

**2020 SECURITY PLAN
TEMPLATE INSTRUCTIONS
SUBMISSION DEADLINE:
6/1/2020**

TABLE OF CONTENTS

Introduction.....	3
Required Reporting	3
Reporting Tool.....	3
Logging into the Portal.....	3
Portal Navigation	4
SPECTRIM Support & Tips	7
2020 Security Plan Changes.....	8
Community College Reporting	8
Submission Deadline Change	8
Additional Security Objectives	8
Associated Controls Review	8
Data Security Plan	9
Higher Education Data Security Policies Removal.....	9
Low Maturity Roadmap.....	9
Vulnerability Report Changes.....	9
SECURITY PLAN DASHBOARD & REPORTS	10
Dashboard	10
Security Plan Content	11
Texas Cybersecurity Framework	11
Security Plan Template Overall Record	11
General Information	11
Security Objectives Inline Edit Report.....	11
Data Security Plan Questions.....	12
Management Approval and Acknowledgement	12
Security Plan Template (Security Objectives).....	12
Vulnerability Report Questionnaire	15
Submission & Reporting	16
Submitting the Plan to DIR	16
% Complete and Objective Completion Status	16
Acknowledgment Status	16
Vulnerability Report Status	17
Exporting/Reporting.....	17
Summary Export	18
Detailed Export	18

Roadmap & Challenges Export.....	19
Resources & Assistance	20
Resources	20
Agency Security Plan Webpage.....	20
Executive Written Acknowledgement Form	20
New Security Objective Pattern Controls	20
Security Objective Control Definitions	20
Security Plan Template Excel Version	20
Vulnerability Report Electronic Version	20
Support.....	20
DIR GRC Team	20
Archer Support Requests	20
Appendix.....	21
Table of Figures	21
Version History	21

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, Texas Government Code;
2. Incorporate the network security services provided by DIR to the agency under Chapter 2059;
3. Identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;
4. Identify risk management and other measures taken to protect the agency's 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 years (June 1, 2020). Additionally, with the implementation of SB 64 (86R), community colleges are subject to the information security provisions of Chapter 2054, Texas Government Code. This change means that community colleges will be required to complete the security plan template and accompanying reporting requirements for the 2020 planning cycle. 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://grc.archer.rsa.com/Default.aspx>

Username: email address

Instance: 20224



Figure 1: SPECTRIM Login Page

Portal Navigation

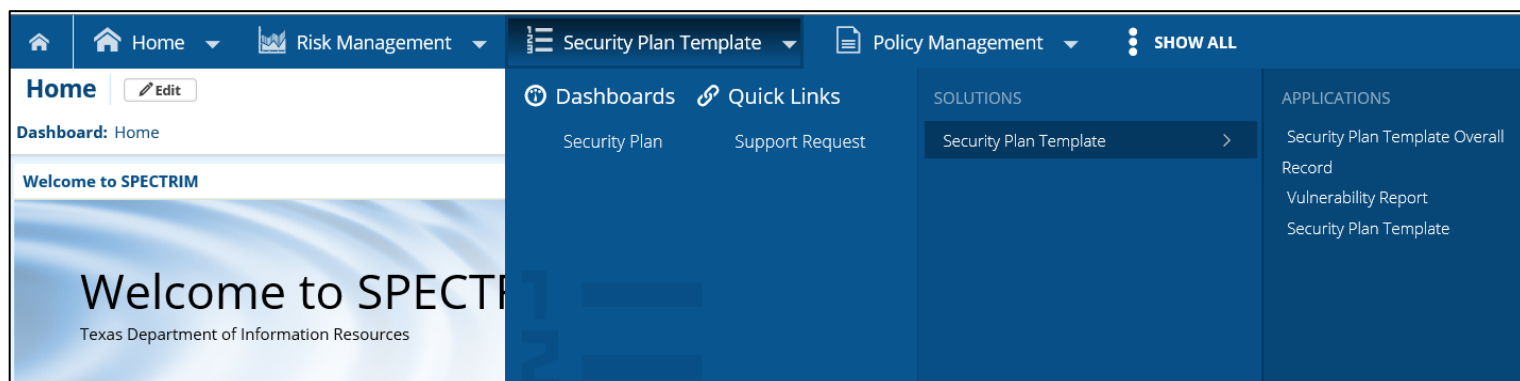


Figure 2: Security Plan Template Workspace Navigation

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.

