2022 Information Security Plan Overview Webinar

March 2022

Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans

Texas Department of Information Resources

Introduction

Sophia Shelton (Presenter)
Governance, Risk, & Compliance Analyst
Policy & Governance Team
Office of the Chief Information Security Officer
Texas Department of Information Resources

Agenda

- Security Plan Overview
- Texas Cybersecurity Framework Overview
- Security Plan Template Overview
- SPECTIM Overview
- Security Plan Template Walkthrough
- Closeout & Resources

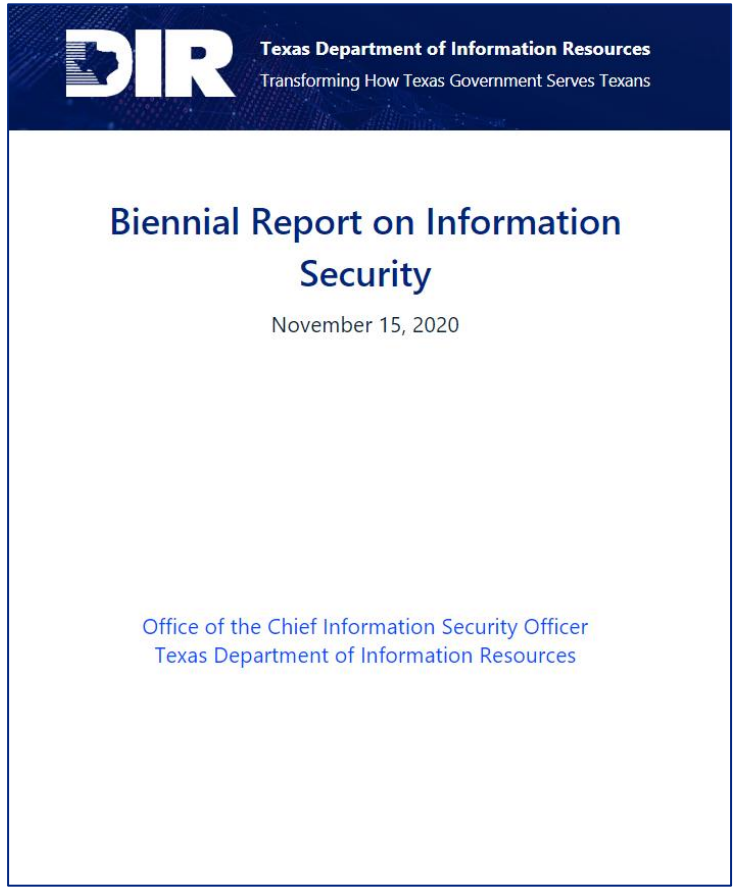
Security Plan Overview

Statutory Requirements

- **Information Security Plan**
  (Sec. 2054.133, Texas Government Code)
- **Data Security Plan for Online & Mobile Applications**
  (Sec. 2054.516, Government Code)
- **Vulnerability Report**
  (Sec. 2054.077, Government Code)
- **Executive Written Acknowledgment of Risk**
  (Sec. 2054.133(e), Government Code)

Information Security Plan

- **Information Security Plan**
  (Sec. 2054.133, Texas Government Code)
  - Information Security Plan Deliverables
    - Agency Security Plans (6/1/2022)
    - Consolidated Report on Information Security (11/15/2022)
  - Required Reporting Entities
    - State Agencies
    - Institutions of Higher Education
    - Community Colleges



Data Security Plan for Online & Mobile Applications

- **Data Security Plan for Online & Mobile Applications**
  (Sec. 2054.516, Government Code)

(a) Each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must:

(1) submit a biennial data security plan to the department not later than June 1 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

(b) The department shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after the department reviews the plan.

- **The Security Plan Template Overall Record**
  This section asks whether such applications are being implemented. If so, the agency is required to complete four additional security objectives to cover the data security plan component.

Functional Area	Objective # 2	Security Objective
Identify	DS1	Secure Application Development
Identify	DS2	Beta Testing
Identify	DS3	Penetration Testing
Identify	DS4	Vulnerability Testing

Vulnerability Report

- **Vulnerability Report**
  (Sec. 2054.077, Government Code)

(a) In this section, a term defined by Section 33.01, Penal Code, has the meaning assigned by that section.
(b) The information security officer of a state agency shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than June 1 of each even-numbered year, 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.
(c) Except as provided by this section, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552.
(d) The information security officer shall provide an electronic copy of the vulnerability report on its completion to:
(1) the department;
(2) the state auditor;
(3) the agency's executive director;
(4) the agency's designated information resources manager; and
(5) any other information technology security oversight group specifically authorized by the legislature to receive the report.
(e) Separate from the executive summary described by Subsection (b), a state agency shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The summary is available to the public on request.

- **The Vulnerability Report Record**
  This section asks questions relating to vulnerability management.

Executive Written Acknowledgment of Risk

- **Executive Written Acknowledgment of Risk**
  (Sec. 2054.133(e), Government Code)

(e) Each state agency shall include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan.

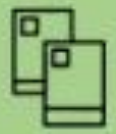
- **Executive Acknowledgement Form**
  Must be signed and uploaded to submit the security plan.

Texas Cybersecurity Framework (TCF) Overview

TCF Structure – Functional Areas

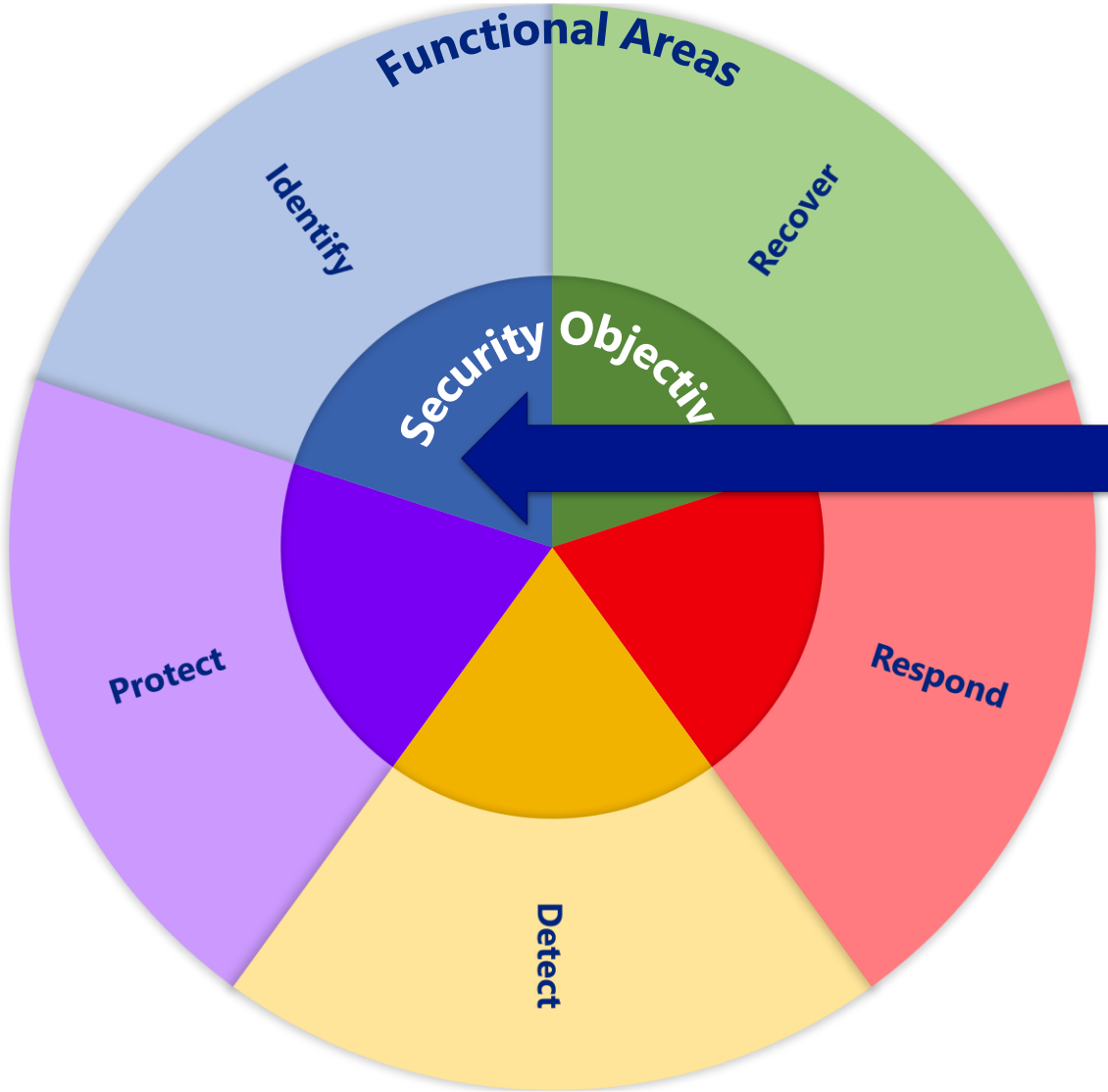
- Functional Areas are divided into five concurrent and continuous functions:
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

TCF Structure – Functional Areas

Functional Area	Description
Identify 	Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect 	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect 	Develop and implement appropriate activities to detect the occurrence of a cybersecurity event.
Respond 	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover 	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

