SPECTRIM Guide:

Monthly Incident Reporting

Updated May 2022

Table of Contents

Introduction

SPECTRIM

To help tie together the overall state security program, DIR has implemented a governance, risk, and compliance software tool available to all state agencies and institutions of higher education. The SPECTRIM portal provides tools for managing and reporting security incidents, conducting risk assessments, storing, and managing organizational policies, performing assessment and authorization (A&A) on information systems, templates for agency security planning activities, and more.

Eligible Entities

The SPECTRIM portal is free for all Texas state agencies, public institutions of higher education, and public community colleges. There is no limit to the number of users each organization can have.

To request an account, ask your agency's Information Security Officer (ISO) to open a support request in the portal or email GRC@dir.texas.gov.

Monthly Incident Reporting

Texas Administrative Code (TAC) RULE §202.23(b)(2) requires agencies and institutions of higher education to submit a report of security-related events to DIR each month no later than nine (9) calendars days after the end of the month. These reports are submitted through the SPECTRIM Portal's Monthly Incident Reporting System. Members of the incident access group with active SPECTRIM accounts will be reminded via system generated notifications prior to the reporting deadline.

Roles

Access Groups

There are different levels of access with SPECTRIM. SPECTRIM access allows users to perform different functions within the SPECTRIM application. The table below is a basic description between the common types of access.

Application	Access Level Name	Description	Capabilities
SPECTRIM	General User	General user role.	• Provides read-only access to basic applications within the system

			• Update rights to records that they have been explicitly assigned • Create, read, and update Application Portfolio Management assessments, exception requests, PCLS requests, and SPECTRIM Support Requests.
SPECTRIM	Incident	Security incident reporting role.	• Create, read, and update incident records and complete the required Monthly Incident Reporting record. • Only users who are a member of the organization's Incident group will receive notifications when new incidents or NSOC alerts are logged.
SPECTRIM	Information Security Office	Security office staff role.	• Access to view and update all the organization's security-related records within the portal. • Create policies, controls, assessment objectives, organization asset records (application, location, and networks), and risk assessments, • Complete the required bi-annual agency security plan. • Create and view TX-RAMP assessment requests associated with their organization

SPECTRIM	Information Resources Manager	Information Resources Manager staff role.	• Create, read, and update rights to create new policies, controls, assessment objectives, organization asset records (application, location, and networks), as well as the ability to complete the organization's bi-annual, required agency security plan. • Create and view TX RAMP assessment requests and engagements for their organization, with limited vendor details.
SPECTRIM	Procurement group	Procurement role for TX-RAMP.	• Grants create, read, and update rights to all TX-RAMP Assessment Requests and Engagement records. • This user does not have access to any other areas of the SPECTRIM portal other than the Third-Party related applications.

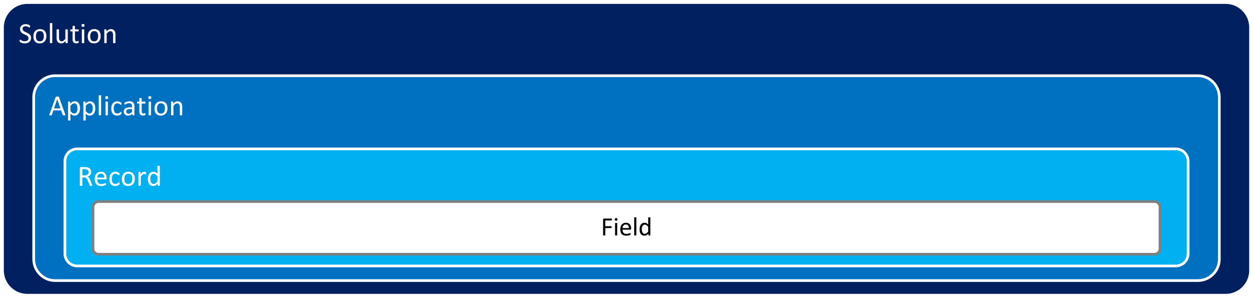
Figure 1. Access Types Table[1]

[1] Users must be a member of the organization's incident group to access incident and monthly incident reporting system applications.

Data Structure

SPECTRIM Data Structure

A SPECTRIM Incident is made of multiple components: Solution, Application, Record, and Field



Solutions group related applications and questionnaires that work together to address a particular business need. By grouping applications into a solution, you can also search those applications as a single entity, access reports for just those, and more.

Applications contain specific types of data records, such as incidents, controls, policies, or assets. The application defines the content and behavior of the individual records.

A **Record** is an individual entry within an application or questionnaire. A record contains fields, which are often arranged in multiple sections.

Fields are the primary building block of any application or questionnaire. All records are made up of fields, which contain specific pieces of data. A field collects data that is displayed as an interface control for your users as they create and update records in an application, questionnaire, solution, and sub-form.