Note: You may need to click on the “Show all” option 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 your progress as you evaluate security controls.

From the dashboard or the workspace selection items, you can enter into 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.

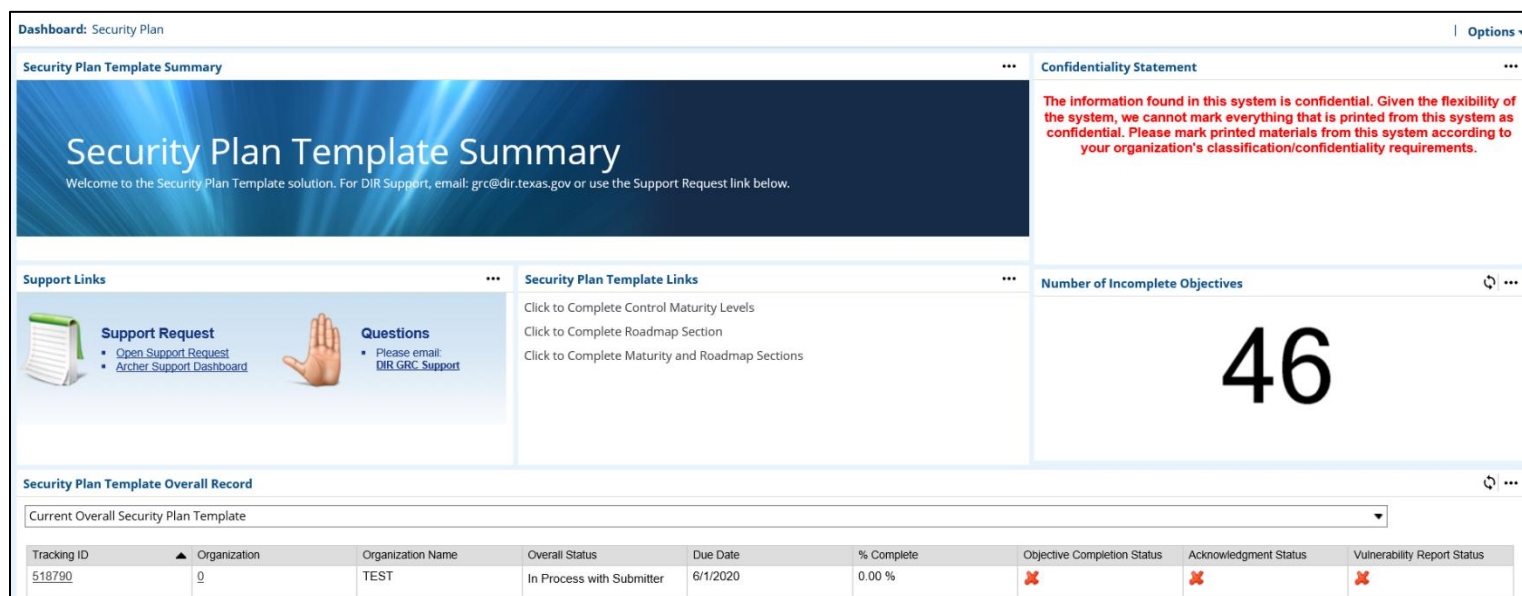


Figure 3: Security Plan Template Dashboard

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. You may also have to 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

Home

Risk Management

Security Plan Template

Policy Management

SHOW ALL

Search

ISO

518790 Security Plan Template Overall Record

NEW COPY SAVE SAVE AND CLOSE EDIT DELETE

RELATED RECALCULATE EXPORT PRINT EMAIL

First Published: 9/4/2019 10:45 AM Last Updated: 9/4/2019 10:45 AM

GENERAL INFORMATION

Tracking ID: 518790

Record Version: Current

Organization:

Organization Name: TEST

Due Date: 6/1/2020

Reporting Year: 2020

% Complete: 0.00 %

Overall Status: In Process with Submitter

Objective Completion Status: ✖

Submitter:

Acknowledgment Status: ✖

Submission Status: In Process

Vulnerability Report Status: ✖

Submit Date:

WEB / MOBILE APPLICATIONS

Confidential Internet Websites: Does the Agency plan to implement any internet-accessible web applications (excluding internal intranets) that process sensitive personal, personally identifiable, or confidential information within the next biennium?
Confidential Mobile Applications: Does the Agency plan to implement any mobile applications that process sensitive personal, personally identifiable, or confidential information within the next biennium?

