technologies
  - Adopting tools for detection of and response to AI-specific cybersecurity risk
  - Educating employees on AI risks and acceptable use
  - Updating internal procurement guidelines for AI solution purchases and contracts
  - Implementing the NIST AI Risk Management Framework
  - Ensuring data quality and integrity
  - Other, write in <enter text>

**Other Advanced Technology**

- 1.09.17 Has your agency considered the use of low-code/no-code development platforms?
- Currently using
  - Planning to use
  - May use
  - Do not use



# Information Resources Deployment Review

## 2024 Instructions

- 1.09.18 Does your agency use distributed ledger technology (or blockchain)?
- Currently using
  - Planning to use
  - May use
  - Do not use and have no plans to use
- 1.09.19 Does your agency employ open-source software development for technology projects?
- Implemented
  - Implementation in progress
  - Planned or planning in progress
  - Under consideration
  - Not implemented and not planned (If selected, skip question 1.09.20 as it is not applicable.)
- 1.09.20 In which of these categories does your agency use open-source software? (Select all that apply.)
- Web server
  - Application server
  - Database server
  - Middleware server
  - Client operating system
  - Server operating system
  - None
  - Other, write in <enter text>

### Methodologies and Tools

- 1.09.21 Does your agency use an Application Portfolio Management (APM) tool?
- In use
  - In progress of implementing
  - Planning to implement
  - No plans to implement
  - If your agency is using, implementing, or planning to implement APM, which tool? write in <enter text>
- 1.09.22 Has your agency implemented a DevOps model?
- Currently using
  - In planning
  - Considering
  - Not planned

## Section 1.10 – Transformation and Modernization

### New

- 1.10.01 What are the main reasons your agency still has legacy systems and applications in place? (Choose three.)
- Workforce challenges
  - Cost
  - Customizations are not easily replicated
  - Data migration challenges
  - Potential for business disruption
  - Did not understand complete portfolio
  - Did not plan for multi-year funding
  - Other, write in <enter text>
- 1.10.02 What is the status of your agency's plan to remediate unsupported software?
- All agency software is current and supported
  - Implemented
  - Implementation in progress
  - Planned or planning in progress
  - Not implemented and not planned
- 1.10.03 What is the maturity level of digital transformation in your agency?
- Initial: Reactive, IT-centric, e-government only
  - Repeatable: Open, transparency-focused, starting to co-create applications
  - Defined: Data-centric, proactive, business-led
  - Controlled: Fully digital, transformation-focused, modular technology
  - Optimized: Smart, predictive, using emerging technology
  - None of the above: Digital transformation practices do not exist
- 1.10.04 Does your agency currently have or plan to have paperless, partially paperless, or paper-on-request (including print mail) processes?
- Yes – all paperless processes (If yes, skip 1.10.05 - 1.10.07; go to 1.10.08)
  - Yes – partially paperless processes
    - If yes, please describe the paper-based processes still in use. Write in <enter text>
  - Yes – paper-on-request only
    - If yes, please describe the paper-on-request processes still in use. Write in <enter text>
  - No, but we plan to have all paperless processes
  - No, but we plan to increase our paperless processes

---

**Coordinate with your agency's Chief Technology Officer, or its equivalent, when completing Section 1.10.**

**For information on advanced technologies and methods, see DIR's Strategic Digital Services webpage.**

---



# Information Resources Deployment Review

## 2024 Instructions

- No, but we plan to implement paper-on-request only
  - No, we do not have paperless processes or plans for paperless processes
    - If no, please describe why, write in <enter text>
  
- 1.10.05 What agency processes include paper-based processes, including partially paperless processes and paper-on-request processes? (Select all that apply.)
  - Print mail
  - Applications for jobs, benefits, licenses, or other externally facing processes
  - Documentation for continuity of operations
  - Printing for internal purposes
  - Other, write in <enter text>
  
- 1.10.06 What are the barriers to going paperless or paper-on-request at your agency? (Select all that apply.)
  - Limited by internal processes
  - Limited by insufficient resources (funding or staff) to make the changes
  - Limited by state or federal law
  - Other, write in <enter text>
  
- 1.10.07 For paperless processes or partially paperless processes that require an application or form with a signature, does your agency require a hard copy or mailed copy of the same application or form with the signature?
  - Yes, for all
  - Yes, for some
  - No
  
- 1.10.08 Describe any electronic notification or digital communication efforts or requirements between your agency and the public.
  - <enter text>
  
- 1.10.09 How would you characterize the maturity of your agency's ability to embrace digital transformation?
  - Initial: Bottom up driven by staff; risk averse and resistant to change
  - Repeatable: Small number of staff engaged in digital projects; change management strategy in development
  - Defined: Digital strategy developed and embraced; focus is on constituents, employees, and how digital services can meet their needs
  - Controlled: All staff embrace digital strategy and are driving a cultural change; staff are redefining roles to align with digital strategy
  - Optimized: Digital culture is embedded into overall culture; staff are always looking for ways to improve digital service delivery
  - None: No willingness to embrace change





# Information Resources Deployment Review

## 2024 Instructions

- 1.10.10 Does your agency currently collect, or would it be interested in collecting, online fees, fines, or payments via credit card or automated bank draft (known as Automated Clearinghouse or ACH withdrawal)?
- Agency currently provides this service
  - Agency currently uses Texas.gov for this service
  - Agency is interested in providing this service or plans to provide it in the next biennium
  - Agency has no need or interest in this service
- 1.10.11 Does your agency incorporate responsive design into constituent-facing application development to optimize application functionality on mobile devices?
- Yes, for all public-facing applications
  - Yes, for some public-facing applications
  - No
- 1.10.12 Does your agency incorporate human-centered design principles into constituent-facing application development to optimize application functionality?
- Yes, for all public-facing applications
  - Yes, for some public-facing applications
  - No
- 1.10.13 Select the option below that best describes your current capability for development of native mobile application
- Initial: No native mobile app development is planned, but interested
  - Repeatable: Researching how a native mobile app might improve delivery of services
  - Defined: Planning or starting to build a native mobile app
  - Controlled: Have developed and deployed a native mobile app
  - Optimized: Managing one or multiple native mobile apps; have in-house staff that know how to develop and maintain native mobile apps
  - None: Do not know what native mobile application development really means
- 1.10.14 How many native mobile apps has your agency developed?
- <Enter a number>

