



2024 Security Plan Template Instructions

September 1, 2023

2024 Security Plan Template Instructions

Submission Deadline: 6/1/2024

Table of Contents

Introduction	1
Required Reporting	1
Reporting Tool	2
Logging into the Portal.....	2
View Mode	4
Edit Mode	5
SPECTRIM Support & Tips.....	5
Security Plan Dashboard & Reports.....	7
Security Plan Content	8
Texas Cybersecurity Framework.....	8
Security Plan Template Overall Record.....	8
Control Review Status	13
Vulnerability Report Questionnaire	14
Submission & Reporting	16
Submitting the Plan to DIR.....	16
% Complete and Objective Completion Status.....	17
Acknowledgment Status	17
Vulnerability Report Status	18
Exporting/Reporting.....	18
Summary Export.....	19
Detailed Export	19
Resources and Assistance	21
Resources	21
Agency Security Plan Webpage	21
Executive Written Acknowledgement Form	21
Texas Cybersecurity Framework Controls and Definitions.....	21
Security Plan Template Excel Version.....	21
Vulnerability Report Electronic Version.....	21
Support.....	21
DIR GRC Team.....	21
SPECTRIM Support Requests.....	21
Table of Figures	22
Version History	22

Introduction

[Section 2054.133, Texas Government Code](#), requires each state agency (including institutions of higher education) to develop and periodically update an information security plan for protecting the security of the agency's information. In developing the plan, agencies shall:

1. Consider any vulnerability report prepared under [Section 2054.077, Government Code](#);
2. Incorporate the network security services provided by DIR to the agency under [Chapter 2059, Government Code](#);
3. Identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of agency information;
4. Identify risk management and other measures taken to protect agency information from unauthorized access, disclosure, modification, or destruction.

Required Reporting

Texas state agencies and institutions of higher education (agencies) that are not-exempt from DIR rules are required to report their information security plans to DIR no later than June 1, of each even-numbered year (June 1, 2024). If you are unsure as to whether your organization is required to complete an information security plan, please contact GRC@dir.texas.gov.

Reporting Tool

Information Security Plans are collected via the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM).

To access the security plan template record, users need to be assigned to the appropriate access group. To request a new user or modify an existing user's credentials, the agency's designated Information Security Officer (ISO) can open an Archer Support Request ticket from within the system, or contact GRC@dir.texas.gov. Archer Support Requests are generally the faster way to obtain assistance.

Logging into the Portal

If you have an active account, you can log into the portal using the following information and your password. If you suspect your account has been inactivated or locked, you will need to reach out to GRC@dir.texas.gov or have someone from your organization open an Archer Support Request on your behalf to have your account reactivated.

URL: <https://dir.archerirm.us/>

Authentication type: SSO Authentication via TDIS (See [SPECTRIM Access](#) for details)

Username: *your email address*

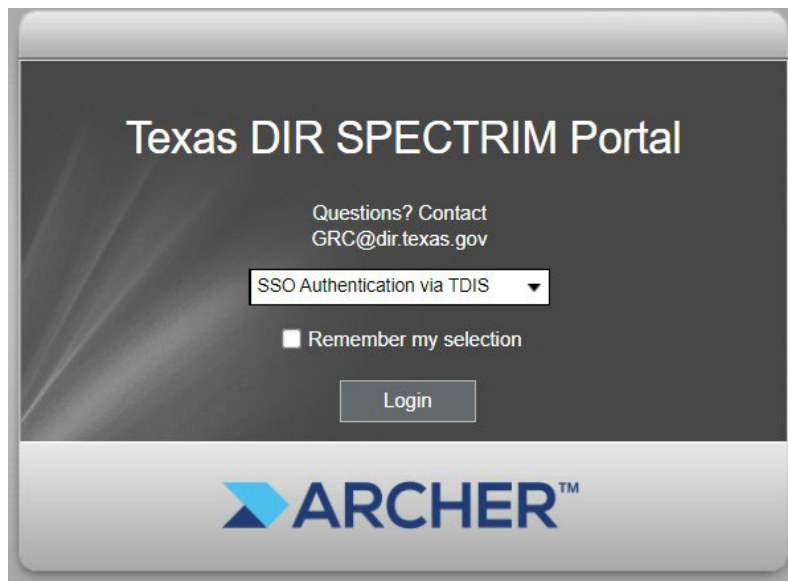


Figure 1: SPECTRIM Login Page

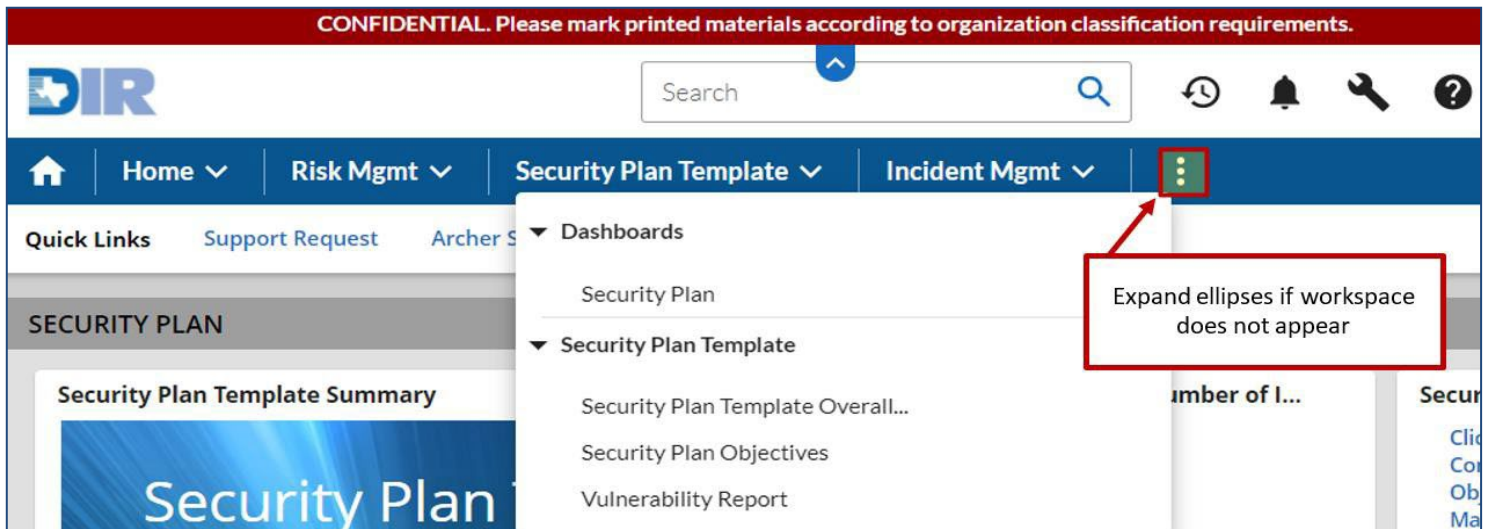


Figure 2: Security Plan Template Workspace Navigation

The SPECTRIM portal is mainly composed of Workspaces, Dashboards, Applications/Questions, and Records. Within the Security Plan Template Workspace Tab, you can access various portions of the security plan.