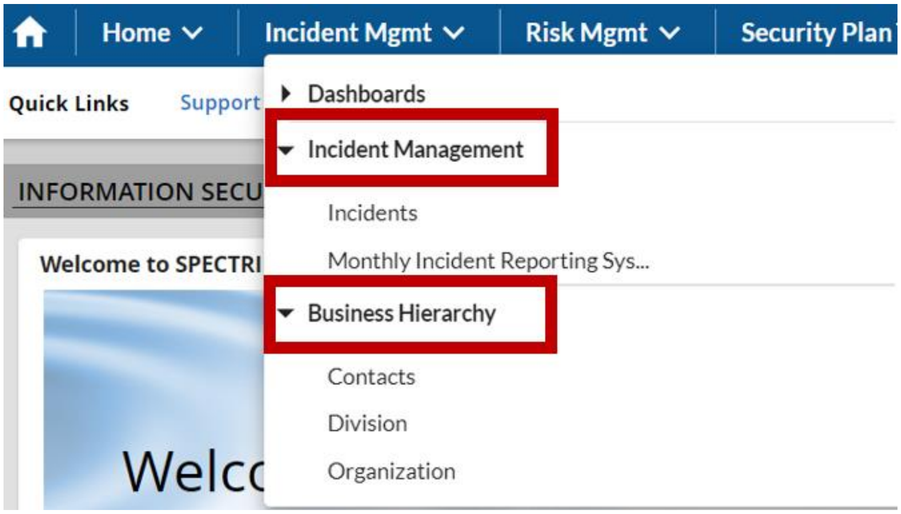
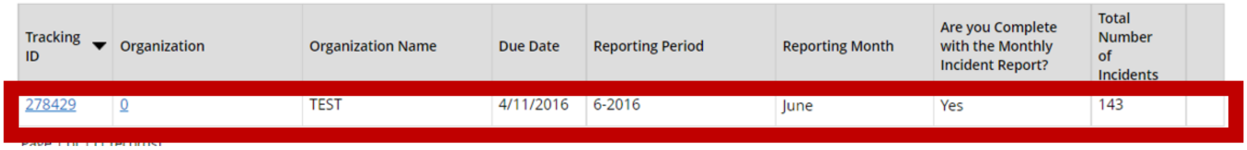
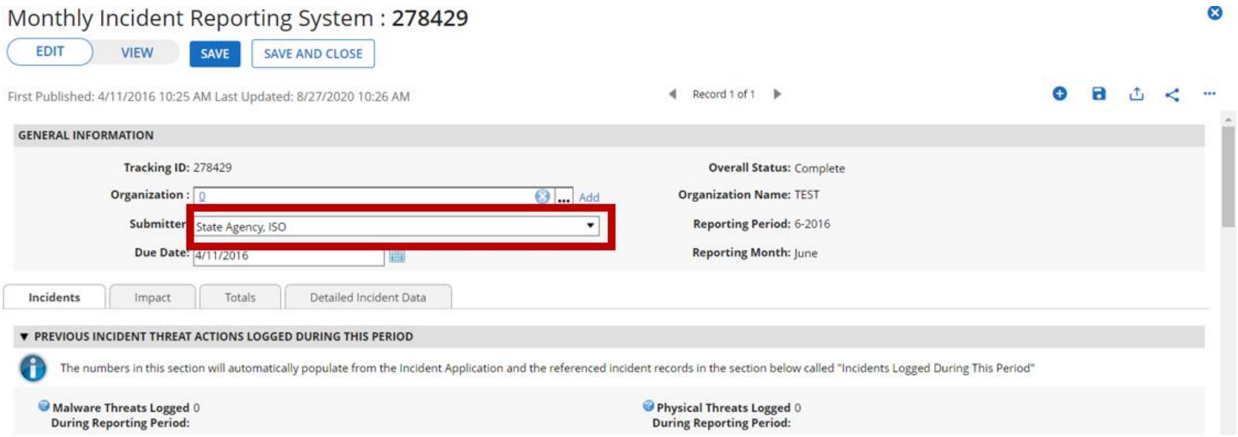


Figure 2. Example of the solutions within Incident Management, nested within each solution are applications



Tracking ID	Organization	Organization Name	Due Date	Reporting Period	Reporting Month	Are you Complete with the Monthly Incident Report?	Total Number of Incidents
278429	0	TEST	4/11/2016	6-2016	June	Yes	143

Figure 3. Example of a record from the Monthly Incident Reporting System application



Monthly Incident Reporting System : 278429

First Published: 4/11/2016 10:25 AM Last Updated: 8/27/2020 10:26 AM

GENERAL INFORMATION

Tracking ID: 278429
Organization : 0
Submitter: State Agency, ISO
Due Date: 4/11/2016
Overall Status: Complete
Organization Name: TEST
Reporting Period: 6-2016
Reporting Month: June

PREVIOUS INCIDENT THREAT ACTIONS LOGGED DURING THIS PERIOD

The numbers in this section will automatically populate from the Incident Application and the referenced incident records in the section below called "Incidents Logged During This Period"

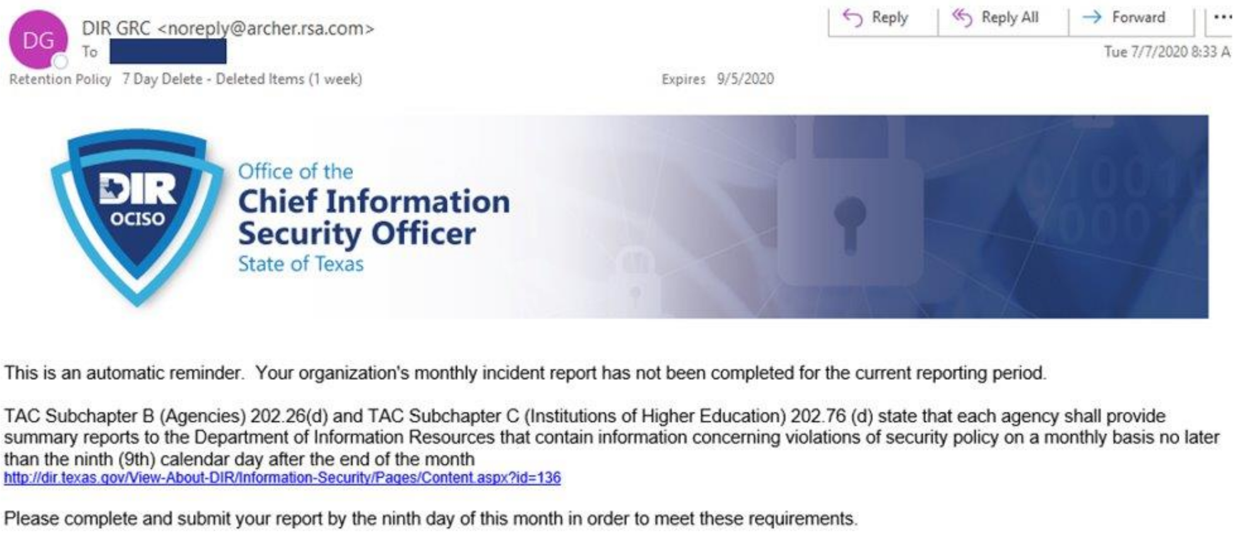
Malware Threats Logged During Reporting Period: 0
Physical Threats Logged During Reporting Period: 0

Figure 4. Example of a field within the Monthly Incident Reporting record

SPECTRIM Navigation

Notification

1. Automated email reminders will be sent to members of the incident group if the monthly report has not been submitted for the current reporting period. Make sure noreply@archer.rsa.com is whitelisted to receive notifications.



DIR GRC <noreply@archer.rsa.com>
To [redacted]
Retention Policy 7 Day Delete - Deleted Items (1 week) Expires 9/5/2020
Tue 7/7/2020 8:33 A

This is an automatic reminder. Your organization's monthly incident report has not been completed for the current reporting period.

TAC Subchapter B (Agencies) 202.26(d) and TAC Subchapter C (Institutions of Higher Education) 202.76 (d) state that each agency shall provide summary reports to the Department of Information Resources that contain information concerning violations of security policy on a monthly basis no later than the ninth (9th) calendar day after the end of the month
http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=136

Please complete and submit your report by the ninth day of this month in order to meet these requirements.