## Section 1.11 – Project Delivery

- 1.11.01 Which of the following project development approaches does your agency use? (Select all that apply.)
- Adaptive (e.g. Agile projects)
  - Predictive (e.g. Waterfall projects) (If selected, skip 1.11.02 as it is not applicable.)
  - Hybrid
  - Other, write in <enter text> (If selected, skip 1.11.02 as it is not applicable.)
  - Not applicable
- 1.11.02 Which of the following agile approaches does your agency use? (Select all that apply.)
- Extreme programming
  - Kanban
  - Scrum
  - SAFe Agile
  - DevOps
  - Scaled Agile
  - Other, write in <enter text>
  - Not applicable
- 1.11.03 Has your agency implemented a standard project management methodology aligned with 1 TAC Chapter 216 for information resources projects?
- Implemented
  - Implementation in progress
  - Planned or planning in progress (If selected, skip 1.11.03a as it is not applicable.)
  - Not implemented and not planned (If selected, skip 1.11.03a as it is not applicable.)
- 1.11.03a Has your agency implemented a methodology that integrates contract management and project management practices?
- Implemented
  - Implementation in progress
  - Planned or planning in progress
  - Not implemented and not planned
- 1.11.04 Has your agency implemented a project classification method aligned with 1 TAC Section 216.11 for information resources projects?

---

Coordinate with your agency's Project Management Office, or its equivalent, when completing Section 1.11.

For information on advanced technologies and methods, see [DIR's Digital Project Services webpage](#).

---

- Implemented
- Implementation in progress
- Planned or planning in progress
- Not implemented and not planned

1.11.05 Does your agency voluntarily use the Texas Project Delivery Framework (TPDF) for non-major IR projects, defined as projects that do not meet the definition of a major information resources project (MIRP)?

- Yes, for all non-major IR projects<sup>8</sup>
- Yes, for some non-major IR projects
- Planning or considering voluntary use of the TPDF for non-major IR projects
- No, TPDF is not being used for non-major IR projects
- No, your agency has never used the TPDF

1.11.06 Which of the following are the greatest challenges your agency faces in achieving IT project success? (Select three.)

- Lack of user involvement
- Incomplete requirements and specifications
- Changing requirements and specifications
- Competing agency priorities
- Technical challenges
- Lack of resources
- Unrealistic expectations
- Unclear objectives
- Unrealistic timeframes
- Lack of organizational change management
- Long budget cycles that do not match modern software design practices
- Procurement or contracting
- Other, write in <enter text>
- Not applicable

**New**

1.11.07 Has your agency implemented a repeatable process for identifying and reporting all MIRPs?

- Yes, a formal policy/process has been published, and is maintained and followed
- Yes, there is a process, but it isn't formalized

---

<sup>8</sup> For question 1.11.05, answer yes if the agency uses some but not all components of the TPDF for non-major IR projects.



- Planning or considering a formal policy/process for identifying and reporting
- No, there is no defined process for identifying and reporting major information resources at the agency

### Section 1.12 – Shared Networks

- 1.12.01 How often does your agency use TEX-AN contracts for purchasing telecommunications services?
- Always
  - Sometimes
  - Never
- 1.12.02 In the next biennium, by how much does your agency expect its overall network bandwidth needs to increase or decrease?
- Decrease Over 100%
  - Decrease 51% - 100%
  - Decrease 25% - 50%
  - Decrease less than 25%
  - No anticipated changes to network bandwidth needs
  - Increase less than 25%
  - Increase 25% - 50%
  - Increase 51% - 100%
  - Increase Over 100%
- 1.12.03 In the next biennium, by how much does your agency expect its internet connection needs to increase? (over current internet bandwidth)
- 0-50Mb
  - 51-100Mb
  - 101 – 500 Mb
  - 500 Mb – 1 Gb
  - Other, write in <enter text>

#### New

- 1.12.04 In the next biennium, what are your agency's plans for telephony services. (Select all that apply.)
- Increase desktop telephones
  - Increase mobile or cellular telephones
  - Increase softphones or unified communications applications such as Microsoft Teams
  - Decrease desktop telephones
  - Decrease mobile or cellular telephones

- Decrease softphones or unified communications applications such as Microsoft Teams
- No changes planned

New

- 1.12.05 How satisfied is your agency with the performance of your agency's video conferencing services?
- Satisfied
  - Neither satisfied or dissatisfied
  - Dissatisfied

- 1.12.06 Is your agency using a .gov domain for email addresses and your agency's website?
- Yes
  - In progress
  - In planning or on roadmap
  - No

New

- 1.12.07 Has your agency implemented a software-defined network?
- Yes
  - In progress
  - In planning
  - No

## Section 1.13 – Data Management and Privacy Practices

### Data Management

- 1.13.01 Does your agency have an employee whose duty is to establish the overall strategy for managing agency data (e.g. Chief Data Officer or designated Data Management Officer)?
- Yes
  - No, but plan to (If selected, skip question 1.13.01a as it is not applicable.)
  - No (If selected, skip 1.13.01a as it is not applicable.)

---

**Coordinate with your agency's Data Management Officers and Privacy Officers when completing Section 1.13.**

**For data management information, see [DIR's Office of the Chief Data Officer webpage](#).**

---

- 1.13.01a Are the data management officer duties the individual's primary or secondary duty?
- Primary duty
  - Secondary duty



- 1.13.02 Does your agency have a data governance program to manage and govern agency data assets?
- Yes
  - In planning
  - No
- 1.13.03 Does your agency have a data management program that oversees the data life cycle including the collection, classification, use, and disposal of agency data?
- Yes
  - In planning
  - No
- 1.13.04 What are the greatest barriers your agency faces in implementing a data governance program? (Select three.)
- Lack of dedicated personnel
  - Lack of executive engagement
  - Lack of qualified staff
  - Competing priorities
  - Lack of perceived interest
  - Resistance from data owners
  - Poor data quality/integrity
  - Other, write in <enter text>
- 1.13.05 Is your agency currently sharing data with another governmental entity?
- Yes
  - In planning (If selected, skip 1.13.05a as it is not applicable.)
  - No (If selected, skip 1.13.05a as it is not applicable.)