You may need to click on the ellipses to see more if the Security Plan Template Workspace does not appear across the top banner of the screen.

The Security Plan Template Dashboard is the primary hub for navigating and viewing the related security plan records. The dashboard will display various reports and allow you to monitor progress as you evaluate security controls.

From the dashboard or the workspace selection items, you can enter the individual components of the security plan – Security Plan Template Overall Record, Security Plan Template Records (Security Objectives, Vulnerability Report, & Assessment Objectives – which are described in detail in a later section.

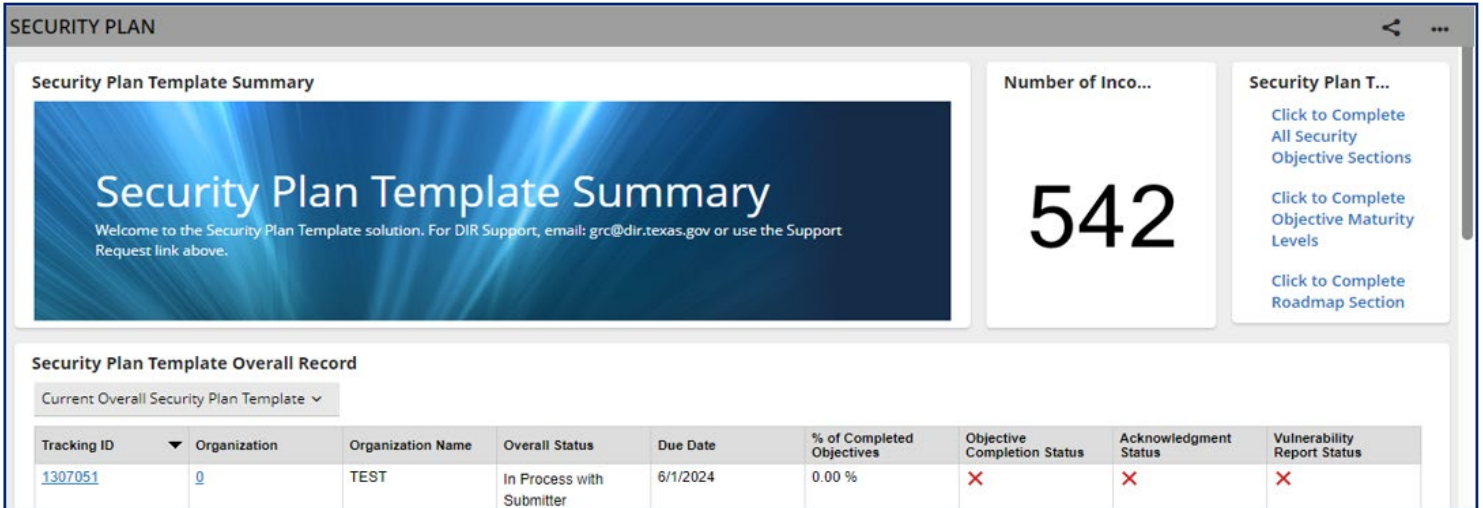


Figure 3: Security Plan Template Dashboard

When navigating the system, be sure not to use the browser's controls. Instead, if you need to return to the previous screen, use the "x" in the upper right-hand corner of the screen. Select the "edit" option when entering a record if the fields are not editable. The two record modes – View & Edit are displayed on the following pages.

View Mode

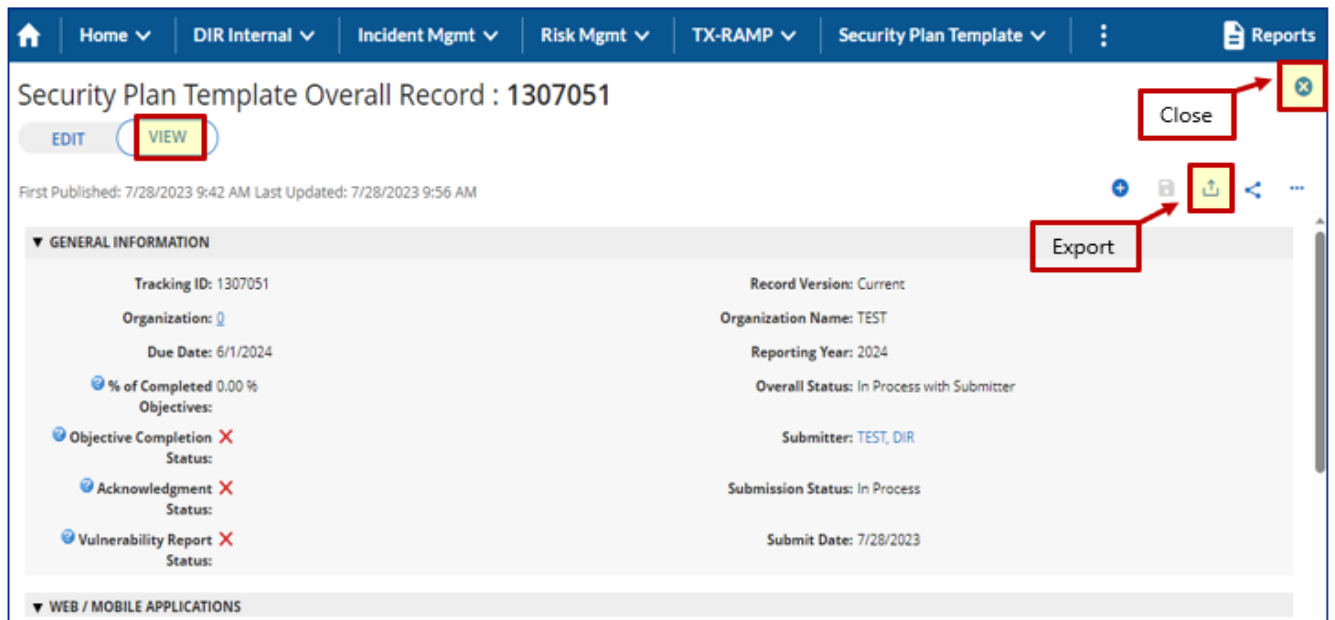


Figure 4: Security Plan Template View Mode

Edit Mode

Security Plan Template Overall Record : 1307051

EDIT VIEW SAVE SAVE AND CLOSE SUBMIT AGENCY SECURITY PLAN

First Published: 7/28/2023 9:42 AM Last Updated: 7/28/2023 9:56 AM

Due Date: 5/1/2024 Reporting Year: 2024

% of Completed 0.00 % Overall Status: In Process with Submitter

Objectives: Objective Completion Status: Acknowledgment Status: Vulnerability Report Status: Submitter: TEST, DIR Submission Status: In Process Submit Date: 7/28/2023