TCF Structure – Security Objectives

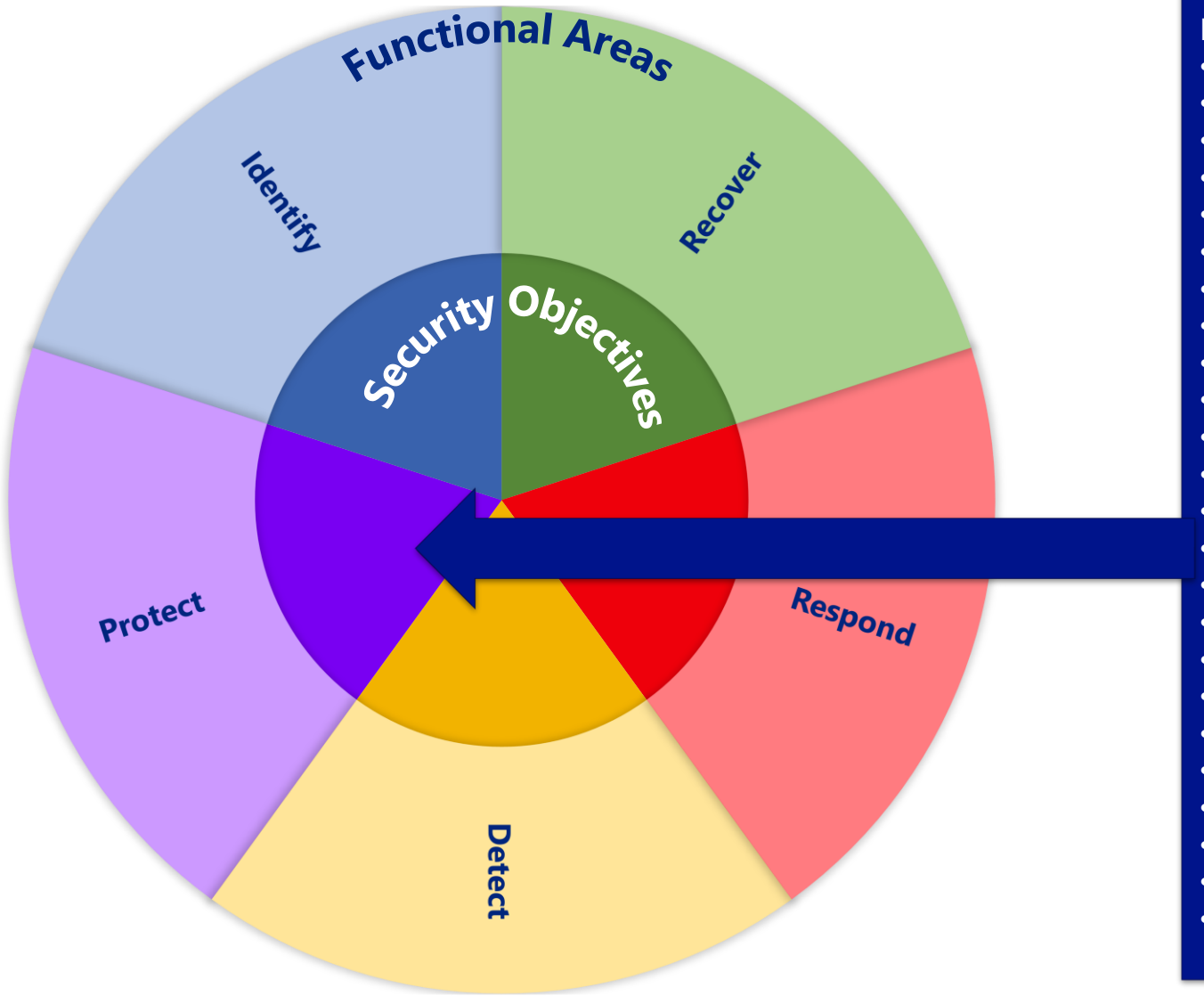
TCF Structure – Security Objectives



IDENTIFY

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

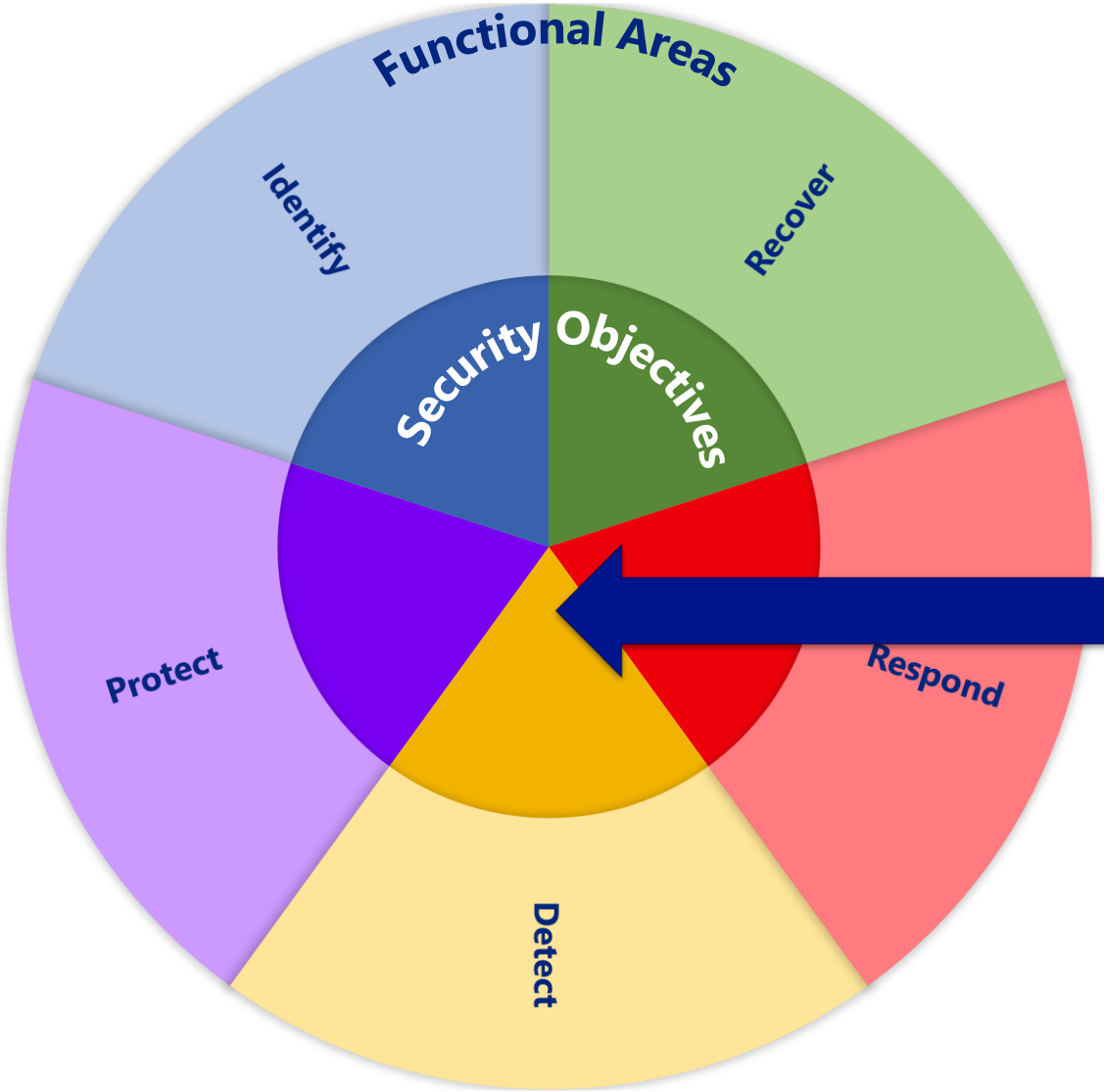
TCF Structure – Security Objectives



PROTECT

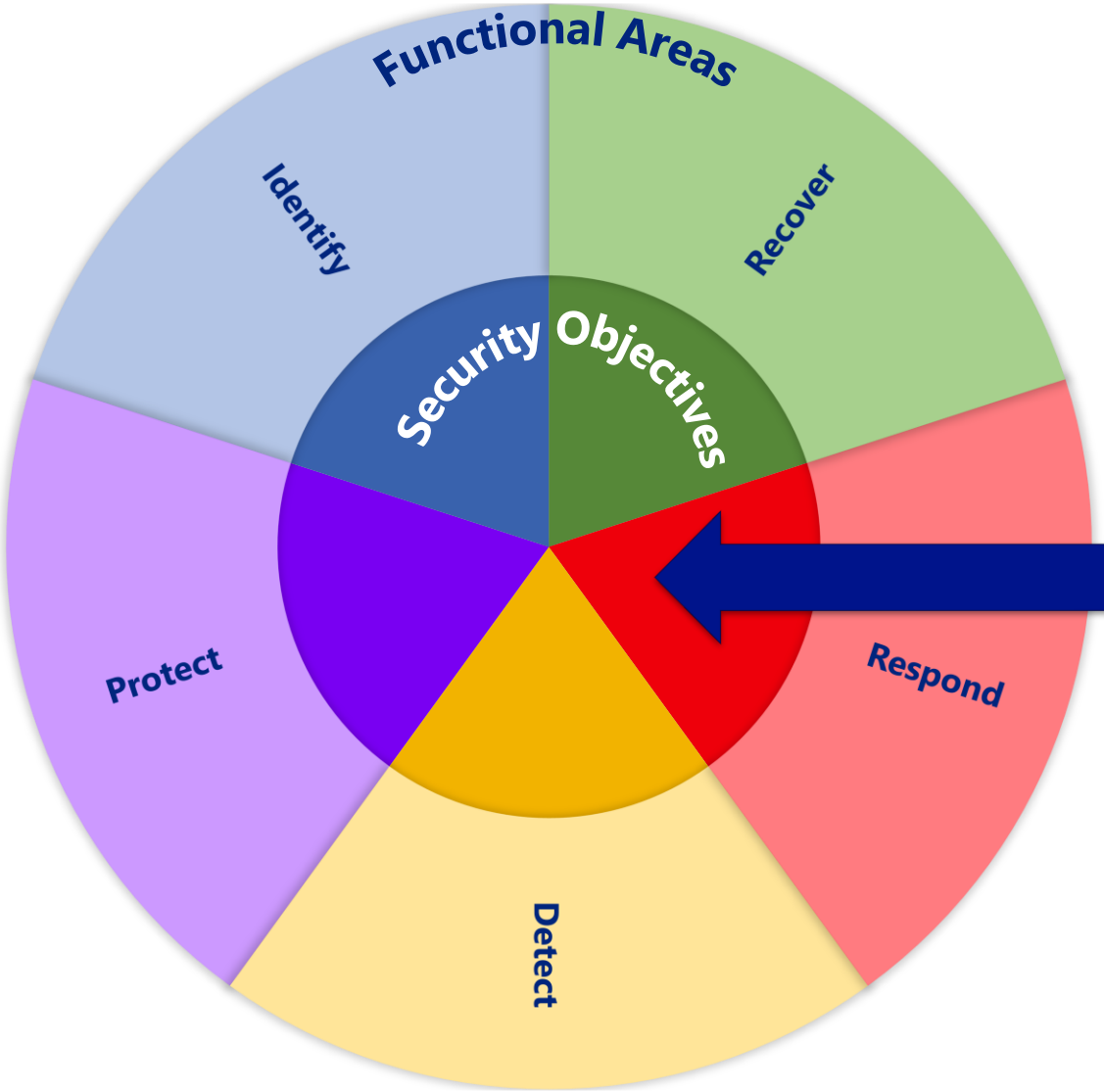
- Enterprise Architecture, Roadmap and Emerging Technology
- Secure System Services, Acquisition and Development
- Security Awareness and Training
- Privacy Awareness and Training
- Cryptography
- Secure Configuration Management
- Change Management
- Contingency Planning
- Media
- Physical and Environmental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

TCF Structure – Security Objectives



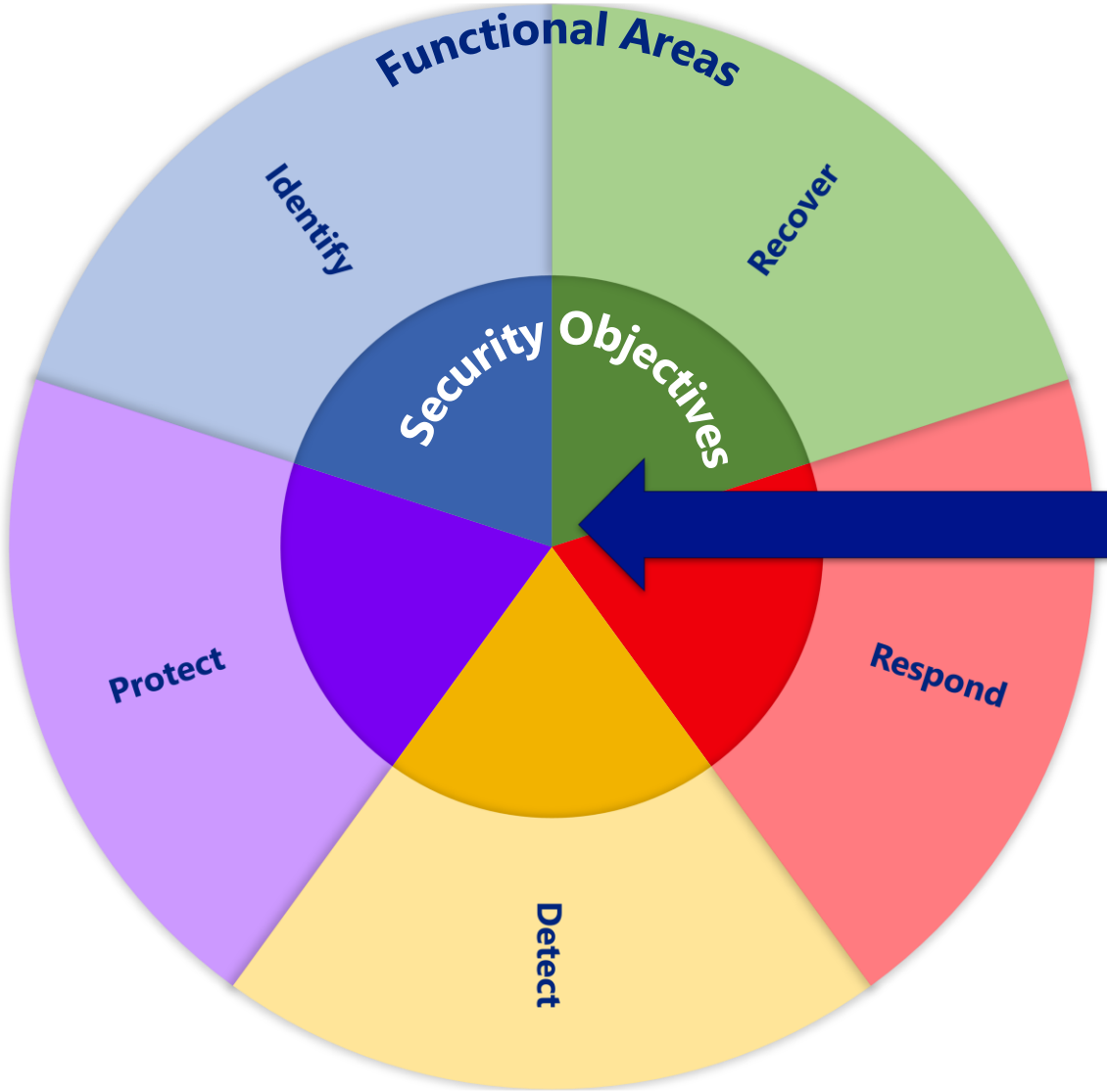
DETECT
- Vulnerability Assessment
- Malware Protection
- Security Monitoring and Event Analysis
- Audit Logging and Accountability

TCF Structure – Security Objectives



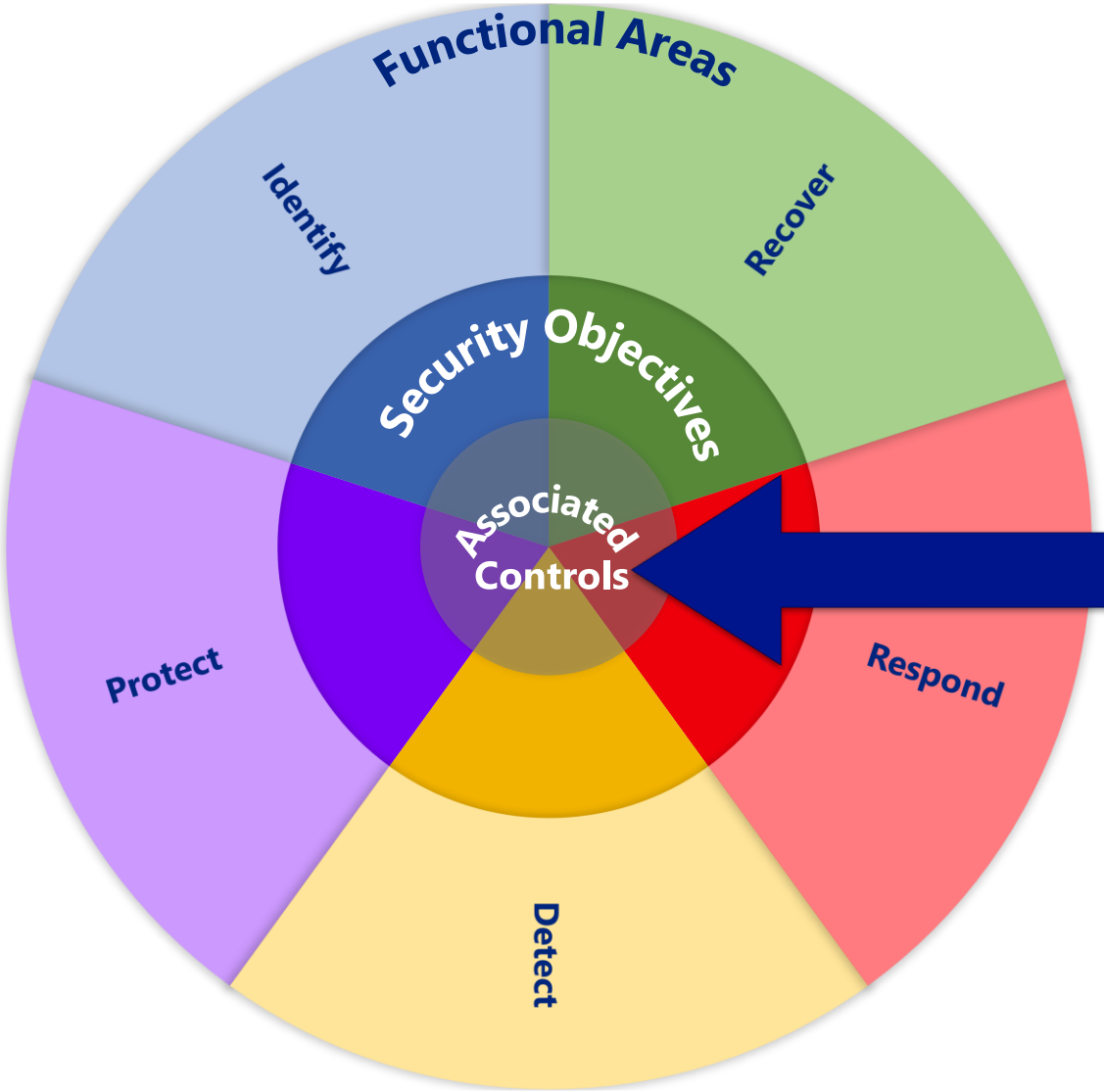
RESPOND
- Cyber-Security Incident Response
- Privacy Incident Response

TCF Structure – Security Objectives



RECOVER
- Disaster Recovery Procedures

TCF Structure – Security Objectives



Security Control Standards Catalog

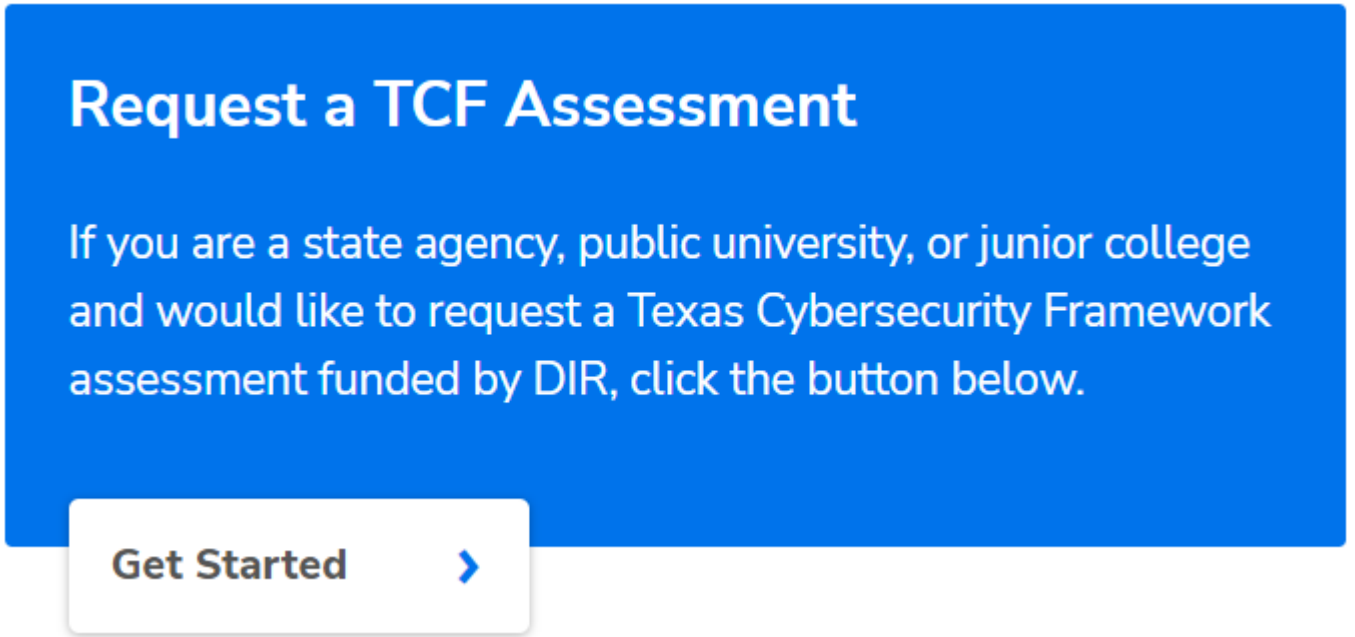
Texas Department of Information Resources

TCF Maturity Model

MATURITY LEVEL	KEYWORDS	DESCRIPTION
0	None, Nonexistent	There is no evidence of the organization meeting the objective.
1	Ad-hoc, Initial	The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.
2	Consistent, Repeatable	The organization has a consistent overall approach to the meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
3	Compliant, Defined	The organization has a documented, detailed approach to meeting the objective, and regularly measure its compliance.
4	Risk-based, Managed	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
5	Efficient, Optimized	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.