Figure 5. Example of an automatic notification to complete the monthly incident report

Dashboard

The Dashboards feature is designed to allow organizations to promote security awareness and efficient, effective communication by providing users with quick access to information. The Monthly Incident reports can be accessed from Security Office Home Dashboard.

1. Expand Home
2. Expand Dashboards
3. Select Information Security Office Home to access this dashboard

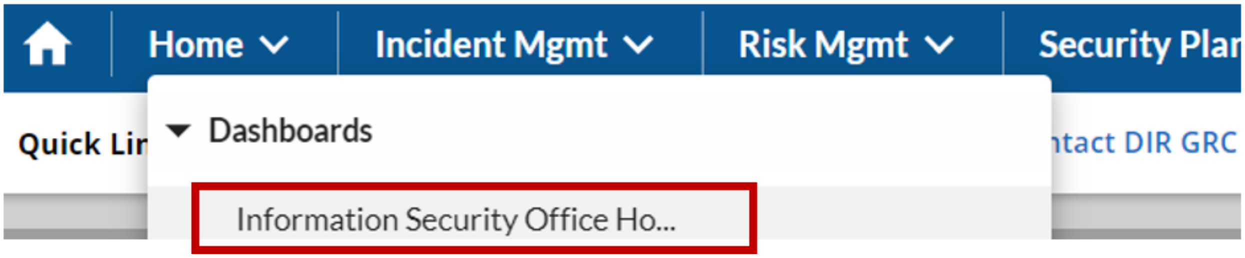


Figure 6. Example of navigating to the Information Security Office Home dashboard

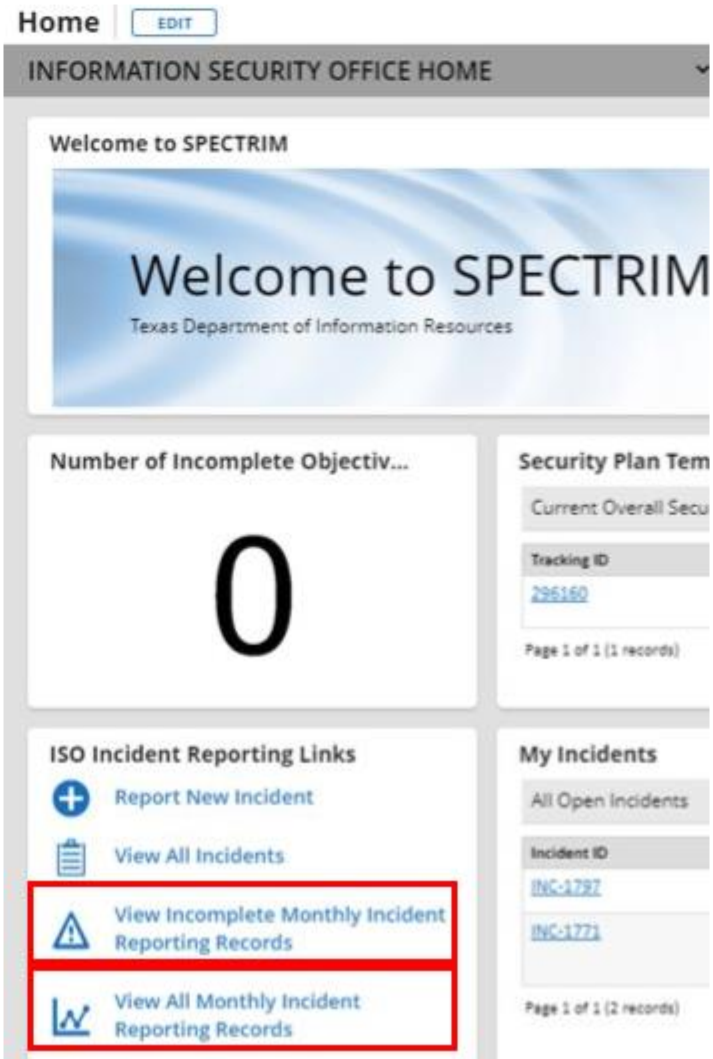


Figure 7. Example of Monthly Incident Reporting reports available from the Dashboard

Monthly Incident Reporting System Record

1. Expand Incident Management
2. Navigate to the Monthly Incident Reporting System application

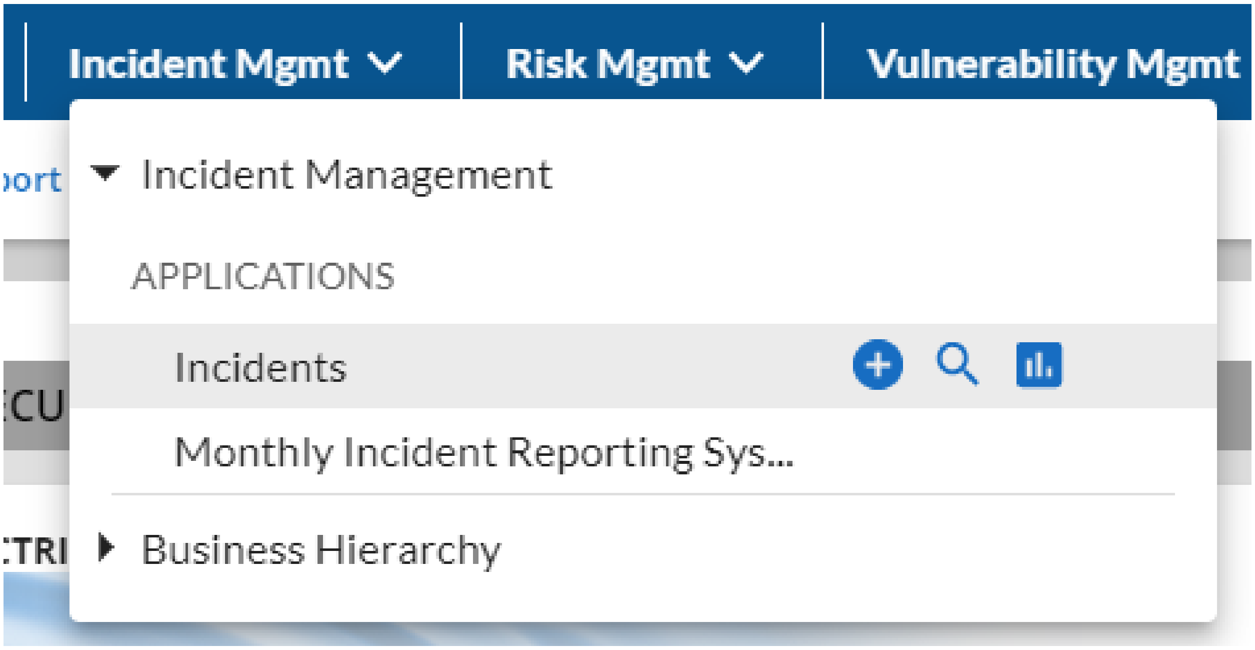


Figure 8. Example of the Incident Management applications

NOTE: The following icons provide a shortcut to directly navigate to the following areas relating the highlighted application. If grayed-out or not visible, the access is unavailable.