WEB / MOBILE APPLICATIONS

Confidential Internet: Does the Agency plan to implement any internet-accessible web applications (excluding Websites: internal intranets) that process sensitive personal, personally identifiable, or confidential information within the next biennium? Yes No

Confidential Mobile: Does the Agency plan to implement any mobile applications that process sensitive personal, personally identifiable, or confidential information within the next biennium? Yes No

SECURITY PLAN OBJECTIVES

Tracking ID	Objective #	Security Objective	% = 100	% of Agency at Lvl 0	% of Agency at Lvl 1	% of Agency at Lvl 2	% of Agency at Lvl 3	% of Agency at Lvl 4	% of Agency at Lvl 5	Organizational Priority	Roadmap Status	Roadmap
1307114			Not Comy									

Figure 5: Security Plan Template Edit Mode

SPECTRIM Support & Tips

- It's best to type directly into the password field as copying text and using password vaults can sometimes cause issues.
- Do not use the browser's controls; use the "x" in the top right corner to navigate to the previous screen.
- Save often, particularly if many fields have been completed or you've been working in the system for an extended period.
- Accounts become inactive after 60 days of not logging into the system.
- Accounts become locked after 5 failed attempts.
- Locked and inactive accounts will render the self-service password reset function inoperable. If you suspect your account is inactive or locked, you will need to contact GRC@dir.texas.gov or have an active user open an *Archer Support Request* in the portal on your behalf to have your account re-activated.
- The system will send you a reminder to log in and keep your account active 10 days prior to and the day before your account becomes inactive. It is recommended to log in at that time to prevent your account from becoming inactive. Inactive accounts will not receive

automated notifications (e.g., NSOC incident alerts) so it is best to try to keep your account active.

- Help text may be found in various formats throughout the portal. If a field has an icon with a question mark next to it, then clicking on that icon will prompt additional help text/context. Additionally, hovering over certain field titles will sometimes display guidance.

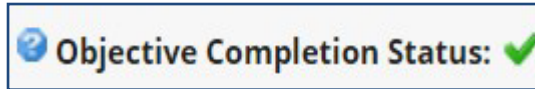


Figure 6: Help Text Icon Example

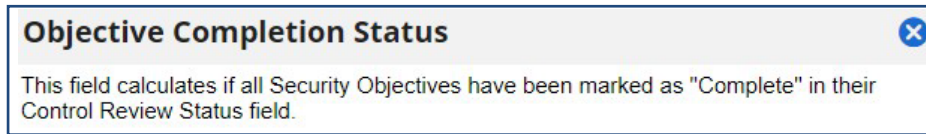


Figure 7: Help Text Popup Example

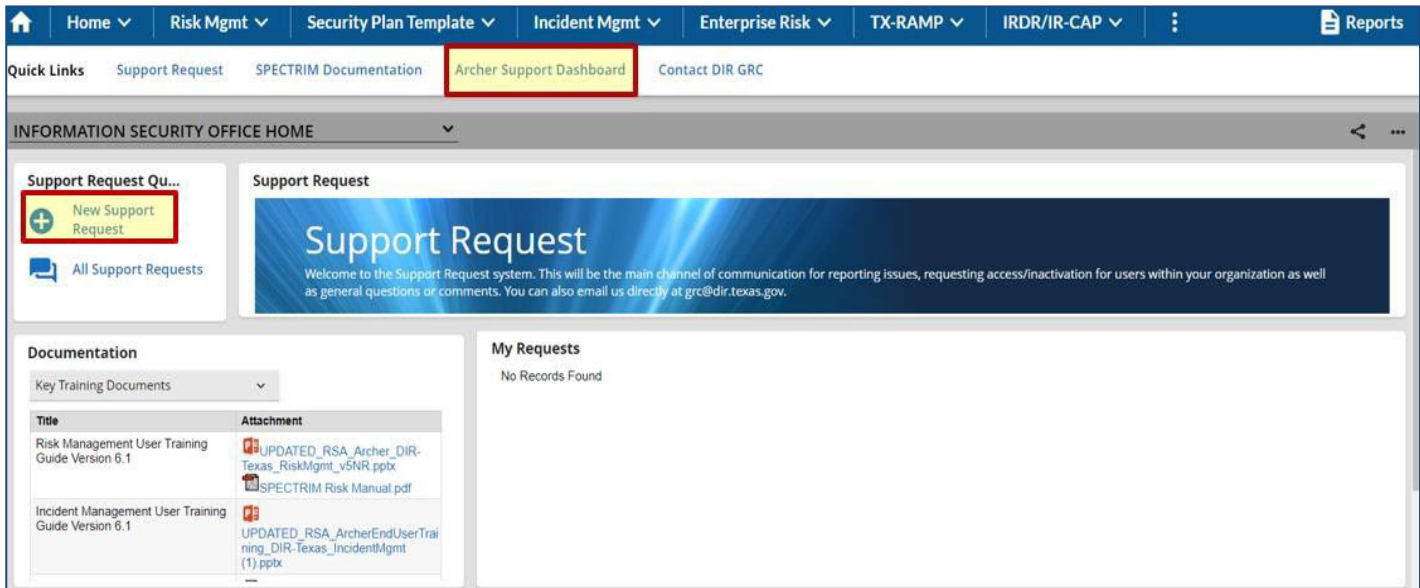


Figure 8: Archer Support Dashboard

Security Plan Dashboard & Reports

The *Security Plan Template Dashboard* allows you to track the completion progress of your agency's security plan. The Quick Links featured in this dashboard provide links to inline edit reports for a quick way to make updates to your organization's key controls in one view.