MSS – TCF Assessments

- DIR-funded TCF Assessments via MSS Program
- Gauge the 'health' of the organization
- Provide a roadmap and suggested plans to improve the security posture
- Compare the organization's security posture to other state organizations



Security Plan Template Overview

Security Plan Template

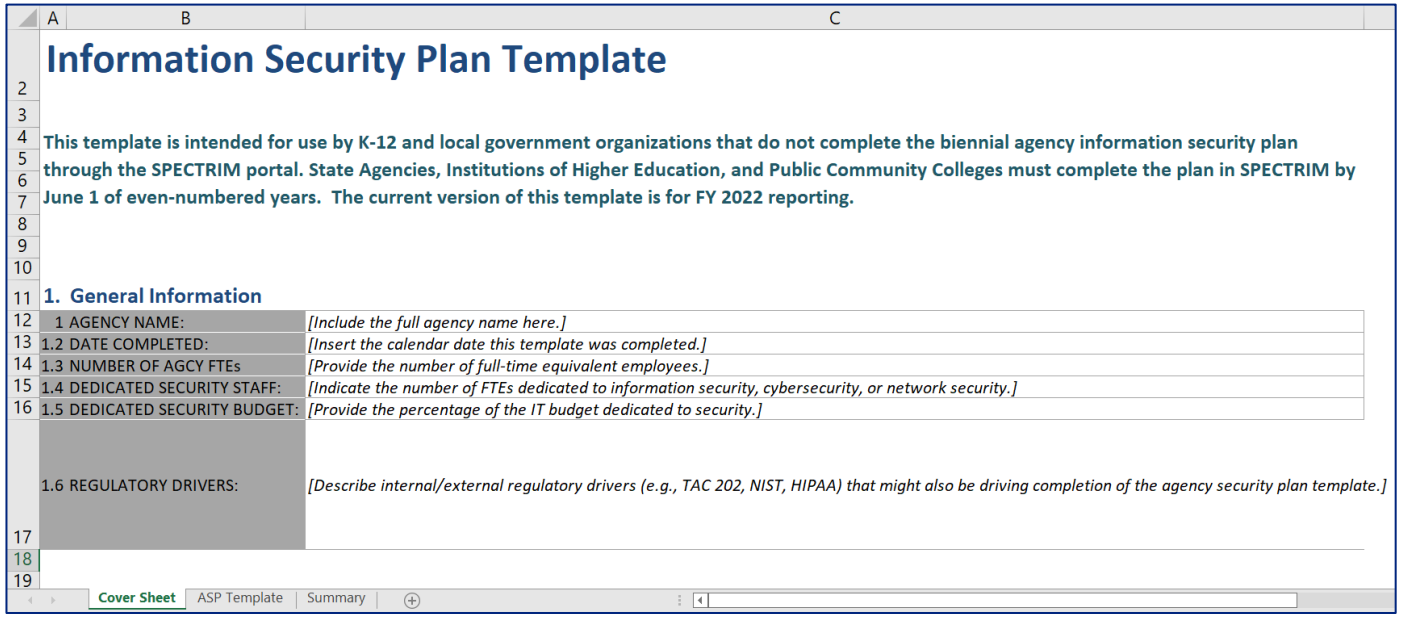
- **Who does this apply to?**
  - State agencies
  - Institutions of higher education
  - Community colleges

- **What needs to be completed?**
  - TCF Security Objective Maturity
  - Security Plan Template Overall
    - Data Security Plan
    - Executive Written Acknowledgment
  - Security Plan Objective
    - Control Activities/Review
    - Challenges/Roadmap
  - Vulnerability Report

- **When is it available?**
  - Available now
  - Due by 6/1/2022

Security Plan Template

- **Where is the Security Plan Template?**
  - Required Entities – SPECTRIM
  - Local Entities – Excel Template



Information Security Plan Template

This template is intended for use by K-12 and local government organizations that do not complete the biennial agency information security plan through the SPECTRIM portal. State Agencies, Institutions of Higher Education, and Public Community Colleges must complete the plan in SPECTRIM by June 1 of even-numbered years. The current version of this template is for FY 2022 reporting.

1. General Information

1 AGENCY NAME:	*[Include the full agency name here.]*
1.2 DATE COMPLETED:	*[Insert the calendar date this template was completed.]*
1.3 NUMBER OF AGCY FTEs	*[Provide the number of full-time equivalent employees.]*
1.4 DEDICATED SECURITY STAFF:	*[Indicate the number of FTEs dedicated to information security, cybersecurity, or network security.]*
1.5 DEDICATED SECURITY BUDGET:	*[Provide the percentage of the IT budget dedicated to security.]*
1.6 REGULATORY DRIVERS:	*[Describe internal/external regulatory drivers (e.g., TAC 202, NIST, HIPAA) that might also be driving completion of the agency security plan template.]*

Cover Sheet | ASP Template | Summary

- **How do I get started?**
  - Live Demo with Q&A Webinar Registration
  - DIR's Information Security Plan website
  - Contact GRC@dir.texas.gov for questions/assistance

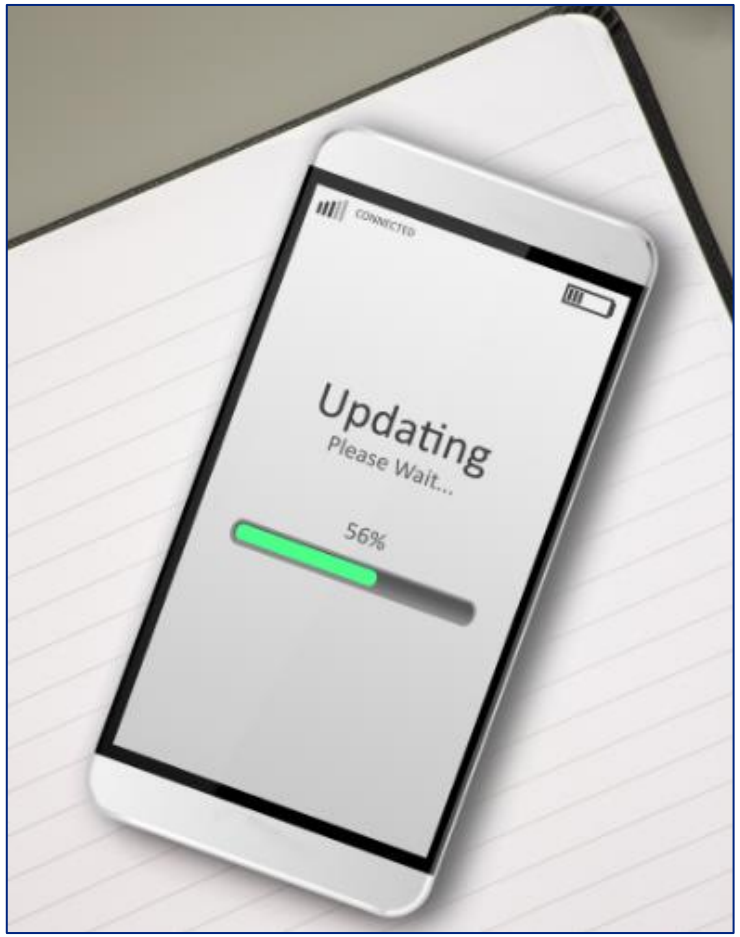
Security Plan Template – 2022 Notable Updates

- **Security Plan Template Overall**
  - Executive Written Acknowledgment

  Updates include:

  1. References to Sec. 2054.519, Government Code. (HB 3834, 86R) have been removed, as this is now reported through Statewide Cybersecurity Awareness Training - Cybersecurity Training Certification for State and Local Governments. Government entities must annually certify their compliance with the training requirements by August 31.

  2. Roles section has been added to provide clarity on the signatures required.



Security Plan Template – 2022 Notable Updates

- **Vulnerability Report**
  - Questionnaire

  Updates include:

  1. Updates to choices to provide additional options
  2. Re-ordered Questions
  3. New Questions

VR-001	What systems or applications does the agency perform vulnerability assessments and scans on prior to implementation? Check all that apply.
VR-009	How often does the agency review data/information flow designs to ensure that controls are still effective and that vulnerabilities are identified and addressed?
VR-011	How often are independent third-party security assessments conducted?
VR-012	How often does the agency conduct security self-assessments?
VR-013	What is the percentage of agency coverage in these assessments?
VR-016	How often are the agency's servers patched?
VR-017	How often does the agency patch network equipment?
VR-018	How often does the agency patch workstations?
VR-020	What is the percentage of agency compliance with application patching?
VR-021	What is the percentage of agency compliance with server patching?
VR-022	What is the percentage of agency compliance with network equipment?
VR-026b	Select the challenge(s) preventing remediation of identified vulnerabilities.

SPECTRIM Overview

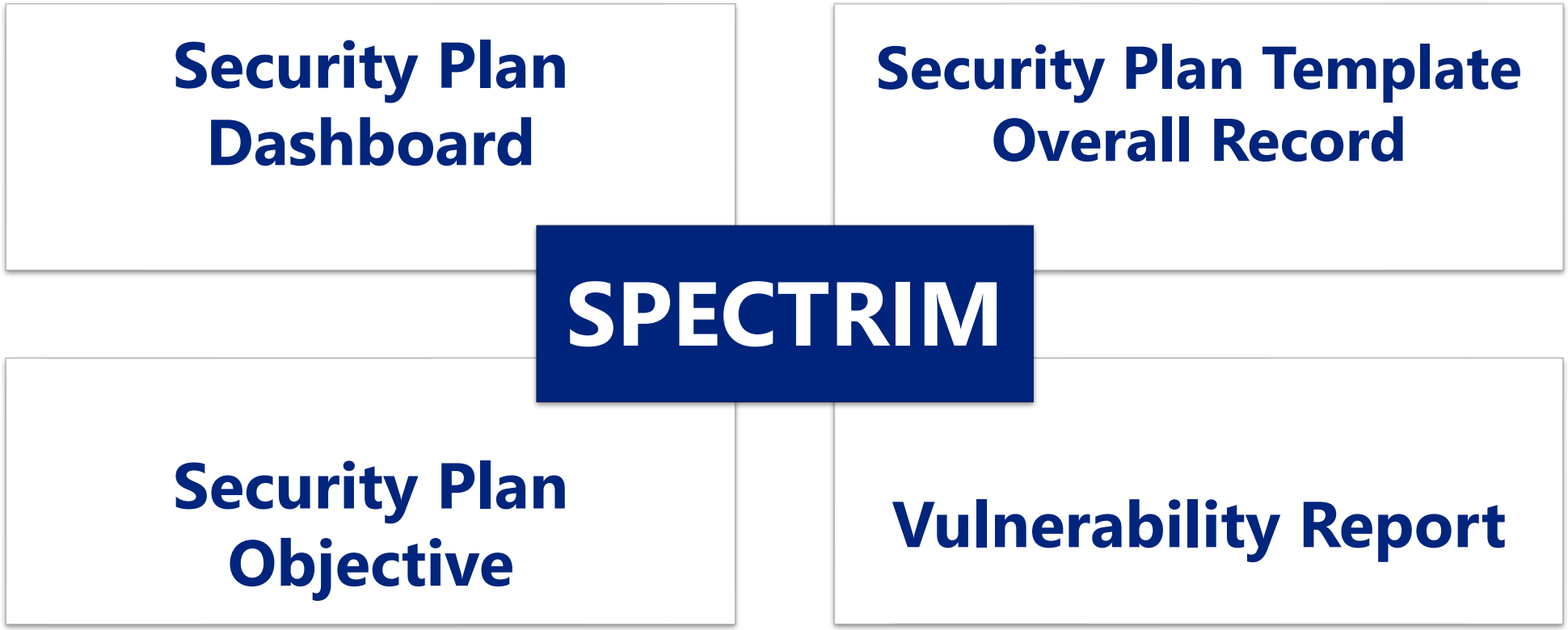
- **Statewide Portal for Enterprise Cybersecurity Threat, Risk, & Incident Management (SPECTRIM)**

- **SPECTRIM Portal**
  https://dir.archer.rsa.com
  - Password resets do not work for locked or inactive accounts.
    - Accounts become inactive after 60 days.
    - Accounts become locked after 5 failed attempts.

- **General Structure**
  - Workspaces/Dashboards/Reports - with historical records
  - Access Groups - Segments access based on business need
  - Applications/Questionnaires - create associations to track holistic impacts
  - Etc.

