2022 Information Resources Deployment Review Instructions

Guidance for Texas State Agencies and Institutions of Higher Education

Submission Deadline, March 31, 2022

Texas Department of Information Resources

Texas Department of Information Resources

Contents

Key Information

Background

The Information Resources Manager (IRM) of each Texas state agency and institution of higher education (IHE) is required by Texas Government Code, Section 2054.0965 to conduct an Information Resources Deployment Review (IRDR) every two years. DIR provides these instructions as guidance for this requirement. Additional information and quick links are available on DIR's website at: https://dir.texas.gov/strategic-planning-and-reporting/irdr-ir-cap.

Reporting Requirements

- **Texas State Agencies** are required by Texas Government Code, Section 2054.0967 to submit IRDR results for review by the Quality Assurance Team (QAT), which includes representatives from DIR, the Legislative Budget Board, and the State Auditor's Office. The online submission through the SPECTRIM portal constitutes a complete submission.
- **Health and Human Services Agencies** are required (Government Code, Section 531.0273(a)(3)) to have their IRDRs reviewed and approved by the Health and Human Services Commission (HHSC) prior to submission.
- **Institutions of Higher Education** (IHEs) are required by Texas Administrative Code, Section 213.40 to complete an Electronic Information Resources (EIR) Accessibility survey. The online submission of IRDR Sections 1.03, 2.02, and 2.03 through the SPECTRIM portal satisfies this reporting requirement. IHEs are exempt from reporting additional IRDR results to DIR by Texas Education Code, 51.406, but have the option to report all completed IRDR section if desired. IHEs must complete the accessibility sections in the SPECTRIM portal.

IRDR Schedule at a Glance

Action	Date
Information Resources Deployment Review (IRDR) - Preview of instructions posted on website.	December 2021
Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) open for data entry.	January 2022
STATE AGENCIES - Deadline to submit all IRDR responses (including IT inventory and application assessment).	March 31, 2022
INSTITUTIONS OF HIGHER EDUCATION - Deadline to submit the EIR accessibility survey responses.	March 31, 2022
STATE AGENCIES - Deadline to complete Information Resource Corrective Action Plans (IR-CAP) for items of non-compliance, if applicable.	May 31, 2022

IRDR Overview

Part 1: Agency Environment provides general information about the agency's information resources (IR) environment.

- There are several new questions in section 1.02 related to security that should be completed in consultation with the agency's Information Security Officer. These include questions on multifactor authentication, incident response, cybersecurity insurance, third party security, cloud security, and risk management.
- Section 1.09 has been expanded to include questions related to emerging technology.
- Section 1.15 includes questions to help DIR develop training and input opportunities for state agencies and IHEs.

Part 2: Compliance with State Standards describes the status of the agency's compliance with key IR-related statutes, rules, and standards. State agencies that are out of compliance in one or more areas are required to submit an Information Resources-Corrective Action Plan (IR-CAP) for approval by DIR. The IR-CAP will be available in the SPECTRIM portal at the time a state agency reports non-compliance. Agencies that fail to submit and obtain approval of their IR-CAPs to DIR are reported to state leadership regarding their inability to develop a plan to reach compliance. Note that if an agency has each IR-CAP approved they will not be reported in the letter.

Part 3: Alignment with State Technology Goals asks agencies about how aligned their IT initiatives are with the statewide technology goals and objectives that are outlined in the State Strategic Plan for Information Resources. Part 3 also asks agencies to identify the amount of progress made on prior statewide technology priorities.

Part 4: IT Inventory asks agencies to provide an inventory of all information resources assets.

- To ease the reporting burden, DIR will populate the fields in this module with the current inventory-related data available from the previous IRDR, the statewide data center, and other DIR sources.
- **For agencies participating in the statewide data center,** please note you may see discrepancies between ServiceNow and SPECTRIM as DIR extracts the data from ServiceNow at a point in time.
- Supplemental instructions will be provided for the inventory and the applicable portfolio management (APM) assessment.

IR-Corrective Action Plans (IR-CAP/Remediation plans)

IRDR reporting agencies are required to complete a remediation plan for each instance of non-compliance that an agency reports in Part 2 of the IRDR. The agency may complete that remediation plan immediately, or by the deadline of May 31, 2022.

General Instructions

Purpose

The IRDR provides a review of the operational aspects of each agency's IR deployment in support of the agency's mission, goals, and objectives. In addition, it illustrates how the agency's IR deployment supports the state's IR direction as described in the State Strategic Plan for Information Resources Management (SSP). Finally, the review provides confirmation by the agency of compliance with the state's IR-related statutes, rules, and standards.

Definitions

Throughout the questions in this document, all references to agencies apply to both state agencies and IHEs, unless otherwise indicated. Definitions of technical terms used in this document are provided in the glossary.

Sensitive and Confidential Information

The questions included in this document are intended to serve as both an internal review of an agency's IT environment and an overview to state leadership of the state's aggregate IT environment. Due to the inherently sensitive nature of system-level cybersecurity information, S.B. 532, 85(R) grants an exception under Chapter 552, Government Code relating to security-related confidential information provided for the purposes of the report. DIR will treat the information collected in Part 4 – IT inventory as confidential.

DIR will comply with the Texas Public Information Act for public information requests for the general content of the IRDR, excluding the IT Inventory. DIR will take the necessary steps to ensure that agencies' systems vulnerabilities are not exposed through this process.

Collection Tool

To access the SPECTRIM portal, navigate to the following URL and enter your appropriate credentials. Internet Explorer or Microsoft Edge best support the functionality of the collection tool. Each Information Resources Manager's credentials will be reactivated before deployment of the collection tool. If the IRM does not log in to the portal within 24 hours of a password reset or reactivation, the account will become inactive. If your account has become inactive, or you need a password reset, please email grc@dir.texas.gov or irdr@dir.texas.gov for assistance.

- URL: https://dir.archer.rsa.com/Default.aspx
- User Name: your agency email address

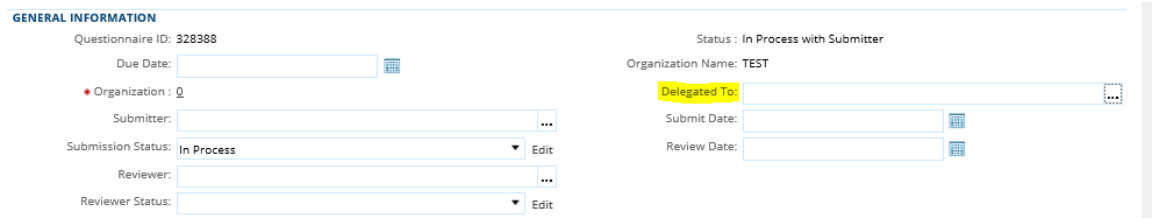
Data can be entered in multiple sessions from various computers, but not with the same user account simultaneously. Only one user will be able to edit a record at a time. All data entered is

saved in a central database and may be viewed and updated in future sessions during the reporting period.

Delegate Function: The IRM is the default owner of the IRDR submission process. However, DIR understands that there is often a need for collaboration in completing the IRDR.

IRMs may find it easier to obtain staff input by distributing this instructions document and entering responses through their account, rather than granting delegation rights to many users.

An IRM may elect to delegate responsibility to one or more individuals with the appropriate SPECTRIM credentials. It should be noted that only one user will be able to edit an IRDR record at a time. At the top of the IRDR data entry page, there is a section marked "Delegate to." To delegate to a person, select the ellipses, and then the appropriate user from the dialogue box. If the IRM wishes to delegate to someone not listed in the dialogue box, new credentials need to



be obtained for that person in SPECTRIM. To make this request, please email grc@dir.texas.gov or irdr@dir.texas.gov for assistance.

Review Function: Additionally, agencies may elect to assign a reviewer to an individual IRDR. This process follows the same steps as the "delegate to" function but will require the reviewer to change the reviewer status to "completed" before allowing the IRM to ultimately submit the IRDR.

Part 4 involves completing the IT asset inventory records within the SPECTRIM portal. Links to the inventory records will be available through the IRDR dashboard and workspace. DIR will be providing supplemental instructions on the inventory record fields, definitions, and mappings to existing data sources such as the CMDB.

DIR recommends that the agency IRM and any additional staff delegated to develop and enter IRDR responses keep this instruction document open while performing their review. **The supplemental instructions include guidance, links, and definitions that do not appear in the collection tool.**

Submission

No signature or hardcopy submission is required. Each IRM is responsible for coordinating the IRDR development and approval process within the agency using established agency practices.

Unless otherwise indicated, a response is required to each question. In some cases, an appropriate response to a question may be "None" or "Not applicable." By statute, the submission deadline for the IRDR is March 31, 2022.

Support

DIR staff is committed to providing support to agencies during the IRDR reporting period. DIR staff will strive to answer all inquiries within one business day. IRMs are encouraged to submit inquiries whenever they do not understand a question or are uncertain how to respond to it.

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

For support with the SPECTRIM portal (e.g. password resets, obtaining credentials) email grc@dir.texas.gov.

Additional Information

Throughout the instructions there are guidance statements providing background information, definitions of terms, and links to related information on the Internet. These guidance statements appear *in italics*. An extensive glossary is also provided at the end of this instruction document.