The screenshot shows the 'SECURITY PLAN' dashboard. It features a 'Security Plan Template Summary' card with a blue background and white text. To the right, a 'Number of Inco...' card displays the number '542'. Further right, a 'Security Plan T...' card contains three links: 'Click to Complete All Security Objective Sections', 'Click to Complete Objective Maturity Levels', and 'Click to Complete Roadmap Section'. Below these is the 'Security Plan Template Overall Record' section, which includes a dropdown menu for 'Current Overall Security Plan Template' and a table with columns: Tracking ID, Organization, Organization Name, Overall Status, Due Date, % of Completed Objectives, Objective Completion Status, Acknowledgment Status, and Vulnerability Report Status. The table shows one record with Tracking ID 1307051, Organization 0, Organization Name TEST, Overall Status 'In Process with Submitter', Due Date 6/1/2024, % of Completed Objectives 0.00 %, Objective Completion Status X, Acknowledgment Status X, and Vulnerability Report Status X.

Figure 7: Dashboard Example

The *Security Plan Template Overall Record iView* displays your organization's current Security Plan Template Overall Record. Each organization needs to submit 42 Key Objectives as well as an Agency Vulnerability Report, so instead of submitting each of those records individually, DIR has created one Security Plan Template Overall Record to allow you to submit all objective and vulnerability report records at once. Additionally, you may use the dropdown menu in the iView to view previously submitted Security Plans.

The screenshot shows the 'Security Plan Template Overall Record' iView. It has a top navigation bar with buttons for 'SAVE', 'MODIFY', 'NEW REPORT', and 'RELATED REPORTS'. Below the navigation bar is a table with columns: Tracking ID, Organization, Organization Name, Record Version, Due Date, Reporting Year, Overall Status, % of Completed Objectives, Objective Completion Status, and Acknowledgment Status. The table shows two records: one with Tracking ID 1028040, Organization 0, Organization Name TEST, Record Version Current, Due Date 6/1/2022, Reporting Year 2022, Overall Status Completed, % of Completed Objectives 100.00 %, Objective Completion Status checkmark, and Acknowledgment Status checkmark; and another with Tracking ID 1307051, Organization 0, Organization Name TEST, Record Version Current, Due Date 6/1/2024, Reporting Year 2024, Overall Status 'In Process with Submitter', % of Completed Objectives 0.00 %, Objective Completion Status X, and Acknowledgment Status X. The 'Reporting Year' column is highlighted with a red box.

Figure 8: Dashboard Overall Record Listing

The *Security Plan Template iView* displays each current Security Objective for easy access to a specific record, if necessary. Reports in this iView display information like the Control Review Status and Organizational Priority of each objective, as well as a listing of all archived security objectives from previously submitted security plans.

Security Plan Content

The Security Plan Template is composed of two applications and one questionnaire, each of which is described in detail below. Additional information on agency security planning can be found on the [DIR Agency Security Plan Webpage](#).

Texas Cybersecurity Framework

The Agency Security Plan template developed by DIR was created through collaboration between government and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies.

The template is divided into five concurrent and continuous functions, which are the same as the National Institute of Standards and Technology (NIST): Identify, Protect, Detect, Respond, and Recover. Within these five areas, DIR has established 40 distinct security objectives. A complete list of the [Control Objectives Descriptions](#) can be found on the DIR website.

A large component of the security plan template involves assessing the degree of maturity across the Texas Cybersecurity Framework security objectives. Organizations can split percentages across the maturity spectrum, provided that the overall percentage totals 100% for each security objective. For example, if one division within an organization comprised of 10 divisions has exceptional maturity for an objective, but the rest would fall into the initial maturity level then the organization may elect to input 10% for Level 5 and 90% for Level 1. This approach allows for some flexibility in the evaluation process, although the resulting security objective average will not be representative of the maturity distribution.

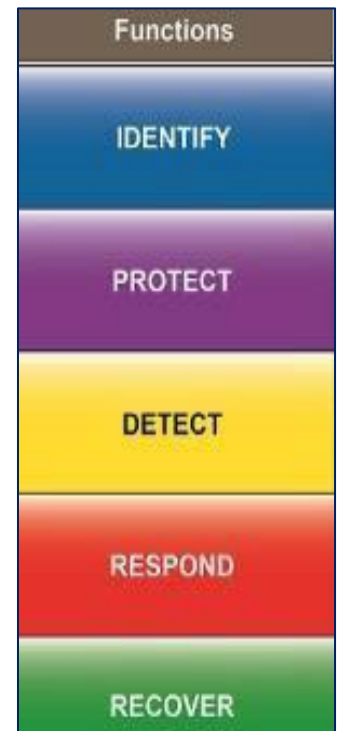


Figure 9: TCF Functional Areas

Security Plan Template Overall Record

General Information

The security plan template overall record contains links to the other components of the security plan (security plan objectives, vulnerability report, etc.). This record allows the organization to track its progress while evaluating the individual security objectives. The overall record also contains a few additional fields that fulfill general reporting requirements.

Security Objectives Inline Edit Report

Organizations can enter the percentage of maturity for each security objective directly from the security plan template overall record via an inline edit report or drill into each security plan template (security objective) record individually to view more information about the objective and complete the associated fields.

The inline edit report allows the organization to enter the percentage of the organization that falls in each pre-defined level of maturity based on the Texas Cybersecurity Framework maturity levels. The report also allows the organization to enter the security objective priority, provide roadmap details, and mark control review status as complete. NOTE: the inline edit report does not provide the same level of detail as reviewing the individual security plan template (security objective) records, which include the individual associated controls and other fields.

Security Objective	% = 100	Control Review Status	% of Agency at Lvl 0	% of Agency at Lvl 1	% of Agency at Lvl 2	% of Agency at Lvl 3	% of Agency at Lvl 4	% of Agency at Lvl 5	Organizational Priority	Roadmap Status
Privacy and Confidentiality	✔	Complete	0	0	30	40	30	0	Medium	Not Started

Figure 10: Inline Edit Report Example

Data Security Plan Questions

The overall security plan template record contains two questions that ask whether the organization plans to implement web or mobile applications that process sensitive or confidential information within the next biennium. If an organization responds affirmatively to either of these questions, four additional security objectives are created to fulfill the data security plan requirements of [Section 2054.516, Government Code](#). Additionally, the organization can indicate whether they would be interested in leveraging DIR’s Managed Security Services program to conduct penetration and vulnerability testing prior to implementing the application.