- **Questions or Assistance**
  - Open an SPECTRIM Support Request or
  - Contact GRC support GRC@dir.texas.gov

Security Plan Template Workspace



Security Plan Template Workspace

Security Plan Dashboard

- Track Status

Security Plan Template Overall Record

SPECTRIM

Security Plan Objective

Vulnerability Report

Security Plan Template Workspace

Security Plan Dashboard

- Track Status

Security Plan Template Overall Record

- General Information
- Security Plan Objectives
- Data Security Plan (Web/Mobile Applications)
  - Management Approval and Acknowledgment (Executive Written Acknowledgment)

SPECTRIM

Security Plan Objective

Vulnerability Report

Security Plan Template Workspace

Security Plan Dashboard

- Track Status

Security Plan Template Overall Record

- General Information
- Security Plan Objectives
- Data Security Plan (Web/Mobile Applications)
  - Management Approval and Acknowledgment (Executive Written Acknowledgment)

SPECTRIM

Security Plan Objective

- General Information
- Relevant Control Activities
- Scores/Results
- Associated Controls
- Challenges
- Roadmap
- Archived responses

Vulnerability Report

Security Plan Template Workspace

Security Plan Dashboard

- Track Status

Security Plan Template Overall Record

- General Information
- Security Plan Objectives
- Data Security Plan (Web/Mobile Applications)
  - Management Approval and Acknowledgment (Executive Written Acknowledgment)

SPECTRIM

Security Plan Objective

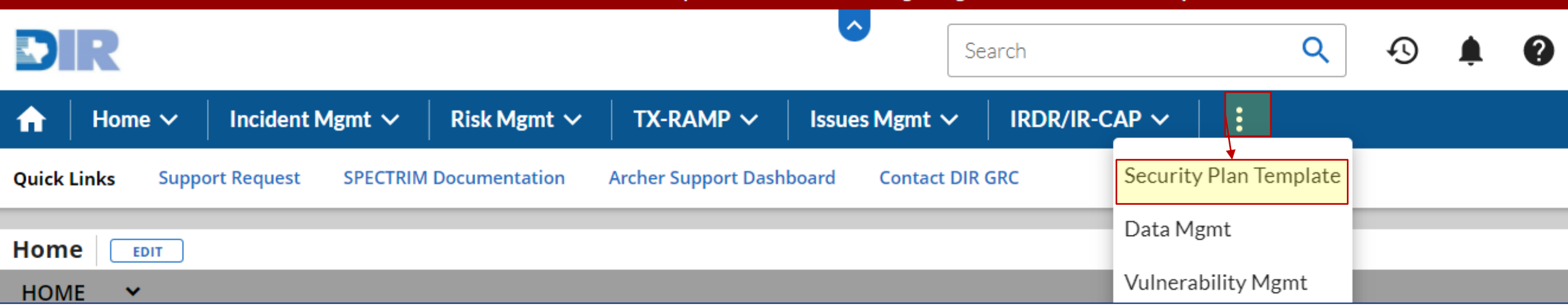
- General Information
- Relevant Control Activities
- Scores/Results
- Associated Controls
- Challenges
- Roadmap
- Archived responses

Vulnerability Report

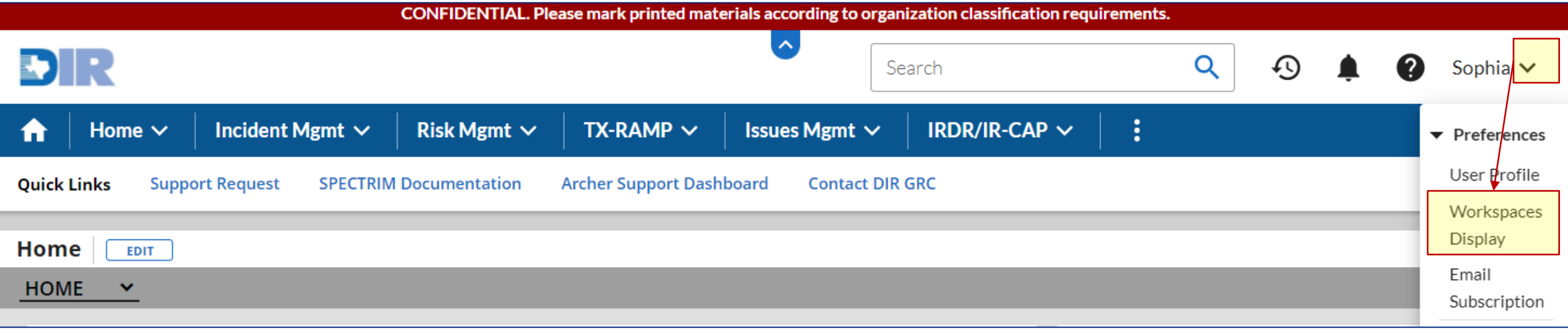
- General Information
- Vulnerability Report Assessment
- Vulnerability Report Attachments

SPECTRIM
Security Plan Template Walkthrough

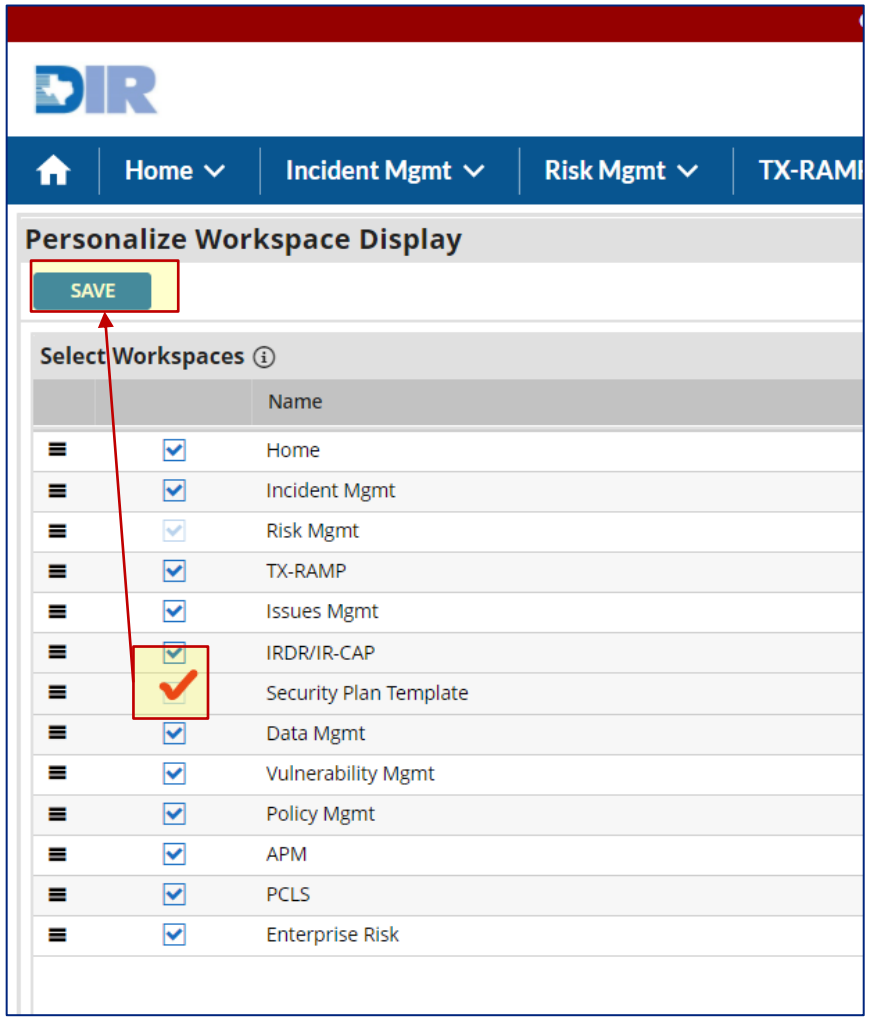
Security Plan Template Workspace



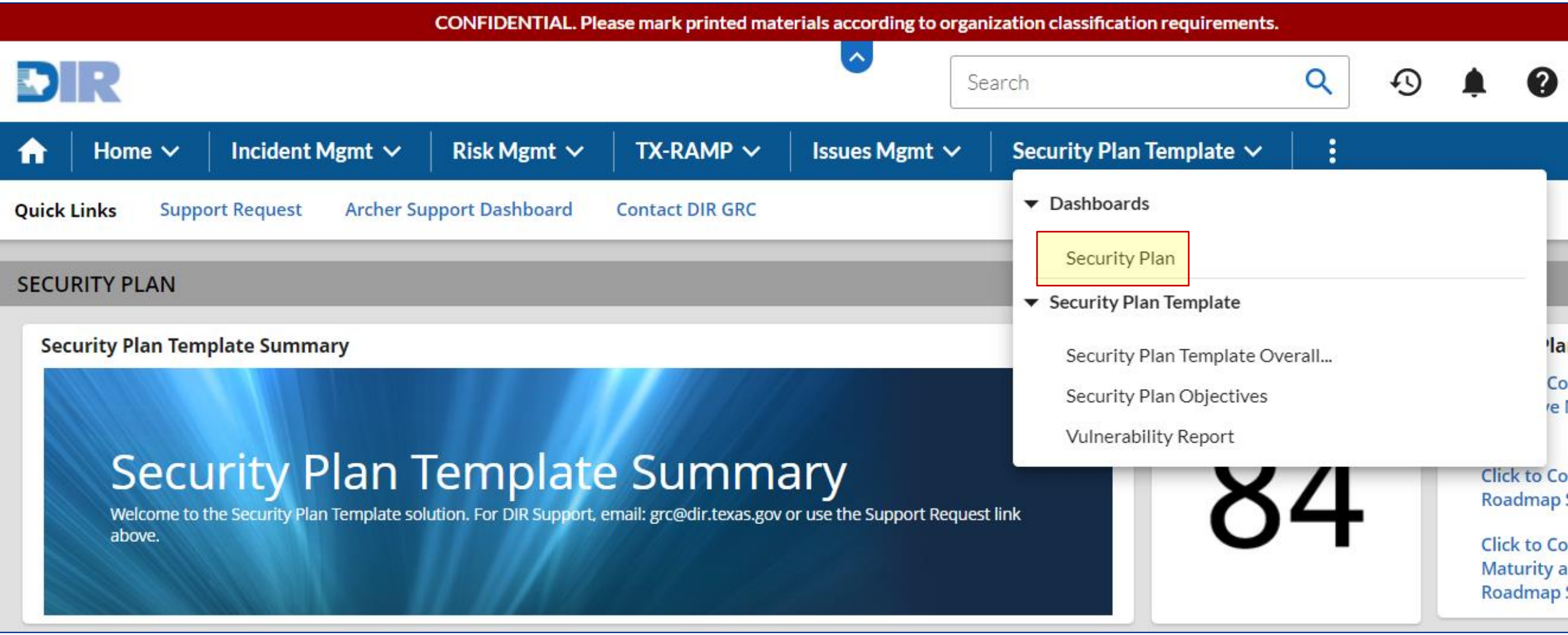
Security Plan Template Workspace – Workspace Display



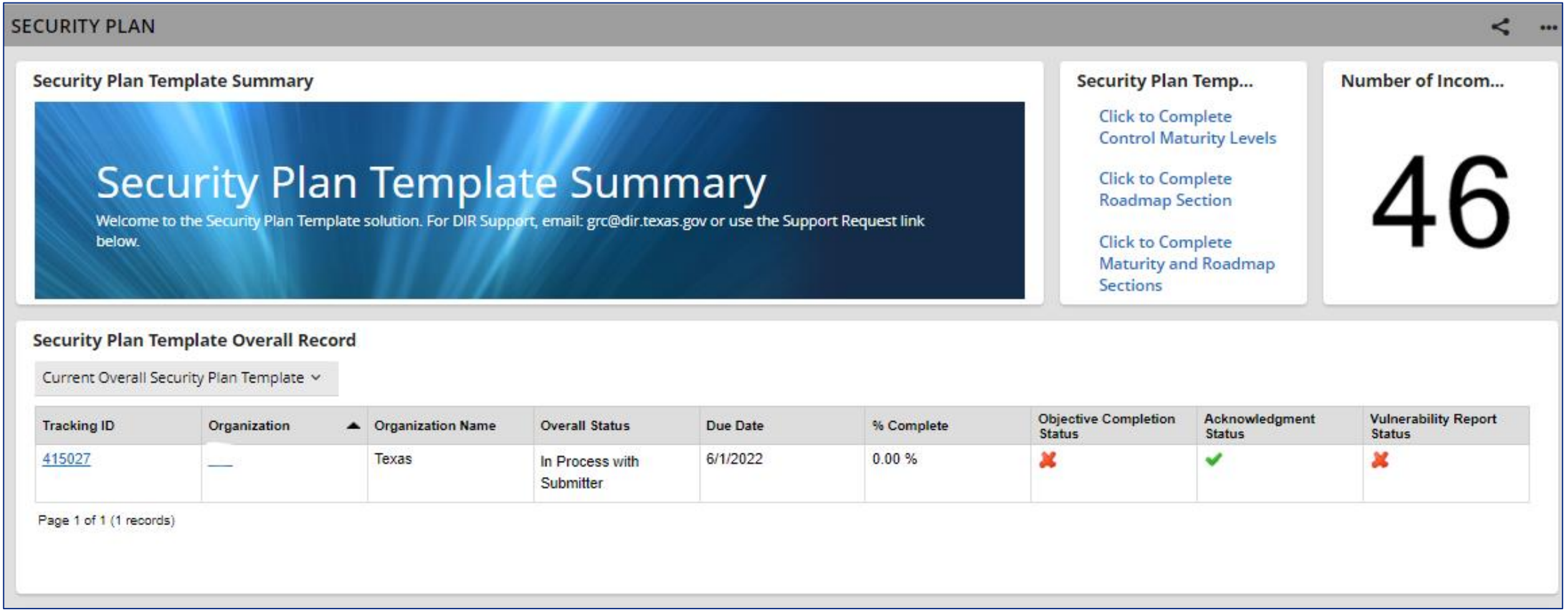
Security Plan Template Workspace – Workspace Display