Please visit DIR's IRDR page periodically to check for any new announcements, updates, or frequently asked questions. DIR may also post information and reminders about the IRDR on the tx-irm mailing list.

Section 1.01 - Information Resources Management

1.01.01 Does your Information Resources Manager play a significant role in the following? Choose 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 the agency develop a technology roadmap/tactical plan?

○ Yes
○ In planning
○ No

1.01.03 Does the agency stream audio or video of board meetings on the internet?

○ Yes, audio only
○ Yes, video and audio
○ No, but plan to stream board meetings in the future
○ No, and no plans to stream board meetings in the future
○ The agency does not have a board

1.01.04 Does the agency plan to allow board members to virtually participate in board meetings during next biennium?

○ Yes, audio only
○ Yes, video
○ 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 board

1.01.05 For which of the following categories does the agency evaluate maturity levels? Choose all that apply.

□ Information Security
□ Data Management
□ Accessibility
□ Contracting and Procurement
□ Enterprise Architecture
□ Application Development
□ Project Management
□ Quality Management
□ Strategic Planning
□ Governance
□ Cloud
□ COOP/DR
□ Mobility
□ Identity and Access Management
□ Digital Transformation
□ Other, write in

1.01.06 Does your agency leverage managed technology infrastructure services?
○ No
○ Yes

1.01.06a Please list all vendors and briefly describe their role in managing the agency's IT infrastructure.
<enter text>

Section 1.02 - Information Security

The IRM should coordinate with the agency's Information Security Officer (ISO) in developing responses to questions in this section. For additional information, refer to DIR's Information Security page.

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 ISO report in the agency?
○ Information Resources Manager or CIO
○ Executive Director (or equivalent)
○ Other executive level position
○ Other, write in

1.02.03 How often does the Executive Director (or equivalent) sign off on high security risks?
○ Always
○ Sometimes
○ Occasionally
○ Rarely
○ Never

1.02.04 How many dedicated (100% of time or full-time) security professionals does the agency employ? Enter a number.
<number>

1.02.05 How many dedicated (100% of time or full-time) security contractor positions does the agency have/plan to have over the next biennium? Enter a number.
<number>

1.02.06 Is your combined agency staffing level sufficient for addressing your security needs?
○ Yes
○ No

1.02.06a How many dedicated (100% of time or full-time) security professionals would the agency require to adequately fulfill security program needs? Enter a number
<number>

Security Budget

1.02.07 Does the agency budget include line items for information security?
- ○ Yes
- ○ No

1.02.08 What is the agency's information security funding as a percentage of overall agency budget? Enter a percentage.
<number>

1.02.09 What is the agency's information security funding as a percentage of its overall information technology funding? Enter a percentage.
<number>

1.02.10 Characterize the biennial trending in 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

1.02.11 Does the agency budget the adequate resources and funds to be available to address the operational and financial impacts of a cybersecurity event/incident?
- ○ Yes
- ○ In planning
- ○ No

Security Practices

1.02.12 What are your agency's top five security initiatives for the biennium? Select up to five.
- □ Developing security strategy
- □ Security governance
- □ Aligning security initiatives with those of the business
- □ 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
- □ Other, write in

1.02.13 What are the largest barriers your agency faces in addressing security? Select up to three.
- □ Lack of executive or management support
- □ Lack of support from business stakeholders
- □ Lack of clarity on mandate, 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 (i.e., 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

Multifactor Authentication

1.02.14 Which of the following best describes the agency's multifactor authentication capabilities?
- ○ Multifactor authentication has not been implemented on any agency systems.
- ○ Multifactor authentication has been enabled on critical agency systems.
- ○ Multifactor authentication has been enabled on most agency systems.
- ○ Multifactor authentication has been enabled on all agency systems.

1.02.14a Please describe the extent of multifactor authentication deployment within your agency.
<text>

1.02.14b What percentage of agency users are covered by multifactor authentication? Enter a number
<Number>

Endpoint Detection and Response (EDR)

1.02.15 Which of the following best describes the agency's EDR capabilities?
- ○ EDR has been enabled through O365.
- ○ DIR's Statewide EDR product has been implemented.
- ○ Another EDR product has been implemented.
- ○ Plan to implement EDR using DIR's statewide EDR program.
- ○ EDR has not been implemented on any agency systems.

1.02.15a On what types of deceives has EDR been implemented? (select all that apply)
- □ Desktop/laptop systems
- □ Servers
- □ Tablets
- □ Phones
- □ None of the above

Zero Trust

1.02.16 Which of the following best describes the 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.

1.02.16a What would be your interest in a statewide Zero Trust initiative similar to DIR's statewide EDR initiative so economies of scale can be achieved?
- ○ Definitely interested.
- ○ Somewhat interested.
- ○ Not interested.

Incident Response

1.02.17 How often does the agency review/revise its security incident response plan and procedures?
- ○ Every 6 months or less
- ○ Annually
- ○ Every other year
- ○ No formal revision schedule exists
- ○ Agency does not have incident response plan

1.02.17a How often does the 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 incident response plan

Cybersecurity Insurance

1.02.18 Does the agency have any form of cybersecurity insurance?
- ○ 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? Choose all that apply.
- □ Breach notification
- □ Business interruption
- □ Credit monitoring
- □ Incident response services
- □ Media liability
- □ Professional liability
- □ Ransomware/Extortion
- □ Regulatory fines
- □ N/A
- □ Other, write in

1.02.18c What is your approximate annual premium for your policy?
If multiple policies, provide total premium costs

$<enter a number>

1.02.18d What is your approximate annual liability coverage for your policy?8
If multiple policies, provide total liability coverage

$<enter a number>

1.02.18e What is your deductible?
$<enter a number>

1.02.18f Have you seen an increase in premium, deductible, and decrease in coverage?
Yes
No
N/A

1.02.18g If yes, how much has the increase been in premium?
%<enter a number>

1.02.18h How much has the increase been in deductible?
%<enter a number>

1.02.18i How much has the decrease been in coverage?
%<enter a number>

Third-party Security

1.02.19 Does the agency integrate security requirements into third-party service contract agreements?
- ○ Yes, for all third-party contracts
- ○ Yes, for contracts involving confidential/regulated data
- ○ No

1.02.19a How often does the 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

1.02.20 Which of the following cybersecurity standards, frameworks, or best practices are leveraged by the organization? Choose all that apply.
- □ ISO/IEC 27000 Series
- □ NIST Risk Management Framework
- □ NIST Cybersecurity Framework
- □ Center for Internet Security Controls
- □ Control Objectives for Information and Related Technologies (COBIT)
- □ Committee of Sponsoring Organizations (COSO)
- □ FFIEC "Cybersecurity Assessment Tool"
- □ Health Information Trust Alliance) HITRUST
- □ OCTAVE
- □ Factor Analysis of Information Risk (FAIR)
- □ Cybersecurity Maturity Model Certification (CMMC)□
- □ OWASP
- □ Other, write in

1.02.21 Which of the following regulations/standards are applicable to the organization? Choose all that apply.
- □ HIPAA
- □ CJIS
- □ FERPA
- □ GLBA
- □ PCI DSS
- □ GDPR
- □ DFARS
- □ SOX
- □ IRS 1075

Section 1.03 – Electronic and Information Resources (EIR) Accessibility

The IRM should coordinate with the agency's EIR Accessibility Coordinator in completing this section. Institutions of Higher Education are required to submit this section.

1.03.01 Has your agency participated in the state's free website accessibility scanning program?
- ○ Yes *(skip 1.03.01a)*
- ○ No, but plan to *(skip 1.03.01a)*
- ○ No

See information about DIR's Accessibility Web Scanning Program.

1.03.01a If not, 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 own scanning program or service
- ○ Other: ___

1.03.02 Does the agency test new and changed agency web pages and website designs for accessibility compliance?
- ○ Yes - all pages
- ○ A subset of all pages
- ○ No *(skip 1.03.02a-1.03.02b)*
- ○ Not applicable *(skip 1.03.02a-1.03.02b)*

1.03.02a How does the agency test new and changed agency web page/site designs for accessibility compliance? Choose all that apply.
- □ Manual testing is performed during development of new pages
- □ Manual testing is performed before deploying changed pages
- □ Automated testing is performed on live web pages
- □ Manual testing is performed at key checkpoints in the contracting and procurement process
- □ Manual or automated testing is performed when a problem is identified

1.03.02b What percentage of the agency's publicly-facing web pages are in full compliance with state accessibility requirements, 1 TAC 206 and 213?
<Enter a percentage:>

1.03.03 Does the agency test new and changed agency web-based applications for accessibility compliance?
- ○ Yes - all pages
- ○ A subset of all pages
- ○ No *(skip 1.03.03a-1.03.03b)*
- ○ Not applicable *(skip 1.03.03a-1.03.03b)*

1.03.03a How does the agency test new and changed agency web-based applications for accessibility compliance? Choose all that apply.
- □ Manual testing is performed during application development
- □ Manual testing is performed before deploying changes
- □ Manual testing is performed at key checkpoints in the contracting and procurement process
- □ Manual testing is performed during scheduled review cycles
- □ Manual testing is performed when a problem is identified

1.03.03b What percentage of the agency's publicly-facing web-based applications, are in full compliance with state accessibility requirements, 1 TAC 206 and 213?
<Enter a percentage:>