Executive Written Acknowledgement of Risk

[Subsection 2054.133\(e\)](#) requires that agencies include a written acknowledgement of risks identified during the planning process signed by the organization’s executive staff. DIR has provided a standard Executive Written [Acknowledgement Form](#) that can be used to obtain the appropriate signatures and upload via a field within the security plan template overall record. The written acknowledgment form may be adjusted to include more executive signature blocks if necessary. Additionally, within the *Management Approval and Acknowledgment Section* there are multiple fields for detailing the approval and acknowledgment of the security plan.

Security Plan Template (Objectives)

Each objective (40 core objectives, 4 conditional, 2 new) has its own record that asks the organization to assess the security objective’s maturity on a scale from 0 (Non-existent) to 5 (Optimized). For objectives that are designated as either Level 4 (Risk-based) or Level 5 (Optimized), the organization is required to input details as to how the effectiveness and efficiency of the objective is measured.

Note: For organizations that submitted a 2022 Security Plan, each 2024 Security Objective has been pre-populated with the previous reporting period’s information. You will need to update each objective to reflect the current maturity of each objective.

The organization is also asked to describe relevant control activities, identify challenges to implementation, and provide roadmap details or actions the organization plans to take to improve the maturity associated with the security objective.

▼ GENERAL INFORMATION	
Tracking ID: 1307114	Record Version: Current
Organization: Q	Organization Name: TEST
Functional Area:	Reporting Year: 2024
Objective #:	
Security Objective:	
Definition/Objective:	
<input checked="" type="checkbox"/> % = 100: ●	<input checked="" type="checkbox"/> Objective Review Open Status:
▼ RELEVANT CONTROLS	
<input checked="" type="checkbox"/> Relevant Control Activities in Place:	

Figure 11: Security Objective General Info & Relevant Control Fields

Under the “Relevant Controls” section of the security objective records, there is a listing of the associated DIR controls catalog (control standards). These control standard records allow you to view any risk assessment findings associated to each control to assist in determining the maturity of each objective. Be sure to click on “View All” to see the full listing of associated controls.


▼ SCORES/RESULTS							
 This section shows the percentage complete as well as the average of the percentages in each section. It also shows the number of findings that are associated with the security objective that is being assessed.							
Total Percentage of All Maturity Levels: 100 %				Average Maturity : 2.94			
Total Open Findings: 0				Total All Findings: 1			
▼ ASSOCIATED CONTROLS Add New Lookup View All							
Control Name	Control Number	Organization	Functional Area	Functional Sub-Area	Total Open Findings	Total All Findings	State Implementation Date
Accounting of Disclosures	AR-08-0	Q	Identify	Privacy and Confidentiality	0	0	
Consent	IP-01-0	Q	Identify	Privacy and Confidentiality	0	0	
Data Integrity and Data Integrity Board	DI-02-0	Q	Identify	Privacy and Confidentiality	0	0	
Data Quality	DI-01-0	Q	Identify	Enterprise Security Policy, Standards and Guidelines Privacy and Confidentiality	0	0	
Data Retention and Disposal	DM-02-0	Q	Identify	Privacy and Confidentiality	0	0	

Figure 13: Security Objective Associated Controls

After reviewing the number of associated control findings and previously supplied data, evaluate your organization’s security objective maturity on a scale of 0 to 5, providing percentages for each level. Your total percentage across all levels must add up to 100. The % = 100 field in the “General Information” section provides a snapshot into the total maturity percentage for the security objective.

Total Percentage of All Maturity Levels: 100 %	Average Maturity : 2.94
Total Open Findings: 0	Total All Findings: 1

Figure 12: Maturity % Indicator Icons

▼ LEVEL 0: NON EXISTENT	
<p>Level 0 Pattern Controls: Privacy Policies do not exist</p> <p>% of Agency at Lvl 0: There is no evidence of the organization meeting the objective.</p>	<input type="text" value="2"/> %
▼ LEVEL 1: INITIAL	
<p>Level 1 Pattern Controls: Privacy is rarely considered when determining the controls placed on information</p> <p>% of Agency at Lvl 1: The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.</p>	<input type="text" value="2"/> %
▼ LEVEL 2: REPEATABLE	
<p>Level 2 Pattern Controls: Privacy is treated in a uniform manner through the organization, but is mainly a reaction to external incidents or regulations.</p> <p>% of Agency at Lvl 2: The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.</p>	<input type="text" value="2"/> %
▼ LEVEL 3: DEFINED	
<p>Level 3 Pattern Controls: Applicable privacy standards and regulations are incorporated into the organizations security program</p> <p>% of Agency at Lvl 3: The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.</p>	<input type="text" value="90"/> %

Figure 14: Example Security Objective Pattern Control Definitions

After assessing the maturity of the objective, the organization should describe any challenges they face when implementing the objective, attach documentation and provide comments surrounding those challenges.

Challenges to Implementation:

- Inadequate Funding
- Inadequate Staffing
- Lack of Planning
- Competing Priorities - Financial
- Competing Priorities - Staffing/Time
- Inadequate Knowledge, Skills, or Abilities of Current Staff
- Lack of Interest
- Lack of Management Support/Sponsorship
- Organizational Reluctance to Change
- Technical Barriers - Incompatibility
- Technical Barriers - Legacy Systems
- Other

None

Challenges to Implementation Comments:

Figure 15: Challenges to Implementation Example

Finally, the Roadmap section should be used to describe and track any plan(s) to improve the implementation and maturity posture of an objective. You can designate the Organizational Priority, select target Start and End Dates, and provide a plan in the roadmap text box. Attachments can also be uploaded to support the roadmap.

ROADMAP

Organizational Priority: Medium

Start Date: 7/28/2023

End Date:

Roadmap Status: In Progress

Roadmap: We plan on implementing a systematic approach that will ensure compliance with this security objective Sec. 411.00431.

Roadmap Attachments

Name	Size	Type	Upload Date
No Records Found			

Figure 16: Roadmap Example

Control Review Status

Each individual control has a selection option for when the security objective assessment and planning details have been completed. To indicate that the security objective is finalized, the submitter should change the selection option in the *Control Review Status* field to "Complete" and save the record. Note that the % = 100 field should have a green check mark next to it before saving the completed record.

GENERAL INFORMATION

Tracking ID: 1307114

Record Version: Current

Organization: [input] Add

Organization Name: TEST

Functional Area:

Reporting Year: 2024

Objective #:

Security Objective:

Definition/Objective:

☑ % = 100: ●

SECURITY OBJECTIVE REVIEW COMPLETED

Or

Objective Review Not Completed Complete

Status:

Figure 17: Control Review Status Field

Vulnerability Report Questionnaire

[Section 2054.077, Government Code](#) requires information security officers to prepare or have prepared a report, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use. The Vulnerability Report questionnaire may be completed through the security plan template overall record by selecting the Add New button in the top right corner of the "Vulnerability Report" section.