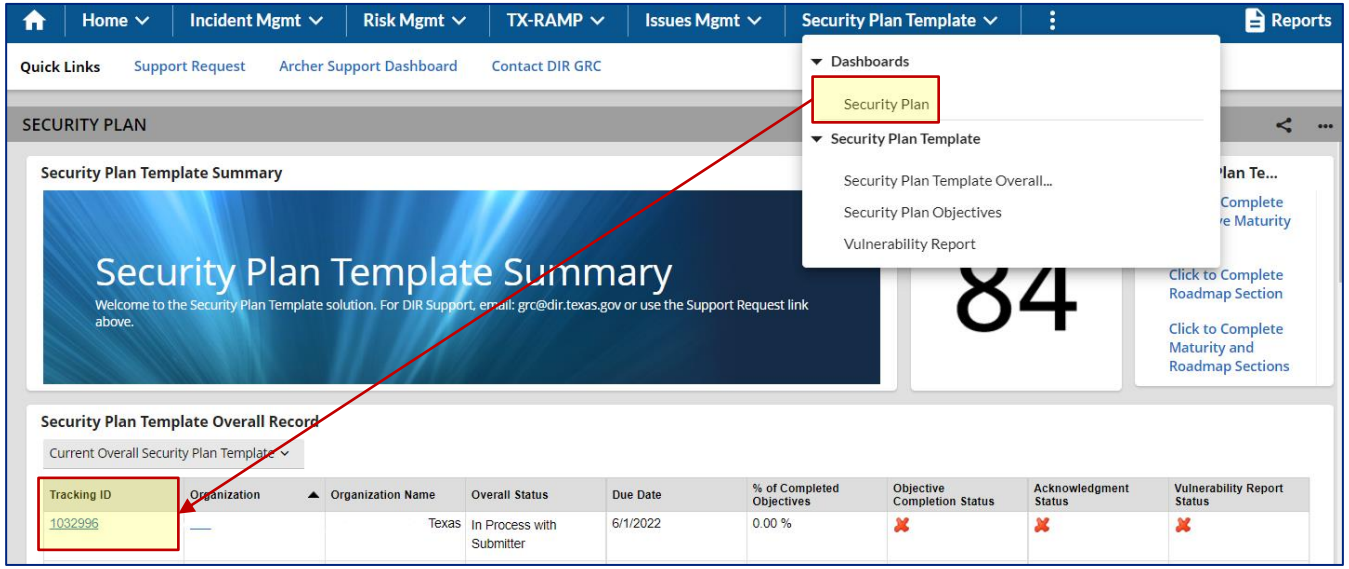
Navigating: Security Plan Dashboard

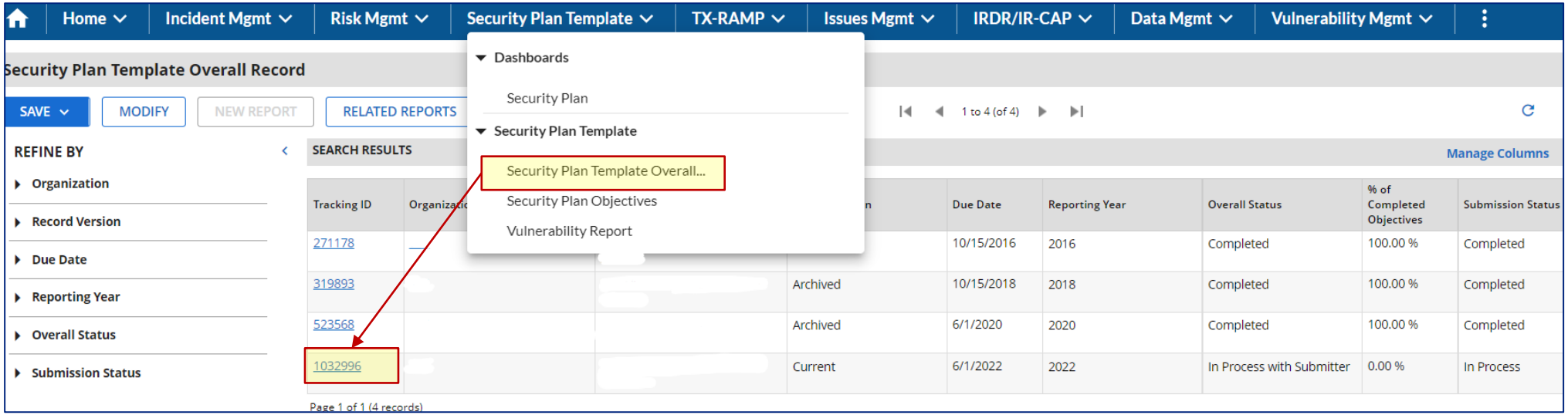


Security Plan Dashboard

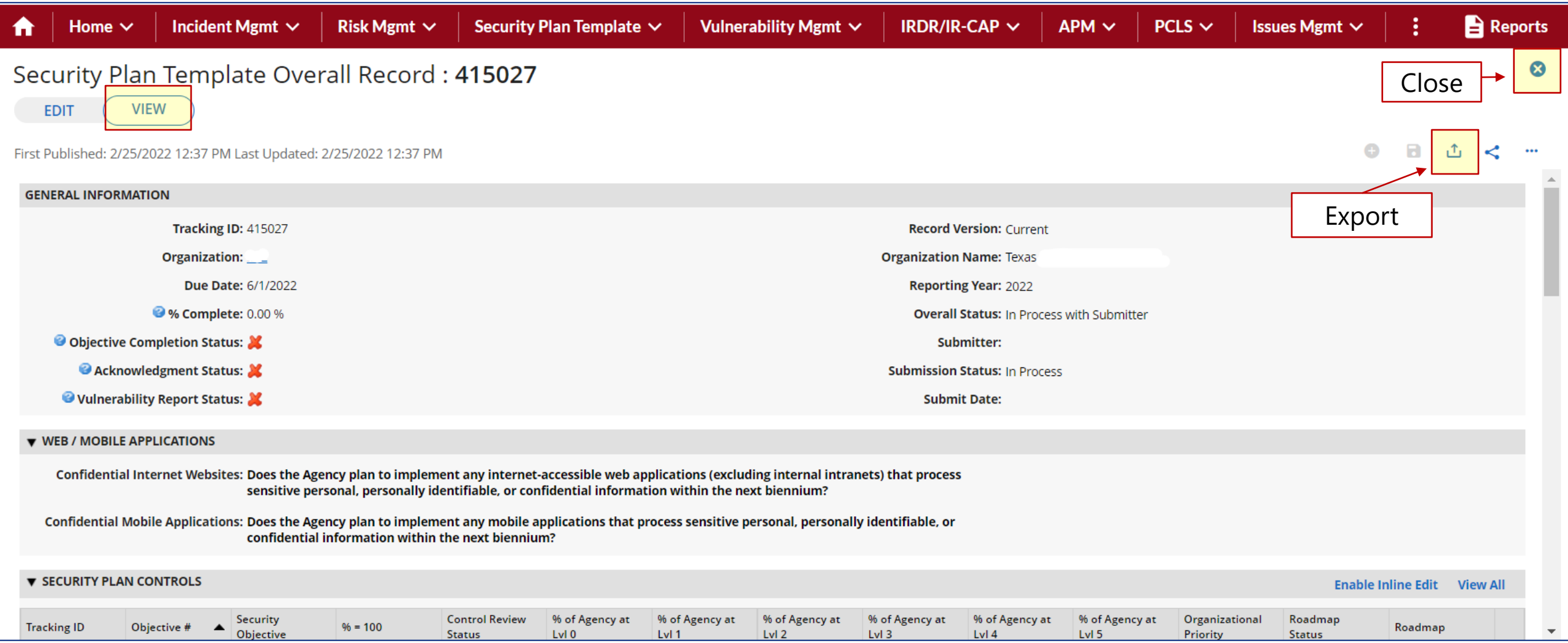


Navigating: Security Plan Template Overall Record

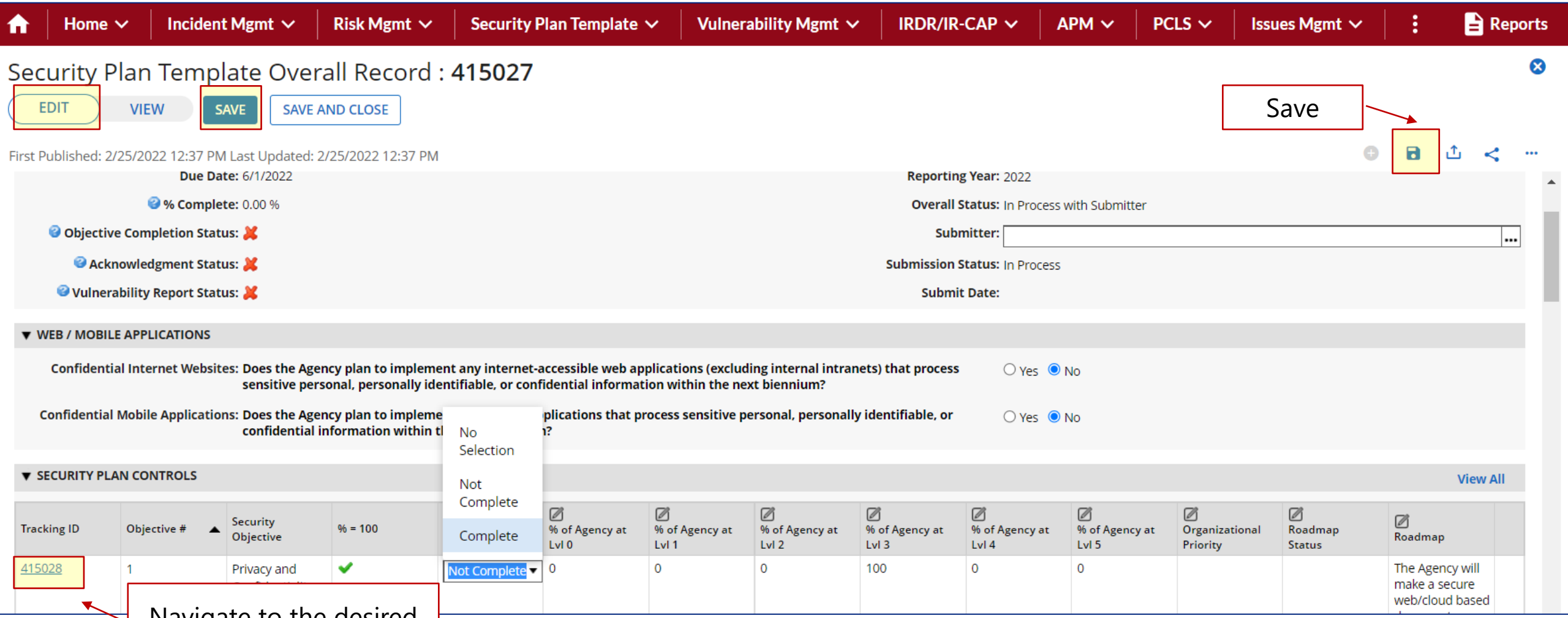




Security Plan Template Overall Record – View Mode

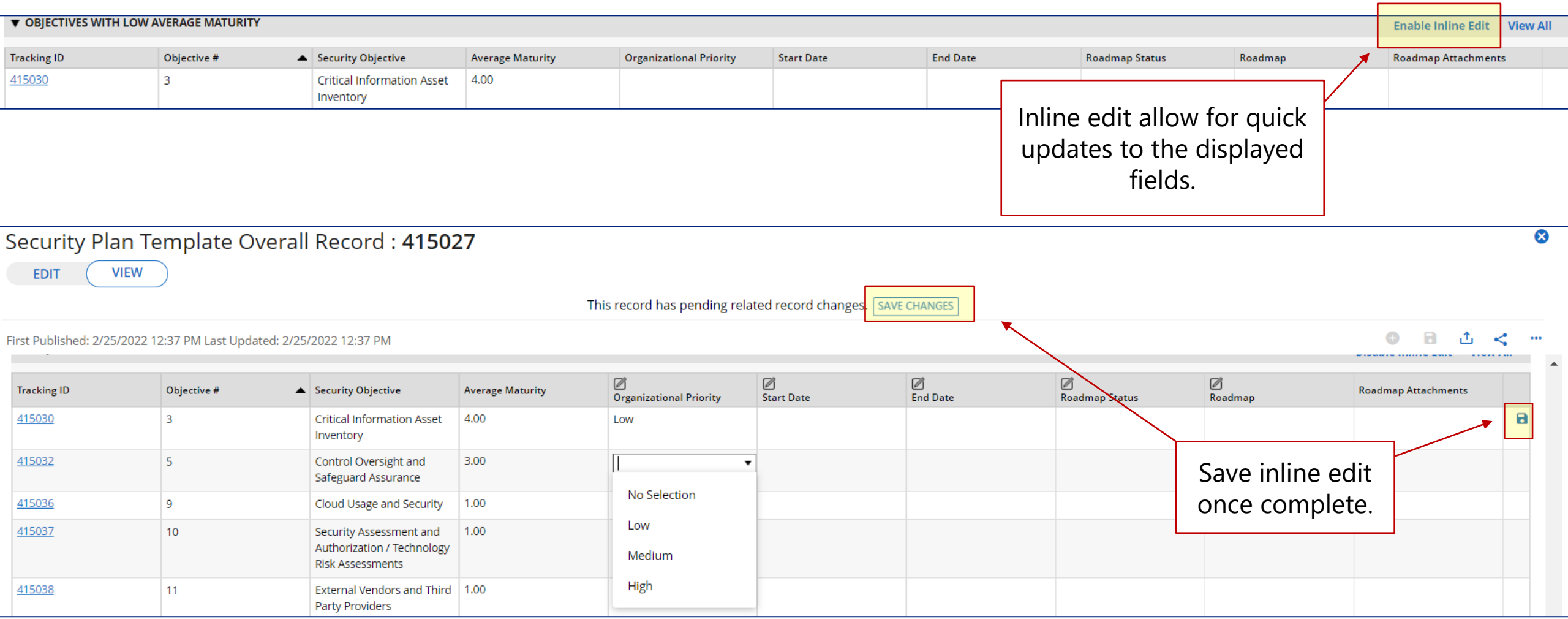


Security Plan Template Overall Record – Edit Mode

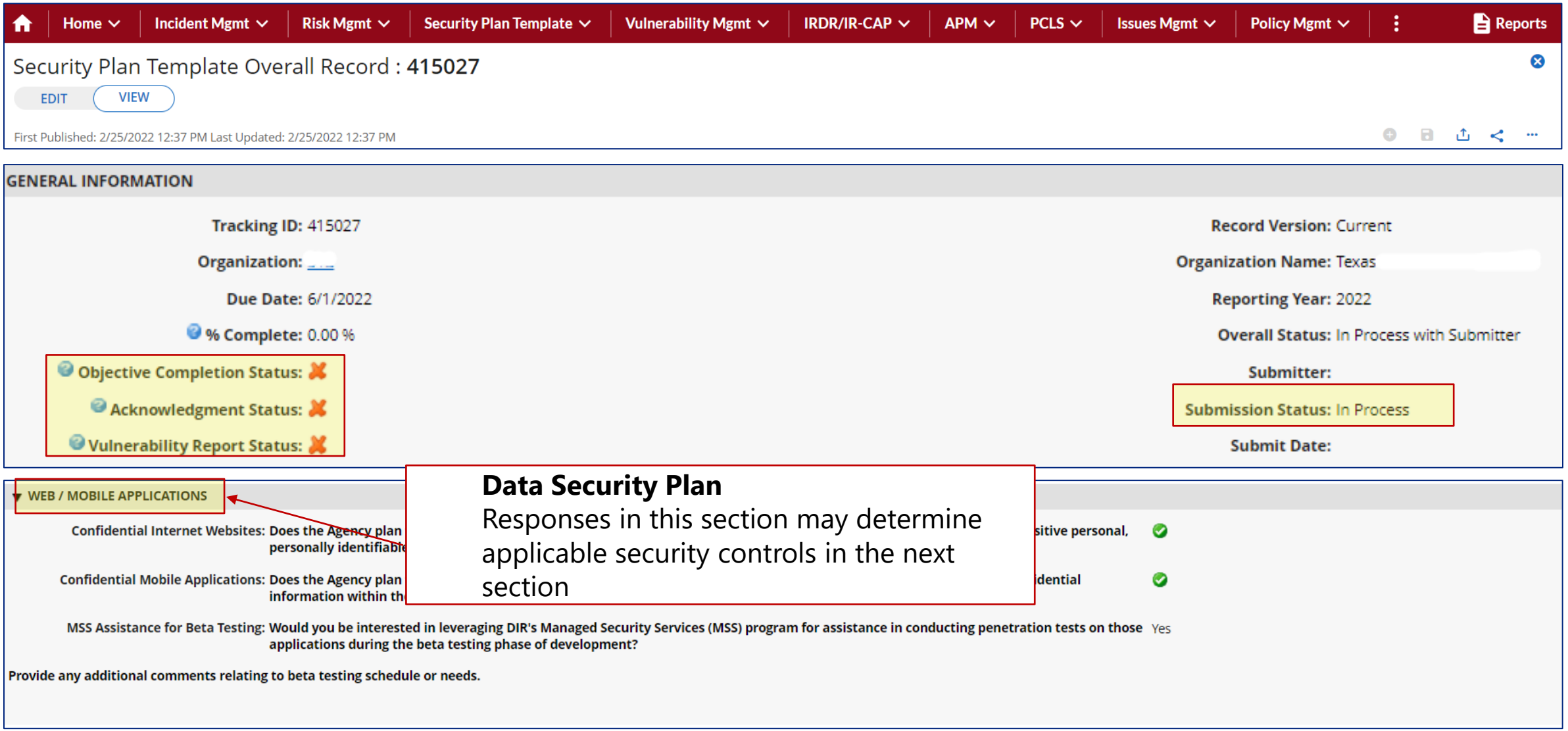


Navigate to the desired record for detailed edits.