1.03.04 Does the agency document results of accessibility compliance testing?
- ○ Yes - always
- ○ Sometimes
- ○ No
- ○ The agency does not perform accessibility compliance testing

1.03.04a Does the agency take corrective action based on the results of accessibility compliance testing?
- ○ Yes – always
- ○ Sometimes
- ○ No

1.03.05 What types of challenges has the agency faced when attempting to achieve compliance with state accessibility requirements? Select up to five.
- □ None
- □ Accessibility not considered a priority at my agency
- □ Lack of staff with required knowledge/skill sets
- □ Lack of available training to raise accessibility compliance
- □ Lack of executive support for accessibility initiatives
- □ Insufficient budget for staff, training, or technology
- □ Accessibility not integrated into agency development
- □ Accessibility not integrated into agency procurement processes
- □ Limitations in technology used in agency development environments
- □ Limitations in the accessibility of vendor procured solutions
- □ Limitations in Commercial-Off-The-Shelf software (COTS)
- □ Conflicting regulations (from other regulatory agencies) prevent compliance
- □ Other, write in

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 2.0)	<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 EIR offerings procured	<status>
Percentage of accessible applications developed	<status>
Total number of accessibility exceptions or exemptions	<status>
Other, write in	<status>

1.03.07 Has your agency begun to implement accessibility technical standards defined in WCAG 2.0 level AA for new website and web application development?
- ○ Yes
- ○ In planning
- ○ No

1.03.08 What percentage of your Accessibility Coordinator's time is dedicated to accessibility?
- ○ Full time
- ○ 75-99%
- ○ 50-74%
- ○ 25-49%
- ○ 0-24%

1.03.09 Is your agency aware of DIR's Enterprise wide free EIR accessibility learning management system, Access University?
- ○ Yes
- ○ No

1.03.10 Does your agency have staff registered for courses in DIR's Enterprise wide free EIR accessibility learning management system, Access University?
- ○ Yes, several
- ○ Some
- ○ No

1.03.11 How valuable and effective is having DIR's Enterprise wide free EIR accessibility learning management system, Access University, and its content available your agency in achieving accessibility compliance to 1 TAC 213 and 1TAC 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 the agency implemented ongoing or daily remote working solutions to support alternative workplace arrangements?
- ○ Implemented
- ○ In progress
- ○ In planning
- ○ No

1.04.02 Does the 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 the agency maintain a written disaster recovery plan for information resources in support of its Continuity of Operations Plan (COOP) or Business Continuity Plan (BCP)?
- ○ Yes, implemented
- ○ Yes, as part of the DCS disaster recovery plan
- ○ No, in progress *(skip 1.04.03a-1.04.03b)*
- ○ No *(skip 1.04.03a-1.04.03b)*

1.04.03a Has the agency's COOP or BCP been revised or updated in the last 12 months?
- ○ Yes
- ○ No

1.04.03b Has the agency COOP or BCP been tested in the last 12 months other than the pandemic response?
- ○ Yes
- ○ No

1.04.04 Does the agency utilize cloud services or disaster-recovery-as-a-service (DRaaS) in COOP or BCP plans?
- ○ Yes
- ○ Considering
- ○ No

1.04.04a Has the agency successfully tested the disaster recovery related application(s) for compatibility with cloud services?
- ○ Yes
- ○ In progress
- ○ No

Section 1.05 - Electronic Records Management

The IRM should consult with the agency's Records Management Officer (RMO) and Data Management Officer (DMO) to complete the following section. The RMO is responsible for your agency's records management program including your agency's records retention schedule that lists all records series and their retention periods for all state records of your agency. The program includes policies and procedures for final disposition of state records according to their retention requirements including digital preservation for their full retention period. For archival state records, this includes preservation or transfer to the by the Texas State Library and Archives Commission including those electronic records that can transferred to the Texas Digital Archive.

For the purposes of this section, digital data is defined as electronic computerized data (i.e. non-analog storage). If the agency does not know the answer to a specific question, we ask that you use your best judgement in reporting an approximation.

1.05.01 For which of the following areas does the agency have a policy or policy provision relating to digital data and records management practices? Choose all that apply.
- □ Data classification (public, sensitive…)
- □ 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

1.05.02 Does the agency use any automated tools to enforce records retention policy?
- ○ Yes
- ○ In planning
- ○ No (skip 1.05.02a)

1.05.02a For which of the following categories does, or will, the agency enforce automated retention? Choose all that apply.
- □ Databases
- □ Desktops/Local Drives
- □ Email
- □ Enterprise File Shares
- □ Software-as-a-Service/Platform-as-a-Service (e.g. SharePoint, Salesforce, etc.)
- □ Other, write in

1.05.03 Which digital preservation techniques are used in the agency? Choose 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

1.05.04 Does the agency anticipate increasing its spending on digital storage within the next two years?
○ Yes
○ No (skip 1.05.04a)
○ Unsure (skip 1.05.04a)

1.05.04a How much do you anticipate the agency's digital storage spending to increase over the previous biennium (FY20-FY21)?
○ 0-5%
○ 5-10%
○ 10-20%
○ 20-50%
○ Over 50%
○ Unknown

1.05.05 What are the largest barriers the agency faces regarding the management of electronic records and digital data storage? Select up to 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

1.05.06 Which of the following levels best describes the agency's information security data classification policies and processes?
○ Level 0: Data classification policies and procedures do not exist.
○ Level 1: 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.
○ Level 2: Data classification policies and processes are defined and repeatable. Across the organization, there is a common understanding of what are the organization's most important and sensitive information. Data owners have been identified for most information.
○ Level 3: 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.
○ Level 4: 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.
○ Level 5: Data is managed based on classification levels that align to business need and mission criticality.

1.05.07 How often does the 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

1.05.08 Does the agency store digital data that exceeds its established retention requirements?
○ Yes
○ No (skip 1.05.08a-1.05.08b)
○ Unknown (skip 1.05.08a-1.05.08b)

1.05.08a Approximately, what percentage of data stored beyond its required retention schedule is unnecessary as of September 1, 2021 (FY 22)?
<Enter a percentage:>

1.05.08b What are the primary reason(s) for storing digital data and records beyond the established retention requirements? Select up to 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
□ Other, write in

1.05.09 Does the agency track the volume of digital records disposed (destroyed, transferred to archives, etc.)?
○ Yes
○ No (skip 1.05.09a)

1.05.09a What was the approximate volume of digital records dispositioned in FY 21?
<number> GB

1.05.10 Do the storage solutions utilized allow the 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 are implemented? Choose 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

1.05.12 For data stored in locally hosted agency managed servers and storage devices (excluding workstations), which of the following security controls are implemented? Choose 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

Digital Transformation

Texas Government Code Sec. 2054.069 requires DIR to establish a digital transformation guide to provide guidance and direction to agencies in developing their own digital transformation strategy.

For the purposes of this section, digital transformation is defined as the integration of technology into all areas of a business, including people, processes, and tools, to fundamentally change how an agency operates and delivers value to constituents and employees.

1.05.13 What is the status of digital transformation in your agency?
○ Level 0: Digital transformation practices do not exist
○ Level 1: Initial (e-government only, reactive, IT-centric)
○ Level 2: Repeatable (open, transparency-focused, starting to co-create applications)
○ Level 3: Defined (data-centric, proactive, business-led)
○ Level 4: Controlled (fully digital, transformation-focused, modular technology)
○ Level 5: Optimized (smart, predictive, using emerging technology)

1.05.14 Does the agency have paperless or paper-on-request processes in place?
○ Yes – all paperless processes
○ Yes – partially paperless processes
○ Yes – mostly paper-on-request
○ No

1.05.15 Describe any electronic notification or digital communication efforts between the agency and the public.
<enter text>

1.05.16 How would you characterize the organization's ability to embrace digital transformation?
○ Level 0: No willingness to embrace change
○ Level 1: Initial (bottom up driven by staff; risk-averse and resistant to change)
○ Level 2: Repeatable (small number of staff engaged in digital projects; change management strategy in development)
○ Level 3: Defined (digital strategy developed and embraced; focus is on constituents and employees and how digital can meet their needs)
○ Level 4: Controlled (all staff embrace digital strategy and is driving a cultural change; staff redefining roles to align with digital strategy)
○ Level 5: Optimized (digital culture is embedded into overall culture; staff always looking for ways to improve digital service delivery)

Section 1.06 - Contracting

1.06.01 Does the agency attempt to negotiate a lower price when procuring technology goods and services through the DIR Cooperative Contracts program?
- ○ Yes, frequently
- ○ Yes, sometimes
- ○ No

1.06.01a How frequently is the 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

1.06.02 How many Automated Information System (AIS) procurements, as defined by Section 2157.001, Government Code, that will exceed $10 million during the entire contract term, including optional renewals and extensions, does your agency plan to make in the biennium?
- ○ Less than 5
- ○ 5-10
- ○ 11-15
- ○ Over 15

1.06.03 What additional products or services would you like to see on DIR Cooperative Contract?
<text>

1.06.04 How many Statements of Work (SOW) does the agency anticipate submitting to DIR in the biennium?
- ○ 0-5
- ○ 6-10
- ○ 11-20
- ○ 21-30
- ○ 31-50
- ○ 51-100
- ○ More than 100
- ○ Other, write in

1.06.05 How many Cooperative Contracts exemptions does the agency anticipate submitting to DIR in the biennium?
<number>

1.06.05a For what types of products/services is the 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 the agency intend to leverage in the biennium?
○ 0-5
○ 6-10
○ 11-20
○ Over 20
○ Other, write in

1.06.07 For which of the following technology categories would the agency be interested in participating in a bulk purchase initiative? Choose 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
□ 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

View DIR current bulk purchase initiatives

1.06.08 Approximately, how many agency staff are involved with IT contract negotiation?
<number>

1.06.08a Of the number above, approximately, how many agency staff have taken the statutory-required DIR IT Negotiations training?
<number>

1.06.08b Of the number remaining to be trained, how many agency staff plan to attend training in the upcoming biennium?
<number>

Section 656.050, Government Code, requires state agency personnel directly involved in contract negotiations for the purchase of information resources technologies to complete the training developed by the department (DIR).