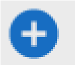


Figure 9. Create a new record

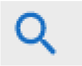


Figure 10. Perform a search

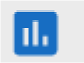
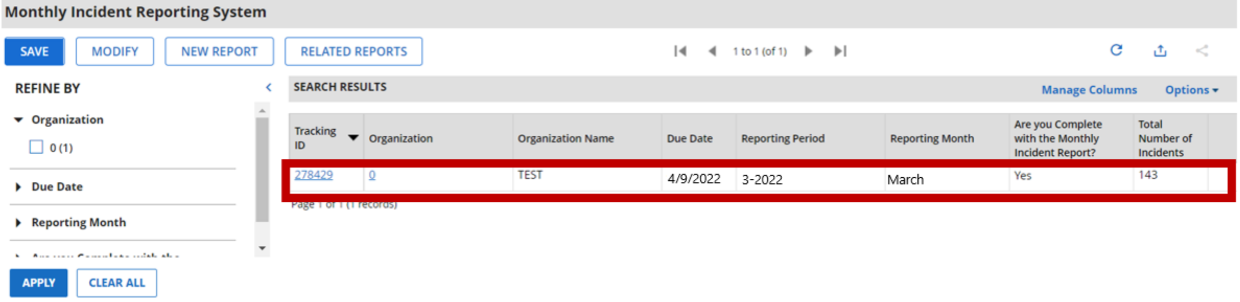


Figure 11. View existing reports

3. Find the Monthly Incident Reporting record for the appropriate reporting period
4. Select the desired record



Monthly Incident Reporting System

REFINE BY

- Organization
  - □ 0 (1)
- Due Date
- Reporting Month

SEARCH RESULTS

Tracking ID	Organization	Organization Name	Due Date	Reporting Period	Reporting Month	Are you Complete with the Monthly Incident Report?	Total Number of Incidents
278429	0	TEST	4/9/2022	3-2022	March	Yes	143

Page 1 of 1 (1 records)

Figure 12. Example of a Monthly Incident Reporting record. This example indicates the completed record was due by 4/9/2022 for the month of March 2022.

Searches and Reports

Search enables you to perform searches within a specific application or questionnaire. Besides keywords and phrases, search provides other options to narrow search results: you can select which fields to display in the search results, use filters to show only the information you want, sort records in the search, and configure the display options on the search results page.

1. Once within a desired application (such as Monthly Incident Reporting System)
2. Either use the left REFINE BY pane to filter your search
   a. Click APPLY