### New

- 1.13.05a List the types of data and government entities with which your agency currently shares data.
- Write in <enter text for data type and government entity>
- 1.13.06 Does your agency have a business intelligence or analytics platform?
- Agency is highly invested and has substantial capabilities
  - Agency has some capabilities
  - Agency is investigating solutions
  - Agency is not investigating solutions



# Information Resources Deployment Review

## 2024 Instructions

- 1.13.07 How many public information requests did your agency resolve by directing the requestor to access publicly accessible electronic data or the Texas Open Data Portal?
- <Enter a number>
- 1.13.08 Has your agency established data-driven policy goals?
- Yes
  - In planning
  - No
- 1.13.09 Has your agency conducted a data maturity assessment of its data governance program?
- Yes
  - In planning
  - No, as we currently do not have a designated Data Management Officer
  - No, as we need assistance to complete it
  - No, other reason, write in <enter text>

### Privacy Practices

New

- 1.13.10 Which of the following types of personal information does your agency collect from or about constituents? (Select all that apply.)
- Contact information (including phone numbers, email addresses, and mailing addresses)
  - Financial, billing, or account information
  - Social security numbers
  - Driver's license numbers
  - Dates of birth
  - Medical information
  - Education information
  - Criminal history information
  - Geolocation data
  - Facial recognition or biometric information
  - Our agency does not collect any personal information about constituents
  - Other, write in <enter text>

New

- 1.13.11 Does your agency dedicate resources to privacy and the protection of personal information?
- Yes, our agency has a designated employee(s) to set policy and address privacy matters for the agency, and privacy is their primary function

- Yes, our agency has at least one employee with some privacy expertise who is authorized to address policies and questions related to privacy, but privacy is not their primary function
- No, our agency has no dedicated internal staff with privacy expertise, but we use outside resources when necessary
- No, our agency has no dedicated privacy resources
- Other, write in <enter text>

New

- 1.13.12 Does your agency offer privacy-specific training to employees?
- No, we do not offer any employee training specific to privacy.
  - Yes, we offer voluntary privacy training for employees who choose to participate.
  - Yes, we provide mandatory privacy training for all employees.

New

- 1.13.13 Does your agency have a policy that requires employees to report potential breaches or inadvertent releases of sensitive personal information?
- Yes
  - In planning
  - No

New

- 1.13.14 Does your agency have established procedures for identifying, responding to, and reporting a data breach that involves sensitive personal information?
- Yes
  - In planning
  - No

## Section 1.14 – Training and Planning

- 1.14.01 Which of the following topics are of interest to your agency for training or learning and collaboration opportunities? (Select all that apply.)
- Accessibility Scanning Program
  - Application Portfolio Management
  - Artificial Intelligence
  - Business Intelligence
  - Cloud Services
  - Cooperative Contracts Program
  - Cybersecurity
  - Data Management
  - Data Visualization
  - Digital Accessibility
  - Digital Transformation and Modernization





# Information Resources Deployment Review

## 2024 Instructions

- Distributed ledger technology (includes blockchain)
- Innovative Procurement Lab
- IT Workforce Development (e.g. Skills-based Training, Building Partnerships for Technology Workforce)
- Legislative Appropriations Request (LAR) and Technology Funding
- Prioritization of Cybersecurity and Legacy Systems
- Process Automation
- Shared Technology Services (includes Data Center Services)
- Statements of Work for Technology Purchases
- Texas Open/Closed Data Portal
- Texas Project Delivery Framework
- Strategic Planning for Information Resources Management
- Other, write in <enter text>

### New

- 1.14.02 Which training or learning and collaboration formats are most valuable to your agency's employees? (Select all that apply.)
- Centers of Excellence
  - Conferences
  - In-person format
  - Hybrid format (in-person with online delivery option)
  - On-demand format (pre-recorded or learn at your own pace)
  - Virtual/online format
  - Workshops
  - Webinars
  - Workgroups or user groups with frequent interaction
  - Other, write in <enter text>

### Section 1.15 – Optional Comments on Agency IT Environment

- 1.15.01 OPTIONAL. Enter any comments related to your agency environment sections listed in Part 1. Please include the IRDR question number(s) for reference.
- <text>

## Part 2: Compliance with State Standards

For each requirement, choose the answer that best represents your agency's current compliance status. In most cases, the two allowed answers are:

- **In compliance.** Your agency has fully implemented the requirement.
- **Not in compliance.** Your agency has not fully implemented the requirement as of the IRDR deadline (March 31, 2024). Your agency may be actively working toward compliance, but you should report the status as of March 31, 2024. You have the opportunity to provide an explanation of why your agency may not be in compliance when you complete the IRCAP for each instance of noncompliance.

### Section 2.01 – Security

- 2.01.01 Each agency must annually review and approve their security program for compliance with the 1 TAC Chapter 202 Information Security Standards.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 202.20\(7\), 202.70\(7\).](#)

- 2.01.02 Each agency must conduct a biennial security risk assessment.
- In compliance
  - Not in compliance

[Government Code Section 2054.515; 1 Texas Administrative Code Sections 202.23\(c\), 202.73\(c\).](#)

- 2.01.03 The information security officer or designee is responsible for approving security risk acceptance, transference, or mitigation decision(s) in coordination with the information owner for systems identified with a Low or Moderate residual risk and the state agency head for all systems identified with residual High Risk.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 202.25, 202.75.](#)

- 2.01.04 All authorized users of agency information resources must be required to formally acknowledge that they will comply with security policies and procedures before they are granted access to information systems.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 202.22\(a\)\(3\)\(C\), 202.72\(a\)\(3\)\(C\).](#)

- 2.01.05 Each agency must use the network security services provided through DIR's Network Security Operations Center (NSOC) unless the department determines that the agency's requirement for network security services cannot be met at a comparable cost through the center.
- In compliance
  - Not in compliance

[Government Code Sections 2059.102\(c\), 2059.102\(d\).](#)

- 2.01.06 Each agency must remove restricted personal information from any associated storage device before selling or transferring data processing equipment to a person who is not a state agency or other agent of the state.
- In compliance
  - Not in compliance

[Government Code Section 2054.130, 1 Texas Administrative Code Sections 202.26\(a\), 202.76\(a\).](#)

- 2.01.07 Each agency must designate an information security officer that (1) reports to executive-level management; (2) has authority on information security for the entire agency; (3) possesses the training and experience required to perform the duties required by DIR rules; and (4) to the extent possible, has information security duties as that officer's primary duty.
- In compliance
  - Not in compliance

[Government Code Section 2054.136, 1 Texas Administrative Code Sections 202.21, 202.71.](#)

New

- 2.01.08 Each agency must develop a data use agreement, update that agreement at least biennially, and obtain signatures to the agreement from agency employees who handle sensitive information, including financial, medical, personnel, or student data.
- In compliance
  - Not in compliance

[Government Code Section 2054.135.](#)

New

- 2.01.09 Each agency must classify the data produced from or used in all information resources technology projects, including application development projects, to determine appropriate data security and applicable retention requirements upon initiating an information resources project.
- In compliance
  - Not in compliance

[Government Code Section 2054.161.](#)