1.06.09 Has your procurement division implemented Agile Contracting?
- Yes
- In planning
- No

Section 1.07 - Hardware/Software Environment

Client Hardware Environment

For each category of end-user computing device, what is the approximate number of devices used in the 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	<number>
1.07.07	Basic cell phones	<number>
1.07.08	Printers - network and dedicated	<number>

For each category of end-user computing device, what is the planned refresh cycle? Select one of the following: "1 year," "2 years," "3 years," "4 years", "5 years," "6+ years."

1.07.09	Desktops, owned	<refresh cycle>
1.07.10	Desktops, leased or seat managed	<refresh cycle >
1.07.11	Laptops, owned	<refresh cycle >
1.07.12	Laptops, leased or seat managed	<refresh cycle >
1.07.13	Tablet computers	<refresh cycle >
1.07.14	Smartphones	<refresh cycle >
1.07.15	Basic cell phones	<refresh cycle >
1.07.16	Printers - network and dedicated	<refresh cycle >

1.07.17 What is the approximate average age of desktops and laptops currently in use by the agency?
○ 1 year ○ 2 years ○ 3 years ○ 4 years ○ 5 years ○ 6+ years

1.07.18 What is the approximate age of the oldest desktops or laptops currently in use by the agency?
○ 1 year ○ 2 years ○ 3 years ○ 4 years ○ 5 years
○ 6 years ○ 7 years ○ 8 years ○ 9 years ○ 10+ years

Client Software Environment

1.07.19 What is the agency's current primary client operating system?

- ○ Microsoft Windows 7
- ○ Microsoft Windows 8
- ○ Microsoft Windows 10
- ○ Apple Macintosh OS X, 10.12
- ○ Apple Macintosh OS X, 10.13
- ○ Apple Macintosh OS X, 10.14
- ○ Apple Macintosh OS X, 10.15
- ○ Other, write in

1.07.20 If the agency is planning or considering migration to a newer primary client operating system in the biennium, which will it be?

- ○ No migration is currently planned or considered
- ○ Microsoft Windows 7
- ○ Microsoft Windows 8
- ○ Microsoft Windows 10
- ○ Apple Macintosh OS X, 10.12
- ○ Apple Macintosh OS X, 10.13
- ○ Apple Macintosh OS X, 10.14
- ○ Apple Macintosh OS X, 10.15
- ○ Other, write in

1.07.21 What is the agency's current primary client office productivity suite?

- ○ Microsoft Office 2007
- ○ Microsoft Office 2010
- ○ Microsoft Office 2013
- ○ Microsoft Office 2016
- ○ Microsoft Office 2019
- ○ Apple iWork
- ○ Microsoft Office 2008 for Macintosh
- ○ Microsoft Office 2011 for Macintosh
- ○ Microsoft Office 2013 for Macintosh
- ○ Microsoft Office 2016 for Macintosh
- ○ Microsoft Office 2019 for Macintosh
- ○ Google Apps for Government
- ○ Other, write in

1.07.22 If the agency is planning or considering upgrade to a newer office productivity suite in the biennium, which will it be?
- ○ No upgrade currently planned or considered
- ○ Microsoft Office 2013
- ○ Microsoft Office 2016
- ○ Microsoft Office 2019
- ○ Apple iWork 2014
- ○ Microsoft Office 2011 for Macintosh
- ○ Microsoft Office 2013 for Macintosh
- ○ Microsoft Office 2016 for Macintosh
- ○ Microsoft Office 2019 for Macintosh
- ○ Google Apps for government
- ○ Other, write in

Server Environment

Note: For agencies participating in Data Center Services, respond to questions 1.07.23-1.07.28 concerning only servers not included in the Data Center Services contract (i.e. servers not managed by DCS vendors).

1.07.23 How many physical hardware hosts exist in the agency's virtualized server environment? Enter a number only.
<number>

1.07.24 How many virtual server instances exist in the agency's virtualized server environment? Enter a number only.
<number>

1.07.25 How many physical server instances exist in the agency's non-virtualized server environment? Enter a number only.
<number>

1.07.26 What is the refresh cycle for physical servers managed by the agency?
- ○ 3 years
- ○ 4 years
- ○ 5 years
- ○ 6 or more years

1.07.27 What is the approximate average age of servers currently managed by the agency?
- ○ 1 year
- ○ 2 years
- ○ 3 years
- ○ 4 years
- ○ 5 years
- ○ 6+ years

1.07.28 What is the approximate age of the oldest servers currently managed by the agency?
- ○ 1 year
- ○ 2 years
- ○ 3 years
- ○ 4 years
- ○ 5 years
- ○ 6 years
- ○ 7 years
- ○ 8 years
- ○ 9 years
- ○ 10+ years

Network Environment

1.07.29 What is the status of agency support for IPv6?
- ○ Complete
- ○ In progress
- ○ In planning
- ○ Not planned

1.07.30 Does the agency leverage Single Sign On capability?
- ○ Yes
- ○ Considering
- ○ No

1.07.31 Does the 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

Microservices

1.07.32 What is the status of deployment of Microservices in the agency?
- ○ Currently using
- ○ Planning to use
- ○ May use
- ○ Do not use

Section 1.08 - E-Learning

1.08.01 Which of the following types of technology are used in training programs provided by the agency? Choose 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 SaaS solution
- □ Other, write in
- □ None

1.08.02 Does the agency have a Learning Management System (LMS)?
- ○ Yes; name of primary LMS: _____
- ○ In progress; name of primary LMS: _____
- ○ Considering
- ○ No

1.08.03 Which of the following technologies does the agency use regarding personnel training? Choose all that apply.
- □ Online training developed by the agency
- □ Online training, third-party
- □ Tracking systems for personnel training/certifications
- □ Curriculum development and content management
- □ None
- □ Other, write in

Answer question 1.08.04 as accurately as possible, based on information that is currently available in the agency. DIR is not requesting that agencies perform additional research into procurement records, etc., solely to answer these questions. Report training that the agency provided; that is, training that the agency took primary responsibility for delivering, hosting, or distributing. Report training provided to state employees only, not students or constituents. However, if available training data does not distinguish among these groups, the agency may report based on available data. Even an agency with no defined training department generally provides some training to its employees, such as state-mandated discrimination training.

1.08.04 Approximately, what percentage of training provided by the agency is internet-based (Online self-paced, online-instructor led, webinars, etc.)?
<percentage>

Section 1.09 - Emerging Technologies

1.09.01 Does any part of the agency develop, maintain, or use geographic information/data? Choose all that apply.
□ Develop
□ Maintain
□ Utilize
□ None of the above (skip 1.09.02-1.09.04)

1.09.02 Is the geographic information/data your agency develops or maintains required by state law to fulfill agency duties?
○ Yes
○ No (skip 1.09.02a)

1.09.02a Provide the names, short description, and statutory references that relate to the geographic data
<text>

1.09.03 Does the agency provide public access to those geospatial datasets it develops or enhances? Choose 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: _____

1.09.04 Does the agency deploy one or more GIS web map services?
○ Yes
○ In planning
○ No, but would like to in the future
○ No

1.09.05 Is the agency interested in participating in a Texas imagery enterprise offering that would provide high resolution aerial imagery with automatic updates and completely accessible in a cloud environment?
○ My agency is currently participating in the Texas Imagery Program
○ Interested
○ Not currently interested, but may be in the future
○ Not interested

1.09.06 Does the agency share or obtain GIS services or data through another governmental entity or institution of higher education?
○ Yes, which agencies; _____
○ No

1.09.07 In which of the following categories does the agency leverage cloud services? Choose all that apply.

□ Active Directory
□ Office productivity software- Collaboration and planning tools
□ Email
□ Enterprise CRM - Human Resources
□ Enterprise CRM – 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

1.09.08 What are the largest barriers facing cloud adoption? Select up to three.

□ Application incompatibility
□ Application currency
□ Organizational practices/culture changes
□ Competing priorities
□ Migration costs
□ Network connectivity between cloud and local servers
□ Security considerations
□ Complexity/Technical skills
□ Cost management and control
□ Regulatory compliance considerations
□ Bandwidth issues
□ Other, write in

1.09.09 In which of these categories does the agency use open source software? Choose all that apply.

□ Web server
□ Application server
□ Database server
□ Middleware server
□ Client operating system
□ Server operating system
□ None
□ Other, write in