Security Plan Template Overall Record – Inline Edit



Security Plan Template Overall Record – Sections



Data Security Plan

Responses in this section may determine applicable security controls in the next section

Security Plan Template Overall Record – Sections

▼ SECURITY PLAN CONTROLS

Disable 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
415028	1	Privacy and Confidentiality	✔	Not Complete	0	0	0	100	0	0			The Agency will make a secure web/cloud based document
415029	2	Data Classification	✔	Not Complete	0	0	50	50	0	0			
415030	3	Critical Information Asset Inventory	✔	Not Complete	0	0	0	0	100	0			
415031	4	Enterprise Security Policy, Standards and Guidelines	✔	Not Complete	0	0	100	0	0	0			
415032	5	Control Oversight and Safeguard Assurance	✔	Not Complete	0	100	0	0	0	0			

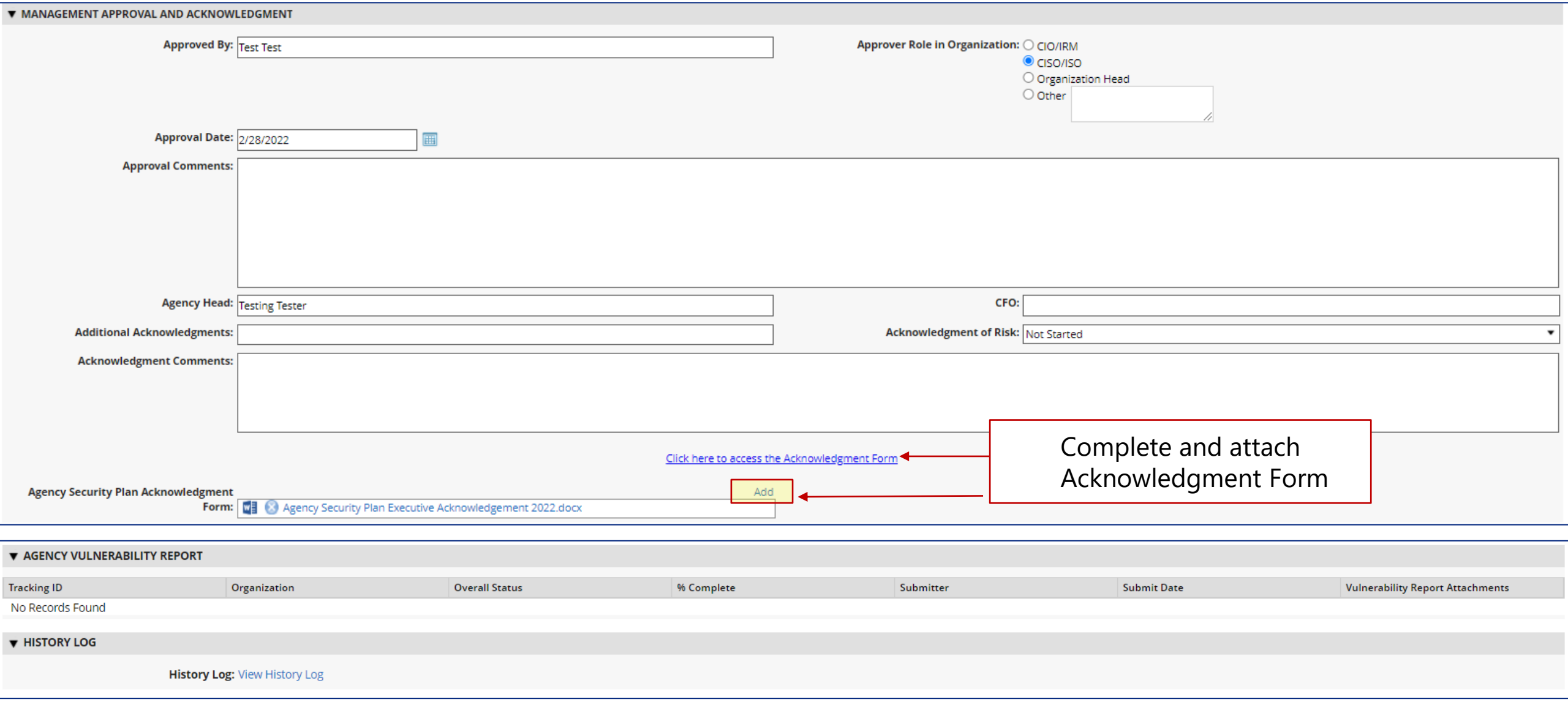
▼ OBJECTIVES WITH LOW AVERAGE MATURITY

Enable Inline Edit | View All

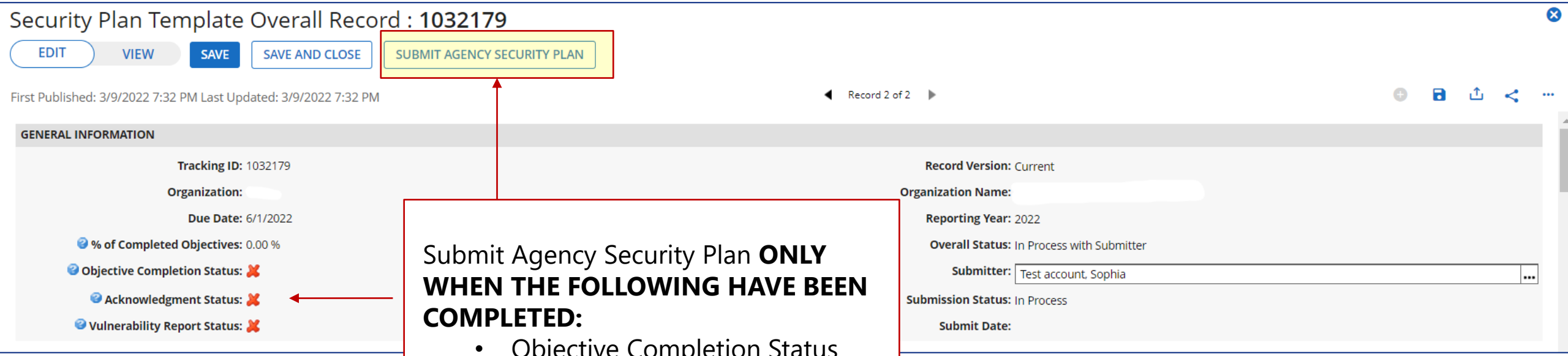
Tracking ID	Objective #	Security Objective	Average Maturity	Organizational Priority	Start Date	End Date	Roadmap Status	Roadmap	Roadmap Attachments
415036	9	Cloud Usage and Security	1.00						
415037	10	Security Assessment and Authorization / Technology Risk Assessments	1.00						
415038	11	External Vendors and Third Party Providers	1.00						

The security objectives below have an average maturity level of less than 2.0. It is highly recommended that organizations document a roadmap strategy to raise the average maturity for each objective listed.

Security Plan Template Overall Record – Sections



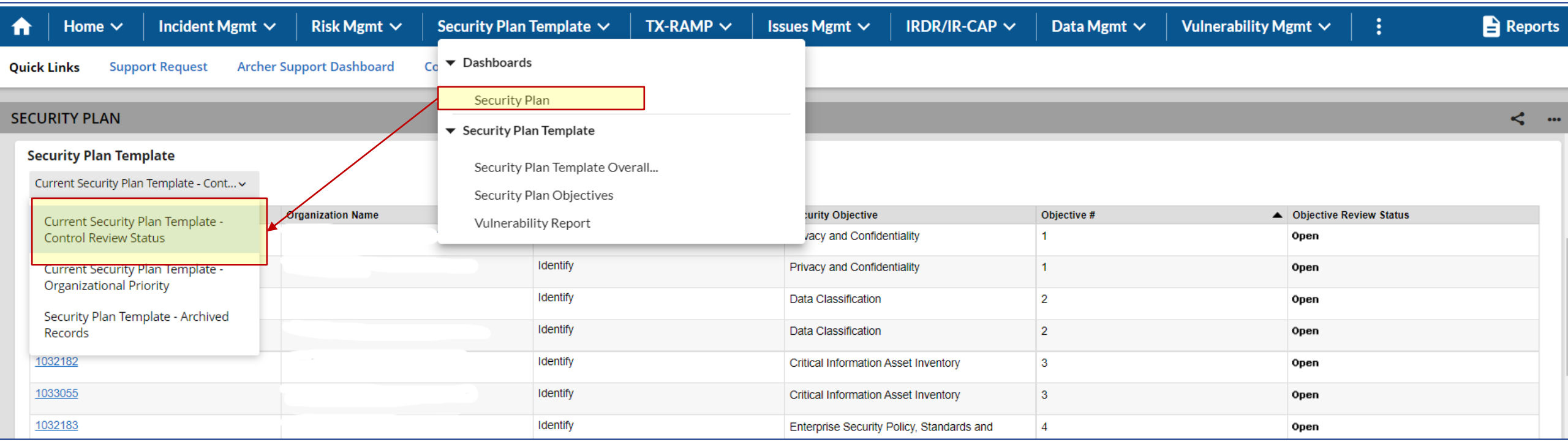
Security Plan Template Overall Record – Submission



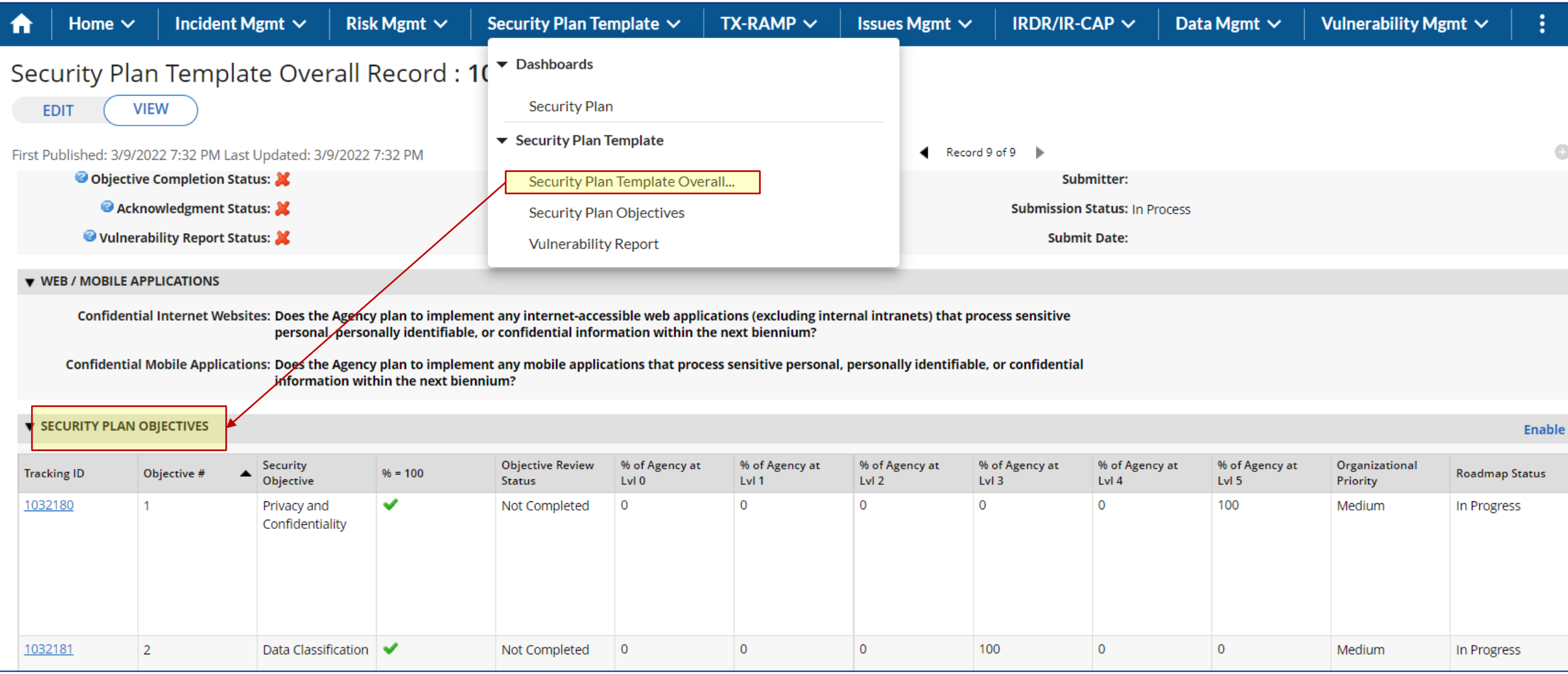
Submit Agency Security Plan **ONLY WHEN THE FOLLOWING HAVE BEEN COMPLETED:**

- Objective Completion Status
- Acknowledgment Status
- Vulnerability Report Status