## Section 2.02 – State Websites

- 2.02.01 Each agency must comply with all state website accessibility standards and provisions.
- In compliance
  - Not in compliance
- [1 Texas Administrative Code Sections 206.50\(e\), 206.70\(e\)](#)
- 2.02.02 Each agency must meet the minimum requirements for publishing a privacy notice on its homepage and on key public entry points, or its site policy page.
- In compliance
  - Not in compliance
- [Government Code Section 559.003, 1 Texas Administrative Code Sections 206.52, 206.72](#)
- 2.02.03 Each agency that has a website requiring a user to share personal identifying information must conduct a transaction risk assessment and implement appropriate privacy and security safeguards prior to providing access to information services on the site.
- In compliance
  - Not in compliance
  - No part of the agency's website requires a user to share personal identifying information
- [1 Texas Administrative Code Sections 206.52\(d\), 206.72\(d\)](#)
- 2.02.04 Each agency with a web page containing a form that collects information about an individual, their computer network location, or their identity must have a link to the agency's associated privacy notice.
- In compliance
  - Not in compliance
  - No forms on the agency's website request personal information from the public
- [Effective April 18, 2020, webpages must comply with the standards referenced in US Section 508 Chapter 7 Section 702.10 of the Workforce Rehabilitation Act \(Web Content Accessibility Guidelines 2.0 or higher\).](#)
- [Texas Administrative Code 206 established April 2020 as the date for compliance with the new standards.](#)
- [IHEs must complete Section 2.02.](#)

[Government Code Section 559.003](#), [1 Texas Administrative Code Sections 206.52\(e\)](#), [206.72\(e\)](#)

2.02.05 Each agency must comply with requirements related to linking to, using, or copying information from agency websites and protecting the personal information of the public who access agency information through agency websites.

- In compliance
- Not in compliance

[1 Texas Administrative Code Sections 206.53\(a\)](#), [206.73\(a\)](#)

2.02.06 Each agency must meet the minimum requirements for publishing a linking notice on its homepage and on key public entry points<sup>9</sup> or its site policy page.

- In compliance
- Not in compliance

[1 Texas Administrative Code Sections 206.53](#), [206.73](#)

2.02.07 A state agency that posts a high-value data set on its website shall provide DIR with information needed to post a link to the high-value dataset on Texas.gov.

- In compliance
- Not in compliance
- The agency has no high-value datasets to post
- The agency is in the process of providing the required information to DIR

[1 Texas Administrative Code Sections 206.55](#), [206.75](#)

2.02.08 Each agency must comply with suggestions for agency cost savings provisions.

- In compliance
- Not in compliance
- Exempt (IHEs only)
- Exempt (Agency has fewer than 1,500 employees)

[1 Texas Administrative Code Section 206.56](#)

2.02.09 Each agency must display a link to the Texas Veterans Portal on the agency's homepage.

- Yes

---

<sup>9</sup> See glossary for definition of key public entry point.

- Yes, but not on the homepage
- No

Office of the Governor, 2016 Directive

### Section 2.03 – Electronic and Information Resources Accessibility

- 2.03.01 Each agency must comply with all listed accessibility standards for products and services. **IHEs must complete Section 2.03.**
- In compliance, without the use of accessibility exceptions
  - In compliance, with one or more accessibility exceptions approved by the agency head
  - Not in compliance

1 Texas Administrative Code Sections 213.10-213.16, 213.30-213.36

- 2.03.02 Each agency must comply with all accessibility compliance exceptions and exemptions provisions.
- In compliance
  - Not in compliance

1 Texas Administrative Code Sections 213.17(1)-(5), 213.37(1)-(5)

- 2.03.03 Each agency must comply with accessibility procurement provisions.
- In compliance
  - Not in compliance

1 Texas Administrative Code Sections 213.18(b)-(g), 213.38(b)-(g)

- 2.03.04 Each agency must comply with accessibility training and technical assistance provisions.
- In compliance
  - Not in compliance

1 Texas Administrative Code Sections 213.19(b), 213.39(b)

- 2.03.05 Each agency must complete the accessibility survey<sup>10</sup> and support its responses with agency documentation by the deadline established by DIR.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 213.20\(b\), 213.40\(b\)](#)

- 2.03.06 Each agency must comply with all EIR accessibility policy and coordinators provisions.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 213.21\(b\)-\(f\), 213.41\(b\)-\(f\)](#)

## Section 2.04 – Geographic Information Systems

- 2.04.01 If the agency originates or adds content to a digital geospatial dataset and distributes it to other agencies or the public, it must offer the dataset in at least one format that is readily usable by a variety of GIS software packages.
- In compliance
  - Not in compliance
  - No geospatial datasets are distributed by the agency

[1 Texas Administrative Code Chapter 205](#)

- 2.04.02 If the agency acquires a federal or other public domain geospatial dataset, it must make it available to other agencies and the public via the agency's website and/or the Texas Natural Resources Information System.
- In compliance
  - Not in compliance
  - No public domain geospatial datasets are acquired by the agency

[1 Texas Administrative Code Chapter 205](#)

- 2.04.03 If the agency originates or adds content to a digital geospatial dataset and distributes it to other agencies or the public, it must prepare and distribute standardized metadata documentation for each dataset.

---

<sup>10</sup> A completed submission of the Accessibility Components of the Information Resources Deployment Review satisfies the reporting requirement provision for state agencies and institutions of higher education.

- In compliance
- Not in compliance
- No geospatial datasets are distributed by the agency

[1 Texas Administrative Code Chapter 205](#)

## Section 2.05 – Electronic Records Management

- 2.05.01 Each agency must meet the minimum requirements for the policies and procedures for the management of electronic state records.
- In compliance
  - Not in compliance
  - The agency has no state records in electronic form and therefore requires no policies under this section

[13 Texas Administrative Code Section 6.93](#)

- 2.05.02 Each agency must meet the minimum requirements for the management of all electronic state records.
- In compliance
  - Not in compliance
  - The agency has no state records in electronic form

[13 Texas Administrative Code Section 6.94](#)

- 2.05.03 Each agency must meet the additional record requirements for archival, permanent, and vital electronic state records.
- In compliance
  - Not in compliance
  - The agency has no archival, permanent, or vital electronic state records

[13 Texas Administrative Code Section 6.95](#)

- 2.05.04 Each agency must meet the minimum requirements for the final disposition of all electronic state records.
- In compliance
  - Not in compliance
  - The agency has no electronic records for disposition

[13 Texas Administrative Code Section 6.97](#)

- 2.05.05 Each agency must meet the minimum requirements for the management of all electronic transactions and signed records.