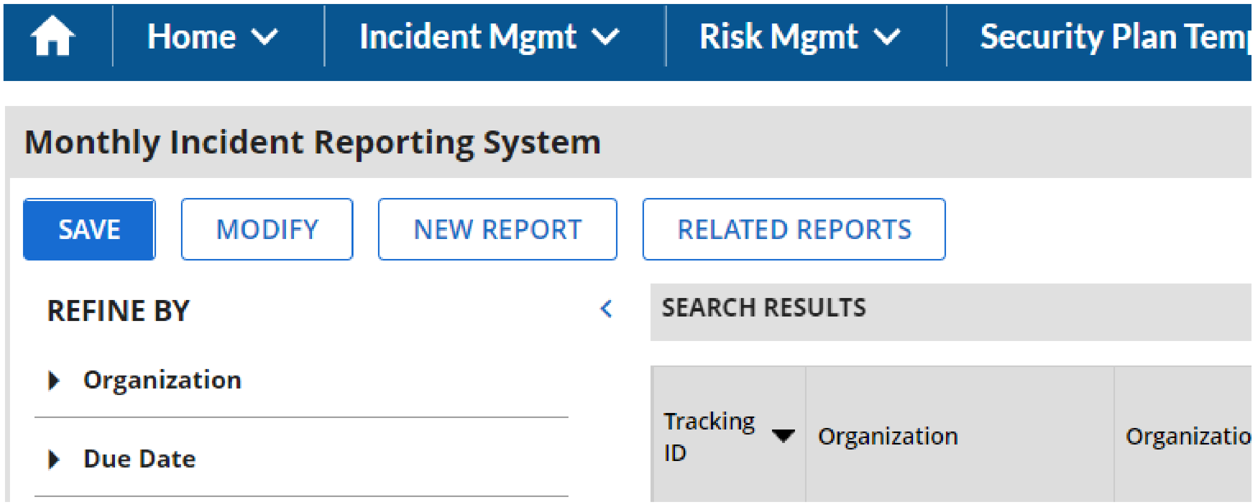


Figure 13. Example of the different options to refine your search

3. Or select the MODIFY button to further refine your search
   a. Click SEARCH button to once parameters have been set

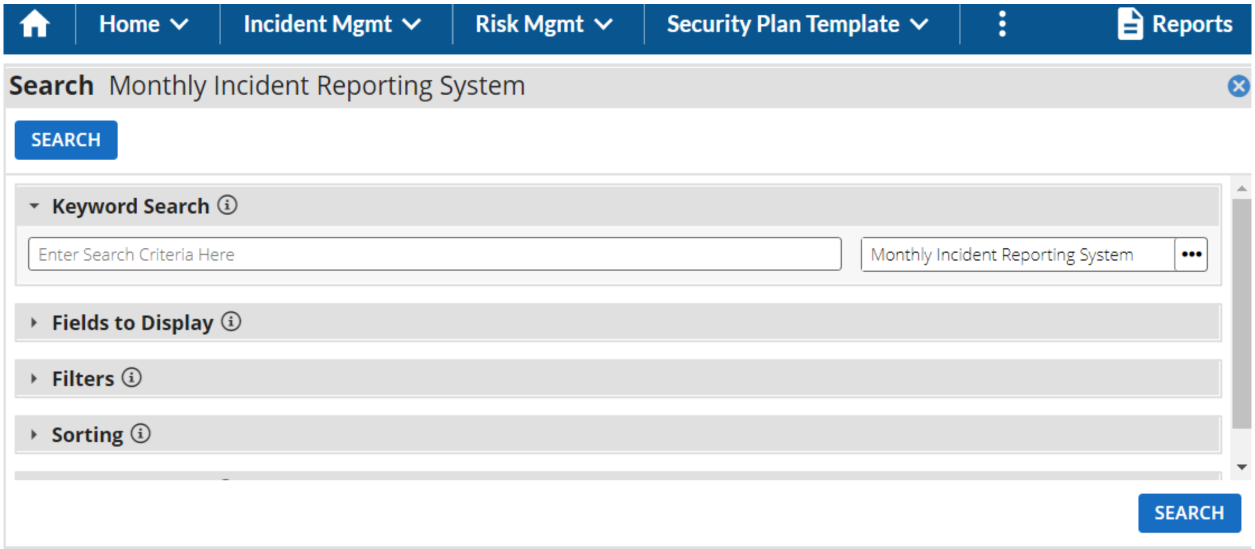
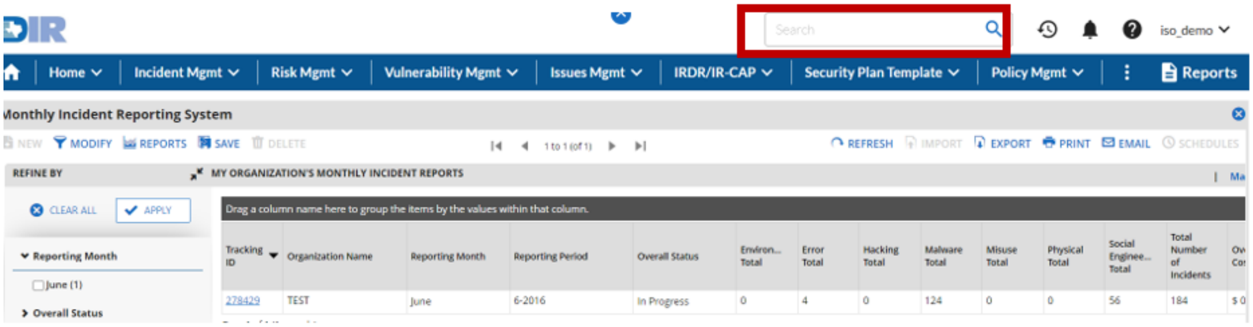


Figure 14. Example of the different parameters available to refine your search

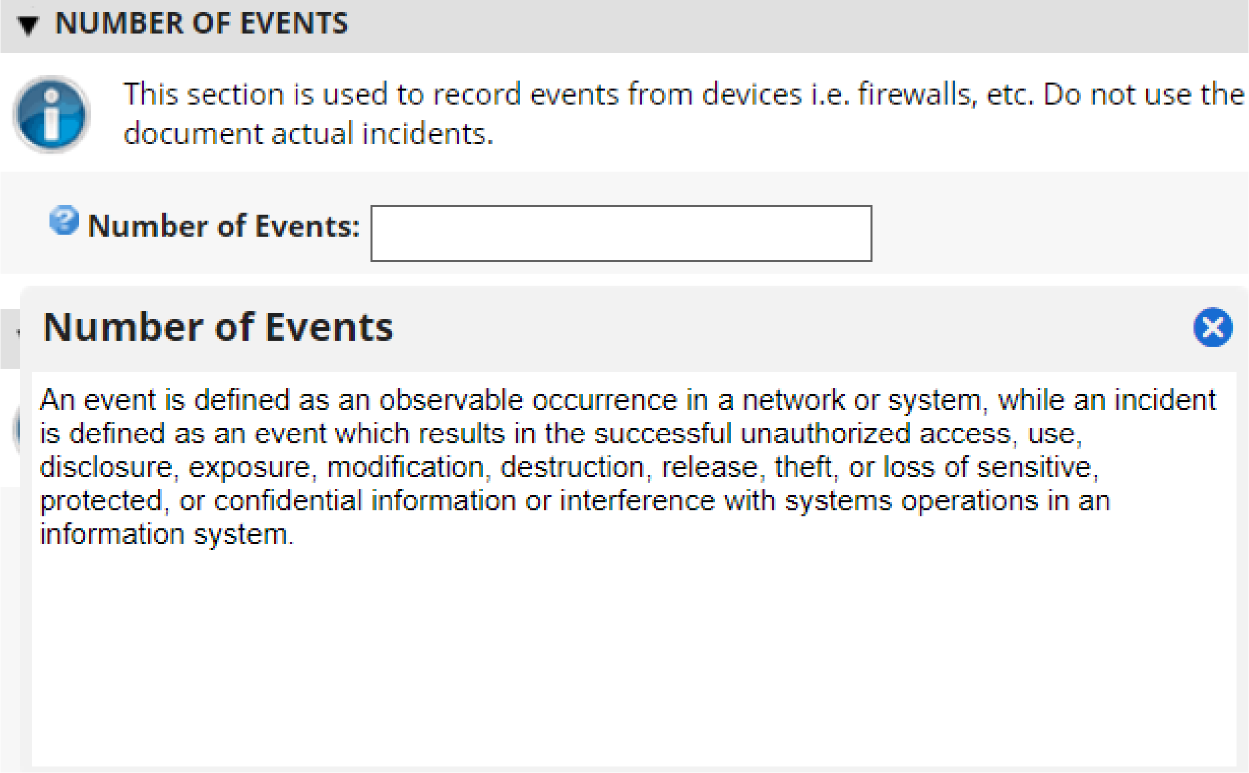


Tracking ID	Organization Name	Reporting Month	Reporting Period	Overall Status	Environ... Total	Error Total	Hacking Total	Malware Total	Misuse Total	Physical Total	Social Enginee... Total	Total Number of Incidents	Ov Co
278429	TEST	June	6-2016	In Progress	0	4	0	124	0	0	56	184	$ 0

Figure 15. Global search bar will search beyond the application and search throughout SPECTRIM

Additional Information

For further guidance on the meaning of a field. Some fields will have a blue circled "?" ? to provide additional, clarifying information.



▼ NUMBER OF EVENTS

This section is used to record events from devices i.e. firewalls, etc. Do not use the document actual incidents.