1.09.10 What is the status of deployment of desktop virtualization in the agency?
- ○ Currently using
- ○ Planning to use
- ○ May use
- ○ Do not use

1.09.11 What is the status of deployment of server virtualization in the agency?
- ○ Currently using
- ○ Planning to use
- ○ May use
- ○ Do not use

1.09.12 What is the status of any form of containerization technology (e.g. application containers, O.S. containers) in the agency?
- ○ Currently using
- ○ Planning to use
- ○ May use
- ○ Do not use

1.09.13 Define your agency maturity with intelligent automated solutions.
- ○ Initial
- ○ Repeatable
- ○ Defined
- ○ Controlled
- ○ Optimized

1.09.14 For what categories has your agency deployed intelligent automation solutions: (Select all that apply)
- □ Chatbots
- □ Data analysis
- □ Human resources management
- □ Process improvement
- □ Customer relationship management
- □ Inventory control
- □ Other: _____
- □ None of the above

1.09.15 What are your agencies top priorities regarding intelligent automation solutions (select up to 3)
- □ 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

1.09.16 What are the largest barriers to deploying intelligent automated solutions in your agency? (select all that apply)

□ Lack of dedicated personnel
□ Lack of executive engagement
□ Lack of qualified staff
□ Competing priorities
□ Lack of perceived interest
□ Budgetary restrictions

1.09.17 What is the status of low-code or no-code within your agency?

○ Currently using
○ Planning to use
○ May use
○ Do not use

1.09.18 What is the status of Blockchain within your agency?

○ Currently using
○ Planning to use
○ May use
○ Do not use

1.09.19 What is the status of *Application Portfolio Management (APM)* within the agency?

○ Application Portfolio Management in use
○ In progress of implementing Application Portfolio Management
○ Planning to implement Application Portfolio Management
○ No plans to implement Application Portfolio Management

1.09.20 What is the status of a *DevOps* methodology within the agency?

○ Currently using
○ In planning
○ Considering
○ Not planned

Section 1.10 - Legacy Applications

A legacy application may be based on COTS or custom software, or a combination of such systems. An application can be considered "legacy" due to being old (e.g. 20 years), but also because it has liabilities or limitations related to supportability, risk, and agility. Such limitations may include lack of software and hardware support and the inability to acquire either internal or outsourced staffing, equipment, or technical support. The term may also describe the inability of an application to adequately support business requirements or meet expectations for use of modern technologies, such as workflow, instant messaging (IM), and user interface. (Based on NASCIO, Modernizing Legacy Systems, 2008)

1.10.01 Based on the assumption that security is always a factor, what are the main legacy applications issues facing the agency? Choose up to three.
□ Software maintenance upgrades - limited or unavailable
□ Extensibility, adaptability, agility - inability to enhance or revise
□ Application development tools - limited expertise ("dead" languages)
□ Documentation - non-existent or out-of-date
□ Software - no longer available or difficult to obtain
□ Technical support - unavailable or difficult to obtain
□ Hardware maintenance - limited or unavailable
□ Hardware - no longer available, limited or no support
□ Recoverability - uncertain how or where to recover
□ Accessibility - remediation cost, time, feasibility
□ None
□ Other, write in

1.10.02 What is the status of a plan to remediate unsupported software in the agency?
○ All agency software is current and supported
○ Implemented
○ Implementation in progress
○ Planned or planning in progress
○ Not implemented and not planned

Unsupported Software refers to Software for which there are no longer commercial, vendor, or in-house support options, or software that relies on other unsupported applications or components.

1.10.03 Approximately what percentage of your organization's overall application portfolio do you believe requires modernization today?
<Enter a number>

1.10.03a What do you expect that percentage will be in 3 years?
<Enter a number>

Section 1.11 - Project Delivery

1.11.01 Which of the following project development approaches does the agency use? Choose all that apply.
□ Adaptive (e.g. Agile projects)
□ Predictive (e.g. Waterfall projects) (skip 1.11.02a)
□ Hybrid
□ Other, write in (skip 1.11.02a)
□ N/A

1.11.02a Which of the following agile approaches does the agency use? Choose all that apply.
- □ Extreme programming
- □ Kanban
- □ Scrum
- □ Other, write in
- □ N/A

1.11.02b Does the 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

1.11.03 What is the status of implementing a standard project management methodology for technology projects in the agency?
- ○ Implemented
- ○ Implementation in progress
- ○ Planned or planning in progress *(skip 1.11.03a)*
- ○ Not implemented and not planned *(skip 1.11.03a)*

1.11.03a Has the 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 the agency implemented a project classification method as required by TAC 216.11 for technology projects?
- ○ Implemented
- ○ Implementation in progress
- ○ Planned or planning in progress
- ○ Not implemented and not planned

1.11.05 Does the agency voluntarily use the Texas Project Delivery Framework for non-major IR projects?
- ○ Yes, for all non-major IR projects
- ○ Yes, for some non-major IR projects
- ○ Planning or considering voluntary use of the Framework for non-major IR projects
- ○ No, Framework is not being used for non-major IR projects
- ○ No, the agency has never used the Texas Project Delivery Framework

Answer yes even if the agency uses only some parts of the Framework for non-major IR projects.

1.11.06 Describe any recommendations or feedback associated with use of the Framework templates and instructions.
<text>

1.11.07 Which of the following are the largest challenges the agency faces in achieving IT project success? Select up to three.
□ Lack of User Involvement
□ Incomplete Requirements & Specifications
□ Changing Requirements & 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/Contracting
□ Other, write in
□ N/A

Section 1.12 - Digital Services

1.12.01 Does the agency currently collect, or would it be interested in collecting, online fees, fines or payments via credit card or automated bank draft (ACH)?
○ 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 two years
○ Agency has no need or interest in this service

1.12.02 Does the agency currently allow constituents to submit applications or forms via the Internet?
○ Yes
○ Considering
○ No *(skip 1.12.02a)*

1.12.02a Does the agency require a mailed copy of the same application or form with a signature?
○ Yes, for all
○ Yes, for some
○ No

1.12.03 Does the agency incorporate responsive design into public-facing application development to optimize application functionality on mobile devices?
○ Yes, for all public-facing applications
○ Yes, for some public-facing applications
○ No

1.12.04 Does the agency incorporate human centered design principles into public-facing application development to optimize application functionality?
○ Yes, for all public-facing applications
○ Yes, for some public-facing applications
○ No

1.12.05 Select the option below that bests describes your current capability for development of native mobile application.
- ○ Level 0: Don't know what native mobile application development really means
- ○ Level 1: Initial (no native mobile app development is planned)
- ○ Level 2: Repeatable (researching how a native mobile app might improve delivery of services)
- ○ Level 3: Defined (planning or starting to build a native mobile app)
- ○ Level 4: Controlled (have developed and deployed a native mobile app)
- ○ Level 5: Optimized (managing one or multiple native mobile apps; have in-house staff that know how to develop and maintain native mobile apps)

1.12.06 How many native mobile apps has your agency developed? <enter a number>

1.12.07 Is your agency interested in receiving a digital transformation maturity model assessment?

Section 1.13 - Shared Networks

1.13.01 How often does the agency use TEX-AN contracts for purchasing telecommunications services?
- ○ Always
- ○ Sometimes
- ○ Never

1.13.02 In the biennium, by how much does the 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%

1.13.03 In the biennium, by how much does the agency expect its internet connection needs to increase?
- ○ 0-50Mb
- ○ 51-100Mb
- ○ 101-500Mb
- ○ 500Mb-1Gb
- ○ Other, write in

1.13.04 How would the agency prefer to use video conferencing services?
○ Utilize PC-Based applications (Zoom, WebEx, Teams, etc.)
○ Provide your own conferencing platform in house
○ Fully managed service available on a subscription basis, i.e. a videoconferencing room available in the capitol complex by reservation

1.13.05 Does the agency utilize an audio/video record and replay option on its website for public meetings?
○ Yes
○ In progress
○ In planning
○ No

1.13.06 Has the agency implemented the Texas.gov domain for its website?
○ Yes
○ In progress
○ No
○ Not applicable (institutions of higher education only)

Section 1.14 - Data Management

1.14.01 Does the agency have an employee whose duty is to establish the overall strategy to manage the agency's data (e.g. chief data officer or designated data management officer)?
○ Yes
○ No, but plan to *(skip1.14.01a)*
○ No *(skip1.14.01a)*

1.14.01a If yes, provide name, title, and email and reporting manager name and title:
<enter text>

1.14.01b Is this the individual's primary or secondary duty?
○ Primary duty
○ Secondary duty

1.14.02 Does the agency have a data governance structure to manage and govern agency data assets?
○ Yes
○ In planning
○ No

1.14.03 Does the 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

1.14.04 What are the largest barriers your agency faces in implementing a data management and governance program? Select up to 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

1.14.05 Is the agency currently sharing data with another governmental entity?
○ Yes
○ In planning
○ No

1.14.06 What is the status of deployment of business intelligence/analytics within the agency?
○ Agency is highly invested and has substantial capabilities
○ Agency has some capabilities
○ Agency is investigating solutions
○ Agency is not investigating solutions

1.14.07 Approximately, how many of the public information requests were addressed by directing the requestor publicly accessible electronic data or the official open data Internet website, the Texas Open Data Portal? Provide number if readily available.
<number>

1.14.08 Has the agency established data driven policy goals?
○ Yes
○ In planning
○ No

1.14.09 Has the agency conducted a data maturity assessment of the agency's data governance program?
○ Yes
○ No

Section 1.15 - Training and Planning

1.15.01 Which of the following topics would your agency be interested in receiving training or consultation on or participate in workgroups for? Choose all that apply.