SECURITY PLAN CONTROLS

Enable Inline Edit View All

Tracking ID	Objective #	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	Roadmap
518791	1	Privacy and Confidentiality	✔	Not Complete	2	2	2	90	2	2	Medium	Not Started	We plan on implementing a systematic

Figure 4: Security Plan Template View Mode

Edit Mode

518790 Security Plan Template Overall Record

NEW COPY SAVE SAVE AND CLOSE VIEW DELETE

EXPORT PRINT EMAIL

First Published: 9/4/2019 10:45 AM Last Updated: 9/4/2019 10:45 AM

GENERAL INFORMATION

Tracking ID: 518790

Organization: Q

Due Date: 6/1/2020

% Complete: 0.00 %

Objective Completion Status: ✖

Acknowledgment Status: ✖

Vulnerability Report Status: ✖

Record Version: Current

Organization Name: TEST

Reporting Year: 2020

Overall Status: In Process with Submitter

Submitter:

Submission Status: In Process

Submit Date:

WEB / MOBILE APPLICATIONS

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

Confidential Mobile Applications: 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 CONTROLS

[View All](#)

Tracking ID	Objective #	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	Roadmap
518791	1	Privacy and Confidentiality	✓	Not Complete	2	2	2	90	2	2	Medium	Not Started	We plan on implementing a systematic approach that will ensure compliance with

Figure 5: Security Plan Template Edit Mode

SPECTRIM Support & Tips

- Password vaults and copying text into the password field can sometimes cause issues. It may be best to type directly into the fields.
- Do not use the browser's controls, use the "X" in the upper-right hand 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 this 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 made 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.

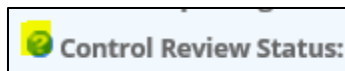


Figure 6: Help Text Icon Example

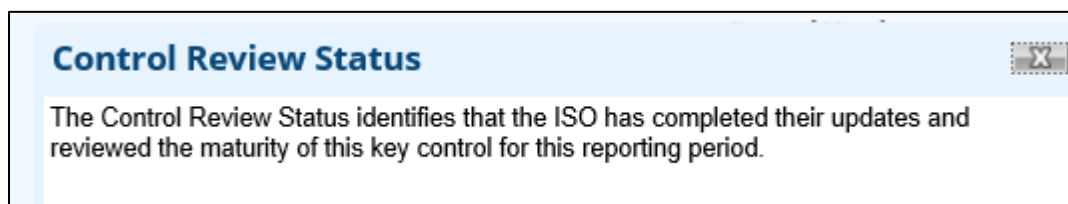


Figure 7: Help Text Popup Example

- Contact GRC@dir.texas.gov for questions and assistance with the SPECTRIM portal.



Figure 8: Archer Support Request iView

2020 SECURITY PLAN CHANGES

Community College Reporting

[SB 64 \(86R\)](#) amended Sec. 2054.0075, Government Code as follows:

Sec. 2054.0075. EXCEPTION: PUBLIC JUNIOR COLLEGE. This chapter does not apply to a public junior college or a public junior college district, except as necessary to comply with information security standards and for participation in shared technology services, including the electronic government project implemented under Subchapter I and statewide technology centers under Subchapter L [~~except as to Section 2054.119, Government Code~~].

This legislation created the requirement for community colleges to complete the information security plan, as well as designate an Information Security Officer and adhere to the information security standards outlined in [Texas Administrative Code Chapter 202](#). If you are a public community college and have not received SPECTRIM credentials to complete the security plan, please contact GRC@dir.texas.gov for additional information.

Submission Deadline Change

[SB 241 \(86R\)](#) amended Sec. 2054.113(c), Government Code as follows:

(c) Not later than June 1 [~~October 15~~] of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the department. Subject to available resources, the department may select a portion of the submitted security plans to be assessed by the department in accordance with department rules.