Navigating: Security Plan Objective

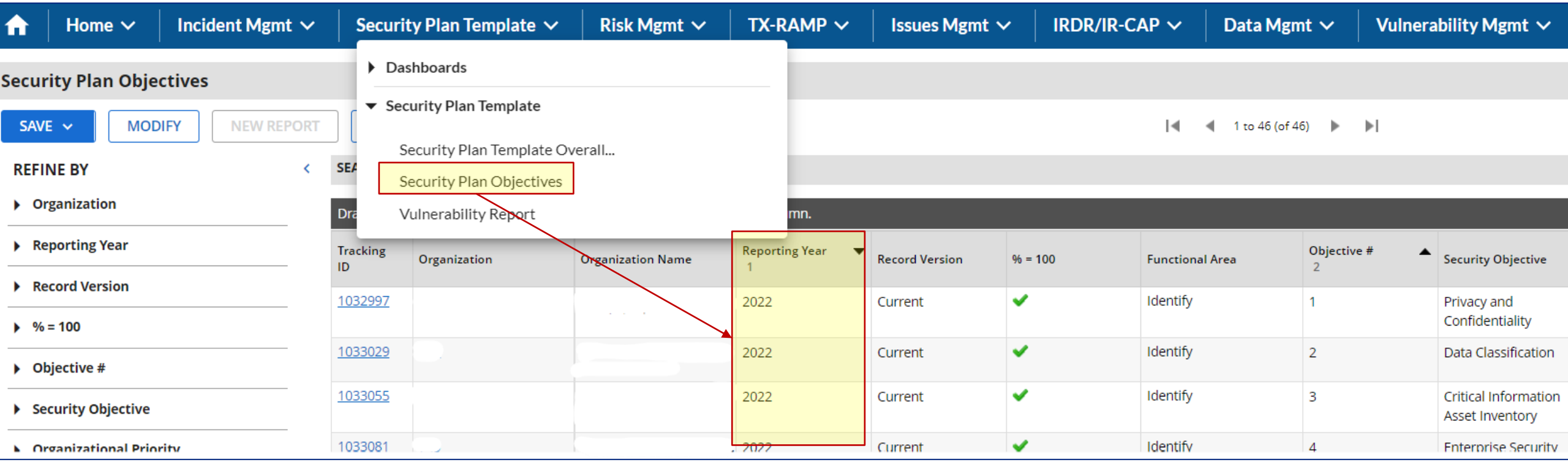


Navigating: Security Plan Objective

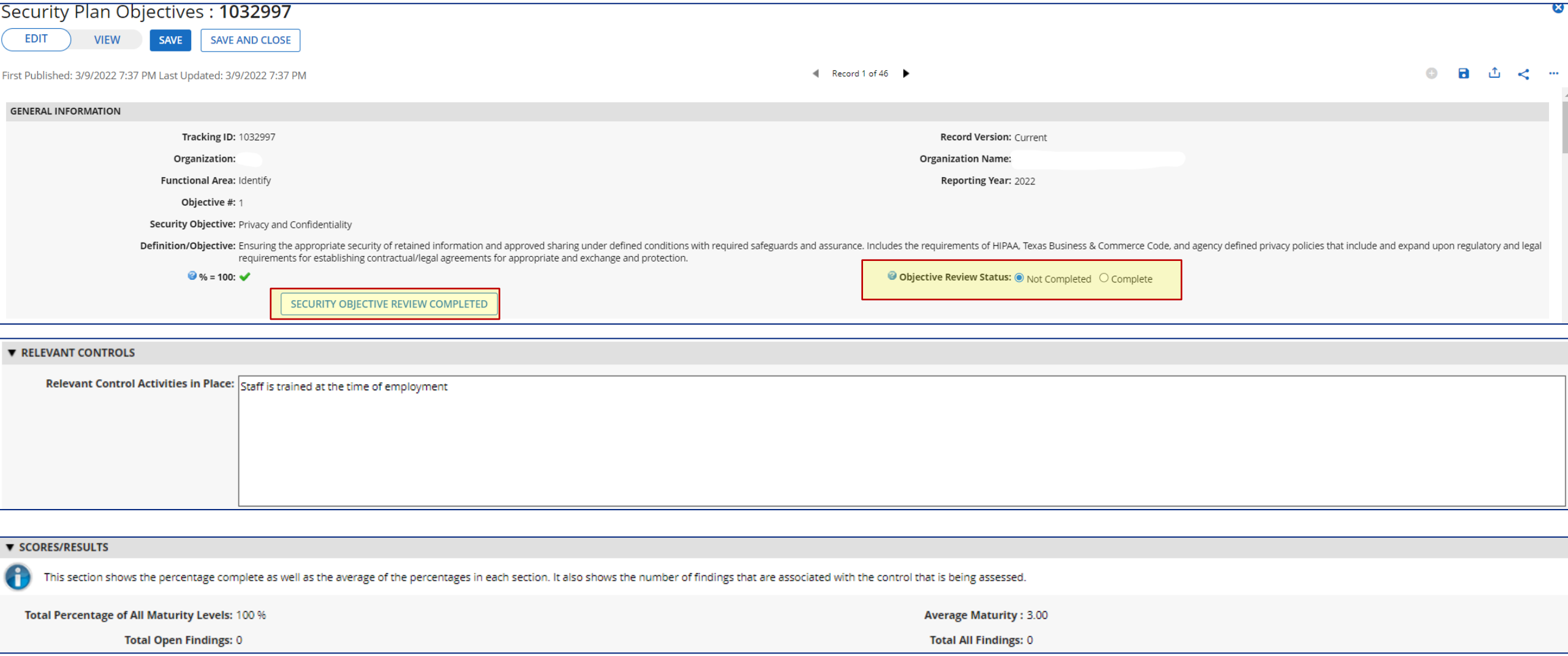


Tracking ID	Objective #	Security Objective	% = 100	Objective Review Status	% of Agency at Lvl 0	% of Agency at Lvl 1	% of Agency at Lvl 2	% of Agency at Lvl 3	% of Agency at Lvl 4	% of Agency at Lvl 5	Organizational Priority	Roadmap Status
1032180	1	Privacy and Confidentiality	✔	Not Completed	0	0	0	0	0	100	Medium	In Progress
1032181	2	Data Classification	✔	Not Completed	0	0	0	100	0	0	Medium	In Progress

Navigating: Security Plan Objective



Security Plan Objective – Sections



Security Plan Objective – Sections

▼ **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. 0 %

▼ **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. 0 %

▼ **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. 50 %

▼ **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. 50 %

▼ **LEVEL 4: MANAGED**

Level 4 Pattern Controls: The organizational structure supports a focus on privacy and confidentiality as a distinct discipline.

% of Agency at Lvl 4: The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations. 50 %

How is Effectiveness of the Control Measured?: On an annual basis the Privacy Program is evaluated. The risk is evaluated using our internal method and presented upon. Thereafter, responses and remediation efforts are coordinated through our project management group.

Security Plan Objective – Sections

▼ **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. 0 %

▼ **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. 0 %

▼ **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. 50 %

▼ **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. 50 %

▼ **LEVEL 4: MANAGED**

Level 4 Pattern Controls: The organizational structure supports a focus on privacy and confidentiality as a distinct discipline.

% of Agency at Lvl 4: The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations. 50 %

How is Effectiveness of the Control Measured?: On an annual basis the Privacy Program is evaluated. The risk is evaluated using our internal method and presented upon. Thereafter, responses and remediation efforts are coordinated through our project management group.

Security Plan Objective – Sections

▼ LEVEL 5: OPTIMIZED

Level 5 Pattern Controls: Privacy is treated by the organization as a business output.

% of Agency at Lvl 5: The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner 0 %

How is the Efficiency of the Control Measured?:

▼ CHALLENGES TO IMPLEMENTATION

Challenges to Implementation:

- ☐ Competing Priorities - Financial
- ☐ Competing Priorities - Staffing/Time
- ☐ Inadequate Funding
- ☐ Inadequate Knowledge, Skills, or Abilities of Current Staff
- ☐ Inadequate Staffing
- ☐ Lack of Interest
- ☐ Lack of Management Support/Sponsorship
- ☐ Lack of Planning
- ☐ Organizational Reluctance to Change
- ☐ Technical Barriers - Incompatibility
- ☐ Technical Barriers - Legacy Systems
- ☐ Other
- ☐ None

Challenges to Implementation Attachments: Add

Challenges to Implementation Comments:

Security Plan Objective – Sections

▼ ROADMAP

Organizational Priority:

Start Date: End Date:

Roadmap: The Agency will make a secure web/cloud based document

Roadmap Status: ○ Not Started ○ In Progress ○ Completed ○ Not Applicable

Roadmap Attachments: Add

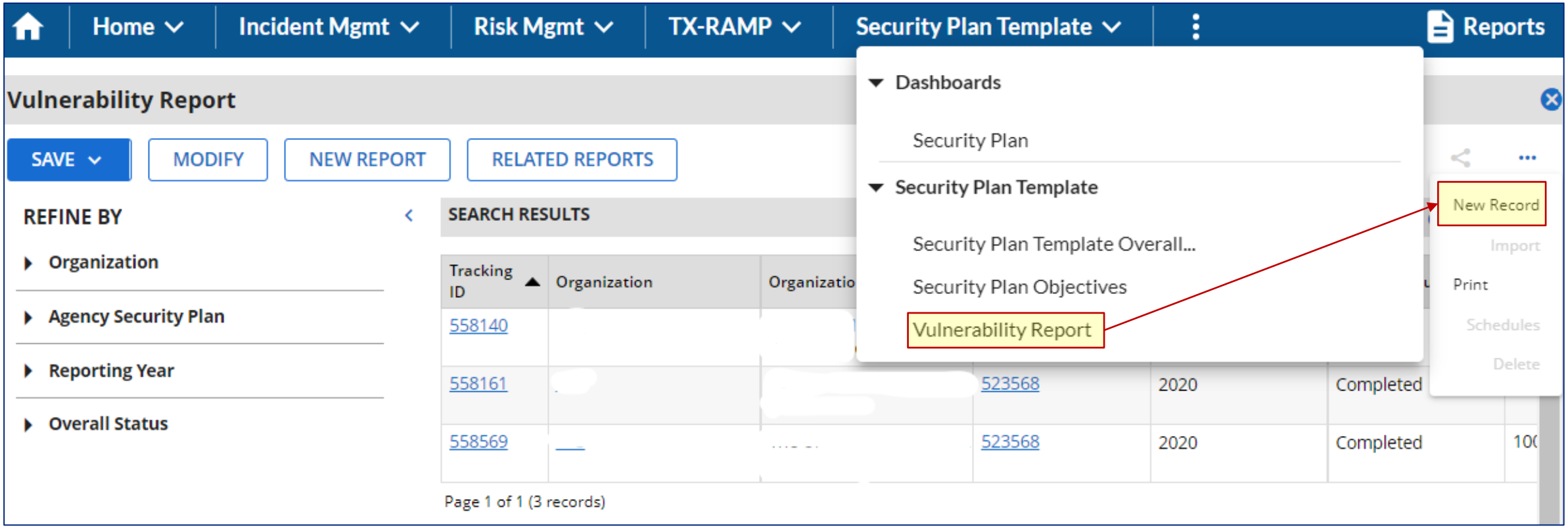
▼ ARCHIVED SECURITY PLAN TEMPLATE OBJECTIVE

Tracking ID	Reporting Year	Objective #	Security Objective	% 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	Relevant Control Activities in Place
297026	2020	1	Privacy and Confidentiality	0 %	0 %	0 %	100 %	0 %	0 %	Staff is trained at time of employment