- In compliance
- Not in compliance
- The agency has no electronic transactions or electronically signed records to manage

[13 Texas Administrative Code Section 6.98](#)

- 2.05.06 Each agency must properly preserve electronic records in its custody that are archival state records or that need archival review.
- In compliance
  - Not in compliance
  - No electronic state records in its custody that are archival state records or that need archival review

[Government Code Sections 441.186, 441.180\(2\)](#)

## Section 2.06 – Additional Standards

- 2.06.01 Each agency shall ensure that its information resources manager (IRM) is part of the agency's executive management and reports directly to the agency's executive director or deputy executive director.
- In compliance
  - Not in compliance

[Government Code Section 2054.075\(b\)](#)

- 2.06.02 Each agency's IRM shall meet or exceed the IRM continuing education requirements established by DIR.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Sections 211.11, 211.21](#)

- 2.06.03 The agency shall institute, approve, and publish an operating procedure that communicates an agency-wide approach for information technology project management practices that meets DIR's established standards.
- In compliance
  - Not in compliance
  - Not applicable as the agency has not conducted an IT project in the past two years

[1 Texas Administrative Code Sections 216.10, 216.20](#)

- 2.06.04 The agency shall satisfy all requirements of the Texas Project Delivery Framework for every major information resources project.
- In compliance
  - Not in compliance
  - Not applicable as the agency has not conducted a major information resources project in the past two years

[Government Code Subchapter J](#)

- 2.06.05 The agency shall satisfy all requirements of the Texas Project Delivery Framework for major contracts.
- In compliance
  - Not in compliance

[Government Code Subchapter J](#)

- 2.06.06 Each agency must purchase IT commodity items in accordance with the IT commodity purchasing requirements established in 1 Texas Administrative Code Chapter 212.
- In compliance
  - Not in compliance

[1 Texas Administrative Code Chapter 212](#)

- 2.06.07 A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply with statutory notification requirements in the event of a breach of system security.
- In compliance
  - Not in compliance

[Business and Commerce Code, Title 11, Section 521.053, Government Code Section 2054.603](#)

- 2.06.08 If an agency's governmental body holds an open or closed meeting by video conference call, the systems used must comply with the minimum standards.
- In compliance
  - Not in compliance
  - No governmental body meetings are held by video conference

[1 Texas Administrative Code Chapter 209](#)

New

- 2.06.09 Each state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency shall complete a cybersecurity training program certified under Section [2054.519](#).
- In compliance
  - Not in compliance

[Government Code Section 2054.5191](#)

New

- 2.06.10 A state agency shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under Section [2054.519](#) as selected by the agency.
- In compliance
  - Not in compliance

[Government Code Section 2054.5192](#)

### Part 3: State Strategic Plan for Information Resources Management

#### Section 3.01 – Alignment with 2024-2028 State Strategic Plan Technology Objectives

Questions 3.01.01-3.01.15 contain the objectives described in the [2024-2028 SSP](#).

Indicate the extent to which your agency’s initiatives are aligned with each SSP Objective.

Question Number	Objectives	Not aligned	Minor alignment	Moderate alignment	Significant alignment	Does not apply to my agency
3.01.01	Customer Experience Strategies (1.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.02	Digital Accessibility (1.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.03	Connectivity and Continuity (1.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.04	Secure Identity and Access Management (1.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.05	Data Governance (2.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.06	Data Literacy (2.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.07	Reliable Analytics (2.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.08	Data Security and Privacy (2.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.09	IT Workforce Skills (3.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.10	Talent Development (3.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.11	Resilient Teams (3.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.12	Workplace Culture (3.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.13	Organizational Readiness (4.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.14	Accelerate Modernization (4.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.01.15	Guidance for Emerging Technologies (4.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

### Section 3.02 – Progress Toward 2022-2026 State Strategic Plan Technology Objectives

Questions 3.02.01-3.02.16 contain the objectives described in the [2022-2026 SSP](#). Indicate the level of overall progress your agency has made toward each SSP Objective.

Question Number	Objectives	No progress	Minor progress	Moderate progress	Significant progress	Optimized/fully adopted	Does not apply
3.02.01	Risk-based Security Practices (1.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.02	Cybersecurity Education and Training (1.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.03	Regional Cybersecurity Engagement and Response (1.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.04	Cost-Effective Cybersecurity Tools (1.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.05	Data Governance (2.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.06	Data Security and Privacy (2.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.07	Data Analytics (2.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.08	Open Data (2.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.09	Strategic Roadmap (3.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.10	Digital Maturity (3.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.11	Human-Centered Applications (3.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.12	Mobile Applications (3.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.13	Legacy Modernization (4.1)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.14	Flexible and Adaptable Approaches (4.2)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.15	Emerging Technologies (4.3)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.02.16	Adaptable Workforce (4.4)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



### Part 4: IT Inventory

#### Overview

Part 4: IT Inventory provides guidance to IRMs for the review and update of the required inventory<sup>11</sup> (broken into devices inventory and applications inventory in SPECTRIM) of their agency's IR assets. DIR uses the information from this inventory to complete legislatively mandated reports,<sup>12</sup> that provide a statewide perspective of information technology infrastructure and associated business applications used by state agencies.

**Part 4 does not apply to IHEs.**

DIR prepopulates some inventory fields with the most recent data from previous IRDRs. For agencies participating in the statewide data center, DIR linked (through an applications programming interface or API) the devices inventory in ServiceNow to SPECTRIM. The API updates the IRDR devices inventory daily to synchronize it with the ServiceNow devices inventory. It does not update the IRDR applications inventory. You must carefully review and update both the devices and applications inventories to ensure that they are accurate and complete.

#### Sensitive Inventory Data

DIR complies with the Texas Public Information Act<sup>13</sup> for all public information requests. Due to the inherently sensitive nature of information related to computer network security, DIR treats the inventory information collected through the IRDR as confidential. DIR will request a decision from the Office of the Attorney General for all public information requests seeking IRDR inventory information. As you complete your agency's IRDR inventory, please exclude all potentially system-compromising information from your written communications with DIR.

#### Guidance for Completing the Inventory

DIR is required to collect information on the status and condition of each state agency's information technology infrastructure, including agency servers, mainframes, major databases, and cloud services.<sup>14</sup> In addition, each agency's IRDR must include an inventory of major information systems, applications, managed infrastructure, and other IT equipment. This inventory is collected in the devices and applications inventories in SPECTRIM, except the managed infrastructure inventory, which is captured in Part 1: Agency IT Environment.

---

<sup>11</sup> See Government Code Sections [2054.068](#) and [2054.0965](#).

<sup>12</sup> See Government Code Sections [2054.068\(d\)](#) and [2054.069](#).

<sup>13</sup> See Government Code Chapter [552](#).