□ Accessibility Scanning Program
□ Application Portfolio Management
□ Artificial intelligence and machine learning
□ Business intelligence and visualization programs
□ Cloud services
□ Cooperative Contracts Bulk Purchase Program
□ Cyber security
□ Data center services
□ Disaster recovery
□ EIR Accessibility Learning Management System (Access University)
□ Innovative Procurement Lab
□ Practical blockchain
□ Statement of work
□ Texas Open/Closed Data Portal
□ Texas Project Delivery Framework
□ Data Management/Open Data
□ Digital Transformation Guide
□ Learning Management Systems for IT Workforce Development
□ State Information Resources Strategic Plan
□ Other, write in

Section 1.16 - Optional Comments on Agency Information Technology Environment

1.16.01 OPTIONAL. Enter any comments related to the agency environment sections listed in Part 1. Include the IRDR question number(s) for reference.
<text>

Part 2 – Compliance with State Standards

Agencies should review technology-related statutes and rules referenced in Part 2 and identify the status of compliance with each requirement. DIR will use agency responses to identify and evaluate the extent to which agencies, and the state, are complying with key statutes and rules related to information resources.

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

- **In compliance.** The agency has fully implemented the requirement.
- **Not in compliance.** The agency has not fully implemented the requirement as of the due date of IRDR submission (March 31, 2020). The agency may be actively working toward compliance, but it is the status as of March 31 that should be reported.

Section 2.01 - Security

The IRM should coordinate with the agency's Information Security Officer in completing this section.

2.01.01 Each agency must have annual reviews of their security program for compliance with the 1 TAC 202 Security Standards.
○ In compliance
○ Not in compliance

See 1 TAC Sections 202.20(7) 202.70(7)

2.01.02 Each agency must perform and document an annual security risk assessment.
○ In compliance
○ Not in compliance

See 1 TAC Sections 202.21(b)(6), 202.71(b)(6)

2.01.03 Approval of security risk acceptance, transference, or mitigation decision shall be the responsibility of the information security officer or designee, in coordination with the information owner, for systems identified with a Low of Moderate residual risk and the state agency head for all systems identified with residual High Risk.
○ In compliance
○ Not in compliance

See 1 TAC 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

See 1 TAC Sections 202.22(3)(C), 202.72(3)(C)

2.01.05 Each agency must use the network security services provided through DIR's NSOC when possible and may not purchase network security services unless DIR cannot provide them at a comparable cost.
○ In compliance
○ Not in compliance
○ Exempt (IHEs only)

See Sec. 2059.102(c), 2059.102(d), Texas Government Code

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

See Sec. 2054.130, Texas Government Code

2.01.07 Each agency must designate an information security officer that (1) reports to executive level management; (2) has authority for information security for the entire agency; (3) possesses training and experience required to administer the functions described under this chapter; and (4) whenever possible, has information security duties as that official's primary duty.
○ In compliance
○ Not in compliance

See 1 TAC Sections 202.2(1), 202.7(1)

2.01.08 Each agency must submit a monthly security incident report to DIR via the SPECTRIM portal no later than the 10th day of the following month.
○ In compliance
○ Not in compliance

See 1 TAC Sections 202.23(b)(2), 202.73(b)(2)

Section 2.02 - State Websites

The IRM should coordinate with the agency's EIR Accessibility Coordinator in completing this section. Institutions of Higher Education are required to submit this section.

Please note that TAC 206 was updated in February 2018, harmonizing with technical standards in Section 508 of the Workforce Rehabilitation Act (Web Content Accessibility Guidelines 2.0). TAC 206 language has set a date of compliance with the new standards for April 2020. Therefore, agencies should answer the following section based on their current compliance posture.

2.02.01 Each agency must comply with all state website accessibility standards and provisions as defined in 1 TAC 206.50 or 1 TAC 206.70.
○ In compliance
○ Not in compliance

See 1 TAC Sections 206.50(e), 206.70(e)

2.02.02 Each agency must publish a privacy notice on its homepage and on key public entry points, or Site Policy page, addressing all listed standards in 1 TAC 206.52(c).

○ In compliance
○ Not in compliance

See 1 TAC Sections 206.52, 206.72

2.02.03 Each agency that has a website that requires user identification 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 user identification

See 1 TAC Sections 206.52(d), 206.72(d)

2.02.04 A web page containing a form that requests information from the public must have a link to the associated privacy notice.
○ In compliance
○ Not in compliance
○ No forms on the agency's website request information from the public

See 1 TAC Sections 206.52(e), 206.72(e)

2.02.05 Each agency must comply with listed standards 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

See 1 TAC Sections 206.53(a), 206.73(a)

2.02.06 Each agency must publish a linking notice on its homepage and on key public entry points, or Site Policy page, addressing all listed standards in 1 TAC 206.53(c).
○ In compliance
○ Not in compliance

See 1 TAC Sections 206.53, 206.73

NOTE: See Glossary for definition of Key public entry point.

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

See 1 TAC Sections 206.55, 206.75

2.02.08 Each agency must comply with suggestions for agency cost savings provisions as defined in 1 TAC 206.56 or 1 TAC 206.76.
- ○ In compliance
- ○ Not in compliance
- ○ Exempt (IHEs only)

See 1 TAC Sections 206.56

2.02.09 Per the Governor's 2016 directive, all state agencies must display a link to the Texas Veterans Portal on the agency's homepage. Does the agency currently fulfill this directive?
- ○ Yes
- ○ Yes, but not on the homepage
- ○ No

Section 2.03 - Electronic and Information Resources (EIR) Accessibility

The IRM should coordinate with the agency's EIR Accessibility Coordinator in completing this section. Institutions of Higher Education are required to submit this section.

2.03.01 Each agency must comply with all listed accessibility standards for products and services as defined in 1 TAC 213.10-213.16 or 1 TAC 213.30-213.36.
○ In compliance, without the use of accessibility exceptions
○ In compliance, with one or more accessibility exceptions approved by the agency head
○ Not in compliance

See 1 TAC Sections 213.10-213.16, 213.30-213.36

2.03.02 Each agency must comply with all Accessibility Compliance Exceptions and Exemptions provisions as defined in 1 TAC 213.17(1) -(5) or 1 TAC 213.37(1) -(5).
○ In compliance
○ Not in compliance

See 1 TAC Sections 213.17(1)-(5), 213.37(1)-(5)

2.03.03 Each agency must comply with Accessibility Procurement provisions as defined in 1 TAC 213.18(b)-(g) or 1 TAC 213.38(b)-(g).
○ In compliance
○ Not in compliance

See 1 TAC Sections 213.18(b)-(g), 213.38(b)-(g)

2.03.04 Each agency must comply with Accessibility Training and Technical Assistance provision as defined in 1 TAC 213.19(b) or 1 TAC 213.39(b).
○ In compliance
○ Not in compliance

See 1 TAC Sections 213.19(b), 213.39(b)

2.03.05 Each agency must comply with Accessibility Survey and Reporting Requirements provision as defined in 1 TAC 213.20(b) or 1 TAC 213.40(b).
○ In compliance
○ Not in compliance

See 1 TAC Sections 213.20(b), 213.40(b)

A completed submission of the Accessibility Components of the Information Resources Deployment Review satisfies the reporting requirements provision for state agencies and Institutions of Higher Education.

2.03.06 Each agency must comply with all EIR Accessibility Policy and Coordinators provisions 1 TAC 213.21(b)-(f) or 1 TAC 213.41(b)-(f).
○ In compliance
○ Not in compliance

See 1 TAC Sections 213.21(b)-(f), 213.41(b)-(f)

Section 2.04 - Geographic Information Systems

Institutions of higher education that use GIS only in academic or research settings may respond "In compliance" to items 2.04.01 through 2.04.03.