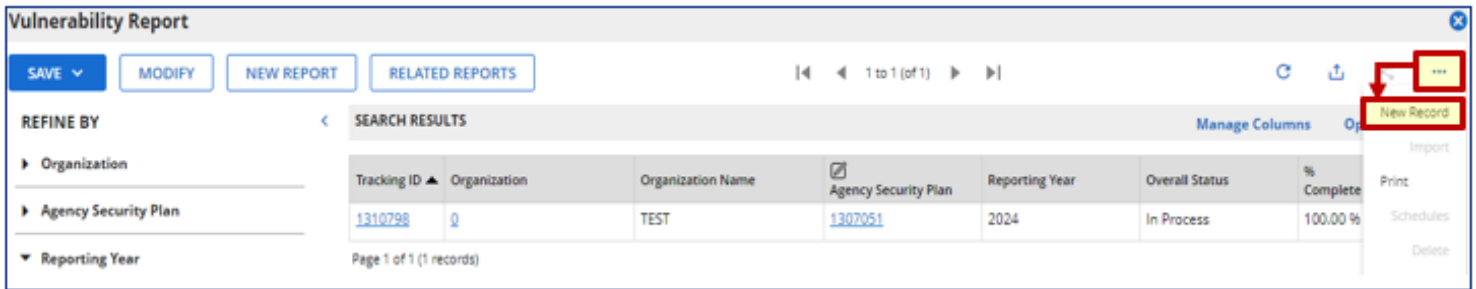


Figure 18: Add/Launch Vulnerability Report

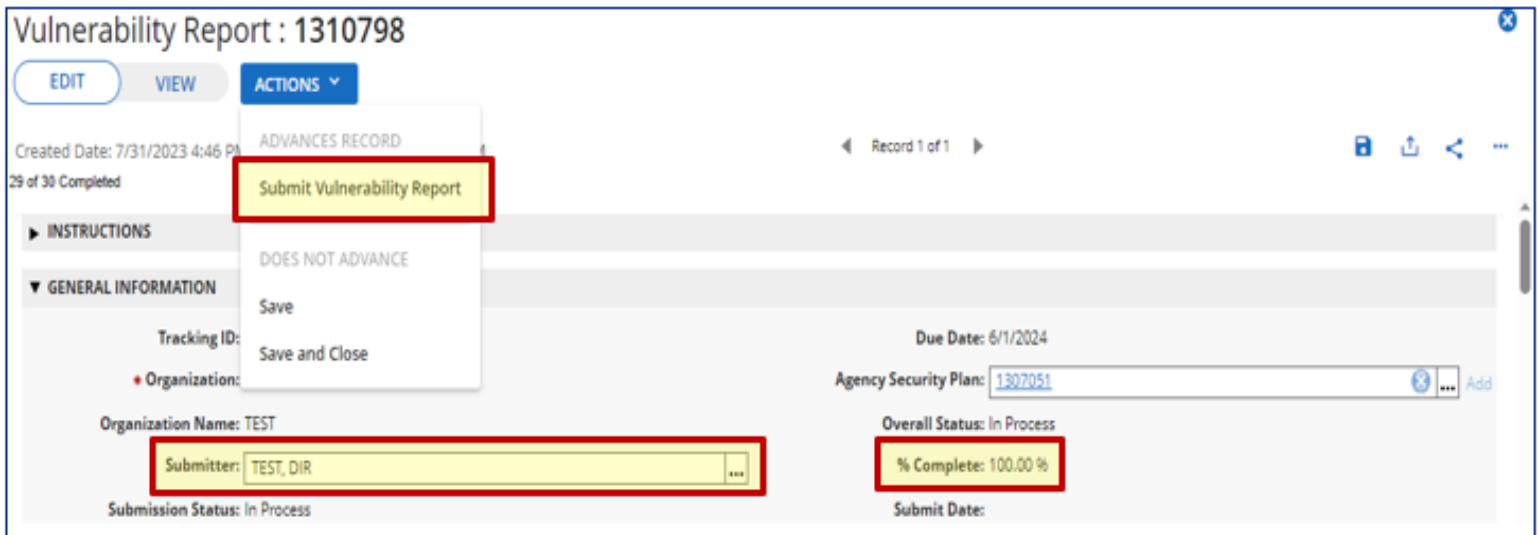


Figure 19: Vulnerability Report Required Fields & Submission Button

The questionnaire contains high-level questions concerning the organization’s vulnerability management practices and allows the user to upload additional files if necessary. Once the submitter field has been populated and all the questions answered, the user should select the “Submit Vulnerability Report” button in the top left corner of the questionnaire.

▼ VULNERABILITY REPORT ASSESSMENT

VR-001: What systems or applications does the agency perform vulnerability assessments and scans on prior to Production implementation? Check all that apply.

- IoT (Network Connected) Devices
- Mobile Applications
- Network Devices
- Servers
- Web Applications
- Workstations

VR-002: How often does the agency conduct web application vulnerability scanning?

- Never
- Prior to Implementation Only
- Monthly
- Quarterly
- Annually
- Biennially
- Ad-Hoc

Figure 20: Vulnerability Report Question Example

Submission & Reporting

Submitting the Plan to DIR

The overall security plan cannot be submitted until the % of controls reviewed equals 100%, the vulnerability report questionnaire is submitted, and the executive acknowledgment of risk form has been completed & uploaded to the attachment field. In the "General Information" section, the *Objective Completion Status*, *Acknowledgment Status*, and *Vulnerability Report Status* fields are used to guide users through the Security Plan process.

The screenshot shows the "General Information" section of a Security Plan Template Overall Record for ID 1307051. The record is published on 7/28/2023 at 9:42 AM and last updated on 7/28/2023 at 9:56 AM. It is record 5 of 904. The section includes fields for Tracking ID (1307051), Organization (empty), Due Date (6/1/2024), Record Version (Current), Organization Name (TEST), Reporting Year (2024), Overall Status (In Process with Submitter), Submitter (TEST, DIR), Submission Status (In Process), and Submit Date (7/28/2023). The "Objectives" section shows three items: Objective Completion (Status: X), Acknowledgment Status (Status: X), and Vulnerability Report (Status: checkmark). The "% of Completed" is 0.00%.

Figure 21: Overall Record General Information Section

Once the Objective Completion Status, Acknowledgment Status, and Vulnerability Report Status fields have all been marked as "Completed" and are designated with green checkmarks, the Security Plan may be submitted.