Number of Events:

Number of Events

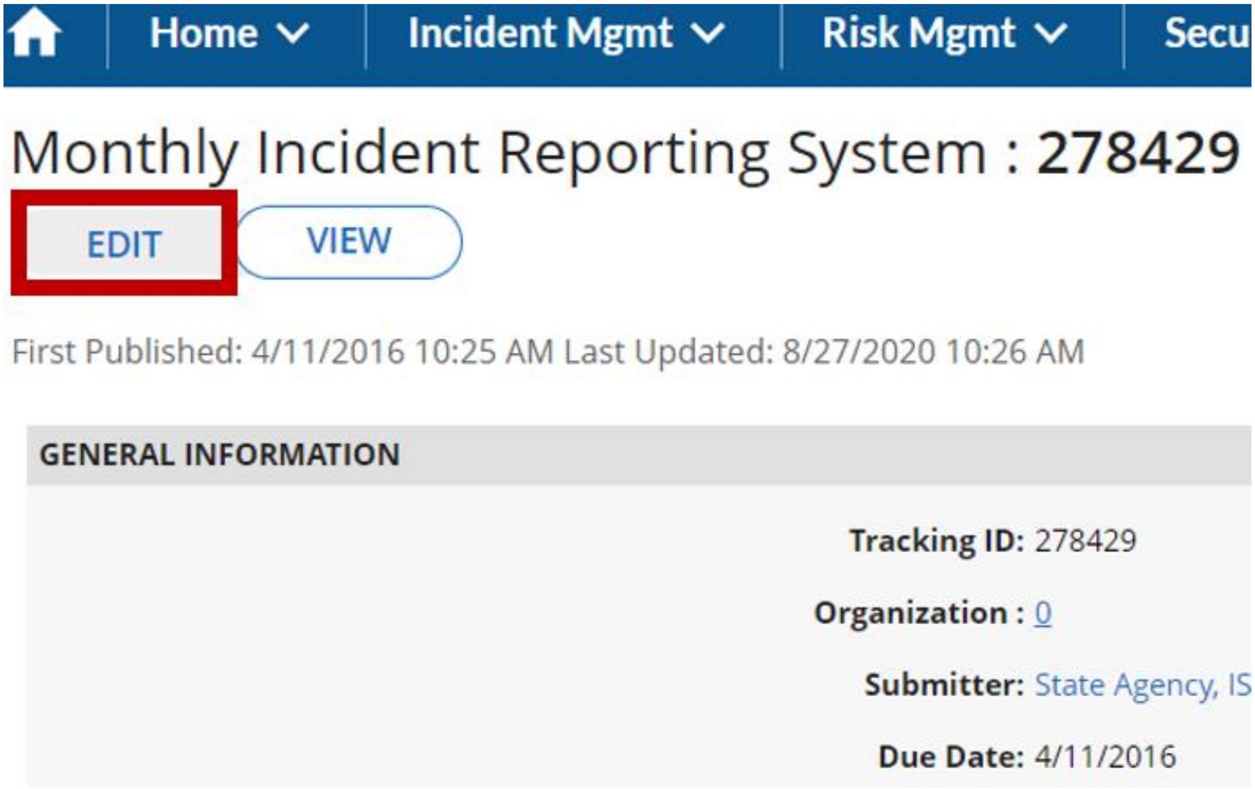
An event is defined as an observable occurrence in a network or system, while an incident is defined as an event which results in the successful unauthorized access, use, disclosure, exposure, modification, destruction, release, theft, or loss of sensitive, protected, or confidential information or interference with systems operations in an information system.

Figure 16. Example of additional information for the Number of Events field, within the Monthly Incident Reporting System record

Monthly Incident Reporting

Input Monthly Incident Reporting Record

1. Select Edit to modify (located at the top, left of the record)



Monthly Incident Reporting System : **278429**

First Published: 4/11/2016 10:25 AM Last Updated: 8/27/2020 10:26 AM

GENERAL INFORMATION

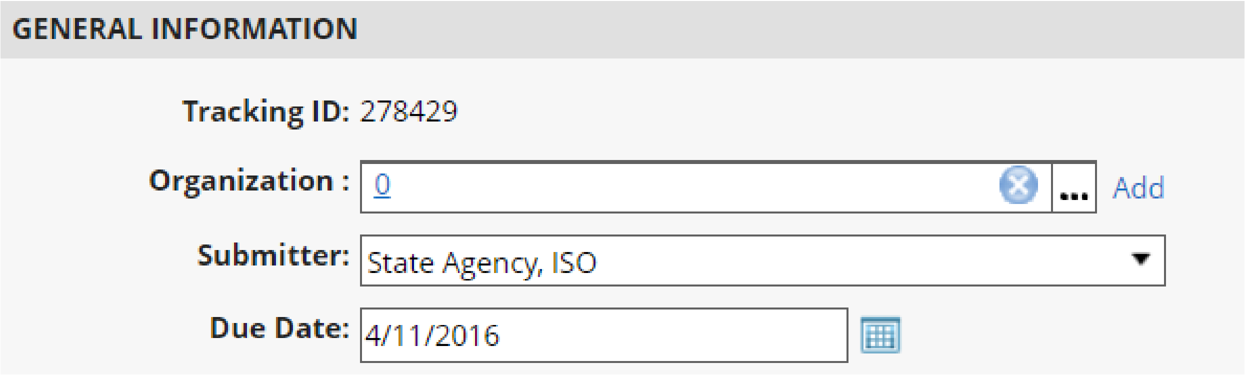
Tracking ID: 278429

Organization : 0

Submitter: State Agency, IS

Due Date: 4/11/2016

Figure 17. Modify a record by selecting Edit



GENERAL INFORMATION

Tracking ID: 278429

Organization : 0

Submitter: State Agency, ISO

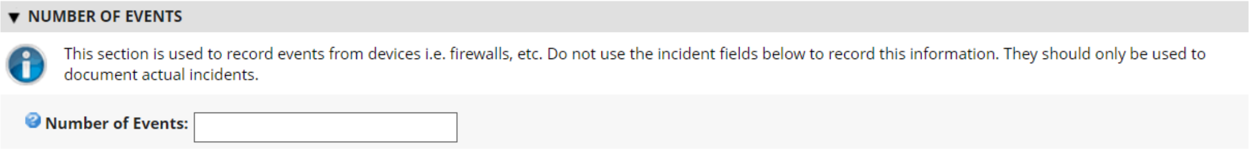
Due Date: 4/11/2016

Figure 18. Once Edit has been selected, fields will have the ability to be updated

2. Update the appropriate fields as needed for your agency.
3. Tabs, such as the Impact tab gives you the option to track additional metrics on incident impacts such as costs, downtime, response time, etc.