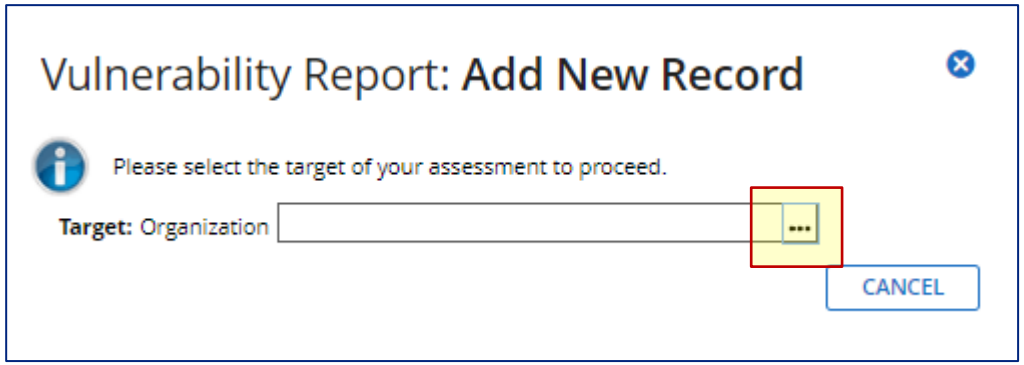
▼ HISTORY LOG

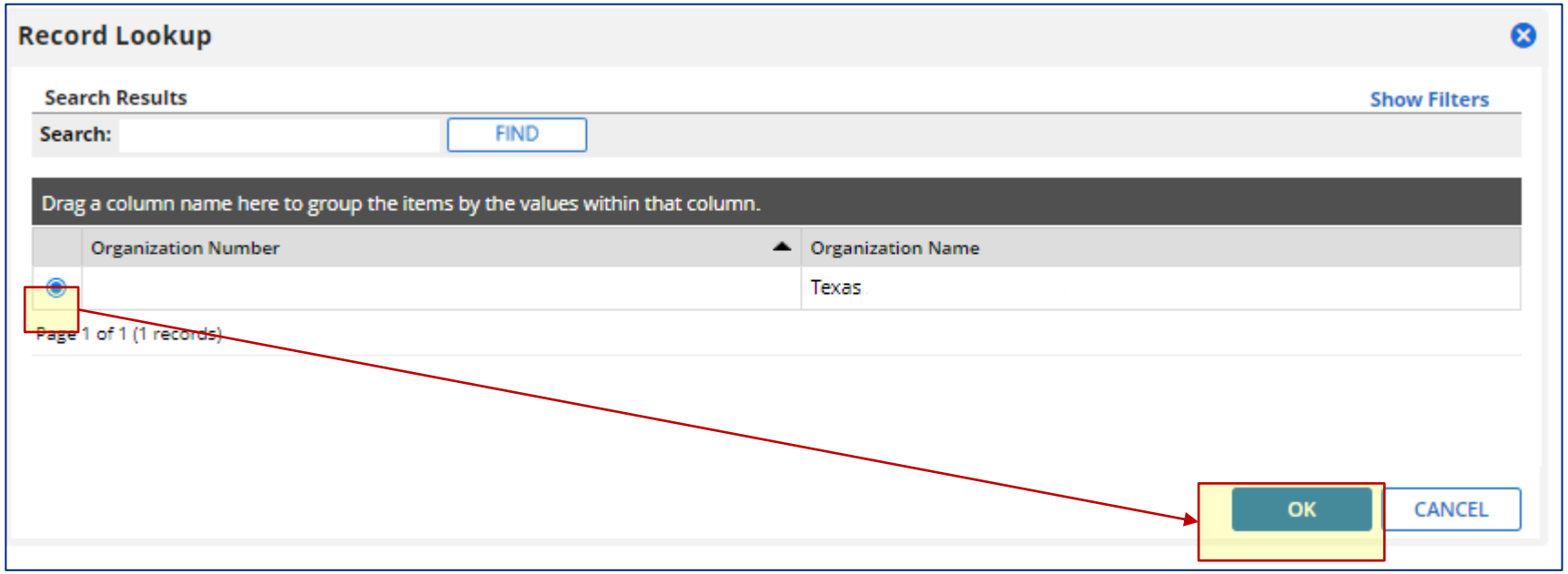
History Log: View History Log

Navigating: Vulnerability Report

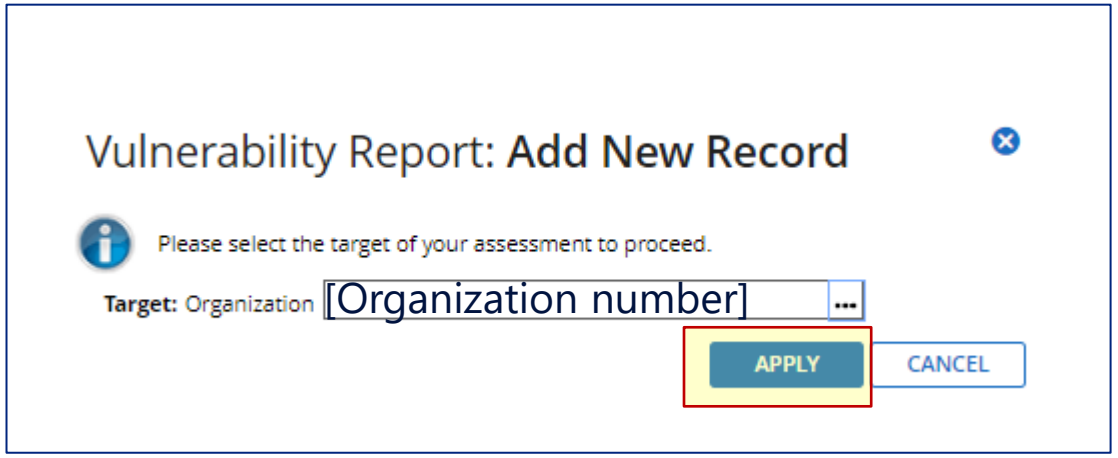


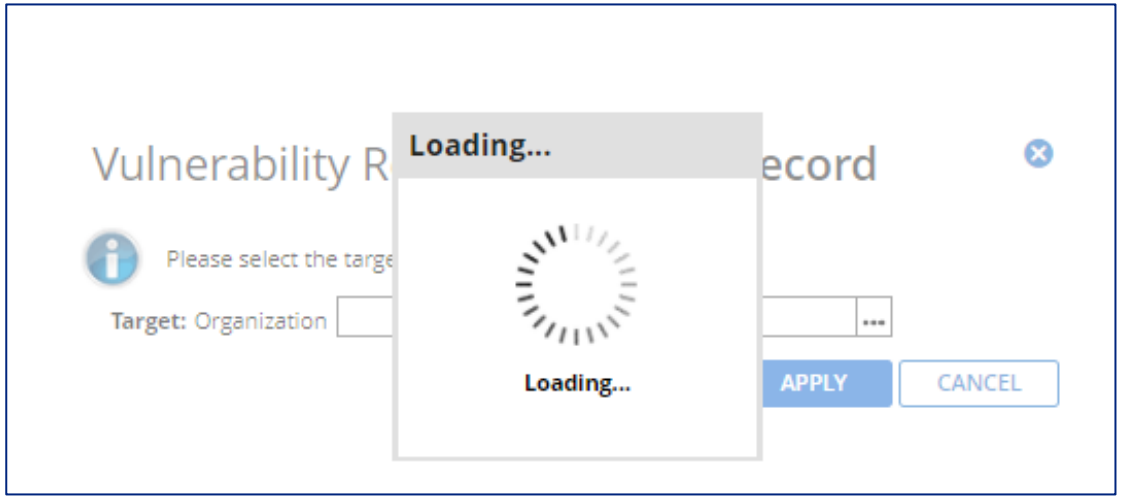
Vulnerability Report – Add New Record



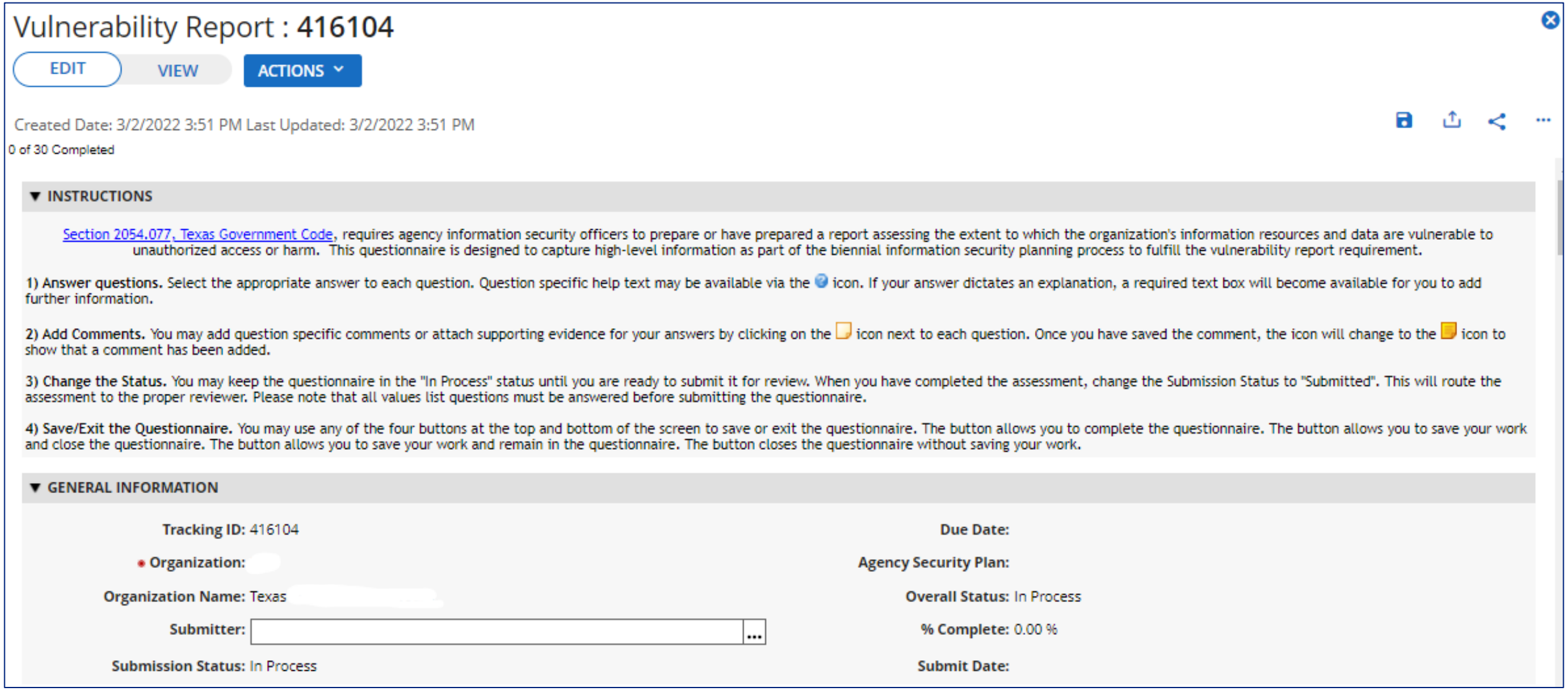


Vulnerability Report – Add New Record





Vulnerability Report – Sections



Vulnerability Report – Sections

▼ VULNERABILITY REPORT ASSESSMENT

VR-001: What systems or applications does the agency perform vulnerability assessments and scans on prior to 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

VR-003: How often does the agency conduct network vulnerability scanning?

- ○ Never
- ○ Monthly
- ○ Quarterly
- ○ Annually
- ○ Biennially
- ○ Ad-Hoc
- ○ Continuously

Vulnerability Report – Sections

VR-024: On average, approximately what percentage of vulnerabilities identified during assessment are remediated between assessment periods?

- ○ 0 to 10%
- ○ 10 to 25%
- ○ 25 to 50%
- ○ 50 to 75%
- ○ 75 to 90%
- ○ 90 to 100%

VR-025: Does the agency document vulnerability/patching exceptions?

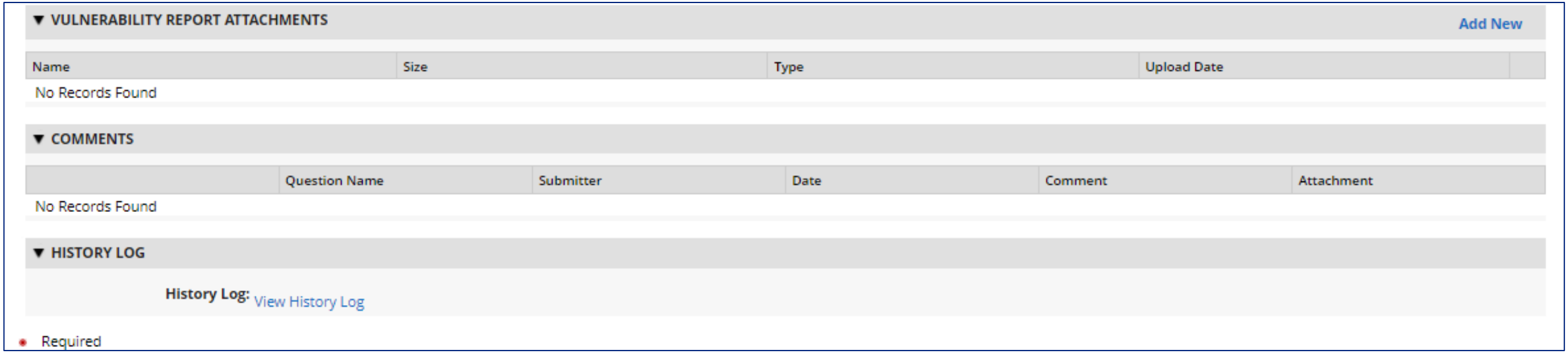
- ○ Yes
- ○ Sometimes
- ○ No

VR-026: Does the agency have any known production system vulnerabilities that cannot be patched or remediated?

- ○ Yes
- ○ No

Additional Comments: Optional: provide any additional comments regarding the vulnerability report or your organization's vulnerability management practices.

Vulnerability Report – Sections



▼ VULNERABILITY REPORT ATTACHMENTS

Add New

Name	Size	Type	Upload Date
No Records Found			

▼ COMMENTS

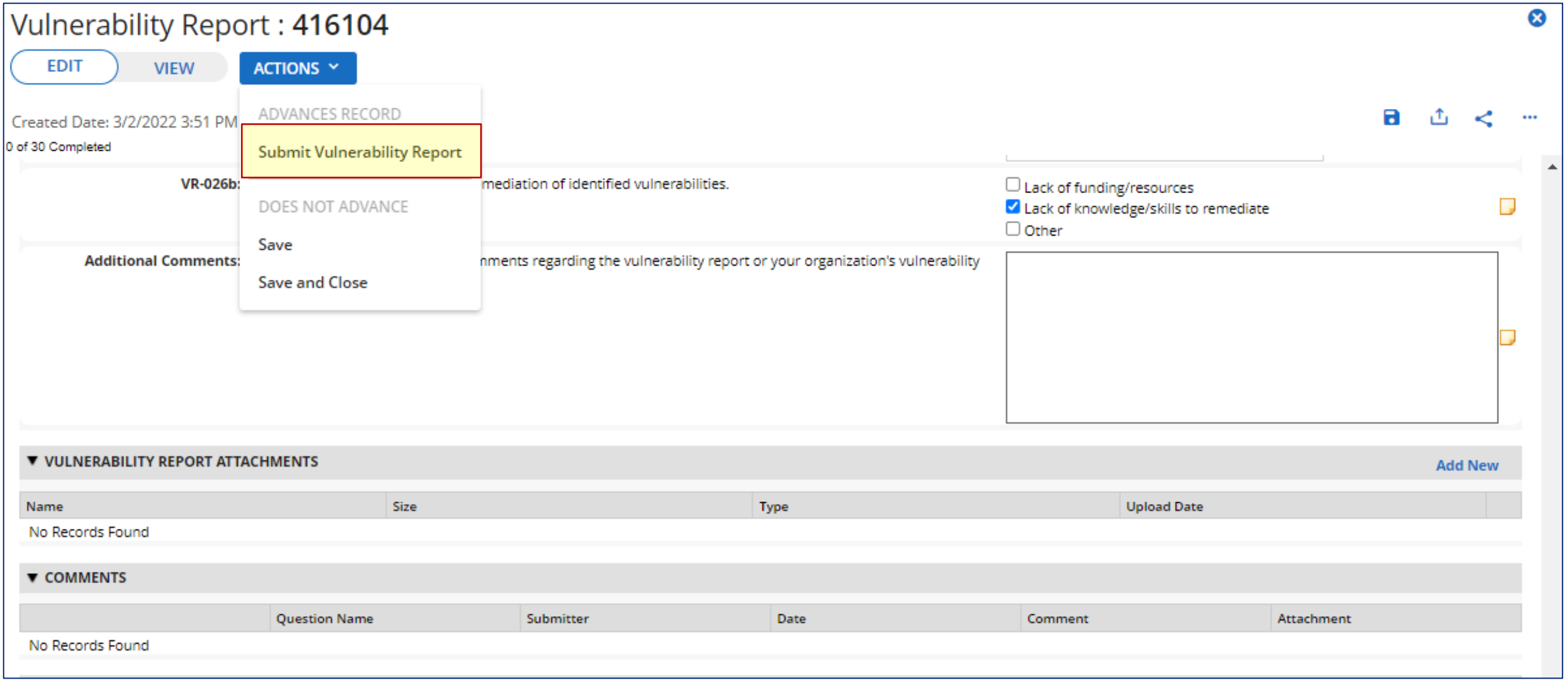
	Question Name	Submitter	Date	Comment	Attachment
No Records Found					

▼ HISTORY LOG

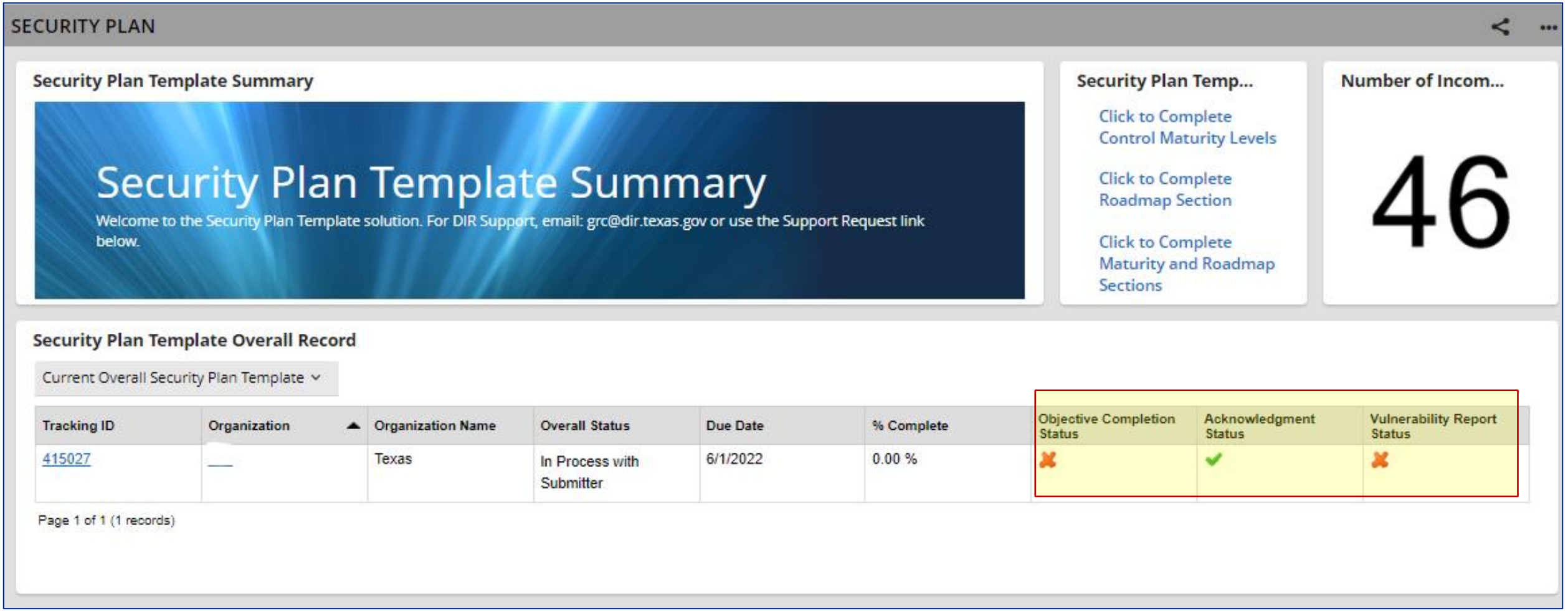
History Log: View History Log

• Required

Vulnerability Report – Sections



COMPLETE SUBMISSION



Additional Resources

DIR's Information Security Plan website

- https://dir.texas.gov/information-security/security-policy-and-planning/information-security-plan?id=5

DIR's SPECTRIM website

- https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/statewide-portal-enterprise?id=136

SPECTRIM Portal

- https://dir.archer.rsa.com/

Conclusion

- Security Plan Overview
- Texas Cybersecurity Framework Overview
- Security Plan Template Overview
- SPECTIM Overview
- SPECTRIM Demo
- Live Questions & Answers - March 31, 2022
- For assistance, contact GRC@DIR.TEXAS.GOV

Live Demo with Questions & Answers

March 31, 2022
9:00 AM – 10:30 AM

Presented by:
Matt Kelly
Deputy CISO for Policy and Governance
Texas Department of Information Resources

Raine Drosdick
Technical Consultant
RSA Archer Professional Services

Sophia Shelton
Governance, Risk, & Compliance Program Analyst
Texas Department of Information Resources

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR

Texas Department of Information Resources

Transforming How Texas Government Serves Texans