The screenshot shows the "General Information" section of a Security Plan Template Overall Record for ID 1307051. The record is published on 7/28/2023 at 9:42 AM and last updated on 7/28/2023 at 9:56 AM. It is record 5 of 904. The section includes fields for Tracking ID (1307051), Organization (empty), Due Date (6/1/2024), Record Version (Current), Organization Name (TEST), Reporting Year (2024), Overall Status (Completed), Submitter (TEST, DIR), Submission Status (In Process), and Submit Date (7/28/2023). The "Objectives" section shows three items: Objective Completion (Status: In Process), Acknowledgment Status (Status: X), and Vulnerability Report (Status: checkmark). The "% of Completed" is 4.76%. A red box highlights the "Objective Completion In Process" status, and another red box highlights the "Submission Status: In Process" dropdown menu.

Figure 22: Submission Indicators and Status Field

% Complete and Objective Completion Status

Within the "General Information" section of the overall security plan template record, the % Complete field automatically calculates the number of security objectives (security plan template records) that have had their *Control Review Status* marked as "complete." This allows the user to have a general understanding of how many security objectives have been completed relative to the number of required security objectives to be completed. The % Complete field drives the *Objective Completion Status*. If no security objectives have been reviewed, the Objective Completion Status is "Not Started" and represented by a red X. Once all objectives have been reviewed and the % Complete is 100%, the Objective Completion Status is "Completed" and displays a green checkmark.

Acknowledgment Status

The *Acknowledgment Status* field is driven off the *Agency Security Plan Acknowledgment Form* field. Once a signed, Executive Acknowledgment has been attached and the Overall Security Plan saved, the *Acknowledgment Status* will change to "Completed."

MANAGEMENT APPROVAL AND ACKNOWLEDGMENT

Approved By: Name 1

Approval Date: 7/31/2023

Approval Comments:

Agency Head: Name 2

CFO: Name 3

Additional Acknowledgments: Notes about Acknowledgment

Acknowledgment of Risk: Acknowledged

Acknowledgment Comments:

[Click here to download the Acknowledgment Form](#)

Agency Security Plan Acknowledgment Form: Add

Figure 23: Executive Acknowledgment Form Upload

Vulnerability Report Status

The *Vulnerability Report Status* field determines if a Vulnerability Report questionnaire has been submitted by the agency. If no Vulnerability Report has been added, the *Vulnerability Report Status* is "Not Started" and displays a red X. Once the Vulnerability Report has been completed and submitted, the *Vulnerability Report Status* will change to "Completed" and will display a green checkmark.

Exporting/Reporting

Once the security plan template has been completed, the organization can export directly from the system into mail merged word documents for streamlined reporting. Additionally, non-mail merged exports can be performed when the "export" button is not shaded out in the top right corner of the screen:

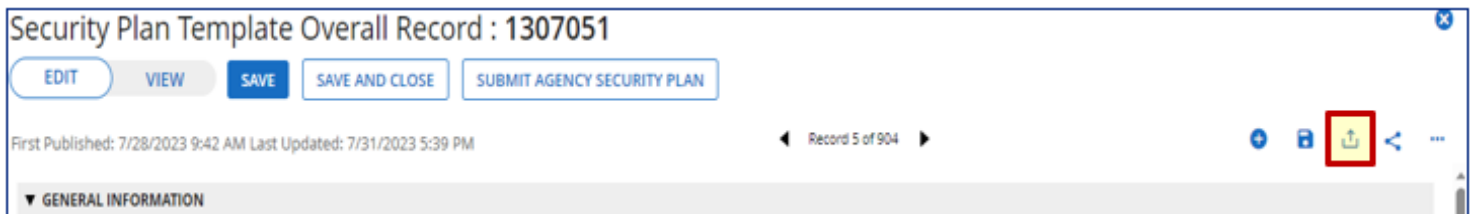


Figure 24: Overall Security Plan Record Export Button

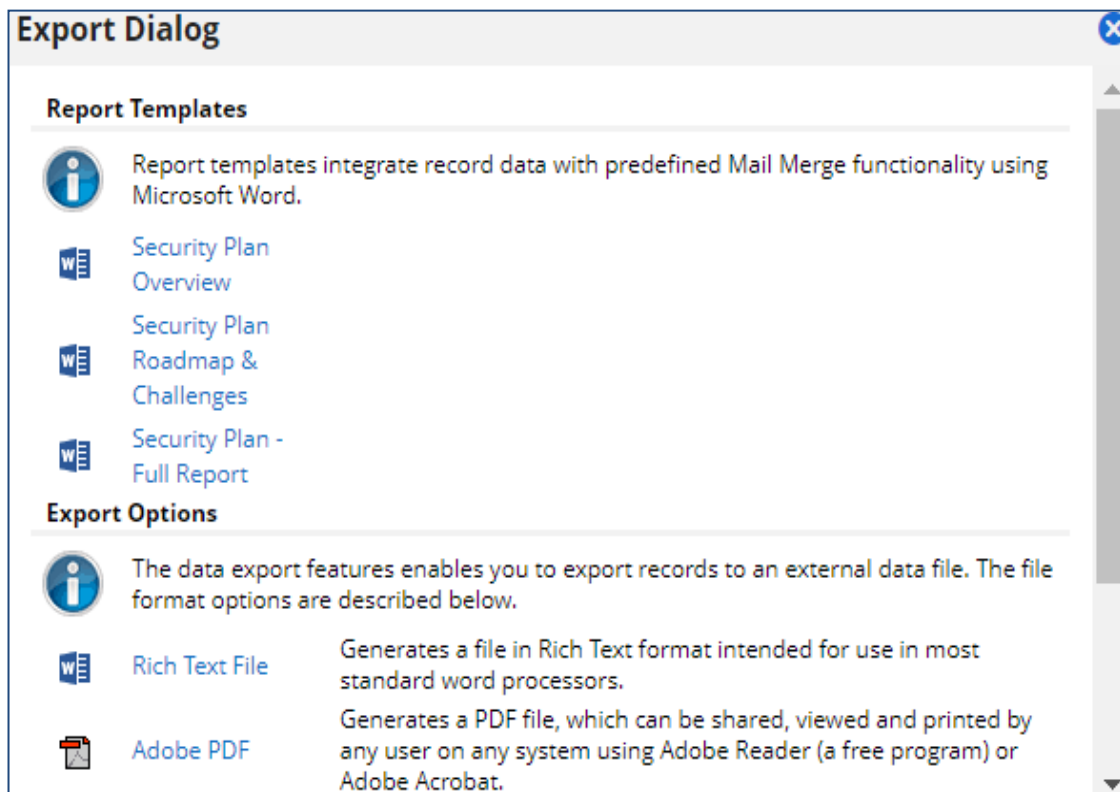


Figure 25: Security Plan Mail Merge Report Options

Summary Export

The summary/overview export can be performed from the overall security plan template record by selecting the “export” button and the appropriate mail merge report. The downloaded word document will contain the maturity distributions for each security objective, along with roadmap details, and challenges for implementation as seen below.