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

See 1 TAC 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

See 1 TAC 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 standardized metadata documentation for each dataset, and distribute this metadata with the dataset.
○ In compliance
○ Not in compliance
○ No geospatial datasets are distributed by the agency

See 1 TAC Chapter 205

Section 2.05 - Electronic Records Management

2.05.01 Each agency must meet the minimum requirements for the policies and procedures required for the management of all electronic state records as defined by 13 TAC 6.93.
○ In compliance
○ Not in compliance
○ The agency has no electronic state records in electronic form therefore requires no policies under this section

See 13 TAC Section 6.93

2.05.02 Each agency must meet the minimum requirements for the management of all electronic state records as defined by 13 TAC 6.94.
○ In compliance
○ Not in compliance
○ The agency has no electronic state records in electronic form

See 13 TAC Section 6.94

2.05.03 Each agency must meet the additional record requirements for archival, permanent, and vital electronic state records as defined by 13 TAC 6.95
○ In compliance
○ Not in compliance
○ The agency has no archival, permanent, or permanent electronic state records

See 13 TAC Section 6.95

2.05.04 Each agency must stay up to date on Texas State Library and Archives Commission resources for electronic state records as defined by 13 TAC 6.96.
○ In compliance
○ Not in compliance
○ The agency has no electronic state records to maintain

See 13 TAC Section 6.96

2.05.05 Each agency must meet the minimum requirements for the final disposition of all electronic state records as defined by 13 TAC 6.97.
○ In compliance
○ Not in compliance
○ The agency has no electronic records for disposition

See 13 TAC Section 6.97

2.05.06 Each agency must meet the minimum requirements for the management of all electronic transactions and signed records as defined by 13 TAC 6.98.
○ In compliance
○ Not in compliance
○ The agency has no electronic transactions or electronically signed records to manage

See 13 TAC Section 6.98

2.05.07 Each agency must ensure that electronic records in its custody that are archival state records or that need archival review are properly preserved.
○ In compliance
○ Not in compliance
○ No electronic state records are maintained by the agency that are archival state records

See TGC Sections 441.186 and 441.180(2)

Section 2.06 - Additional Standards

2.06.01 Each agency shall provide that its information resources manager is part of the agency's executive management and reports directly to a person with a title functionally equivalent to executive director or deputy executive director.
○ In compliance
○ Not in compliance
○ The agency has designated a joint IRM, who is employed by another agency

See TGC Section 2054.075(b)

2.06.02 Each agency's IRM shall meet or exceed the IRM continuing education requirements.
○ In compliance
○ Not in compliance

See 1 TAC 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, meeting listed standards.
○ In compliance
○ Not in compliance
○ The agency has not conducted an IT project in the past (If the need for an IT project arises, the agency should contact DIR for guidance on a suitable operating procedure).

See 1 TAC 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

See TGC Sections 2054.301 through 2054.307

Major IR Project Criteria - If your agency has had no major IR projects in the last two years, select "In compliance."

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

See TGC Sections 2054.301 through 2054.307

This requirement applies to certain major contracts as defined in the State of Texas Contract Management Guide. If your agency has had no major contracts in the last two years, select "In compliance."

2.06.06 Unless it is an institution of higher education, each agency must purchase IT commodity items in accordance with the IT commodity purchasing program guidelines.
○ In compliance
○ Not in compliance
○ Exempt (IHEs only)

See 1 TAC Chapter 212

2.06.07 A state agency that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply, in the event of a breach of system security, with the notification requirements of Section 521.053, Business and Commerce Code and Sec. 2054.1125, Texas Government Code.
○ In compliance
○ Not in compliance
○ No breach of sensitive personal information has occurred since September 1, 2009

See Business and Commerce Code, Title 11, Section 521.053

2.06.08 If the agency holds an open or closed meeting by video conference call, the systems used must comply with the approved standards.
○ In compliance
○ Not in compliance
○ No agency meetings are held by video conference call

See 1 TAC Chapter 209

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

See Sec. 2054.5191, Texas Government Code

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

See Sec. 2054.5192, Texas Government Code

Part 3 - State Strategic Plan (SSP) for Information Resources Management

Section 3.01 – Alignment Toward 2022-2026 SSP Technology Objectives

For each objective, indicate the extent to which initiatives and activities are aligned with each SSP objective. The table lists the corresponding SSP objective number for easy reference. It is possible that one or more of the objectives may not be applicable to your agency

Question Number	Objectives	Not aligned	Minor alignment	Moderate alignment	Significant alignment	N/A to my agency
3.01.01	Risk-based Security Practices (1.1)	○	○	○	○	○
3.01.02	Cybersecurity Education and Training (1.2)	○	○	○	○	○
3.01.03	Regional Cybersecurity Engagement and Response (1.3)	○	○	○	○	○
3.01.04	Cost-Effective Cybersecurity Tools (1.4)	○	○	○	○	○
3.01.05	Data Governance (2.1)	○	○	○	○	○
3.01.06	Data Security and Privacy (2.2)	○	○	○	○	○
3.01.07	Data Analytics (2.3)	○	○	○	○	○
3.01.08	Open Data (2.4)	○	○	○	○	○
3.01.09	Strategic Roadmap (3.1)	○	○	○	○	○
3.01.10	Digital Maturity (3.2)	○	○	○	○	○
3.01.11	Human-Centered Applications (3.3)	○	○	○	○	○
3.01.12	Mobile Applications (3.4)	○	○	○	○	○
3.01.13	Legacy Modernization (4.1)	○	○	○	○	○
3.01.14	Flexible and Adaptable Approaches (4.2)	○	○	○	○	○
3.01.15	Emerging Technologies (4.3)	○	○	○	○	○
3.01.16	Adaptable Workforce (4.4)	○	○	○	○	○

3.01.17 OPTIONAL. Enter any comments related to alignment with toward 2022-2026 State Strategic Plan objectives

Section 3.02 – Progress Toward 2020-2024 SSP Technology Objectives

Questions 3.02.01-3.02.17 contain the objectives described in the 2020-2024 SSP.

For each objective, indicate the level of overall progress your agency has made toward them.

Question Number	Objectives	No progress	Minor progress	Moderate progress	Significant progress	Optimized /fully adopted	N/A to my agency
3.02.01	Security Enhancement Tools (1.1)	○	○	○	○	○	○
3.02.02	Business Continuity Plans (1.2)	○	○	○	○	○	○
3.02.03	Identity and Access Management (1.3)	○	○	○	○	○	○
3.02.04	Legacy Modernization (1.4)	○	○	○	○	○	○
3.02.05	Application Portfolio Management (1.5)	○	○	○	○	○	○
3.02.06	Data Management/Governance (2.1)	○	○	○	○	○	○
3.02.07	Mobile and Digital Methods (2.2)	○	○	○	○	○	○
3.02.08	Business Intelligence (2.3)	○	○	○	○	○	○
3.02.09	Accessible Electronic Information Resources (2.4)	○	○	○	○	○	○
3.02.10	User-Centric Design (2.5)	○	○	○	○	○	○
3.02.11	Agile Procurement Methodologies (3.1)	○	○	○	○	○	○
3.02.12	Shared Technology Services (3.2)	○	○	○	○	○	○
3.02.13	Open Source Software (3.3)	○	○	○	○	○	○
3.02.14	Business Process Automation (3.4)	○	○	○	○	○	○
3.02.15	Artificial Intelligence (AI) (3.5)	○	○	○	○	○	○
3.02.16	Modern Development Approaches (3.6)	○	○	○	○	○	○
3.02.17	Application Portfolio Management (3.7)	○	○	○	○	○	○

3.02.18 OPTIONAL. Enter any comments related to progress toward 2020-2024 State Strategic Plan objectives.
<text>

Part 4 – IT Inventory

General Information

Texas Government Code, Sections 2054.068 and 2054.0965 require DIR to conduct an inventory of agency information technology assets to produce several reports, including an inventory detailing the risks and costs associated with the resolution of high agency security and operational risks. **This section does not apply to Institutions of Higher Education.**

Information that exposes vulnerabilities in agency information systems is to be treated as confidential under Chapter 552, Government Code.

Due to the variety of reporting volumes this inventory requires, DIR will prepopulate as much information as possible to ease the reporting burden for agencies. However, it is the agency's responsibility to ensure that all fields are accurate and completed. Information will be prepopulated from the previously completed IRDR. For Data Center Services customers, information will also be prepopulated from ServiceNow.

Business Application Validation and Assessments

DIR is asking agencies to review and update their application inventory in the SPECTRIM portal. The validation component of this process is critical to the inventory component of the IRDR. When completing the inventory, the agency will be asked to link the relevant infrastructure to business applications. In an effort to streamline the process, not all applications will require an APM. This list of business applications is going to be prepopulated by the applications that the agency previously validated. The assessments of these applications is especially important as they impact agencies requesting funding for cybersecurity and legacy modernization projects through the PCLS methodology.

The IT Inventory instructions will be available in the SPECTRIM portal at launch. Please be sure to review all fields for accuracy prior to submission.

Glossary

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. (Source: Section 2157.001, Government Code)

Accessibility Coordinator *See EIR Accessibility Coordinator.*

ACH Automated Clearinghouse. A nationwide electronic funds transfer system that provides for the inter-bank clearing of credit and debit transactions and for the exchange of information among participating financial institutions. [Source: ACH.com]

Alternative Workplace Arrangements (AWA) Work arrangements that combine non-traditional work practices, settings/locations, or technologies to achieve workplace progress.

Application Portfolio Management Application Portfolio Management's (APM) goal is to describe the inventory of business applications and the resources (e.g., money, staff time, infrastructure, software and hardware assets) required to provide operational support of those applications over their lifetime. APM is closely related to governance and how an agency ensures that business applications are aligned with agency business needs, enterprise architecture (alignment of people, processes, technology), and tracking of effective metrics to measure the cost/value proposition of business applications relative to each other within an agency (or state) portfolio. APM should guide the investment decisions for a business application's lifecycle, particularly balancing between adding features, maintaining infrastructure currency, and modernizing the platform. Effective implementation of APM is an indicator of an organization's information technology services maturity and its ability to respond to business requirements.

Archival State Record Archival state record means 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. [Source: Government Code 441.180(2)]

BCP Business Continuity Plan.

Board Any agency governing body, including a board, commission, council, etc.