Note: Common fields updated on the Incidents tab include:

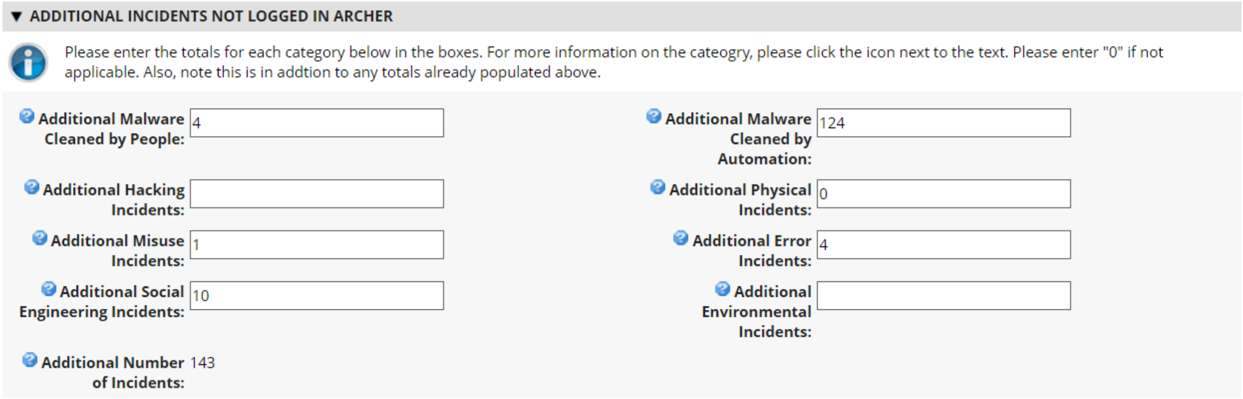
- Submitter – individual submitting the monthly incident report
- Number of Events
- Additional Malware Cleaned by People
- Additional Hacking Incidents
- Additional Misuse Incidents
- Additional Social Engineering Incidents
- Additional Malware Cleaned by Automation
- Additional Physical Incidents
- Additional Error Incidents
- Additional Environmental Incidents


▼ NUMBER OF EVENTS

This section is used to record events from devices i.e. firewalls, etc. Do not use the incident fields below to record this information. They should only be used to document actual incidents.

Number of Events:

Figure 19. Update Number of Events as needed


▼ ADDITIONAL INCIDENTS NOT LOGGED IN ARCHER

Please enter the totals for each category below in the boxes. For more information on the cateogry, please click the icon next to the text. Please enter "0" if not applicable. Also, note this is in addtion to any totals already populated above.

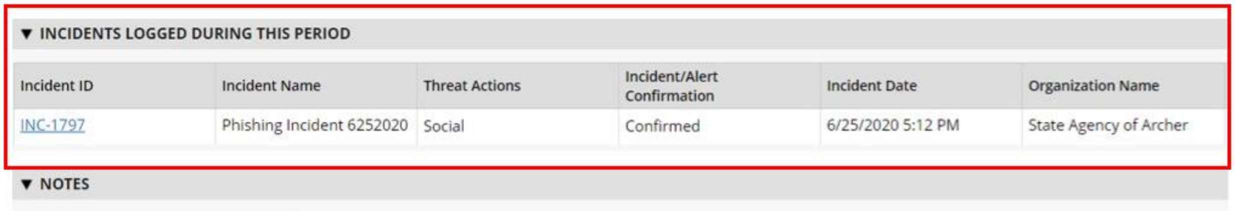
Additional Malware Cleaned by People:	4	Additional Malware Cleaned by Automation:	124
Additional Hacking Incidents:		Additional Physical Incidents:	0
Additional Misuse Incidents:	1	Additional Error Incidents:	4
Additional Social Engineering Incidents:	10	Additional Environmental Incidents:	
Additional Number of Incidents:	143		

Figure 20. Update Additional Incidents Not Logged In Archer section as needed

4. Associate Incidents if needed

    a. Incidents logged during the month will automatically be associated with the monthly report.

    b. Monthly report counts should include any incidents that were **<u>not</u>** logged during that period (totals are combined on the “total” tab for reference



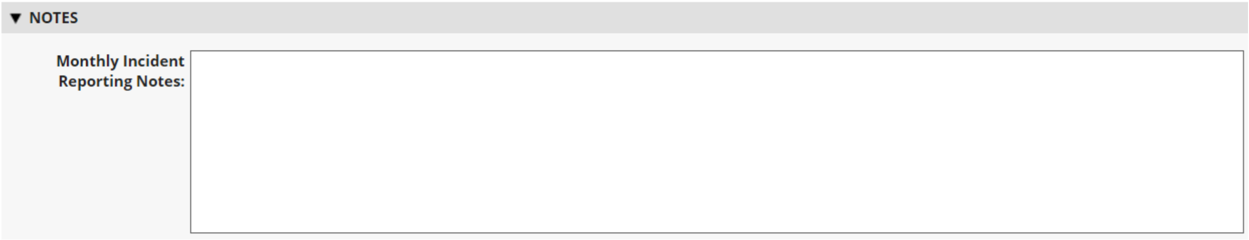
▼ INCIDENTS LOGGED DURING THIS PERIOD

Incident ID	Incident Name	Threat Actions	Incident/Alert Confirmation	Incident Date	Organization Name
INC-1797	Phishing Incident 6252020	Social	Confirmed	6/25/2020 5:12 PM	State Agency of Archer

▼ NOTES

Figure 21. Example of the associated incident for the month of June 2020

5. Add optional notes

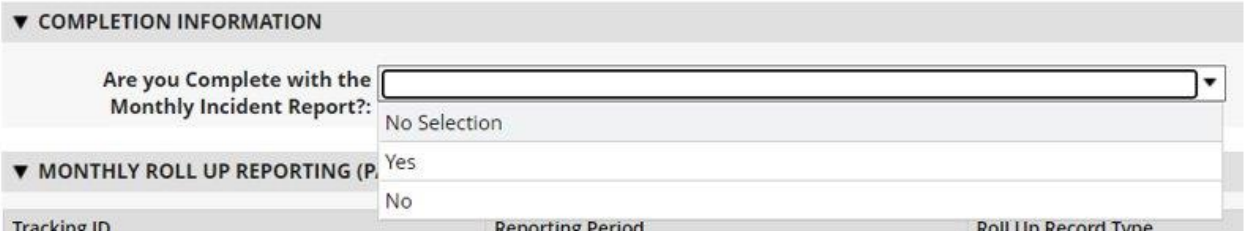


▼ NOTES

Monthly Incident Reporting Notes:

Figure 22. Notes section can be helpful for submitter’s historical reference

6. Upon completion, update “Are you Complete with the Monthly Incident Report?” with a response of Yes.



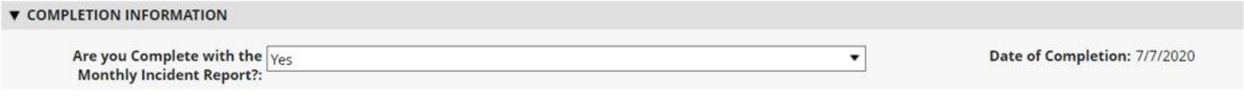
▼ COMPLETION INFORMATION

Are you Complete with the Monthly Incident Report?:

7.