TEST								
2024 SECURITY PLAN								
Submitted On: 05/30/2024 by State Agency, ISO								
Objective	Functional Area	Maturity Level	L0 %	L1 %	L2 %	L3 %	L4 %	L5 %
Privacy and Confidentiality	Identify	2.32	20	18	2	30	30	0
Roadmap: We plan on implementing a systematic approach that will ensure compliance with this security objective. Sec. 411.00431. Challenges to Implementation: Inadequate Funding Inadequate Staffing Competing Priorities - Financial Technical Barriers - Incompatibility Technical Barriers - Legacy Systems								
Data Classification	Identify	2.19	10	30	15	24	18	3
Roadmap: Challenges to Implementation: Inadequate Funding Competing Priorities - Financial								

Figure 26: Security Plan Summary Export Example

Detailed Export

Through the same mechanism, a detailed export of the security plan template is available. The “Security Plan – Full Report” selection will download a document containing all the plan fields for each of the security objectives as shown below:

Tracking ID	1028063
Organization Name	TEST
Objective	Privacy and Confidentiality
Functional Area	Identify
Overall Maturity Level	2.94
Relevant Control Activities in Place	The controls that we have in place regarding privacy and confidentiality are: xyz.
Level 0 Pattern Control	Privacy Policies do not exist
Level 0 %	2
Level 1 Pattern Control	Privacy is rarely considered when determining the controls placed on information
Level 1 %	2
Level 2 Pattern Control	Privacy is treated in a uniform manner through the organization, but is mainly a reaction to external incidents or regulations.
Level 2 %	2
Level 3 Pattern Control	Applicable privacy standards and regulations are incorporated into the organizations security program
Level 3%	90
Level 4 Pattern Control	The organizational structure supports a focus on privacy and confidentiality as a distinct discipline.
Level 4 %	2
How is Effectiveness Measured	in this way
Level 5 Pattern Control	Privacy is treated by the organization as a business output.
Level 5 %	2
How is Efficiency Measured	this is how
Controls Needed	We plan on implementing a systematic approach that will ensure compliance with this security objective. Sec. 411.00431.
Organizational Priority	Medium
Challenges to Implementation	<ul style="list-style-type: none"> Inadequate Funding Inadequate Staffing

Figure 27: Security Plan Detailed Export Example

Roadmap & Challenges Export

The final customized export from the overall security plan template record focuses on the roadmap section for each security objective. This export lists each of the security objective’s maturity, along with the roadmap details, and challenges to implementation as seen in the example below:

Objective	Maturity Levels	Controls Needed	Challenges to Implementation
Privacy and Confidentiality	2.94	We plan on implementing a systematic approach that will ensure compliance with this security objective. Sec. 411.00431.	<ul style="list-style-type: none"> Inadequate Funding Inadequate Staffing
Data Classification	4	This is what we are doing ...	<ul style="list-style-type: none"> Competing Priorities

Figure 28: Security Plan Roadmap Export Example

Resources and Assistance

Resources

Agency Security Plan Webpage

<https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=5>

Executive Written Acknowledgement Form

<https://prod.dir.texas.gov/resource-library-item/agency-security-plan-executive-acknowledgement-2022>

Texas Cybersecurity Framework Controls and Definitions

<https://dir.texas.gov/resource-library-item/texas-cybersecurity-framework-controls-and-definitions>

Security Plan Template Excel Version

<https://dir.texas.gov/resource-library-item/information-security-plan-template>

Vulnerability Report Electronic Version

<https://dir.texas.gov/resource-library-item/2022-security-plan-vulnerability-report-questionnaire>

Support

DIR GRC Team

Contact GRC@dir.texas.gov for questions regarding the Agency Security Plan.

SPECTRIM Support Requests

For SPECTRIM technical assistance (e.g., password resets, account creation/deletion, etc.) open an *Archer Support Request* within the portal or contact GRC@dir.texas.gov.

Table of Figures

Figure 1: SPECTRIM Login Page.....	2
Figure 2: Security Plan Template Workspace Navigation.....	3
Figure 3: Security Plan Template Dashboard.....	4
Figure 4: Security Plan Template View Mode.....	4
Figure 5: Security Plan Template Edit Mode.....	5
Figure 6: Help Text Icon Example.....	6
Figure 8: Archer Support Dashboard.....	6
Figure 7: Help Text Popup Example.....	6
Figure 9: Dashboard Example.....	7
Figure 10: Dashboard Overall Record Listing.....	7
Figure 11: TCF Functional Areas.....	8
Figure 12: Inline Edit Report Example.....	9
Figure 13: Security Objective General Info & Relevant Control Fields.....	10
Figure 15: Maturity % Indicator Icons.....	11
Figure 14: Security Objective Associated Controls.....	11
Figure 16: Example Security Objective Pattern Control Definitions.....	12
Figure 17: Challenges to Implementation Example.....	12
Figure 18: Roadmap Example.....	13
Figure 19: Control Review Status Field.....	13
Figure 20: Add/Launch Vulnerability Report.....	14
Figure 21: Vulnerability Report Required Fields & Submission Button.....	14
Figure 22: Vulnerability Report Question Example.....	15
Figure 23: Overall Record General Information Section.....	16
Figure 24: Submission Indicators and Status Field.....	16
Figure 25: Executive Acknowledgment Form Upload.....	17
Figure 26: Overall Security Plan Record Export Button.....	18
Figure 27: Security Plan Mail Merge Report Options.....	18
Figure 28: Security Plan Summary Export Example.....	19
Figure 29: Security Plan Detailed Export Example.....	20
Figure 30: Security Plan Roadmap Export Example.....	20

Version History

Version	Publish Date	Comments
1.0	2019-09-05	First publication
2.0	2022-03-16	Updates to screenshot links
2.1	2022-05-19	Updates to links and SPECTRIM login information
2.2	2023-09-01	Updates to format, layout, grammar, and links for 2024 plan

Table 1: Document Version History