<sup>14</sup> See Government Code Sections [2054.069\(b\)](#).

### Devices Inventory

You must review and update your agency's IT assets<sup>15</sup> in the devices inventory, add any new IT assets, and indicate the asset's status as active, retired, or a duplicate. For agencies participating in the statewide data center, an API updates the IT assets in the IRDR devices inventory in SPECTRIM daily with data from the ServiceNow device inventory. State law requires<sup>16</sup> agencies to report on agency servers, mainframes, and other IT equipment in the devices inventory. Reporting on other IT assets is optional.

### Applications Inventory

Identifying the connection between your agency's business applications<sup>17</sup> and IT assets provides insight into your agency's security posture and the potential impacts of infrastructure changes on critical applications. The applications inventory in SPECTRIM is a repository of your agency's business applications and includes cloud services. Examples of business applications include payment intake systems and customer information systems.

You must review and update your agency's list of business applications, add any new ones, and verify the accuracy of the information included about each application. You also have the opportunity to complete an Application Portfolio Management (APM) assessment of each application.

Agencies must have a current<sup>18</sup> APM assessment in SPECTRIM for each business application impacted by their planned Prioritization of Cybersecurity and Legacy System (PCLS) projects. As you complete your agency's IRDR applications inventory, please carefully review each application's assessment date in SPECTRIM and consider whether you need to generate a new assessment. Visit DIR's [PCLS Projects webpage](#) for more information on the PCLS projects prioritization process.

### Inventory Attestation and IRDR Submission

Once you review and update the devices and applications inventory, you must attest that each inventory is complete. After completing all four parts of the IRDR, you will need to change the submission status in SPECTRIM from "in-progress" to "submitted."

---

<sup>15</sup> IT assets include, but are not limited to, audio and video equipment, databases, firewalls, hardware, load balancers, mainframes, network storage devices, printers, routers, security devices, servers, storage servers, switches, workstations, and other network assets.

<sup>16</sup> See Government Code Section [2054.069\(b\)](#).

<sup>17</sup> For the purposes of the IRDR inventory, the term "business applications" refers to the solutions, services, and software an organization uses to accomplish specific business functions or operations. They may include integrated hardware, software, data, and applications. They may be developed or customized internally or by a third party.

<sup>18</sup> A current assessment has a "most recent AMP assessment start date" of January 1, 2020, or later.



### Acronym List

<b>ACH</b>	Automated Clearinghouse
<b>AI</b>	Artificial Intelligence
<b>AIS</b>	Automated Information Systems
<b>APM</b>	Application Portfolio Management
<b>AWA</b>	Alternative Workplace Arrangements
<b>CJIS</b>	Criminal Justice Information Services
<b>COOP</b>	Continuity of Operations Plan
<b>COTS</b>	Commercial Off-The-Shelf
<b>CRM</b>	Customer Relationship Management
<b>CTO</b>	Chief Technology Officer
<b>CXO</b>	Chief Experience Officer
<b>DevOps</b>	Development and Operations
<b>DMO</b>	Data Management Officer
<b>ECM</b>	Enterprise Content Management
<b>EDR</b>	Endpoint Detection and Response
<b>EIR</b>	Electronic and Information Resources
<b>FERPA</b>	Family Educational Rights and Privacy Act
<b>GIS</b>	Geographic Information System
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>IaaS</b>	Infrastructure-as-a-Service
<b>IHE</b>	Institution of Higher Education
<b>IPv6</b>	Internet Protocol Version 6
<b>IR</b>	Information Resources
<b>IRM</b>	Information Resources Manager
<b>ISO</b>	Information Security Officer
<b>IT</b>	Information Technology
<b>LMS</b>	Learning Management System
<b>NASCIO</b>	National Association of State Chief Information Officers
<b>NIST</b>	National Institute of Standards and Technology
<b>NSOC</b>	Network Security Operations Center



# Information Resources Deployment Review 2024 Instructions

<b>PaaS</b>	Platform-as-a-Service
<b>QAT</b>	Quality Assurance Team
<b>RMO</b>	Records Management Officer
<b>SaaS</b>	Software-as-a-Service
<b>SPECTRIM</b>	Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management
<b>SME</b>	Subject Matter Expert
<b>TAC</b>	Texas Administrative Code
<b>TEX-AN</b>	Texas Agency Network
<b>TDA</b>	Texas Digital Archive
<b>TBT</b>	Technology-Based Training
<b>TPDF</b>	Texas Project Delivery Framework
<b>TX-RAMP</b>	Texas Risk and Authorization Management Program
<b>WCAG</b>	Web Content Accessibility Guidelines



### Glossary

#### Accessibility Exceptions

Specific situations where individuals or organizations are granted continued support by fellow agencies, despite being unable to comply with Accessibility Guidelines.

#### Agile Contracting

Collaboration between supplier and customer or working together in partnership.

#### Alternative Workplace Arrangements

Combine non-traditional work practices, settings/locations, or technologies to achieve workplace progress.

#### Application Portfolio Management

A framework for managing enterprise IT software applications and software-based services. APM provides managers with an inventory of the company's software applications and metrics to illustrate the business benefits of each application.

#### Apprenticeships

An arrangement in which someone learns an art, trade, or job under another.

#### Archival State Record

A state record of enduring value that will be preserved on a continuing basis by the Texas State Library and Archives Commission or another state agency until the state archivist indicates that based on a reappraisal of the record it no longer merits further retention.

#### Artificial Intelligence

Artificial Intelligence (AI) is using computers to apply advanced analysis and logic-based techniques to interpret events, support and automate decisions, and to take actions. AI includes chat bots, machine learning, and robotics process automation.

#### Automated Clearinghouse

System that agencies use for electronic funds transfer. With ACH, funds are electronically deposited in financial institutions, and payments are made online.

#### Automated Information Systems

Computers and devices on which an information system is automated, a service related to automating information systems, including computer software or hardware, or a telecommunications apparatus or device that serves as a component of voice, data, or video communications network for transmitting switching, routing, multiplexing, modulating, amplifying, or receiving signals on the network and other telecommunications related services.



### Blockchain

An expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network, containing time stamps and reference links to previous transactions. With this information, anyone with access rights can trace back a transactional event, at any point in its history, belonging to any participant.

### Board

A group of people having managerial, supervisory, investigatory, or advisory powers.

### Broadband

Channels that have a wider bandwidth than conventional telephone lines, giving them the ability to carry video, voice, and data simultaneously.

### Business Application

High-level labels used by the agency business and IT organizations to easily reference a group of functions provided by one or more systems. These Business Applications are typically a combination of integrated custom applications, COTS applications and/or engineered systems.