This legislation changed the statutorily mandated deadline of the information security plan from October 15, of each odd-numbered year to June 1, of each even-numbered year. **This iteration of the security plan is due no later than June 1, 2020.**

Additional Security Objectives

Two additional security objectives are being included in this iteration of the security plan template:

- *Audit Logging and Accountability*
- *Information Systems Currency*

These security objectives were created through conversations with the information security community and advisory groups. To promote standardized year-to-year reporting of maturity scores at the organizational and enterprise level, these security objectives will be assessed in addition to the core Texas Cybersecurity Framework security objectives of prior planning cycles. The following cycle (2022) will seek to remove selected security objectives from the framework and permanently replace them with the two new additions. This approach is intended to reduce the possibility of introducing artificially significant differences in reporting maturity metrics. [The security objective definitions and maturity statements](#) can be located on the DIR website as well as within the SPECTRIM portal.

Associated Controls Review

A systematic review of each security objective's associated security controls was conducted to further align with the Texas Cybersecurity Framework Assessments provided through the DIR Managed Security Services program. The controls listed in the associated controls section of each security objective record have been revised and are intended to assist the organization in its assessment of maturity for a given objective.

Data Security Plan

SB 64 (86R) amended Section 2054.516, Government Code, to consolidate the requirements for state agencies and institutions of higher education concerning the implementation of data security plan for websites or mobile applications that process sensitive or confidential data. This legislation also repealed Section 2054.517, Government Code, which required institutions of higher education that implement a web or mobile application that processes sensitive or confidential data submit their security policy to DIR regarding the protection of this information.

The data security plan requirement is fulfilled by completing the evaluation of the additional security objectives created by responding affirmatively to either of the data security plan requirement questions located within the security plan template overall record:

Confidential Internet Websites: Does the agency plan to implement any internet-accessible web applications (excluding internal intranets) that process sensitive personal, personally identifiable, or confidential information within the next biennium?

Confidential Mobile Applications: Does the agency plan to implement any mobile applications that process sensitive personal, personally identifiable, or confidential information within the next biennium?

Responding affirmatively to these questions prompts four additional security objectives— Beta Testing, Secure Application Development, Penetration Testing, & Vulnerability Testing. The assessment of these objectives fulfills the data security plan requirements of Section 2054.516, Government Code.

Higher Education Data Security Policies Removal

Institutions of higher education are no longer required to submit their web/mobile data security policies per SB 64 (86R) repeal of Section 2054.517, Government Code.

Low Maturity Roadmap

Within the security plan template overall record, a new section titled “objectives with low average maturity” will display the security objectives assessed to have a maturity score of less than 2.0. This section is intended to assist the organization with identifying potential areas of improvement and encourage more thorough roadmap and improvement planning for the identified objectives.

Vulnerability Report Changes

The 2018 Security Plan Template included a suggested, but not mandatory, vulnerability report template and asked agencies to upload their vulnerability reports via a link in the overall security plan template record. DIR has created a *Vulnerability Report Questionnaire* to accompany the 2020 Security Plan Template to promote standardized reporting and derive general insights regarding the identification and treatment of vulnerabilities. The questionnaire contains approximately 15 high-level questions about vulnerability management and provides the option for the agency to upload additional files. An electronic [version of the vulnerability report](#) questions can be located on the DIR website.

SECURITY PLAN DASHBOARD & REPORTS

Dashboard

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.