Business Application names are the 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.

Call Center A centralized office handling incoming and outgoing phone calls for customers. Call Center services include help desk, customer support, emergency response, directory assistance, operator services, and similar services.

Checksum A checksum is a small-sized datum derived from a block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage. It is usually applied to an installation file after it is received from the download server. By themselves, checksums are often used to verify data integrity but are not relied upon to verify data authenticity. [source: https://en.wikipedia.org/wiki/Checksum]

Commodity Items (Technology) Technology commodity items are defined in legislation as commercially available hardware, software, and technology services that are generally available to businesses or the public. [Source: DIR IT Commodity Purchasing Program]

Configuration Functional and physical characteristics of hardware or software as set forth in technical documentation or archived in a product; requirements, design, and implementation that define a particular version of a system or system component.

Content Management Content management systems consist 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.

COOP Continuity of Operations Plan.

Cooperative Contracts Program In accordance with TGC Section2157.068, and 1 TAC Chapter 212, each state agency must purchase technology commodity items through contracts established by DIR unless the agency first obtains an exemption. [Source: DIR IT Commodity Purchasing Program]

DevOps (Development and Operations) is an enterprise software development phrase 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.

Disposition, Final 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. [Source: 13 TAC Section 6.1(10)]

Electronic and Information Resources (EIR) Includes information technology and any equipment or interconnected system or subsystem of equipment used in the creation, conversion, duplication, or delivery of data or information. The term electronic and information resources includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, websites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology. [Source: 508 Section 1194.4, Definitions]

EIR Accessibility Coordinator An agency staff member who acts on behalf of the agency in matters relating to accessibility as defined in Chapter 2054, Government Code, and Texas Administrative Code Sections 206 and 213.

Enterprise Concerning the broadest scope of the agency, including all business and technology divisions.

Enterprise Gateway Servers providing End User remote access, and external file sharing. FTP, RAS, BES, FAX, Email Gateway.

Enterprise Resource Planning (ERP) A term for the broad set of activities supported by multi-module application software that helps a business manage its business processes, including operational planning, inventory, procurement, customer service, finance, and human resources. Typically, an ERP system uses or is integrated with a relational database system.

Functional Performance Criteria Modes of operation and information retrieval that supports assistive technology used by people with disabilities (blind or visually impaired, deaf or hard of hearing,

speech, fine motor control or simultaneous actions, etc.) to perform a function. [Source: 1 TAC Section 213.15]

Geographic Information System (GIS) A system of computer hardware, software, and procedures used to store and manipulate electronic maps and related data to solve complex planning and management problems. [Source: www/.wikipedia.org]

Globally-unique Identifier A universally unique identifier (UUID) is a 128-bit number used to identify information in computer systems. The term globally unique identifier (GUID) is also used.

Governance Encompasses the structures and processes for defining and ensuring fulfillment of objectives through consideration of both business and technology services within a common forum.

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. [Source: Senate Bill 701, 82nd Texas Legislative Session]

IHE Institution of Higher Education.

Information Resources Manager (IRM) 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 (Chapter 2054, Government Code). [Source: DIR Information Resources Manager Overview]

Information Security Officer (ISO) 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. [Source: DIR IS Security Policies]

Infrastructure The physical hardware used to interconnect computers and users, as well as the software used to send, receive, and manage transmitted signals.

Instant Messaging The transmission of an electronic message over a computer network using software that immediately displays the message in a window on the screen of the recipient. A computer application that allows for communications in real time, a live chat and e-mail service. [Source: Dictionary.com]

Interoperability The ability of two or more systems or products to work together without special effort. For example, routers and switches in a network require interoperability.

IPv6 Internet Protocol version 6 is the latest revision of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. [Source: www/.wikipedia.org]

ISO 2700x Information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). Provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system, similar in design to management systems for quality assurance and environmental protection. [Source: Wikipedia.com]

IVR Interactive voice response (IVR) is a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via keypad.

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 (LMS) Software that automates administration of learning activities and competencies as well as the logistics of delivering such activities. This may include all types of learning: instructor-led, computer-based training, web or video conferencing, etc.

Legacy Systems A Legacy System may be old (e.g. 20 years) but it may also have liabilities or limitations related to supportability, risk, and agility. Such limitations may include lack of software and hardware support and the inability to acquire either internal or outsourced staffing, equipment, or technical support. The term may also describe the systems inability to adequately support business requirements or meet expectations for use of modern technologies, such as workflow, instant messaging (IM), and user interface. [Based on NASCIO, Modernizing Legacy Systems, 2008]

LPARs Logical Partitioning, a system of taking a computer's total resources – processors, memory and storage – and splitting them into smaller units that each can be run with its own instance of the operating system and applications. [Source: Webopedia.com]

Mainframe A high-performance computer system sued for large-scale computing purposes that require high levels of throughput, availability and security, typically measured in millions of instructions per second (MIPS). Examples of operating systems used by mainframes: zOS, OS/390, VM, z/VM, VSE, OS2200, and Clearpath.

Major Information Resources Project See Project, Major Information Resources.

Messaging Services that use a network to send, receive, and combine messages, faxes, and large data files. Examples are electronic mail and enhanced fax.

Multimedia Multimedia refers to the use of (but not limited to) electronic media to store and experience multimedia content. Media that uses multiple forms of information content and information processing (e.g. text, audio, graphics, animation, video, interactivity) to inform or entertain the (user) audience. [Source: Wikipedia.com]

Network Security and Operations Center (NSOC) HB3112 (79th Texas Legislature) authorizes DIR to establish NSOC on a cost-recovery basis to manage and deliver network security system services to state agencies.

NIST 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. [Source: TechTarget.com]

Operating System Software designed to control the hardware of a specific data-processing system in order to allow users and application programs to make use of it. [Source**:** Dictionary.com]

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.

Project, Major Information Resources As defined in Chapter 2054, Government Code, , any information resources technology project identified in a state agency's biennial operating plan with development costs that exceed $1 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.

Quality Assurance A critical review process to ensure that a task is adequately and correctly performed.

Quality Assurance Team (QAT) The QAT is 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 (RMO). 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, §441.184. [Source: 13 TAC Section 6.1(11)]

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. [Source:13 TAC Section 6.92(11)]

Records Retention Schedule A document prepared in accordance with §6.2 of this title (relating to Submission of Records Retention Schedules for Certification). [Source: 13 TAC Section 6.1(12)]

Records Series A group of identical or related records that are normally used and/or filed together, and that permit evaluation as a group for retention scheduling purposes. [Source: 13 TAC Section 6.1(13)]

Retention Period The period of time during which state records must be maintained before final disposition. [Source: 13 TAC Section 6.1(11)]

Remote Working Solutions Technologies that provide remote employees access to the same information and communications services normally available at their workplace.

Risk The possibility of an act or event occurring that would have an adverse effect on the state, an organization, or an information system. Risk involves both the probability of failure and the possible consequences of a failure.

Self-contained, Closed Products Self-contained, closed products generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. Examples of such products include information kiosks and information transaction machines, copiers, printers, calculators, and fax machines.

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 Each installation of an operating system on a server counts as a server instance. (Ex: IBM: AIX LPAR).

Stakeholder Any individual or group who cares about the effort and cost of a project, wants to see the agency use the results of the product, and needs to provide time and effort to make the product usable.

Standard An approved, documented, and available set of criteria used to determine the adequacy of an action or object.

Strategic Important or essential in relation to a plan of action: *what* is to be accomplished.

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. [Source: 13 TAC Section 6.1(17)]

System Development Life Cycle (SDLC) A structure or method imposed on the development of a system product that includes the activities involved in development and the order in which those activities are executed.

TAC 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. [Source: www.sos.state.tx.us/tac/]

TEX-AN Texas Agency Network.

Texas Digital Archive The Texas Digital Archive (TDA) 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. [Source: DIR Framework Overview]

TGC Texas Government Code.

Video Exchange Service Provides a communications platform allowing organizations to schedule, hold, and playback video conferences over an IP backbone. These calls also include the ability to exchange documents during the call. A key benefit is the ability for end users to schedule and meet (via video) with other compatible users and organizations either intra-agency, inter-agency, or agency to rest of world on an as needed basis without the need to build a dedicated network infrastructure themselves. End user devices range from desktop phones to full dedicated video meeting rooms.

Virtual Server A method of partitioning a physical server computer into multiple servers that each has the appearance and capabilities of running on its own dedicated machine. Each virtual server can run its own full-fledged operating system, and each server can be independently rebooted. [Source: Wikipedia.org]

Virtualization Creation of a virtual, rather than physical version, of an operating system, server, storage device, or network resource.

Voice over Internet Protocol (VoIP) A technology used to transmit voice over a data network using the Internet.

Wi-Fi A popular technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves. [Source: Wikipedia.com]

WiMAX Worldwide Interoperability for Microwave Access, a wireless communications standard designed to enable the delivery of last mile wireless broadband access as an alternative to cable and DSL. [Source: Wikipedia.com]

Workflow Workflow management products automate tasks, procedural steps, organizations or people involved, required input and output information, and tools needed for each step in a business process. These products manage and enforce work progression consistently focusing on processes rather than documentation.

If you have any questions about the content of this document, please email irdr@dir.texas.gov.