### Checksum

A value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions.

### Cloud

A shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

### Cloud Strategy

A strategic document outlining a concise point of view on the cloud's role within an organization that is business driven, aligns with strategic plans, and provides principles for decisions about cloud computing.

### Commodity Items (Technology)

Commercially available hardware, software, and technology services that are generally available to businesses or the public.

### Connectivity

Ability to interconnect platforms and systems including enterprise networking, broadband, 5G services, and enhanced internet services.



# Information Resources Deployment Review

## 2024 Instructions

### Content Management

Consists of technologies used to capture, manage, store, preserve, and deliver content such as images, office documents, graphics, drawings, print streams, Web pages, e-mail, video, and rich media assets.

### Continuity

Preparing for continued government operations during and after a disruption or an emergency, including the preparation, testing, and refinement of business continuity plans and disaster recovery tools.

### Cooperative Contracts Program

In accordance with Government Code Section 2157.068, and 1 Texas Administrative Code Chapter 212, each state agency must purchase technology commodity items through contracts established by DIR unless the agency first obtains an exemption.

### Customer Experience Strategy

A strategic document that outlines an organization's understanding of its customers and the roles, responsibilities, resources, and metrics that will enable a customer-centric culture; for digital government, includes strategies that consider a customer's perceptions and feelings toward an organization based on the sum of all digital experiences that the organization provides.

### Cybersecurity

Securing and protecting government and citizen information.

### Data Analytics Solutions

Technologies for using data to inform planning, provide business intelligence, and enhance decision making; includes predictive, prescriptive, and operationalized analytics.

### Data Governance

The exercise of authority and control over the management of data assets. Data governance guides all other data management functions and includes management of the data lifecycle, data classification and security, and establishing roles such as data officers.

### Data Literacy

The ability to read, write and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied, and the ability to describe the use-case application and resulting value.

### Data Management Tools

Technologies for data management strategies that place organizations in control of their business data; includes the practice of classifying, storing, and terminating data.

### Data Quality

The state of data (including accuracy, completeness, consistency, timeliness, relevance, and validity) that is fit for its intended use in operations, decisions, and planning.

### DevOps

An enterprise software development phrase, short for Development and Operations, used to mean a type of agile relationship between development and IT operations. The goal of DevOps is to change and improve the relationship by advocating better communication and collaboration between these two business units.

### Digital Accessibility

Digital services providing electronic information and services through multiple ways so that communication is not contingent on a single sense or ability.

### Digital Data

Data that has been converted into binary code and is readable by machinery.

### Digital Transformation

A strategic approach to the adoption of digital technologies to create new or improve existing processes, services, and customer experiences; includes simple digitization projects such as moving from traditional, paper-based processes to electronic or online formats as well as transition to mobile applications and cloud-solutions.

### Disaster Recovery

The use of alternative network circuits to re-establish communications channels if primary channels are disconnected or malfunctioning, and the methods and procedures for returning a data center to full operation after a catastrophic interruption.

### Disposition

Final processing of state records by either destruction or archival preservation by the Texas State Library and Archives Commission, by a state agency, or by an alternate archival institution as permitted by Government Code, Chapter 441, Subchapter L.

### Distributed Ledger

A database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people.

### Edge Computing

A computing environment in which information processing, content collection, and delivery are placed closer to the sources and repositories of this information.

### EIR Accessibility Coordinator

An agency staff member who acts on behalf of the agency in matters relating to accessibility as

defined in Government Code Chapter 2054 and 1 TAC Sections 206 and 213.

### **Electronic and Information Resources**

Any equipment or interconnected system of equipment that is used in the creation, conversion, or duplication of information resources. The term includes telephones and other telecommunications products, information kiosks, transaction machines, Internet websites, multimedia resources, and office equipment, including copy machines and fax machines.

### **Endpoint Detection and Response**

An endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats, like ransomware and malware.

### **Enterprise**

An organization that coordinates the operation of one or more processing sites.

### **Enterprise Content Management**

Used to create, store, distribute, discover, archive and manage unstructured content (such as scanned documents, email, reports, medical images and office documents) and ultimately analyze usage to enable organizations to deliver relevant content to users where and when they need it.

### **Enterprise Customer Relationship Management**

A business strategy that optimizes revenue and profitability while promoting customer satisfaction and loyalty. CRM technologies enable strategy, and identify and manage customer relationships, in person or virtually. CRM software provides functionality to companies in four segments: sales, marketing, customer service and digital commerce.

### **Generative AI**

Expands the output of AI systems to include high-value artifacts such as video, narrative, software code, synthetic data through to designs and schematics.

### **Geographic Information System**

A computer system for capturing, storing, checking, and displaying data related to positions on Earth's surface.

### **Governance**

Overseeing the control and direction of something (such as a country or an organization).

### **High-Impact Information Resources**

Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

### High-Value Dataset

Information that can be used to increase state agency accountability and responsiveness, improve public knowledge of the agency and its operations, further the core mission of the agency, create economic opportunity, or respond to need and demand as identified through public consultation. The term does not include information that is confidential or protected from disclosure under state or federal law.

### Identity and Access Management

A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.

### Information Resources

Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

### Information Resources Manager

The IRM oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and in compliance with regulations and agency policies. The IRM position was created by the Legislature (Government Code Chapter 2054).

### Information Security Officer

Responsible executive management for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.

### Information Technology

The entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.

### Infrastructure

Interconnecting physical and virtual technologies such as computing, storage, network, applications to build the foundation for a company's digital operations.

### Infrastructure-as-a-Service

A standardized, highly automated offering in which computing resources owned by a service provider, complemented by storage and networking capabilities, are offered to customers on demand.

### Internet Protocol Version 6

IPv6, the next-generation protocol, ensures availability of new IP addresses far into the future, as

well as promoting the continued expansion and innovation of Internet technology.

### **Internships**

The position of a student or trainee who works in an organization, sometimes without pay, in order to gain work experience or satisfy requirements for a qualification.

### **Interoperability**

When different services can operate effectively and accept services from other systems.

### **IT Workforce Development**

Recruiting and retaining a fully trained and qualified technology workforce.

### **Key Public Entry Point**

A web page specifically designed for members of the public to access official information (e.g., the governing or authoritative documents) from the agency or institution of higher education.

### **Learning Management System**

A software application or web-based technology used to plan, implement and assess a specific learning process.

### **Legacy System**

A computer system or application program that is operated with obsolete or inefficient hardware or software technology.

### **Local Area Network**

A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.

### **Mainframe**

A mainframe is a large-capacity computer system with processing power that is significantly superior to PCs or midrange computers.