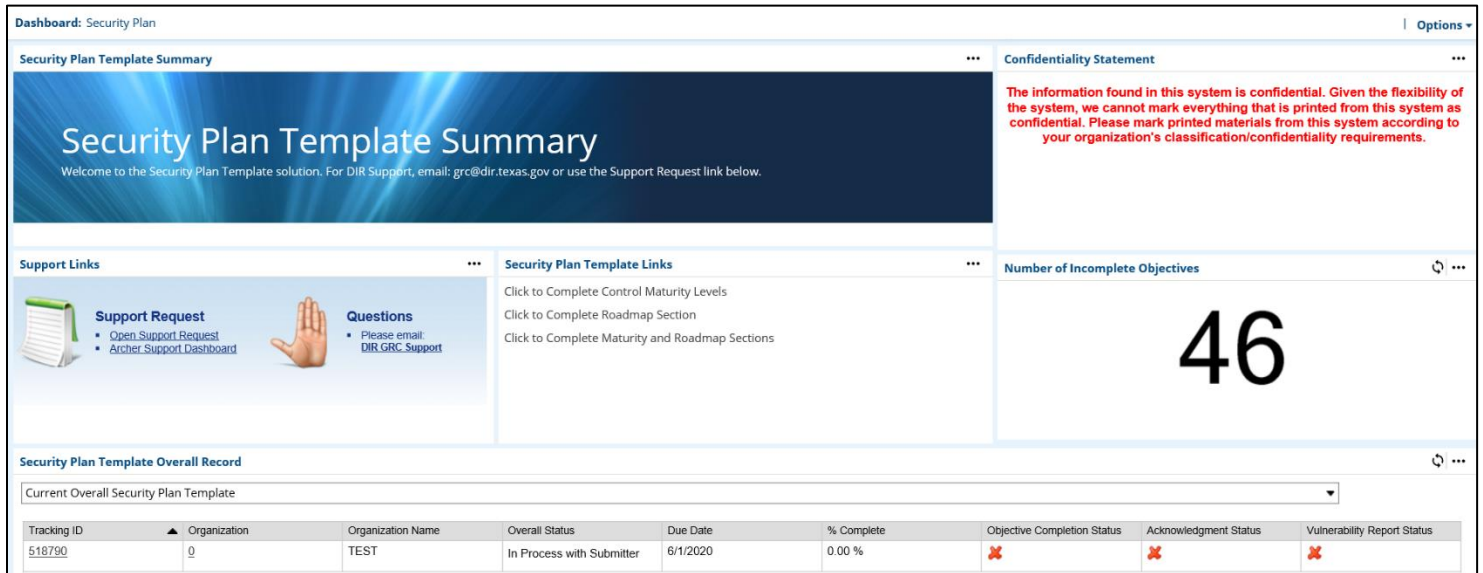


Figure 9: Dashboard Example

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.

Security Plan Template Overall Record						
Archived Security Plan Template Overall Records						
Tracking ID	Organization 1	Organization Name	Record Version	Due Date	Reporting Year 2	
322030	0	TEST	Archived	10/15/2018	2018	
322027	0	TEST	Archived	10/15/2016	2016	

Figure 10: 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 are described in more 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 11: 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 directly 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.

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 12: Inline Edit Report Example

The inline edit report displays asks 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.

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 leverage DIR's Managed Security Services program to conduct penetration and vulnerability testing prior to implementing the application.

Management Approval and Acknowledgement

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 (Security 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 2018 Security Plan, each 2020 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: 518791	Record Version: Current
Organization: <input type="text"/>	Organization Name: TEST
Objective #: 1	Functional Area: Identify
Security Objective: Privacy and Confidentiality	Reporting Year: 2020
% = 100: <input checked="" type="checkbox"/>	Control Review Status: <input type="radio"/> Not Complete <input checked="" type="radio"/> Complete
Definition/Objective: Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.	
▼ RELEVANT CONTROLS	
Relevant Control Activities in Place:	<div>The controls that we have in place regarding privacy and confidentiality are: xyz.</div>

Figure 13: 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 controls (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 control that is being assessed.

Total Percentage of All Maturity 100 %

Average Maturity : 3.30

Levels:

Total All Findings: 2

Total Open Findings: 2

▼ ASSOCIATED CONTROLS

Control Name	Control Number	Organization	Functional Area	Functional Sub-Area	Total Open Findings	Total All Findings	State Implementation Date
Access Control Policy and Procedures	AC-01-0	Q	Identify Protect	Access Control Account Management Enterprise Security Policy, Standards and Guidelines Identification and Authentication Network Access and Perimeter Controls	0	0	2/1/2015
Account Management	AC-02-0	Q	Protect	Access Control Account Management Identification and Authentication Network Access and Perimeter Controls	2	2	2/1/2015

[View All](#)

Figure 14: 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 cross all levels needs to add up to 100. The % = 100 field in the “General Information” section provides a snapshot into the total maturity percentage for the security objective.