Figure 23. Upon completion the following fields within the Completion Information section must be updated

8. Update date for Date of Completion



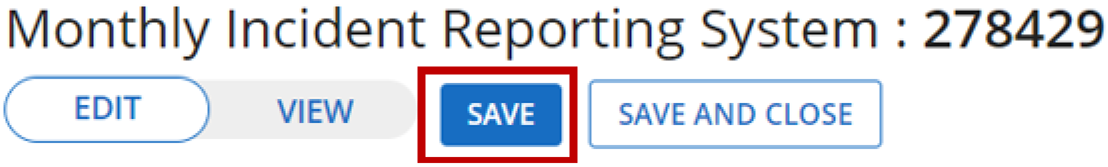
▼ COMPLETION INFORMATION

Are you Complete with the Monthly Incident Report?: Yes

Date of Completion: 7/7/2020

Figure 24. Example of the confirmation that record has been completed

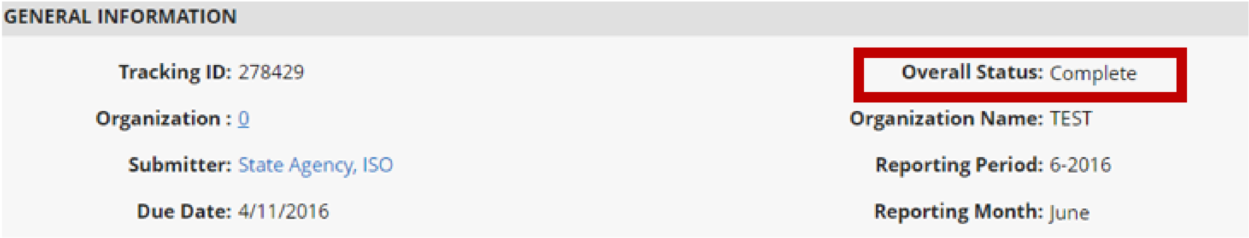
9. Click Save



Monthly Incident Reporting System : 278429

Figure 25. Save the record to finalize completion

10. Overall Status will change to Complete



GENERAL INFORMATION

Tracking ID: 278429

Overall Status: Complete

Organization : 0

Organization Name: TEST

Submitter: State Agency, ISO

Reporting Period: 6-2016

Due Date: 4/11/2016

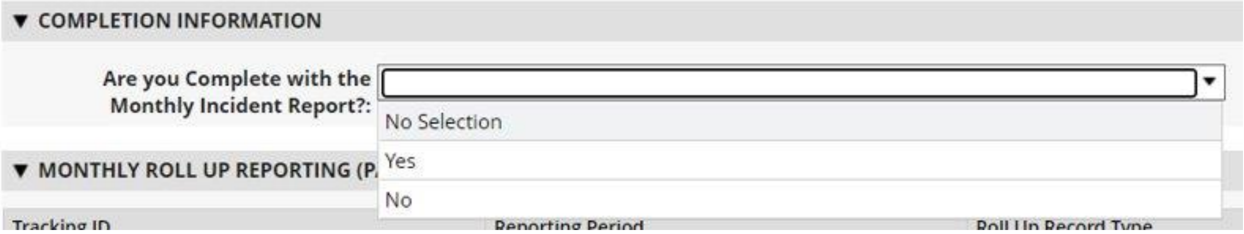
Reporting Month: June

Figure 26. Example of the Overall Status indicating monthly reporting has been completed

Undo/Modify a Completed Monthly Incident Reporting System Record

Submitters can make changes to a Completed monthly incident record prior to the due date but must re-submit to complete the reporting.

1. Go into the desired Monthly Incident Reporting System record
2. Edit the record
3. Scroll down to the Completion Information Section and select No to the question “Are you Complete with the Monthly Incident Report?”

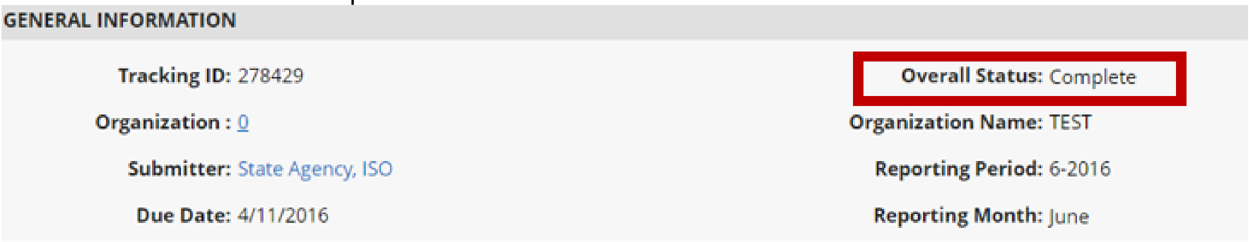


▼ COMPLETION INFORMATION

Are you Complete with the Monthly Incident Report?:

Figure 27. Updating the status of the Monthly Incident Reporting record

4. Save the record
5. You will now be able to update the record as need
6. Once the Monthly Incident Reporting System record has been updated, complete submission by changing “Are you Complete with the Monthly Incident Report?” to a response of Yes.
7. Save the record to complete submission



GENERAL INFORMATION

Tracking ID: 278429	**Overall Status:** Complete
Organization : 0	**Organization Name:** TEST
Submitter: State Agency, ISO	**Reporting Period:** 6-2016
Due Date: 4/11/2016	**Reporting Month:** June

Figure 28. Example of the Overall Status indicating monthly reporting has been completed

Resources

SPECTRIM Portal Login

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

Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) Webpage

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

Support

Archer Support Requests

For SPECTRIM technical assistance submit a Support Request within the SPECTRIM portal or contact GRC@dir.texas.gov.

Table of Figures

Version History

Version	Publish Date	Comments
1.0	2022-05-02	Published guide

Figure 29. Version History Table