### **Major Information Resources Project**

As defined in Government Code Chapter 2054, any information resources technology project identified in a state agency's biennial operating plan with development costs that exceed \$5 million and that requires one year or longer to reach operations status; involves more than one state agency; or substantially alters work methods of state agency personnel or the delivery of services to clients; and any information resources technology project designated by the legislature in the General Appropriations Act, as a major information resources project.

### **Microservices**

A service-oriented application component that is tightly scoped, strongly encapsulated, loosely coupled, independently deployable and independently scalable.



### Multifactor Authentication

A characteristic of an authentication system or an authenticator that requires more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

### National Institute of Standards and Technology

A unit of the U.S. Commerce Department, formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

### Network Security Operations Center

HB3112 (79<sup>th</sup> Texas Legislature) authorizes DIR to establish NSOC on a cost-recovery basis to manage and deliver network security system services to state agencies.

### Open Data

Providing public access to data in standardized and easily usable formats.

### Operating System

Software designed to control the hardware of a specific data-processing system to allow users and application programs to make use of it.

### Paperless Processes

Minimizes use of physical paper in favor of digital documents. Instead of storing documents in file cabinets, they're stored on computers and in the cloud.

### Platform-as-a-Service

A type of cloud offering that delivers application infrastructure (middleware) capabilities as a service.

### Public Cloud

Cloud resources that are not part of the state's two consolidated data centers.

### Privacy Practices

The procedural safeguards providers must implement and adhere to in order to safeguard personally identifiable information and to ensure program participants are advised of their rights.

### Project

An initiative that provides information resources technologies and creates products, services, or results within or among elements of a state agency; and is characterized by well-defined parameters, specific objectives, common benefits, planned activities, a scheduled completion

date, and an established budget with a specified source of funding.

### **Project Management**

A system of procedures, practices, and technologies that provides the planning, organizing, staffing, directing, and controlling necessary to successfully manage a project.

### **Project Management Practices**

Documented and repeatable activities through which a state agency applies knowledge, skills, tools, and techniques to satisfy project activity requirements. Includes practices such as project management methodologies, system development life cycle, program and portfolio management, and the use of automated tools to support the practices.

### **Quality Assurance**

Any systematic process used to determine if a product or service meets quality standards.

### **Quality Assurance Team**

Composed of representatives from DIR, the Legislative Budget Board, and the State Auditor's Office. The Team is responsible for reviewing, approving, and overseeing major information resources projects.

### **Records Management Officer**

The agency head or the person appointed by the agency head to act as the state agency's representative in all issues of records management policy, responsibility, and statutory compliance pursuant to Government Code Section §441.184.

### **Records Management Program**

The program of a state agency undertaken on a continuing and active basis (i.e. not a project) to apply management techniques to the creation, use, maintenance, retention, preservation, and destruction of state records as required by Texas Government Code §441.183.

### **Records Retention Schedule**

A document prepared in accordance with §6.2 of this title (relating to Submission of Records Retention Schedules for Certification).

### **Retention Period**

The period during which state records must be maintained before final disposition.

### **Remote Working Solutions**

A flexible work arrangement in which an employee, under a written remote work agreement, is scheduled to perform work at an alternative worksite and is not expected to perform work at an agency worksite on a regular and recurring basis.

### Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

### Robotics Process Automation

A productivity tool that allows a user to configure one or more scripts (sometimes referred to as “bots”) to activate specific keystrokes in an automated fashion.

### Scalability

The measure of a system’s ability to increase or decrease in performance and cost in response to changes in application and system processing demands.

### Server

Any computer that provides shared processing or resources (e.g., application processing, database, mail, proxy, firewalls, backup capabilities, print, and fax services) to authorized users or other computers over the network. A server includes associated peripherals (e.g., local storage devices, attachments to centralized storage, monitor, keyboard, pointing device, tape drives, and external disk arrays) and is identified by a unique manufacturer’s serial number.

### Server Instance

A collection of SQL Server databases run by a solitary SQL Server service or instance. The details of each server instance can be viewed on the service console which can be web-based or command-line based.

### Shared Technology Services

IT infrastructure, applications, and services shared within and among organizations to gain economies of scale and enable access to the managed technologies needed to support organizational missions and customer experience; refers to shared services in general, not DIR’s shared services program.

### Software-as-a-Service

Software that is owned, delivered, and managed remotely by one or more providers. The provider delivers software based on one set of common code and data definitions that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics.

### Stakeholder

A person, group or organization with a vested interest, or stake, in the decision-making and activities of a business, organization or project.

### Standard

Provide guidance and instruction on how goods and services are to be designed, constructed,

manufactured, handled, conducted, or tested.

### State Record

Any written, photographic, machine-readable, or other recorded information created or received by or on behalf of a state agency or an elected state official that documents activities in the conduct of state business or use of public resources. The term does not include library or museum material made or acquired and preserved solely for reference or exhibition purposes; an extra copy of recorded information preserved only for reference; a stock of publications or blank forms; or any records, correspondence, notes, memoranda, or other documents, other than a final written agreement described by §2009.054(c), associated with a matter conducted under an alternative dispute resolution procedure in which personnel of a state department or institution, local government, special district, or other political subdivision of the state participated as a party, facilitated as an impartial third party, or facilitated as the administrator of a dispute resolution system or organization.

### Strategic Plan

A roadmap for how an organization wants to direct its resources to achieve a defined vision.

### Technology-Based Training

An instructional method that employs technology to deliver content and facilitate learning.

### Telecommunications

The means of electronic transmission of information over distances.

### Telephony

Interactive communication between two or more physically distant parties via the electronic transmission of data.

### Texas Administrative Code

A compilation of all state agency rules in Texas. There are 16 titles, each representing a subject category and related agencies are assigned to the appropriate title.

### Texas Digital Archive

Manages, preserves, and facilitates access to the electronic archival state records collections of the Texas State Library and Archives Commission, including those transferred by State agencies or digitized by the State Archives.

### Texas Project Delivery Framework

The Texas Project Delivery Framework (Framework) establishes a consistent, statewide method for project selection, control, and evaluation based on alignment with business goals and objectives. The Framework consists of five review gates with guidance and tools for each of the gates.



### Unified Communications

Products including equipment, software, and services that provide and combine multiple communications channels such as voice, video, personal and team messaging, voicemail, and content sharing.

### Virtual Server

A server that shares hardware and software resources with other operating systems.

### Virtualization

The simulation of the software and/or hardware upon which other software runs.

### Wide Area Network

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN.

### Workflow

The sequence of steps involved in moving from the beginning to the end of a working process.

### Zero Trust

Term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.