If total maturity is <i>less than</i> 100%:	% = 100: 🟡 Open
If total maturity <i>equals</i> 100%:	% = 100: 🟢
If total maturity is <i>greater than</i> 100%:	% = 100: 🔴

Figure 15: Maturity % Indicator Icons

▼ LEVEL 0: NON EXISTENT	
Level 0 Pattern Controls: Privacy Policies do not exist	
% of Agency at Lvl 0: There is no evidence of the organization meeting the objective.	2 %
▼ LEVEL 1: INITIAL	
Level 1 Pattern Controls: Privacy is rarely considered when determining the controls placed on information	
% of Agency at Lvl 1: The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.	2 %
▼ LEVEL 2: REPEATABLE	
Level 2 Pattern Controls: Privacy is treated in a uniform manner through the organization, but is mainly a reaction to external incidents or regulations.	
% 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.	2 %
▼ LEVEL 3: DEFINED	
Level 3 Pattern Controls: Applicable privacy standards and regulations are incorporated into the organizations security program	
% of Agency at Lvl 3: The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.	90 %

Figure 16: Example Security Objective Pattern Control Definitions

After assessing the maturity of the objective, the organization should describe any challenges that they face when implementing the objective, attaching documentation and providing comments surrounding those challenges if necessary.

Figure 17: 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.

Figure 18: Roadmap Example

Control Review Status

Each individual control has a selection option for when the security objective assessment/planning has 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.

Figure 19: 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 upper-right hand side of the "Vulnerability Report" section.

▼ AGENCY VULNERABILITY REPORT							Add New
Tracking ID	Organization	Overall Status	% Complete	Submitter	Submit Date	Vulnerability Report Attachments	
No Records Found							

Figure 20: Add/Launch Vulnerability Report

The questionnaire contains approximately 15 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 upper left-hand corner of the questionnaire.

▼ VULNERABILITY REPORT ASSESSMENT	
VR-001: How often does the agency conduct web application vulnerability scanning?	<input type="radio"/> Never <input checked="" type="radio"/> Prior to Implementation <input type="radio"/> Monthly <input type="radio"/> Quarterly <input type="radio"/> Annually <input type="radio"/> Biennially <input type="radio"/> Ad-Hoc
VR-002: How often does the agency conduct network vulnerability scanning?	<input type="radio"/> Never <input type="radio"/> Monthly <input type="radio"/> Quarterly <input checked="" type="radio"/> Annually <input type="radio"/> Biennially <input type="radio"/> Ad-hoc <input type="radio"/> Continuously

Figure 22: Vulnerability Report Question Example

⚡ Submit Vulnerability Report	
Created Date: 9/4/2019 3:37 PM Last Updated: 9/4/2019 3:41 PM	
► INSTRUCTIONS	
▼ GENERAL INFORMATION	
Tracking ID: 518838	Due Date: 6/1/2020
+ Organization: <u>Q</u>	Agency Security Plan: <u>518790</u>
Organization Name: TEST	Overall Status: In Process
Submitter: <input type="text"/>	% Complete: 100.00 %
Submission Status: In Process	Submit Date:

Figure 21: Vulnerability Report Required Fields & Submission Button

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*, *Acknowledgement Status*, and *Vulnerability Report Status* fields are used to guide users through the Security Plan process.

GENERAL INFORMATION	
Tracking ID: 296160	Record Version: Current
Organization: Q	Organization Name: State Agency for Archer
Due Date: 6/1/2020	Reporting Year: 2020
% Complete: 34.78 %	Overall Status: In Process with Submitter
Objective Completion Status: In Process	Submitter:
Acknowledgment Status: X	Submission Status: In Process
Vulnerability Report Status: ✓	Submit Date:

Figure 23: 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 check-marks, the Security Plan may be submitted.

GENERAL INFORMATION	
Tracking ID: 518790	Record Version: Current
Organization: Q	Organization Name: TEST
Due Date: 6/1/2020	Reporting Year: 2020
% Complete: 100.00 %	Overall Status: In Process with Submitter
Objective Completion Status: ✓	Submitter: State Agency, ISO
Acknowledgment Status: ✓	Submission Status: Completed
Vulnerability Report Status: ✓	Submit Date: 9/4/2019

Figure 24: 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 represented by 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.”

Click here to access the Acknowledgment Form	
Agency Security Plan Acknowledgment Form:	<input type="text"/> Add

Figure 25: 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 represented by a red X. Once the Vulnerability Report has been completed and submitted, the *Vulnerability Report Status* will change to “Completed” and will be represented by 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 of whichever record can be performed when the “export” button is not shaded out in the upper-right hand corner of the screen:

The screenshot displays the '296160 Security Plan Template Overall Record' interface. At the top, there is a toolbar with buttons for NEW, COPY, SAVE, SAVE AND CLOSE, EDIT, DELETE, RELATED, RECALCULATE, EXPORT (highlighted in yellow), PRINT, and EMAIL. Below the toolbar, the 'GENERAL INFORMATION' section shows details such as Tracking ID: 296160, Organization: Q, Due Date: 6/1/2020, Submitter, Submission Status: In Process, and % Complete: 10.87 %. The 'WEB / MOBILE APPLICATIONS' section contains two questions: 'Confidential Internet Websites: Does the Agency plan to implement any internet-accessible web applications (excluding internal intranets) that process sensitive personal, personally identifiable, or confidential information within the next biennium?' (marked with a green checkmark) and 'Confidential Mobile Applications: Does the Agency plan to implement any mobile applications that process sensitive personal, personally identifiable, or confidential information within the next biennium?' (marked with a red dot).

Figure 26: Overall Security Plan Record Export Button

The screenshot shows the 'Security Plan Template Overall Record: Export Options' dialog box. It features a section titled 'Report Templates' with a description: 'Report templates integrate record data with predefined Mail Merge functionality u Word.' Below this, there are three Word document icons with the following titles: 'Security Plan Overview', 'Security Plan Roadmap & Challenges', and 'Security Plan - Full Report'. At the bottom of the dialog, there is a section titled 'Export Options'.

Figure 27: 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. A word document will be downloaded that contains the maturity distributions for each security objective, along with roadmap details, and challenges for implementation as seen below.

State Agency for Archer								
2020 SECURITY PLAN								
Submitted On: by								
Objective	Functional Area	Maturity Level	L0 %	L1 %	L2 %	L3 %	L4 %	L5 %
Privacy and Confidentiality	Identify	3	0	0	30	40	30	0
Roadmap:								
Challenges to Implementation:								
Competing Priorities - Staffing/Time								
Data Classification	Identify	2.3	20	30	0	0	50	0
Roadmap:								
this is what we're doing...								
Challenges to Implementation:								
Critical Information Asset Inventory	Identify	4.5	0	0	0	0	50	50

Figure 28: 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	296161
Organization Name	State Agency for Archer
Objective	Privacy and Confidentiality
Functional Area	Identify
Overall Maturity Level	3
Relevant Control Activities in Place	
Level 0 Pattern Control	Privacy Policies do not exist
Level 0 %	0
Level 1 Pattern Control	Privacy is rarely considered when determining the controls placed on information
Level 1 %	0
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 %	30
Level 3 Pattern Control	Applicable privacy standards and regulations are incorporated into the organizations security program
Level 3 %	40
Level 4 Pattern Control	The organizational structure supports a focus on privacy and confidentiality as a distinct discipline.
Level 4 %	30
How is Effectiveness Measured	this is how
Level 5 Pattern Control	Privacy is treated by the organization as a business output.
Level 5 %	0
How is Efficiency Measured	
Controls Needed	
Organizational Priority	Medium
Challenges to Implementation	<ul style="list-style-type: none"> Competing Priorities - Staffing/Time

Figure 29: 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	3		<ul style="list-style-type: none">• Competing Priorities - Staffing/Time
Data Classification	2.3	this is what we're doing...	<ul style="list-style-type: none">•
Critical Information Asset Inventory	4.5	this is how we plan to address the issues with this control...	<ul style="list-style-type: none">• Inadequate Funding• Lack of Planning• Lack of time available for formal review and training regarding privacy and confidentiality.
Enterprise Security Policy, Standards and Guidelines	0		<ul style="list-style-type: none">•
Control Oversight and Safeguard Assurance	0		<ul style="list-style-type: none">•

Figure 30: Security Plan Roadmap Export Example

RESOURCES & 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://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Agency%20Security%20Plan%20Executive%20Acknowledgement%202020.docx>

New Security Objective Pattern Controls

<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/New%20Security%20Objectives%20Pattern%20Controls%20Definitions%202020%20Security%20Plan%20Template.pdf>

Security Objective Control Definitions

<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Framework%20Controls%20and%20Definitions.pdf>

Security Plan Template Excel Version

<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/FY%202020%20Agency%20Security%20Plan%20Template.xlsx>

Vulnerability Report Electronic Version

<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Vulnerability%20Report%20Questionnaire%202020%20Security%20Plan%20Template.pdf>

Support

DIR GRC Team

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

Archer 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.

APPENDIX

Table of Figures

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

Version History

Version	Publish Date	Comments
1.0	2019-09-05	First publication

Table 1: Document Version History